

Oracle Argus Safety and Oracle Argus Insight

Installation Guide

Release 8.2.2

F31380-02

July 2020

Copyright © 2020, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

| | |
|-------------------------------------|------|
| Preface | xiii |
| Where to Find More Information..... | xiii |
| Documentation Accessibility | xiii |
| Revision History | xiv |

Part I Prepare to Install Argus

1 System Requirements

| | | |
|-------|---|-----|
| 1.1 | Hardware Requirements..... | 1-1 |
| 1.2 | Software Requirements | 1-2 |
| 1.2.1 | Operating System | 1-2 |
| 1.2.2 | Oracle Components | 1-2 |
| 1.2.3 | Other Components | 1-4 |
| 1.2.4 | Generic—Other Supported Features | 1-4 |
| 1.2.5 | General Installation Notes and Information..... | 1-5 |

2 Install Oracle Database

| | | |
|-------|---|-----|
| 2.1 | Get the Oracle Database Installation Guide..... | 2-1 |
| 2.2 | Install Oracle Database..... | 2-1 |
| 2.2.1 | Database Software Installation Options | 2-1 |
| 2.2.2 | Database Configuration Options..... | 2-2 |
| 2.2.3 | Install and Apply Oracle Patch Set | 2-2 |
| 2.3 | Set Up Argus Safety Database Parameters..... | 2-2 |
| 2.3.1 | Argus Safety Database Instance Parameters (Recommended) | 2-3 |
| 2.3.2 | Additional Database Setup Information | 2-3 |
| 2.4 | Argus Insight Configuration Requirements | 2-4 |
| 2.4.1 | Database Parameters | 2-4 |
| 2.4.2 | Database I/O Configuration | 2-6 |
| 2.4.3 | Recommended Configuration for the Database Server | 2-6 |

Part II Set Up Argus Middle and Client Tiers

3 Install and Configure Argus Safety Web

| | | |
|-----|---------------------|-----|
| 3.1 | Prerequisites | 3-1 |
|-----|---------------------|-----|

| | | |
|-------|---|-----|
| 3.2 | Install Argus Safety Web | 3-1 |
| 3.3 | Configure Load Balancer in Argus Web..... | 3-2 |
| 3.3.1 | Set Up Argus Web Load Balancer IP Address | 3-2 |
| 3.3.2 | Set Up Shared Network Directory | 3-3 |
| 3.4 | Reset IIS | 3-3 |

4 Install Argus Insight

| | | |
|-------|--|-----|
| 4.1 | Install Argus Insight Components onto the Web Server | 4-1 |
| 4.1.1 | Change the APR_USER Password | 4-2 |
| 4.2 | Enable SSL Support for the Argus Insight Website | 4-2 |

5 Configure Web Service Interfaces on Web Server

| | | |
|---------|--|------|
| 5.1 | Argus Web Service Interface | 5-1 |
| 5.1.1 | Argus Web Service Interface Framework | 5-2 |
| 5.2 | Edit .config Files | 5-2 |
| 5.2.1 | Edit the .config file for Outbound Interfaces | 5-2 |
| 5.2.2 | Edit the .config file for Inbound Interface | 5-3 |
| 5.3 | Safety Message | 5-3 |
| 5.4 | MedDRA Interface | 5-3 |
| 5.4.1 | MedDRA Configuration | 5-4 |
| 5.4.1.1 | Enable MedDRA Integration through Argus Console..... | 5-4 |
| 5.4.1.2 | Edit the ArgusWeb/ASP/web.config file | 5-4 |
| 5.4.1.3 | Edit the Argus.NET/web.config file | 5-4 |
| 5.4.2 | MedDRA Encoding Flow | 5-5 |
| 5.4.3 | MedDRA Interface XML Schema | 5-5 |
| 5.4.3.1 | MEDDRA_Request..... | 5-5 |
| 5.4.3.2 | MEDDRA_Response | 5-6 |
| 5.5 | Product Study License Interface | 5-7 |
| 5.6 | WHO Drug Coding Interface | 5-8 |
| 5.6.1 | Configuration | 5-9 |
| 5.6.2 | Drug Dictionary Coding Flow | 5-9 |
| 5.6.3 | WHO Drug Coding: XML Schema..... | 5-9 |
| 5.6.3.1 | Request: WHODrug_Request..... | 5-10 |
| 5.6.3.2 | Response: WHODrug_Response..... | 5-10 |
| 5.7 | Lot Number Interface | 5-10 |
| 5.7.1 | Configuration | 5-11 |
| 5.7.2 | Lot Validation Flow | 5-12 |
| 5.7.3 | Lot Number: XML Schema..... | 5-12 |
| 5.7.3.1 | Request: Lot_Request..... | 5-12 |
| 5.7.3.2 | Response: Lot_Response..... | 5-13 |
| 5.7.4 | Transformation..... | 5-13 |
| 5.8 | Worklist Intake | 5-14 |
| 5.8.1 | Configuration | 5-14 |
| 5.8.2 | Worklist Intake Flow | 5-15 |
| 5.9 | Literature Intake..... | 5-16 |
| 5.9.1 | Configuration | 5-16 |
| 5.9.1.1 | Metadata Configuration | 5-16 |

| | | |
|-------|------------------------------|------|
| 5.9.2 | Literature Intake Flow..... | 5-17 |
| 5.10 | Extended E2B Interface | 5-18 |

6 Install and Start Argus Safety Service

| | | |
|-----|-----------------------------------|-----|
| 6.1 | Install Argus Safety Service..... | 6-1 |
| 6.2 | Start Argus Safety Service..... | 6-1 |

7 Install and Configure Interchange

| | | |
|-----|---|-----|
| 7.1 | Prerequisites | 7-1 |
| 7.2 | Install Interchange Service..... | 7-1 |
| 7.3 | Configure Interchange Service..... | 7-2 |
| 7.4 | Access EDI Gateway Shared Folders | 7-2 |
| 7.5 | Configure Interchange Service .INI File | 7-2 |

8 Configure the Argus Insight Application

| | | |
|---------|---|------|
| 8.1 | Log In to Argus Insight for Configuration and Setup | 8-1 |
| 8.2 | Configure the Argus Insight Application Profile Switches | 8-2 |
| 8.2.1 | Access and Modify the Profile Switches | 8-2 |
| 8.2.2 | Set Up the Populate Data Attributes..... | 8-2 |
| 8.2.3 | Set Up the Email Attributes..... | 8-3 |
| 8.2.4 | Set Up the Attributes Specific ONLY to Argus Mart | 8-4 |
| 8.2.5 | Set Up the Attributes Specific ONLY to BIP | 8-6 |
| 8.2.6 | Set Up the Attributes Specific ONLY to OBIEE | 8-6 |
| 8.3 | Configure Duration Value Bands | 8-7 |
| 8.4 | Configure Derivation Functions..... | 8-8 |
| 8.4.1 | Open the Derivation Fields Dialog Box..... | 8-9 |
| 8.4.2 | Icons in the Derivation Fields Dialog Box..... | 8-9 |
| 8.4.3 | Field Mapping Derivation Rules | 8-10 |
| 8.4.4 | Fields and Check Boxes in the Derivation Fields Dialog Box | 8-10 |
| 8.4.4.1 | LM Table | 8-10 |
| 8.4.4.2 | Suppress..... | 8-10 |
| 8.4.4.3 | Value..... | 8-10 |
| 8.4.4.4 | Priority | 8-12 |
| 8.4.4.5 | SQL | 8-12 |
| 8.5 | Configure the Argus Insight Windows Service..... | 8-12 |
| 8.6 | Configure the IIS File Download Limit | 8-13 |
| 8.6.1 | Configure the Maximum Requesting Entity Body Limit..... | 8-13 |
| 8.7 | Use Export and Import to Copy Configuration Data | 8-14 |
| 8.7.1 | Export Data | 8-14 |
| 8.7.2 | Import Data..... | 8-15 |
| 8.8 | Use Argus Safety to Configure Enterprises for Argus Insight (for Mutli-tenant installation only) 8-16 | |
| 8.9 | Secure Sensitive Configuration and Operational Data..... | 8-17 |

9 Upgrade the Argus Application

| | | |
|-----|--|-----|
| 9.1 | Upgrade Argus Application on the Web Server | 9-1 |
| 9.2 | Upgrade Argus Application on the Transaction Server..... | 9-1 |

10 Set Up the Client Browser

| | | |
|------|--|------|
| 10.1 | Prerequisite | 10-1 |
| 10.2 | Install Files Required to View Reports | 10-1 |
| 10.3 | Configure Internet Explorer | 10-1 |
| 10.4 | Post Application Install or Upgrade | 10-2 |
| 10.5 | Add the Argus Site as a Local Intranet Site..... | 10-2 |
| 10.6 | Add Argus Site to the Enterprise Mode | 10-3 |
| 10.7 | Set Up Compatibility View with Internet Explorer | 10-3 |

11 Post-installation Checks

| | | |
|----------|---|------|
| 11.1 | Post-Installation Tasks | 11-1 |
| 11.1.1 | General Checklist..... | 11-1 |
| 11.1.2 | Configure Worklist Intake on the Web Server | 11-1 |
| 11.1.2.1 | RelsysWindowsService.exe.config..... | 11-2 |
| 11.1.2.2 | Service.config | 11-3 |
| 11.1.2.3 | Intake.config..... | 11-3 |
| 11.1.3 | Verify and Update Network Proxy Settings..... | 11-4 |
| 11.2 | Verify Files Installed on Middle Tier Servers | 11-4 |

12 Other Tasks

| | | |
|--------|-------------------------------------|------|
| 12.1 | Configure Argus.xml File | 12-1 |
| 12.2 | Configure Argus.ini File | 12-1 |
| 12.2.1 | Argus.ini Parameters..... | 12-2 |
| 12.3 | Installation Maintenance Tasks..... | 12-3 |
| 12.3.1 | Install New Components..... | 12-3 |
| 12.3.2 | Uninstall Components | 12-4 |
| 12.3.3 | Remove All Components..... | 12-4 |
| 12.4 | Argus Configuration Files | 12-4 |
| 12.4.1 | Backup Configuration Files..... | 12-5 |

Part III Install or Upgrade Argus Database Tier

13 Install Argus Safety Database

| | | |
|----------|---|------|
| 13.1 | Create Argus Safety Database Schema | 13-1 |
| 13.1.1 | Prepare to execute the DBInstaller | 13-2 |
| 13.1.1.1 | Prerequisites | 13-2 |
| 13.1.1.2 | Install Java | 13-2 |
| 13.1.1.3 | Set Java Install Path | 13-2 |
| 13.1.1.4 | Install XDB Schema for Interchange | 13-3 |
| 13.1.2 | Run Create DBA User Script | 13-3 |
| 13.1.3 | Create Tablespaces (Optional) | 13-4 |

| | | |
|--------|---|-------|
| 13.1.4 | Prerequisites to Create the Schema | 13-4 |
| 13.1.5 | Configure the Database Setup Properties File | 13-5 |
| 13.1.6 | Create the Schema on Windows from the User Interface | 13-7 |
| 13.1.7 | Create the Schema on Windows from a Batch file | 13-9 |
| 13.1.8 | Create the Schema on Linux or Unix | 13-9 |
| 13.2 | Post Fresh Install Steps | 13-9 |
| 13.3 | Validate Argus Safety Database | 13-9 |
| 13.3.1 | Validate Argus Safety Database on Windows | 13-10 |
| 13.3.2 | Validate Argus Safety Database on Linux or Unix | 13-10 |
| 13.4 | Enable and Disable Data Lock Point (DLP) | 13-10 |
| 13.4.1 | Prerequisites | 13-10 |
| 13.4.2 | Enable DLP | 13-11 |
| 13.4.3 | Disable DLP | 13-11 |
| 13.5 | Enable DLP on a Specific Enterprise | 13-11 |
| 13.5.1 | Set Up the Base Database | 13-11 |
| 13.5.2 | Enable DLP on Specific Enterprise or Delta Cases | 13-12 |
| 13.5.3 | Validate the Schema | 13-12 |
| 13.6 | Copy Configuration Data (Optional) | 13-13 |
| 13.6.1 | Set Up the Copy Configuration Tool | 13-13 |
| 13.6.2 | Use the Copy Configuration Tool | 13-13 |
| 13.7 | Create Argus Safety Read-only Database Account (Optional) | 13-14 |

14 Upgrade Argus Safety Database

| | | |
|--------|--|------|
| 14.1 | Prerequisites for Database Upgrade | 14-1 |
| 14.2 | Argus Safety Database Upgrade | 14-1 |
| 14.3 | Post Upgrade Steps | 14-2 |
| 14.4 | Enable Local Locking in Argus Safety | 14-3 |
| 14.5 | Merge a Single Enterprise Safety Database into a Multi-tenant Database | 14-3 |
| 14.5.1 | Prerequisites to Run the Merge Export Step | 14-3 |
| 14.5.2 | Merge Export | 14-3 |
| 14.5.3 | Export the dmp File Copy to the Target Database Server | 14-4 |
| 14.5.4 | Prerequisites to Run the Merge Import Step | 14-4 |
| 14.5.5 | Merge Import | 14-5 |
| 14.5.6 | Synchronize Dictionary Manually | 14-6 |

15 Create the Argus Insight Data Mart Structure

| | | |
|--------|---|-------|
| 15.1 | Before You Run the Argus Insight Installation | 15-1 |
| 15.2 | Configure dbinstaller.properties file | 15-2 |
| 15.3 | Create Argus Insight Database Schema | 15-5 |
| 15.3.1 | Prerequisites | 15-5 |
| 15.3.2 | Create Users in the Argus Safety Database | 15-5 |
| 15.3.3 | Create the DBA User | 15-6 |
| 15.3.4 | Create Fresh Argus Insight Schema | 15-7 |
| 15.3.5 | Validate the Schema | 15-9 |
| 15.3.6 | Create Argus Insight Read-only User | 15-10 |
| 15.4 | Create Database Links | 15-11 |

| | | |
|--------|---|-------|
| 15.4.1 | From Argus Safety to Argus Insight Database..... | 15-11 |
| 15.4.2 | From Argus Insight to Argus Safety (manually) | 15-11 |
| 15.5 | Run Initial ETL | 15-12 |
| 15.6 | Run Additional Grant Scripts for Single DB Instance | 15-13 |

16 Upgrade the Argus Insight Data Mart Structure

| | | |
|------|-----------------------------------|------|
| 16.1 | Prepare for Database Upgrade..... | 16-1 |
| 16.2 | Upgrade Database..... | 16-1 |

Part IV Configure Other Products

17 Configure and Enable Argus Dossier

| | | |
|------|-------------------------|------|
| 17.1 | Prerequisites | 17-1 |
| 17.2 | Configure Dossier | 17-1 |
| 17.3 | Enable Dossier | 17-2 |

18 Install and Configure Axway B2Bi

| | | |
|----------|--|------|
| 18.1 | Create an Axway B2Bi Database Instance | 18-1 |
| 18.2 | Install Axway B2Bi..... | 18-1 |
| 18.3 | Configure Axway B2Bi..... | 18-1 |
| 18.3.1 | Configure Axway B2Bi for Binary File Transmission | 18-3 |
| 18.3.2 | Configure Axway B2Bi Community | 18-4 |
| 18.3.2.1 | Register with the Axway B2Bi Community..... | 18-4 |
| 18.3.2.2 | Add a Partner to the Axway B2Bi Community..... | 18-4 |
| 18.3.2.3 | Register the Receiver's Community on the Sender Server | 18-5 |
| 18.3.3 | Add a Node | 18-5 |
| 18.3.4 | Configure Axway B2Bi Certificates..... | 18-6 |
| 18.3.4.1 | Configure Receiver Axway B2Bi Certificates | 18-6 |
| 18.3.4.2 | Configure Sender Axway B2Bi Certificates | 18-6 |
| 18.3.5 | Configuring EVENTS.XML..... | 18-7 |
| 18.3.6 | Configure Message Processing Settings | 18-8 |
| 18.4 | Test Communication | 18-9 |

19 Install and Configure Oracle B2B

| | | |
|----------|--|------|
| 19.1 | Install Oracle B2B | 19-1 |
| 19.2 | Integrate Oracle B2B with Argus Safety | 19-1 |
| 19.3 | Create Integration tables in B2B Schema | 19-1 |
| 19.4 | Configure Oracle B2B User Interface | 19-2 |
| 19.4.1 | General Configuration > Administration > Configuration | 19-2 |
| 19.4.2 | Document Configuration > Administration > Document | 19-2 |
| 19.5 | Configure Enterprise Manager | 19-2 |
| 19.5.1 | Deploy SOA Composite..... | 19-2 |
| 19.5.2 | Configure SOA Composite..... | 19-3 |
| 19.5.2.1 | AS_BPEL_Outbound Composite | 19-3 |
| 19.5.2.2 | AS_BPEL_Inbound Composite..... | 19-3 |
| 19.6 | Configure Web Logic Console | 19-3 |

| | | |
|--------|---|------|
| 19.6.1 | Data source with JNDI Name as 'eis/DB/ArgusSafety_Outbound' | 19-4 |
| 19.6.2 | Data source as 'jdbc/ArgusSafety_Inbound' | 19-4 |
| 19.6.3 | Data source with JNDI Name as 'eis/DB/ArgusSafety_Inbound' | 19-4 |
| 19.6.4 | DB Adapters for Data Source..... | 19-4 |
| 19.7 | Configure Large Payload Exchange..... | 19-4 |
| 19.7.1 | Outbound Files..... | 19-5 |
| 19.7.2 | Inbound Files..... | 19-5 |
| 19.7.3 | Transaction Time | 19-5 |
| 19.7.4 | General B2B Settings for Large Payloads | 19-5 |
| 19.8 | Configurations for Argus Safety..... | 19-5 |
| 19.8.1 | Configure Oracle B2B..... | 19-5 |
| 19.8.2 | Update for B2B Documents..... | 19-5 |
| 19.8.3 | Argus Console > Reporting Destination Code List | 19-6 |

20 Configure OBIEE or BI Publisher

| | | |
|----------|---|-------|
| 20.1 | Prepare BI Publisher Server..... | 20-1 |
| 20.2 | Set Up BI Publisher for Argus Safety | 20-1 |
| 20.2.1 | Enable a Local Superuser..... | 20-1 |
| 20.2.2 | Create a Database Connection | 20-2 |
| 20.2.3 | Set Up Runtime BI Publisher Time-out | 20-2 |
| 20.2.4 | Configure Oracle Fusion Middleware Security Model | 20-3 |
| 20.3 | Manage Users and Roles..... | 20-3 |
| 20.3.1 | Configure Users, Groups and Roles..... | 20-3 |
| 20.3.1.1 | Create a Group..... | 20-3 |
| 20.3.1.2 | Create a User | 20-4 |
| 20.3.1.3 | Create an Application Role | 20-4 |
| 20.3.2 | Create Application Policies and Set Up Folder Privileges (BI Publisher Standalone only) 20-5 | |
| 20.3.2.1 | Create Application Policies | 20-5 |
| 20.3.2.2 | Manage Folder Privileges..... | 20-6 |
| 20.3.3 | Create Application Policies and Set Up Folder Privileges (OBIEE and BI Integrated Installation only) 20-8 | |
| 20.3.3.1 | Create Application Policies | 20-8 |
| 20.3.3.2 | Manage Folder Privileges..... | 20-9 |
| 20.4 | Upload BI Publisher Reports..... | 20-19 |
| 20.4.1 | Flexible Aggregate Reports | 20-19 |
| 20.4.2 | PMDA R3 Paper Reports | 20-20 |
| 20.5 | Integrate Argus Safety with BI Publisher | 20-20 |
| 20.5.1 | Configure AG Service | 20-20 |
| 20.5.2 | Configure Web Service (Expedited Reports only) | 20-21 |
| 20.5.3 | Add AG Service user to BI Publisher (Expedited Reports only) | 20-21 |
| 20.5.4 | Update SSO Exclusion List..... | 20-21 |
| 20.6 | Argus Console—BIP Common Settings | 20-22 |
| 20.6.1 | Configure BIP Reporting Admin User | 20-22 |
| 20.6.2 | Enable BIP Aggregate Reports and Configure Persistence Data (Flexible Aggregate Reporting only) 20-22 | |
| 20.6.3 | Configure Code Lists..... | 20-23 |

| | | |
|----------|---|-------|
| 20.6.3.1 | Flexible Aggregate Reporting Code Lists | 20-23 |
| 20.6.3.2 | PMDA R3 Paper Forms Code lists | 20-23 |
| 20.7 | Configure Flexible Aggregate Reporting Database | 20-24 |
| 20.7.1 | Execute Argus_BIP_Enable | 20-24 |
| 20.8 | Upgrade BIP Reports to 8.2.2 | 20-25 |

21 Configure the BIP Environment for Argus Insight

| | | |
|----------|---|-------|
| 21.1 | Create PRMART JDBC Connection..... | 21-1 |
| 21.2 | Manage Users and Roles: BI Publisher Standalone Installation with BI Publisher Security ... 21-2 | |
| 21.2.1 | Create Users and Assign Roles to Users..... | 21-2 |
| 21.2.2 | Create Roles, Add Data Sources, and Assign Roles | 21-3 |
| 21.3 | Manage Users and Roles: BI Publisher Standalone Installation with OFM Security | 21-4 |
| 21.3.1 | Create Users and Assign Roles to Users..... | 21-4 |
| 21.3.2 | BI Publisher Standalone Installation in OFM Security | 21-5 |
| 21.3.2.1 | Create Users and Groups | 21-5 |
| 21.3.2.2 | Create Roles and Policies..... | 21-5 |
| 21.3.3 | Create Roles, Adding Data Sources, and Assign Roles in WebLogic Enterprise Manager 21-7 | |
| 21.3.4 | Create Application Policy | 21-9 |
| 21.3.5 | Upload the Argus Insight.xdrz file to BIP..... | 21-9 |
| 21.4 | Configure BIP Users and Roles: Oracle Fusion Middleware Security Model..... | 21-10 |
| 21.4.1 | Configure BIP Roles | 21-11 |
| 21.4.2 | Folder Level Permissions..... | 21-11 |

22 Configure the OBIEE Environment for Argus Insight

| | | |
|--------|---|-------|
| 22.1 | Pre-installation Configuration | 22-1 |
| 22.2 | Configure the OBIEE Repository and Web Catalog using the BAR File | 22-1 |
| 22.2.1 | Import the BAR file in an existing OBIEE instance..... | 22-2 |
| 22.2.2 | Import the BAR file to create a new OBIEE Instance | 22-4 |
| 22.3 | Configure OBIEE Repository and Web Catalog Manually..... | 22-5 |
| 22.4 | Create Users and Groups in OBIEE..... | 22-6 |
| 22.4.1 | Create Users and Groups in WebLogic Server..... | 22-6 |
| 22.4.2 | Create Roles and Policies with Fusion Middleware Control | 22-7 |
| 22.5 | OBIEE Catalog Folder-level Permissions | 22-9 |
| 22.6 | OBIEE Default Application Roles..... | 22-11 |

23 Install Argus Unblinding

| | | |
|------|---------------------------------------|------|
| 23.1 | Prerequisites | 23-1 |
| 23.2 | Install Argus Unblinding Utility..... | 23-1 |

24 Configure Argus Centralized Coding

| | | |
|--------|---|------|
| 24.1 | setup_centralized_coding_interface_schema.bat | 24-1 |
| 24.2 | dms_migration.bat..... | 24-2 |
| 24.2.1 | Single Enterprise Migration in One Execution..... | 24-2 |
| 24.2.2 | All Enterprise Migration in One Execution | 24-2 |

25 Extract, Transform, and Load Data

| | | |
|--------|---|------|
| 25.1 | Prerequisites, Cautions, and Warnings | 25-1 |
| 25.2 | Run the Initial ETL..... | 25-1 |
| 25.2.1 | Generate the Balance Logs..... | 25-2 |
| 25.2.2 | Close the Initial ETL Status Dialog Box..... | 25-3 |
| 25.2.3 | Stop the Execution of ETL | 25-3 |
| 25.3 | Run the Initial ETL Again | 25-3 |
| 25.4 | Process a Failed ETL | 25-3 |
| 25.4.1 | Continue the Failed Initial ETL Process | 25-4 |
| 25.4.2 | Ignore the Failed Initial ETL Process | 25-4 |
| 25.4.3 | Modify the Attributes of ETL Data Exclusion | 25-5 |
| 25.5 | Restart the Initial ETL Process | 25-5 |

Part V Secure Oracle Argus

26 Argus Password Management—Cryptography Tool

| | | |
|--------|--|------|
| 26.1 | Install or Upgrade to Argus Safety 8.2.2..... | 26-1 |
| 26.1.1 | Generate New Cryptography Key | 26-2 |
| 26.1.2 | Argus Safety Database | 26-2 |
| 26.1.3 | Argus Safety Application Servers | 26-2 |
| 26.2 | Reset Password or Change the Cryptography Key | 26-2 |
| 26.2.1 | Reset the ARGUSUSER Password | 26-2 |
| 26.2.2 | Edit Keys | 26-3 |
| 26.2.3 | Re-encrypt Common User Passwords..... | 26-4 |
| 26.2.4 | Generate Encrypted String | 26-5 |
| 26.2.5 | Reset Administrator and System Application User Password | 26-6 |
| 26.2.6 | Reset the Environment if ArgusSecureKey.ini is Lost | 26-6 |
| 26.3 | Manage Argus Insight Cryptographic Key | 26-7 |
| 26.3.1 | Update APR_USER Password | 26-7 |
| 26.3.2 | Copy Initialization Files to Other Servers | 26-7 |
| 26.3.3 | Restart IIS and Run ETL | 26-7 |

A Configure BI Publisher Security Model

| | | |
|-----|---|-----|
| A | Create Custom Roles and Assign Data Sources | A-1 |
| 11. | Create Users and Assign Roles | A-1 |

B Create ODBC Connection for OBIEE Administration Tool for Argus Insight

Preface

You can use this guide to:

- Install Oracle Argus Safety 8.2.2
- Upgrade from Oracle Argus Safety 8.x.x to Oracle Argus Safety 8.2.2
- Install Oracle Argus Insight 8.2.2
- Upgrade from Oracle Argus Insight 8.x.x to Oracle Argus Insight 8.2.2

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.

Revision History

| Date, Version | Description |
|------------------------|---|
| 31-Jul-2020, Version 2 | Added Section 10.4, "Post Application Install or Upgrade" and Chapter 9, "Upgrade the Argus Application." |
| 15-Jul-2020, Version 1 | Initial release. |

Part I

Prepare to Install Argus

Argus Safety and Argus Insight are configurable systems and, based on user needs, you (administrators) may install all or some of the components.

We recommend that you follow the steps in the order presented.

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.

System Requirements

1.1 Hardware Requirements

■ Database Server

| Hardware Requirements | Small | Mid-Sized | Large |
|---|--------------------------------------|--------------------------------------|-----------------------------------|
| RAM | 16 GB | 32GB | >=64 GB |
| CPU or Processor | Equivalent to 2 - 4 Dual Core x 3GHz | Equivalent to 4 - 8 Dual Core x 3GHz | Equivalent to 16 Dual Core x 3GHz |
| Fail Support System (physical standby option) | Dataguard | Dataguard | Dataguard |
| Virtualization | Optional | Optional | Optional |
| Exadata 12c R1 (with 12.1.0.2 or 12.2.0.1) | Optional | Optional | Optional |
| Oracle RAC 12c R1 (with 12.1.0.2 or 12.2.0.1) | Optional | Optional | Optional |
| Oracle RAC 19c | Optional | Optional | Optional |

■ Web Server, Transaction Server, and Interchange Server

| Hardware Requirements | Small | Mid-Sized | Large |
|-----------------------|---|---|---|
| RAM | 8 GB | 16 GB | 16 GB |
| CPU or Processor | 1 Dual Core CPU x 3 GHz | 2 Dual Core CPUs x 3 GHz | 2 Quad Core CPUs x 3 GHz |
| Virtualization | Physical Server or Oracle Virtual Machine (OVM 3.2.10, 64-bit) | Physical Server or Oracle Virtual Machine (OVM 3.2.10, 64-bit) | Physical Server or Oracle Virtual Machine (OVM 3.2.10, 64-bit) |
| Minimum Resolution | 1280 x 1024 | 1280 x 1024 | 1280 x 1024 |

- **Web Client**
 - RAM: 8 GB
 - 3 GHz Dual Core CPU
 - Minimum Resolution: 1280 x 1024
- **Argus Unblinding Tool**
 - RAM: 8 GB
 - 3 GHz Dual Core CPU
 - Minimum Resolution: 1280 x 1024

1.2 Software Requirements

1.2.1 Operating System

| Operating System | DB Server | Web Server | Transaction Server | Interchange Server | Web Client | Argus Unblinding Tool | Dictionary Management Tool |
|------------------------------------|--|------------|--------------------|--------------------|------------|-----------------------|----------------------------|
| | Operating System as certified for Oracle 19c, 12.1.0.2 or 12.2.0.1 | — | — | — | — | | — |
| Microsoft Windows 2016 | — | Yes | Yes | Yes | — | Yes | Yes |
| Microsoft Windows 2012 R2 Standard | — | Yes | Yes | Yes | — | Yes | Yes |
| Microsoft Windows 10 (64-bit) | — | — | — | — | Yes | Yes | — |

1.2.2 Oracle Components

Note: Make sure that you install the same version of Oracle Database Server and Client.

| Oracle Components | DB Server | Web Server | Transaction Server | Interchange Server | Web Client | Argus Unblinding Tool | Dictionary Management Tool |
|--|---|--|--------------------|--------------------|------------|-----------------------|----------------------------|
| Oracle Database Server version 19c, 12.1.0.2, or 12.2.0.1 (Enterprise/Standard Edition 2 over CDB/PDB or non-CDB format) | Yes | — | — | — | — | — | — |
| Oracle Client version 19c, 12.1.0.2, or 12.2.0.1 (64-bit only) with the latest patch set (See Section 2.2.3, "Install and Apply Oracle Patch Set") | — | Yes | Yes | Yes | — | Yes | Yes |
| MTS | — | Yes | Yes | Yes | — | Yes | Yes |
| ODP.NET | — | Yes | Yes | Yes | — | Yes | Yes |
| Java JRE 1.8 or above | — | Yes (Required for Liquibase and WebGate only) | — | — | — | — | Yes |
| Oracle Advanced Security Network Encryption | Optional | — | — | — | — | — | — |
| Oracle XML Developer's Kit (XDK) | Optional (Required only for PMDA R3 Paper Reports) | — | — | — | — | — | — |

1.2.3 Other Components

| Other Components | DB Server | Web Server | Transaction Server | Interchange Server | Web Client | Argus Unblinding Tool | Dictionary Management Tool |
|--|-----------|------------|--------------------|--------------------|------------|-----------------------|----------------------------|
| Microsoft Internet Explorer, Version 11.0 (64-bit) - Compatibility View only | — | — | — | — | Yes | — | — |
| Microsoft Visual C++ 2010 SP1 Redistributable x64 | — | Yes | Yes | Yes | — | Yes | Yes |
| Microsoft Visual C++ 2015 Redistributable x64 | — | Yes | Yes | Yes | — | Yes | Yes |
| Microsoft Access Database Engine 2016 Redistributable x64 | — | — | — | — | — | — | Yes |
| Microsoft .NET 4.7.2 Framework | — | Yes | Yes | Yes | — | Yes | Yes |

1.2.4 Generic—Other Supported Features

| If you are using... | You must install... |
|--------------------------|---|
| Data encryption | <p>Oracle Database TDE feature on the Database Server, which is a part of the Oracle Advanced Security option available for Oracle Database Enterprise Edition:</p> <ul style="list-style-type: none"> 19c (https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/index.html) 12c (https://docs.oracle.com/database/121/ASOAG), or http://www.oracle.com/technetwork/database/options/advanced-security/overview/index.html <p>TDE provides the capability to encrypt sensitive data in the Oracle Database in a manner that is transparent to applications.</p> <p>Argus Safety product has been functionally certified with tablespace level encryption using the Oracle Database TDE feature.</p> |
| Multi-tenant environment | Single Sign-On |
| Single Sign-On | <p>Oracle Identity Management (IDM) version 11.1.2.3</p> <p>For a multi-tenant environment, install the compatible WebGate version 11.1.2.3.0 (64-bit) and apply the WebGate p26540269_111230_MSWIN-x86-64 bundle patch.</p> |

| If you are using... | You must install... |
|---|---|
| Built-in Reports to run the PMDA E2B R3 Paper Reports or Flexible Aggregate Reporting | <ul style="list-style-type: none"> ■ Oracle Business Intelligence Enterprise Edition (OBIEE) 12.2.1.4 ■ Oracle BI Publisher 12.2.1.4 Standalone (for Argus SE only) ■ BI Publisher Desktop tool on the client machine to customize the reports. ■ WebLogic 12.2.1.3 <p>See Chapter 20, "Configure OBIEE or BI Publisher."</p> |
| LDAP for authentication support | LDAP/LDAPS Protocol Version 3.0 |
| E-mail capabilities within Argus | <p>SMTP Protocol.</p> <p>The following Argus Safety components support SMTPS:</p> <ul style="list-style-type: none"> ■ Argus Safety—Supports SMTPS and TLS 1.2 (Forced). Both Implicit and Explicit modes. ■ Axway B2Bi 2.6 SP1—Supports SMTPS and TLS 1.2. Implicit mode only. ■ OBIEE/BIP—Supports SMTPS and TLS 1.2, and must have JDK 1.8 for SMTPS. Both Implicit and Explicit modes. <p>Note that B2B does not supports SMTPS.</p> |
| Documentum for Storage | Documentum DFC 7.2 (32-bit) on Web, Transaction, and Interchange Servers. |
| Faxing capabilities for Expedited Reports | RightFax 10.6 (32-bit) on Transaction Server. |
| E2B Reporting for exchange | <ul style="list-style-type: none"> ■ Oracle B2B 12.2.1.3—Certified with both AS1 and AS2 protocols for E2B exchanges between regulatory authorities and pharmaceutical companies. <p>Apply patch 26795544 to support AES encryption.</p> <ul style="list-style-type: none"> ■ Axway B2Bi 2.6 SP1 |
| Microsoft Windows 2012 R2 Standard | IIS 8.5 |
| Microsoft Windows 2016 | IIS 10 |

Tips:

- Enable HTTP Compressions on your windows server.
- Enable SSL that is supported for your windows server.

1.2.5 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.

Install Oracle Database

Install Oracle Database on the Database Server.

In a multi-tenant environment, you must install the Oracle database with the Oracle Database Server Enterprise edition (and not the Standard edition).

2.1 Get the Oracle Database Installation Guide

Open or download the installation guide for your operating system:

- For version 19c—
<https://docs.oracle.com/en/database/oracle/oracle-database/19/install-and-upgrade.html>
- For version 12.1.0.2—https://docs.oracle.com/database/121/nav/portal_11.htm
- For version 12.2.0.1—
<https://docs.oracle.com/en/database/oracle/oracle-database/12.2/install-and-upgrade.html>

2.2 Install Oracle Database

Follow the instructions in the *Oracle Database Installation Guide*, making selections appropriate for Argus Safety as noted in the following sections.

You can configure the database as part of the database software installation or after, using the Database Configuration Assistant (DBCA). Argus Safety supports installation on either a Container Database (CDB) containing a Pluggable Database (PDB) or a non-CDB database.

For an explanation of which options require an additional license, see the Database Licensing Information User Manual at <http://docs.oracle.com/database/>

2.2.1 Database Software Installation Options

During installation of the database software (binaries, or server code), select the following:

- Advanced or Typical installation
- Time Zone
- Oracle Real Application Clusters (RAC) (Optional)

2.2.2 Database Configuration Options

| Feature or Option | Mandatory | Recommended | Optional | Notes |
|--|-----------|-------------|----------|--|
| Character Set: AL32UTF8 | Yes | — | — | — |
| Oracle Text | Yes | — | — | Included automatically if you install the database during server installation. |
| Oracle JVM | Yes | — | — | Included automatically if you install the database during server installation. |
| Oracle XML DB | Yes | — | — | Included automatically if you use the Oracle Database Configuration Assistant to create the database. http://docs.oracle.com/database/121/ADXDB/appaman.htm#ADXDB2700 |
| Oracle Automatic Storage Management | — | Yes | — | Provides an alternative to conventional volume managers, file systems, and raw devices. |
| Automatic Memory Management | — | Yes | — | Manages instance memory to allow the Oracle Database instance to automatically manage and tune it for you. |
| Oracle Advanced Security Transparent Data Encryption (TDE) | — | Yes | — | Available only for the Enterprise Edition. |
| Oracle Real Application Clusters (RAC) | — | — | Yes | — |
| Oracle Partitioning | — | — | Yes | Available only for the Enterprise Edition. |

2.2.3 Install and Apply Oracle Patch Set

1. Download and install the latest patch set: WINDOWS DB BUNDLE PATCH through Oracle Support.

To install Oracle Client, use the **Custom** option (NOT the Administrator option) and make sure that the **MTS component** is checked explicitly.

2. Set oracle_home to your client home location. For example:

```
SET ORACLE_HOME=<Oracle Client home path>
```

3. Run sqlldr help=y or sqlldr.exe.
4. Apply the latest CPU patch.

2.3 Set Up Argus Safety Database Parameters

2.3.1 Argus Safety Database Instance Parameters (Recommended)

We recommend that you evaluate each site before installation and on an ongoing basis to determine whether these settings are suitable for your business needs.

Note: Argus Safety database compatible parameter should be set as the <current version>.

| # | Database Parameters | Small (under 30,000 cases reported per month) | Mid-Sized (30,000 to 200,000 cases reported per month) | Large (200,000 to 1,000,000 cases reported per month) | Very Large (over 1,000,000 cases reported per month) |
|----|------------------------------------|--|---|--|---|
| 1 | MEMORY_TARGET | 10 GB | 16-24 GB | 32-64 GB | >64 GB |
| 2 | PROCESSES | Expected concurrent users + 100 | Expected concurrent users + 100 | Expected concurrent users + 100 | Expected concurrent users + 100 |
| 3 | MEMORY_MAX_TARGET | >= value set for MEMORY_TARGET | >= value set for MEMORY_TARGET | >= value set for MEMORY_TARGET | >= value set for MEMORY_TARGET |
| 4 | OPTIMIZER_SECURE_VIEW_MERGING | FALSE | FALSE | FALSE | FALSE |
| 5 | CURSOR_SHARING (Mandatory) | EXACT | EXACT | EXACT | EXACT |
| 6 | WORKAREA_SIZE_POLICY | AUTO | AUTO | AUTO | AUTO |
| 7 | JOB_QUEUE_PROCESSES | 25 | 25 | 25 | 25 |
| 8 | DB_BLOCK_SIZE (bytes) | 8192 | 8192 | 8192 | 8192 |
| 9 | NLS_LENGTH_SYMANICS (Mandatory) | CHAR | CHAR | CHAR | CHAR |
| 10 | GLOBAL_NAMES | TRUE | TRUE | TRUE | TRUE |

2.3.2 Additional Database Setup Information

| # | Setting | Small (under 30,000 cases reported per month) | Mid-Sized (30,000 to 200,000 cases reported per month) | Large (200,000 to 1,000,000 cases reported per month) | Very Large (over 1,000,000 cases reported per month) |
|---|-----------------------------------|--|---|--|---|
| 1 | Number and Size of Redo Log Files | 5 Groups * 100 MB | 5 Groups * 100 MB | 5 Groups * 100 MB | 5 Groups * 100 MB |
| 2 | TEMP Tablespace Size | 8 GB | 16 GB | 32 GB | >=64 GB |

| # | Setting | Small (under 30,000 cases reported per month) | Mid-Sized (30,000 to 200,000 cases reported per month) | Large (200,000 to 1,000,000 cases reported per month) | Very Large (over 1,000,000 cases reported per month) |
|---|----------------------|--|--|---|---|
| 3 | Undo Tablespace Size | 8 GB | 16 GB | 32 GB | >=64 GB |

2.4 Argus Insight Configuration Requirements

2.4.1 Database Parameters

[Table 2–1](#) lists the database parameters and the values that must be set for Argus Insight.

For those parameters that require a numeric value, [Table 2–1](#) 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 2–1 Database Parameters for Argus Insight

| Database Parameter | Required Value |
|---|---|
| COMPATIBLE (for Oracle 12c 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: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 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 <p>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.</p> |
| 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 |

2.4.2 Database I/O Configuration

Table 2–2 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) | | | |

2.4.3 Recommended Configuration for the Database Server

Table 2–3 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.

Part II

Set Up Argus Middle and Client Tiers

During the installation, the information in this manual may be different from what you see on your monitor if additional modules were selected during the Argus Safety Web Installation.

Prerequisites:

- Obtain a domain account with Local Administrator privileges.
- In case of application upgrade, make sure to [Backup Configuration Files](#) of the existing Argus Safety application before setting up the machines.

Recommendation:

- [Generate New Cryptography Key](#), and place the updated ArgusSecureKey.ini file under the .\Windows folder of the web server.
- You may need to reinstall the printer driver for site printers after setting up Argus Safety middle and client tiers.

If the current installed Argus Safety version does not support upgrade:

1. From your Windows folder, backup the **ArgusSecureKey.ini** file.
2. When the installation is complete, replace the exiting **ArgusSecureKey.ini** file with the backed up file in the Windows folder.

Replace the file on all the Windows servers.

Install and Configure Argus Safety Web

3.1 Prerequisites

- Make sure that the regional settings are US settings.
- Install [Internet Information Services](#) (IIS).
- [Generate New Cryptography Key](#), and place the updated ArgusSecureKey.ini file under the .\Windows folder of the server.

Note: To set up ASP.NET correctly, you must install IIS before running Windows Updates.

If Windows Updates are run before installing the IIS, Windows Updates will install Microsoft.Net without setting up the ASP.NET. In this scenario, refer to Microsoft Support on how to re-register ASP.NET in IIS.

This is usually accomplished by running aspnet_regiis.exe -i from the.NET v4.0.30319 folder.

3.2 Install Argus Safety Web

1. Log in as the Administrator on the system where Argus Safety is being installed.
2. Copy the installation package to the local directory of the target machine.
3. Open the Argus Safety folder and click **setup.exe**.
4. In the Argus Suite Solution Components Installation Wizard screen, click **Next**.
5. Enter the User Name and Company Name, and click **Next**.
6. In the Default Directory screen, to select the default installation directory where the Argus Suite Solution Components will be installed, click **Browse**.
7. To display the Argus Suite Components list, click **Next** and select the default installation directory.
8. Under the **Web Server**, select **Argus Safety Web**, and click **Next**.

The Argus Suite Solution Components Report Directory appears.

Note: (Optional) You can now install Argus Insight while installing Argus Safety by selecting it from the list of modules.

9. Select the directory where temporary reports will be stored.

You can browse through any path or leave this as default (C:\Temp).

10. (Optional) To configure minimum security on this server, enter the domain account login credentials, and click **Next**.

The Setup Status screen appears with the installation progress.

Note: If the minimum security is not being setup, leave these fields blank, and click **Next**.

11. To configure a database, click **Yes** when prompted.

12. Enter a database name and click **Next**.

This database name will appear on the Argus Login page.

13. Enter the database SID and click **Next**.

14. To add an additional database to the Argus Login page, click **Yes** when prompted to configure database settings.

15. In the Setup Completed screen, click **Finish**.

16. Click **OK** to reboot the system.

17. Set up the Argus Cryptography key by following the instructions in the [Section 26.1.3, "Argus Safety Application Servers"](#).

18. After setting up the application servers, copy the **ArgusSecureKey.ini** file from the **.\Windows** folder of the system, where the database is created or upgraded, and replace the **.\Windows** folder of each installed application server.

3.3 Configure Load Balancer in Argus Web

To set up a Load Balancer in Argus, you need to setup:

- The Argus Web Load Balancer IP Address
- The Load Balanced Folders
- The Shared Network Directory

3.3.1 Set Up Argus Web Load Balancer IP Address

If Argus Web is being installed in a Load Balanced Environment, the Load Balancer IP Address must be configured in Argus Console.

1. Log in to Argus Console.
2. From System Configuration Menu, select System Management.
3. Click the Network Settings Folder.
4. Do the following, and click **Save**.
 - For non-SSL environment, enter the IP Address or Argus URL.

- For an SSL environment, enter the SSL URL.

3.3.2 Set Up Shared Network Directory

The network directory is a shared directory that will be the same for all load balanced Web Servers.

Update **argus.ini** for messagecachepath=<shared directory for the message cache>.

3.4 Reset IIS

To make the latest data or configurations available to the rest of the system, reset IIS when the changes have been made to the following areas:

1. Changes in configuration files:
 - Argus.ini
 - Argus.xml
2. Changes in following screens through Console:
 - Common Fields
 - System Management
 - Enabled Modules

Install Argus Insight

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

4.1 Install Argus Insight Components onto the Web Server

Note: If you are upgrading Argus Insight from 8.2 to Argus Insight 8.2.1, first uninstall the application using Argus Insight application, and then run the Argus Insight 8.2.1 Installer.

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

1. Download the Argus Insight software from My Oracle Support 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, and click **Next**.

The Select Features dialog box appears.

6. Clear any feature that you do not want to install and click **Next**.

By default, the wizard installs all features.

7. In the Choose Destination Location dialog box, 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 Argus Insight is configuring your new software along with the progress bar.

8. (Optional) To configure minimum security on this server, enter the domain account login credentials, and click **Next**.

The Setup Status screen appears with the installation progress.

Note: If the minimum security is not being setup, leave these fields blank, and click **Next**.

Note: When Argus Insight is installed after the Argus Safety on the same server for which minimum security is already configured, then minimum security for Argus Insight components are not applied.

To configure the domain user for Argus Insight, run the installer again. In the installation wizard:

1. Select **Modify** and click **Next**.
2. Select **Reset Domain Password** and enter the parameters.

This will set minimum security again for both Argus Safety and Argus Insight.

9. In the Setup Completed screen, click **Finish**.
10. Click **OK** to restart the Argus Insight Web Server.

4.1.1 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.

To modify the APR_USER password, see [Section 26.3.1, "Update APR_USER Password."](#)

4.2 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**.

Configure Web Service Interfaces on Web Server

5.1 Argus Web Service Interface

The Argus Web Service Interface supports outbound Interfaces (MedDRA, WHO Drug and LOT Number) which provide the capability to integrate with customer-hosted web services and inbound web services (the Product-Study-License Interface) hosted on the Argus Safety Web Server.

All web service-based interfaces communicate with the standard SOAP 1.2 Protocol and use WS-Addressing and WS-Security. The Argus web service interface leverages Windows Communication Foundation to generate WS-Addressing and WS-Security header information. We recommended testing this message before moving too far into business testing. For more information on these specifications, see the OASIS and W3C websites.

You can edit a standard .config file to select which integrations to enable, which transport protocol to use, and authentication details.

All errors are handled through a SOAP fault. Should an error occur, logical or otherwise, a SOAP fault should be thrown by the host and caught by the client. The client application (web) of Argus displays the details of the SOAP fault to the user when possible. Argus web services throw SOAP faults when an error occurs.

The Argus Safety web service interface in this release supports the following integrations through Web Service:

| Interface | Description |
|--|---|
| MedDRA (outbound) | MedDRA Drug web service interface provides a mechanism to integrate customer-hosted MedDRA coding systems with Argus Safety via web services. |
| WHO Drug (outbound) | WHO Drug web service interface provides a mechanism to integrate customer-hosted WHO coding systems with Argus Safety via web services. |
| Lot Query (outbound) | Lot Number web service interface provides a mechanism to integrate customer-hosted central product information systems with Argus Safety via web services. |
| Product Study License(PSL) - (inbound) | PSL web service interface provides a mechanism to integrate customer central system to push or query PSL data via web services hosted on the Argus Safety Web Server. |

In a multi-tenant Argus system:

- Endpoint configuration of central MedDRA and WHO Drug web service is at the global level. Enterprise if configured to use MedDRA and WHO Drug web service interface uses same endpoint to connect.
- Endpoint configuration of Lot Number Interface is defined at an enterprise level. Enterprise if configured to use Lot Interface uses enterprise specific endpoint configuration.
- Outbound Interface: Message payload must have an 'EnterpriseShortName'.
- Inbound Interface: Message payload must have an 'EnterpriseShortName'.

5.1.1 Argus Web Service Interface Framework

Each outbound/inbound web service request/response is enclosed in a SOAP envelope that begins with a SOAP header, followed by a Body statement that contains a unique node under the SAFETY_MESSAGE node. This node uniquely identifies the Interface being used for Inbound/Outbound communication. When implementing the customer side of the interface, follow the structure defined by Oracle in the XSD/WSDL files located in the following directory:

<Argus Web Install Path>\Integrations\XSD

<Argus Web Install Path>\Integrations\WSDL

For example, C:\Program Files\Oracle\ArgusWeb\ASP\Integrations\XSD

5.2 Edit .config Files

5.2.1 Edit the .config file for Outbound Interfaces

1. Navigate to the root of the ArgusWeb directory.
2. Open the **web.config** file in a text editor.
By default, the bindings are provided for:
 - basic HTTP traffic
 - basic SSL communication
3. Update the **address** attribute of the endpoint nodes to point to the correct web service address.
4. To use encryption, set the **bindingConfiguration** attribute of the endpoint node as **WSHttpBinding_IReSysService_Secure**.
Additional binding configurations may also be created and used.
Note that the binding configurations between the host and the client must be compatible for successful communication.
5. To transmit the authentication information, add credentials in the **ClientCredentials** section of each endpoint node.
6. To transform messages, use either a custom transformation assembly or an XSLT. Lot Number and WHO Drug coding interfaces leverages this feature.
 - Update the **TransformerConfiguration** section to map an endpoint to a transformer.

- If multiple transformers are specified for a particular endpoint, they are executed in the order in which they appear in the configuration file.
- The transformers configured by Oracle should not be modified, but additional transformers may be added if necessary.

5.2.2 Edit the .config file for Inbound Interface

All inbound integrations (file based) are handled by the Argus Safety Windows Service.

1. Navigate to the `.\ArgusWeb\ASP\Argus.NET\Bin` directory.

2. Open the **RelsysWindowsService.exe.config** file in a text editor.

This configuration file provide reference configuration files of the configured integrations.

3. To enable an integration, in the **RelsysConfigurationFiles** section, uncomment the required **add** node (s).
4. To disable an integration, in the **RelsysConfigurationFiles** section, comment the required **add** node (s).
5. In the **DatabaseConfiguration** section, enter the database credentials.

5.3 Safety Message

The XML message required by each integration varies and is defined by its own schema. However, each schema follows a standard. The root node of every XML Safety Message in inbound and outbound interface is **SAFETY_MESSAGE** with the following node or attribute:

| Node/Attribute Name | Description |
|---------------------|---|
| Type | This is an enumeration (currently either "Request" or "Response") to identify the directionality of the message. |
| EnterpriseShortName | <ul style="list-style-type: none"> ■ In the Argus Safety multi-tenant environment, EnterpriseShortName is a part of message payload for all outbound and inbound interfaces. ■ In the Argus Safety single-tenant environment, EnterpriseShortName is not a part of message payload for the outbound interfaces and is not required for inbound interface. |
| EXTENSION | Every Safety Message may also contain an EXTENSION node with CUSTOM sub nodes. These are for future expandability and currently unused. |

5.4 MedDRA Interface

The MedDRA Encoding Web Service Interface integrates customer-hosted central MedDRA dictionary web service with Argus Safety. Argus Safety expects the data from the central MedDRA dictionary web service in a defined format as specified by the MedDRA dictionary schema.

In a multi-tenant setup, endpoint configuration of central the MedDRA web service is stored at global level and all the enterprises in Argus Safety uses the same web service endpoint. The **EnterpriseShortName** attribute present in the request message payload identifies which enterprise has initiated the web service request.

This interface supports both English and Japanese MedDRA dictionaries.

Note: To upload the dictionaries, refer to the *Oracle Argus Safety Administration Guide*.

5.4.1 MedDRA Configuration

5.4.1.1 Enable MedDRA Integration through Argus Console

1. From Argus Safety Web, open Console and select System Configuration > System Management.
2. Expand the **Case Processing** tree branch, then and select **Dictionary Browser**.
3. To use web services, select the **Argus Safety MedDRA Coding Method** radio button.
4. If the web service hosting MedDRA is not available, fails, or does not return a valid match, check the **Use Local MedDRA if Term not found by Web Services** checkbox. (Optional)
5. To use local MedDRA J, check the **Use Local MedDRA for Japanese terms** checkbox.

5.4.1.2 Edit the ArgusWeb/ASP/web.config file

1. Navigate to ArgusWeb/ASP.
2. Open the **web.config** file in a text editor.
3. Search for **endpoint** and update the following attributes:
 - **address**—to point to the correct web service address
 - **name**—MedDRA
 - **bindingConfiguration**—to use encryption

Note that the binding configurations between the host and the client must be compatible for successful communication.

The endpoint configuration might look something like this:

```
<endpoint address="http://remotewebsevice/MedDRAAutoEncode.svc"
binding="wsHttpBinding" bindingConfiguration="WSHttpBinding_IRelsysService_
Unsecure" contract="IRelsysService" name="MedDRA">
```

5.4.1.3 Edit the Argus.NET/web.config file

1. Navigate to ArgusWeb/ASP/Argus.NET.
2. Open the **web.config** file in a text editor.
3. Search for **endpoint** and update the following attributes:
 - **address**—to point to the correct web service address
 - **name**—MedDRA
 - **key**—version of MedDRA XML being used

For example,

- `<add key="MedDRAXMLVersion" value="2.0"/>`, or
- `<add key="MedDRAXMLVersion" value="1.1"/>`, or
- `<add key="MedDRAXMLVersion" value="1.0"/>`

- **bindingConfiguration**—to use encryption

Note that the binding configurations between the host and the client must be compatible for successful communication.

- **paths**—to add path for both the Request and Response XSDs based on the version being used

For example,

- `<add InputXSD="..\..\Integrations\XSD\v2.0\MedDRA_Response.xsd" />`
- `<add InputXSD="..\..\Integrations\XSD\v2.0\MedDRA_Request.xsd" />`

5.4.2 MedDRA Encoding Flow

When Argus Safety makes a call to the web service, it populates the REPORTED and CODED nodes with data entered by the user. The REPORTED term is essentially a verbatim term while the coded term is the term that is expected to be coded by the remote system. The returned message contains a PATHS node with PATH sub-nodes that have been encoded by the remote system. Argus Safety displays the returned LLTs in the MedDRA browser from which you can select the correct LLT. Note that the MedDRA Browser does not open on the Case Bookin screen.

If autoencoding is enabled and finds an exact match, Argus Safety places the encoded LLT term in the case form. If autoencoding finds multiple matches, the system uses the primary path. If autoencoding is not enabled or does not find any matches, or the web service is unavailable, Argus Safety loads the MedDRA browser with local dictionary information, if the system is configured to allow this.

5.4.3 MedDRA Interface XML Schema

Schema files for request and response are located in the *<Argus Web Install Path>\Integrations\XSD* directory.

Verify the MedDRA Interface request and response functions for the following schema files.

5.4.3.1 MEDDRA_Request

Argus Safety makes a web service request to the externally hosted central product information system as defined in this schema.

- Schema File

Version 1.0

Top level file: `\v1.0\MedDRA_Request.xsd`

Sublevel file: `\v1.0\Base.xsd`

Version 1.1

Top level file: `\v1.1\MedDRA_Request.xsd`

Sublevel file: `\v1.0\Base.xsd`

Version 2.0

Top level file: \v2.0\MedDRA_Request.xsd

Sublevel file: \v1.0\Base.xsd

- Namespace

http://www.oracle.com/Argus/MedDRA_Request/v1.0

http://www.oracle.com/Argus/MedDRA_Request/v1.1

http://www.oracle.com/Argus/MedDRA_Request/v2.0

- Node/Attribute Name Description

The MEDICAL_DICTIONARY node is the first child node identifying MedDRA integration.

5.4.3.2 MEDDRA_Response

Argus Safety expects the central MedDRA dictionary to send the response in this format.

- Schema File

Version 1.0

Top level file: \v1.0\MedDRA_Response.xsd

Sublevel file: \v1.0\Base.xsd

Version 1.1

Top level file: \v1.1\MedDRA_Response.xsd

Version 2.0

Top level file: \v2.0\MedDRA_Response.xsd

- Namespace

http://www.oracle.com/Argus/MedDRA_Response/v1.0

http://www.oracle.com/Argus/MedDRA_Response/v1.1

http://www.oracle.com/Argus/MedDRA_Response/v2.0

- Node/Attribute Name Description

| Node/Attribute Name | Description |
|---------------------|--|
| Action | <p>Must have the value Auto.</p> <p>This attribute must be present in the request when a full hierarchy is required to be passed back to auto encode the term without using the MedDRA Browser. With an "Auto" message, the system requires that an LLT Term be passed in the request. If the full hierarchy is not found or returned, the system will open the MedDRA Browser and display the LLTs returned for manual encoding by the user using the local MedDRA instance. If multiple paths are returned, the Primary SOC path is used.</p> |

| Node/Attribute Name | Description |
|--------------------------|---|
| Source | <p>An enumerated value that specifies additional information that may be required for coding based on origination as follows:</p> <ul style="list-style-type: none"> Reaction <ul style="list-style-type: none"> Case Form Patient Tab Patient Tab Other Relevant History Reaction Case Form Patient Tab Parent Tab Other Relevant History Reaction Indication <ul style="list-style-type: none"> Case Form Patient Tab Patient Tab Other Relevant History Indication Case Form Patient Tab Parent Tab Other Relevant History Indication Condition should be verbatim <ul style="list-style-type: none"> Case Form Patient Tab Patient Tab Other Relevant History Verbatim Case Form Patient Tab Parent Tab Other Relevant History Verbatim Lab <ul style="list-style-type: none"> Console Code Lists Lab Test Type Description <ul style="list-style-type: none"> Case Form Events Tab Event Tab Description to be Coded Case Form Events Tab Death Information Cause of Death and Autopsy Results Description as Reported Diagnosis <ul style="list-style-type: none"> Argus Case Form Analysis Tab Analysis Tab Company Diagnosis Syndrome |
| Term (v 1.0) | The TERM node specifies the information about a specific term that is either being looked up or populated with data and supports Reported and Coded nodes. |
| Term (v 1.1/2.0) | The TERM node specifies the information about a specific term that is either being looked up or populated with data and supports Reported, Coded, and Lang nodes. |
| Primary | The Primary attribute is Y if the term is the Primary SOC path for the selected term. In the event that multiple terms are returned for a MedDRA level, this attribute is only be available on the primary term. |
| PATHS/PATH (version 1.0) | The PATHS node has a PATH subnode for each MedDRA hierarchy returned. MedDRA hierarchy with English terms only. |
| PATHS/PATH (version 1.1) | Contains MedDRA hierarchy with English and Japanese terms (without support for the J term currency detail). |
| PATHS/PATH (version 2.0) | Contains MedDRA hierarchy with English and Japanese terms (with support for the J term currency detail) for the LLT term. |

5.5 Product Study License Interface

This section provides information for integrating with an external Product Study License configuration system.

Detailed steps and examples on using the PSL interface are available through the Technical Reference Manuals (TRMs). Customers can download these TRMs through the Oracle Consulting or Customer Support teams.

1. Navigate to `<Install Path>\Oracle\ArgusWeb\ASP\Integrations`.
2. Open the **Service.config** file in a text editor.
3. Search for **DatabaseConfiguration**, and update the following attributes:
 - **DBName**—TNS of the Argus database.
 - **DBUser**—User name of an Argus Safety Service user. The PSL web service uses this User Context to perform updates in the Argus Safety Database.
4. To secure the configuration, set the **bindingConfiguration** attribute either manually or through the Service Config utility.

Additional binding configurations may also be created and used.

Note that the binding configurations between the host and the client must be compatible for successful communication.

5. To add logging information, use one of the following:
 - **Relsys Logger**—Logs information about errors, warnings, and processing of the PSL web service code. The logger internally uses **log4net** component to perform the logging.

Update the **logConfig** attribute with one of the following values:

- Error (default)
- Warning
- Information
- Verbose

To save log as a specific file, update **RollingLogFileAppender** with the filename. Make sure the web service has read/write permissions to this folder.

- **SOAP Message RequestLogger**—Logs all the incoming and outgoing SOAP messages of the PSL web service. The messages are stored internally in the Argus Safety Database and are not available for querying.

To disable this logging, set **Enabled** as **false**.

```
<TransformersConfiguration> <Transformers> <add Transformer="RequestLogger"
InterfaceType="Inbound" RequestType="Request,Response"
MessageType="SoapMessage" Enabled="False" Metadata=""
Assembly="ConsoleInterface"
Type="Relsys.ArgusConsole.ConsoleInterface.Common.DBLoggerFactory" />
</Transformers> </TransformersConfiguration>
```

5.6 WHO Drug Coding Interface

WHO Drug web service Interface provides a mechanism to integrate customer-hosted central WHO Drug coding web service with Argus Safety. Argus Safety expects the data from central WHO Drug Coding system in defined format as specified by WHO Drug Coding schema.

In a multi-tenant setup, endpoint configuration of central WHO drug coding web service is stored at global level and all enterprises in Argus Safety will use the same

web service endpoint. 'EnterpriseShortName' attribute will be present in the request message payload to identify which Enterprise initiated the web service request.

5.6.1 Configuration

■ Argus Console

Drug Dictionary integration must be enabled using Argus Console. This can be done by opening Console from Argus Web and selecting "System Configuration > System Management" from the menu. Expand the "Case Processing" tree branch and select "Dictionary Browser". Select the radio button to use web services under the "Argus Safety WHO Drug Coding Method" section.

An optional checkbox is also available to determine whether Argus has to use the local WHODrug instance if the web service hosting the drug dictionary is not available, fails, or does not return a valid match.

■ Web.Config

Web.config file on each web server under must have the endpoint with the "name" attribute of "WHODrug" properly configured. At a minimum, the "address" attribute must be changed. Optionally, depending on the bindings employed, the "bindingConfiguration" attribute may also need to be changed. The 'BindingConfiguration' section must have a valid binding for the configured "bindingConfiguration" attribute.

Sample endpoint configuration with binding configuration:

```
<endpoint address="http://remotewebsevice/WHODrugLookup.svc"
binding="wsHttpBinding" bindingConfiguration="WSHttpBinding_IRelsysService_
Unsecure" contract="IRelsysService" name="WHODrug"></endpoint>
```

5.6.2 Drug Dictionary Coding Flow

When Argus makes a call to the web service, it will populate the 'DRUG_NAME' node. Argus Safety expects the central drug dictionary to populate all possible information in the response XML as per define Drug Dictionary Interface response schema. Argus will display this information in a browser from which the user can select the correct drug.

If the web service does not return any results or is unavailable, Argus will present the user with the WHODrug browser with local dictionary information if the system is configured to allow this.

Note: If an ingredient is returned that is not in the 'LM_INGREDIENTS' table of Argus, the ingredient will not be stored with the case. ATC code is also not stored with the case data. Both of these items are visible in the browser, however.

5.6.3 WHO Drug Coding: XML Schema

Schema files for request and response are located in the <Argus Web Install Path>\Integrations\XSD directory.

Validate WHO drug coding request and response against the following schema files.

5.6.3.1 Request: WHODrug_Request

Argus Safety will make a web service request to externally hosted Central Drug Dictionary as defined in this schema.

Schema File

Top level file: /v1.0/WHODrug_Request.xsd

Sublevel file: /v1.0/Base.xsd

Namespace

http://www.oracle.com/Argus/WHODrug_Request/v1.0

where v1.0 is the version of the schema

| Attribute/Node name | Description |
|---------------------|--|
| DRUG_DICTIONARY | First Child node under SAFETY_MESSAGE which represents the WHO Drug Dictionary integration |
| DRUG/DRUG_NAME | WHO Drug Name that needs to be searched in central WHO Drug Coding system. |

5.6.3.2 Response: WHODrug_Response

Argus Safety expects Central Drug Dictionary to send the response in this format.

Schema File

Top level file: /v1.0/WHODrug_Response.xsd

Sublevel file: /v1.0/Base.xsd

Namespace

http://www.oracle.com/Argus/WHODrug_Response/v1.0

where v1.0 is the version of the schema

| Attribute/Node name | Description |
|---------------------|---|
| DRUG_DICTIONARY | First Child node under SAFETY_MESSAGE which represents the Drug Dictionary integration. |
| DRUGS/DRUG | WHO DRUG details |

5.7 Lot Number Interface

Lot Number Interface provides a mechanism to integrate customer-hosted central product information systems with Argus Safety via Web service. Argus Safety expects the data from hosted web service in defined format as specified by Lot Number schema. Argus Safety stores the web service Configuration at an enterprise level to support integration with different central product information system per Enterprise. 'EnterpriseShortName' attribute will be present in the request message payload to identify which Enterprise initiated the web service request.

Lot Number Query Interface also provides a mechanism for central product information system to pass custom data to Argus Safety system using 'Lot/Custom' node defined in Lot Number Schema. Data passed in the custom node will be stored in Argus user defined fields of Dosage Regimen section.

5.7.1 Configuration

Lot Number Interface needs to be enabled using Argus Console. This can be done by opening Console from Argus Web and selecting **System Configuration > System Management** from the menu. Expand the **Case Processing** tree branch and select **Lot Number Processing**. Following configurations are supported.

- **Use Centralized Lot Number Validation**

Yes—Allows Lot Lookup in Case Form to query central product information system to get Lot Number Information.

NO—Lot Lookup in Case Form uses lot numbers defined in Product Configuration under Argus Console >Business Configuration.

- **Allow users to enter non-configured Lot Numbers**

Yes—Allows user to enter non-configured Lot Number

No—Mandates user to only select Lot Number from Lot Lookup Dialog.

This switch is applicable when the lot validation service fails or is unable to provide a match for the lot number.

- **Lot Number Web Service Configuration XML**

Lot Number Interface support endpoint, binding and transformation configuration of Web Service at an enterprise level. This allows customer to integrate an enterprise in Argus Safety with different central product information system.

Configuration file must have the endpoint with the "name" attribute of "LotQuery" properly configured.

At a minimum, the "address" attribute must be changed. Optionally, depending on the bindings employed, the "bindingConfiguration" attribute may also need to be changed. The BindingConfiguration section must have a valid binding for the configured "bindingConfiguration" attribute.

The endpoint configuration might look something like this:

```
<endpoint address="http://remotewebsevice/LotValidate.svc"
binding="wsHttpBinding" bindingConfiguration="WSHttpBinding_IRelsysService_
Unsecure" contract="IRelsysService" name=" LotQuery"></endpoint>
```

```
<add Transformer="LotQuery2" Assembly="RelsysInterfaceComponents"
Type="Relsys.InterfaceComponents.XSLTFactory" InterfaceType="Outbound"
RequestType="Response" MessageType="RelsysMessage" Enabled="true"
TransformID="LOT_NUMBER"
Metadata="InputValidationXSD=/Integrations/XSD/v1.0/Lot_Response.xsd;" />
```

- **Lot Number Web Service XSLT**

XSLT file required for transforming the response XML. This is only required in case Central Product Information system is passing custom attributes which need to be save as part of Case data in dosage regimen user defined fields.

Note: Argus Safety provides sample config and XSLT files which can be accessed by clicking Create button in 'Lot Number Processing' configuration screen as discussed above.

5.7.2 Lot Validation Flow

When Argus makes a call to the web service, it will populate the 'LOT_NUMBER' node with data provided by the user. The external lot validation system can provide zero, one, or many results in multiple LOT nodes.

Argus reaction to various counts of returned lots:

- Zero—Argus displays a message that the lot number could not be validated; based on the system configuration, the user may be able to keep the entered lot number, in which case Argus creates a red denotation indicating that the lot number was not validated.
- One—Argus keeps the user-entered lot number and creates a green denotation indicating a successfully validated lot.
- Many—Argus displays a dialog from which the user can select the correct lot number; once selected, Argus creates a yellow denotation indicating that the lot number was validated, but the user had to select from multiple matches.

The lot validation interface also allows for custom data to be returned, such as Albumin or Thermisol which is not natively supported by Argus. This data is then stored in the user-defined fields available on the active case form page.

5.7.3 Lot Number: XML Schema

Schema files for request and response are located in the <Argus Web Install Path>\Integrations\XSD directory.

Validate Lot Number request and response against the following schema files.

5.7.3.1 Request: Lot_Request

Argus Safety will make a web service request to externally hosted central product information system as defined in this schema.

Schema File

Top level file:

\v1.0\Lot_Request.xsd

Sublevel file:

\v1.0\Base.xsd

\v1.0\ProductFamilyEntity.xsd

Namespace

http://www.oracle.com/Argus/Lot_Request/v1.0

where version 1.0 is the version of the schema

Nodes/Attributes

| Attribute/Node name | Description |
|---------------------|--|
| LOT_LOOKUP | First Child node under SAFETY_MESSAGE which represents the Lot integration |
| LOT | Argus defined complex type element having following elements and attributes: <ul style="list-style-type: none"> LOT_NUMBER EXPIRATION_DATE |

5.7.3.2 Response: Lot_Response

Argus Safety expects Central Lot Number Web service to send the response in this format:

Schema File

Top level file:

/v1.0/Lot_Response.xsd

Sublevel file:

/v1.0/Base.xsd

/v1.0/ProductFamilyEntity.xsd

Namespace

http://www.oracle.com/Argus/Lot_Response/v1.0

where v1.0 is the version of the schema

| Attribute/Node name | Description |
|---------------------|--|
| LOT_LOOKUP | First Child node under SAFETY_MESSAGE which represents the Lot Number integration. |
| LOT | <ul style="list-style-type: none"> LOT Number Expiration Date Custom <p>Provides a mechanism</p> <p>Name: Attribute value is used to identify Case Form field that is to be populated with data in the node.</p> <p>Metadata: Attribute value is used as labels in the LOT Number selection dialog displaying the data.</p> |

5.7.4 Transformation

If custom data is to be passed back by the lot validation service, then it is also necessary to modify the 'LotIncomingTransform.xslt' file, located in the '.\ArgusWeb\ASP\Bin' directory. This transformation file reads the CUSTOM tags passed back by the lot validation service and maps them to the Argus user-defined fields.

The CUSTOM tag has a "Name" attribute, which is used by the XSLT to identify to which Argus field to map. The corresponding "Metadata" attribute is used simply to

display a label in the lookup dialog if necessary. The XSLT file must be synchronized between all web servers in a web farm scenario.

Specific Argus fields must be placed within the `xsl:attribute` tags of the XSLT in a comma delimited form. The system will attempt to populate each Argus field specified by the value of the CUSTOM tags. If a field does not exist, no exception is thrown. In this fashion, if different pages in the case form have different definitions for the user-defined fields, the system can still properly populate the values in the fields.

It is inadvisable to modify any piece of the XSLT file with the exception of the piece that is shown in the example below. Consider the web service returns a CUSTOM node like:

```
<CUSTOM Name="Albumin" Metadata="Albumin Status">19.5 mg/gC</CUSTOM>
And the LotIncomingTransform.xslt contains the snippet:
<xsl:template match="@*" mode="CaseField">
  <xsl:choose>
    <xsl:when test=".='Thermisol'">
      <xsl:attribute name="CaseField">CASE_DOSE_REGIMENS_UD_TEXT_1,CASE_DOSE_
REGIMENS_UD_TEXT_2</xsl:attribute>
    </xsl:when>
    <xsl:when test=".='Albumin'">
      <xsl:attribute name="CaseField">CASE_DOSE_REGIMENS_UD_TEXT_3,CASE_DOSE_
REGIMENS_UD_TEXT_4</xsl:attribute>
    </xsl:when>
  </xsl:choose>
</xsl:template>
```

Then the value of 19.5 will be mapped to both user defined text fields 3 and 4. If only one of the fields is on the active case form page, the other field will be ignored.

5.8 Worklist Intake

This section provides information for integrating with an external system generating potential case data.

CASE_INTAKE is the first child node identifying a worklist intake integration.

5.8.1 Configuration

Worklist Intake integration currently employs a file drop system. The drop directories should be on a shared path. The directories can be optionally unique to a user site and configured as such in Console. The first step is to set these directory references up in Console under the "User Sites" code list. For each user site, simply specify the UNC for the "Intake File Path" (they can all be the same or different).

Argus Safety Windows Service provides the mechanism by which the files are processed. Since a network resource is being accessed, it is essential that the service run as a domain account and not as the Local System Account (which is the default). To change this, stop the Argus Safety Windows Service by opening the Services control panel and double-clicking the Argus Safety Windows Service and clicking the Stop button. Next click the Log On tab and select the radio button for "This account". Enter valid domain user credentials and click OK.

The service itself contains additional configuration information in the `RelsysWindowsService.exe.config` file located in the `.\ArgusWeb\ASP\Argus.NET\Bin` directory. This file references the `Intake.config` file to obtain configurations specific to Worklist Intake. Simply uncomment the two "add" nodes in the "RelsysConfigFilesSection" that reference the `Intake.config` file in their

"filePath" attributes. Also verify that the DatabaseConfiguration section in this file has a valid database and user credentials with which to connect to the database and access Argus data.

In the same folder the Service.config file also requires some changes to specify information about the assemblies needed to process Worklist Intake messages. Similarly to the RelsysWindowsService.config file, uncomment the two "add" nodes whose "name" attributes refer to "Case Intake" and "Case Intake Ack".

Once configured, use the Services control panel to restart Argus Safety Windows Service. A successful configuration is evident when four new folders are then created in the shared file path (IN, OUT, INTERMEDIATE, and FAILURES).

If the shared folder happens to be on the same physical machine as the server on which "Argus Windows Service" is running, you can optionally configure the service to access the shared folder directly as a local folder instead of as a network shared path. The following configuration in Intake.config would enable this:

```
<FolderConfiguration>
  <MonitorFolders MonitorAllConfiguredFolders="true"
MonitorLiteratureFolder="false">
    <add FolderPath="<configured share in console>" Monitor="true"
AlternatePath="C:\CaseIntake"/>
  </MonitorFolders>
</FolderConfiguration>
```

In the above configuration, MonitorAllConfiguredFolders can be set to false if you want to configure that server to accept Intake files only for the folders configured in the above section and for which Monitor is set to true.

5.8.2 Worklist Intake Flow

When an XML file is dropped in the IN folder of the configured Intake folder, Argus picks up the file and does an initial verification. If there are any attachments specified in the XML, they and the XML are moved to a GUID-created subfolder of the Intermediate folder. All the relevant data is extracted from the XML and stored in the database. During the parsing and extraction, if there are any errors, the unique folder and its associated XML and file attachments are moved to Failures folder. A file called Error.xml will be generated in that folder which contains more information about the failure. If an e-mail address is configured in Intake.config, an e-mail is also generated and processed via AGService.

Worklists for intake are based on user site. They are populated based on either the path in which the initial file was dropped (as per the configuration in Argus Console the path is associated to a specific user site) or by the value of the SITE node contained within the XML itself. If there is a conflict, the SITE node value takes precedence.

The Intake records that are absorbed into Argus are visible to the Argus User in Worklist Intake screen in Argus or in Affiliate. The Argus user can do one of two operations on the Intake record.

1. Accept—When the user accepts an Intake, the case form book-in screen is shown which will contain information and attachments pre-populated from the Intake record.
 - If user books in a case, a response is generated which contains the case ID and case number. The attachment details and response XML are placed in the Out folder.

- If user adds a follow up to an existing case, a similar response is generated as above and the response XML is placed in the OUT folder.
- 2. Reject—When the user rejects an Intake record, a response is generated which contains the Rejection Reason and the attachment details. This response XML is placed in the OUT folder.

Similarly, an Affiliate user can create a local event from an Intake record from within Affiliate. The flow is similar to that mentioned above with the exception that the response XML would contain the Local Event Number instead of the case number.

5.9 Literature Intake

This section provides information for setting up Literature Intake. Argus accepts files of the following formats for Literature Intake.

- WORLD MEDICAL & DRUG INFORMATION SERVICE (WMDIS) (in the form of .xls or .xlsx file format)
- JAPIC (in the form of .txt file format)

5.9.1 Configuration

Literature Intake integration employs a file drop system. The drop folder should be on a shared path. The folder must be configured in Console under System Configuration > Common Profile Switches > Argus J.

The edit box provided for "Shared Path for Literature Intake" must be configured with the UNC file path of the shared folder. Argus Safety Windows Service provides the mechanism by which the files are processed. Since a network resource is being accessed, it is essential that the service run as a domain account and not as the Local System Account (which is the default). Argus Release Media

To change this, stop the Argus Safety Windows Service by opening the Services control panel and double-clicking the Argus Safety Windows Service and clicking the Stop button. Next click the Log On tab and select the radio button for "This account". Enter valid domain user credentials and click OK.

The service itself contains additional configuration information in the RelsysWindowsService.exe.config file located in the .\ArgusWeb\ASP\Argus.NET\Bin directory. This file references the Intake.config file to obtain configurations specific to Worklist Intake. Simply uncomment the two "add" nodes in the "RelsysConfigFilesSection" that reference the Intake.config file in their "filePath" attributes. Also verify that the DatabaseConfiguration section in this file has a valid database and user credentials with which to connect to the database and access Argus data. In the same folder the Service.config file also requires some changes to specify information about the assemblies needed to process Worklist Intake messages.

5.9.1.1 Metadata Configuration

1. Go to the Argus Web server machine.
2. Open the service.config file located at
`<Argus Install Path>\ArgusWeb\ASP\Argus.NET\Bin\`
3. In the service.config file, the metadata configuration is:

```
<add Name="Case Intake" Assembly="CaseIntakeServiceComponent"
Type="Relsys.CaseIntakeServiceComponent.FSWManager"
Metadata="InvokeDirect=true;PollInterval=1000;CaseIntake=true;LitIntake=true;
```

```
UseLocalInterimFolder=true; LocalInterimFolder=C:\Temp\CaseIntake" />
```

Similarly to the Service.config file, uncomment the "add" node whose "name" attribute refer to "Case Intake". Ensure that 'LitIntake' is set to true in the Metadata configuration as shown below:

```
<add Name="Case Intake" Assembly="CaseIntakeServiceComponent"
Type="Relsys.CaseIntakeServiceComponent.FSWManager" Metadata="InvokeDirect=true;
PollInterval=1000;CaseIntake=true;LitIntake=true" />
```

In the same folder, the Intake.config file needs some changes. Set the MonitorLiteratureFolder attribute to true in FolderConfiguration/MonitorFolders section as shown below:

```
<FolderConfiguration>
<MonitorFolders MonitorAllConfiguredFolders="false"
MonitorLiteratureFolder="true">
<!-- <add FolderPath="<configured share in console>" Monitor="true"
AlternatePath="C:\LiteratureIntake"/> -->
</MonitorFolders>
</FolderConfiguration>
```

Once configured, use the Services control panel to restart Argus Safety Windows Service. A successful configuration is evident when four new folders are then created in the shared file path (IN, OUT, INTERMEDIATE, and FAILURES).

If the shared folder happens to be on the same physical machine as the server on which "Argus Windows Service" is running, you can optionally configure the service to access the shared folder directly as a local folder instead of as a network shared path. The following configuration in Intake.config would enable this:

```
<FolderConfiguration>
<MonitorFolders MonitorAllConfiguredFolders="false"
MonitorLiteratureFolder="true">
<add FolderPath="<configured share in console>" Monitor="true"
AlternatePath="C:\LiteratureIntake"/>
</MonitorFolders>
</FolderConfiguration>
```

5.9.2 Literature Intake Flow

When a WMDIS or JAPIC file is dropped in the IN folder of the configured Literature Intake folder, Argus picks up the file and does an initial verification. The file is first moved to a GUID-created subfolder of the Intermediate folder. All the relevant data is extracted from the file and stored in the database. During the parsing and extraction, if there are any errors, the unique folder and the file in it are moved to Failures folder. A file called Error.xml will be generated in that folder which contains more information about the failure. If an e-mail address is configured in RelsysWindowsService.exe.config, an e-mail is also generated and processed via AGService. The Literature Intake Worklist shows all the records extracted from the above mentioned files.

The Argus user can do one of the following operations on the Literature Intake record.

- Accept
- Reject
- Assign User
- Assign Literature Type

- Modify Product Family

5.10 Extended E2B Interface

For more details, from the [Argus Safety OHC](#) page, download the Technical Reference Manuals, and refer to the *Oracle Argus Interchange ICSR Extensibility Guide*.

Install and Start Argus Safety Service

6.1 Install Argus Safety Service

1. Log in as the administrator on the system where Argus Safety is being installed.
2. Copy the installation package to the local directory of the target machine.
3. Open the Argus Safety folder and click **setup.exe**.
4. In the Argus Suite Solution Components Installation Wizard, click **Next**.
5. Enter the User Name and Company Name, and click **Next**.
6. In the Default Directory screen, to select the default installation directory where the Argus Suite Solution Components will be installed, click **Browse**.
7. To display the Argus Suite Components list, click **Next** and select the default installation directory.
8. Under **Transaction Server**, select **Argus Safety Service**, and click **Next**.
The Argus Suite Solution Components Report Directory appears.
9. Select the directory where temporary reports will be stored, and click **Next**.
You can browse through any path or leave this as default (C:\Temp).
10. In the Setup Completed dialog box, click **Finish**.
11. In the Argus Suite Setup dialog box, click **OK** to reboot the system.
12. See [Chapter 12, "Other Tasks"](#) for information about tasks that must be completed after the Argus Safety service has been installed.
13. To set up the Argus Cryptography Key, refer to [Section 26.1.3, "Argus Safety Application Servers"](#).
14. To configure the Argus Safety Service user passwords, refer to [Section 26.2.4, "Generate Encrypted String"](#).

6.2 Start Argus Safety Service

Before you can start the Argus Safety Service, you must configure a single process or it will fail to start. To configure the Argus Safety Service process, refer to the *Argus Safety Service Administration Guide*.

To start the Argus Safety Service:

1. Select Start > Control Panel > Administrative Tools.
2. Double-click the Component Services shortcut.
3. In the left navigation pane, click **Services**.
4. From the list of services (in the right navigation pane), right-click the Argus Safety Service, and click **Properties**.
5. In the Argus Safety Service Properties > General tab, from the **Startup type** drop-down, select **Automatic**.
6. Click the **Log On** tab, select **This account**, enter the parameters, and click **OK**.

Note: You must enter a domain account with access to the domain printers.

7. Click **Start**.
8. Click **OK**.

Note: You can view the log file at the specified path in the Interchange Service INI file.

Install and Configure Interchange

The Argus Interchange Server is meant to off-load Interchange Service from the Argus Transaction Server. Alternatively, Interchange Service can be installed on the Transaction Server itself. To configure Interchange Services through Interchange Mapping user interface, both must be installed on the same system.

7.1 Prerequisites

1. Obtain a domain account with local administrator privileges.
2. Create a network account to enable Interchange Service to communicate with the e-mail system and access the shared folders on the Axway B2Bi Server.

7.2 Install Interchange Service

1. Log in as the Administrator on the system where Argus Safety is being installed.
2. Copy the installation package to the local directory of the target machine.
3. Open the Argus Safety folder and click **setup.exe**.
4. In the Argus Suite Solution Components Installation Wizard, click **Next**.
5. Enter the User Name and Company Name, and click **Next**.
6. In the Default Directory screen, to select the default installation directory where the Argus Suite Solution Components will be installed, click **Browse**.
7. To display the Argus Suite Components list, click **Next** and select the default installation directory.
8. Under **Transaction Server**, select **Argus Interchange Service**, and click **Next**.
The Argus Suite Solution Components Report Directory appears.
9. Select the directory where temporary reports will be stored, and click **Next**.
You can browse through any path or leave this as default (C:\Temp).
10. Click **Yes** to configure a database for Argus Interchange.
11. Enter the database name as you want it to appear in Argus Interchange and click **Next**.
12. Enter the database SID and click **Next**.
13. To add an additional database to Argus Interchange, click **Yes**.
14. In the Setup Completed dialog box, click **Finish**.

15. Click **OK** to reboot.
16. To set up the Argus Cryptography Key, refer to [Section 26.1.3, "Argus Safety Application Servers"](#).

7.3 Configure Interchange Service

1. Select Start > Control Panel > Administrative Tools.
2. Double-click the Component Services shortcut.
3. In the left navigation pane, click **Services**.
4. From the list of services (in the right navigation pane), right-click the Argus Interchange Service, and click **Properties**.
5. In the Argus Interchange Service Properties > General tab, from the **Startup type** drop-down, select **Automatic**.
6. Click the **Log On** tab, select **This account**, enter the parameters, and click **OK**.

Note: You must enter a domain account with access to the domain printers.

7. Click **OK**.

Note: You can view the log file at the specified path in the Interchange Service INI file.

7.4 Access EDI Gateway Shared Folders

1. Log in to the machine where Interchange Service is installed.
2. Browse to the data folder in the EDI Gateway installation directory.

Note: If the data folder is not shared, contact the System Administrator for access to the folders.

3. Verify that you can access the following folders:
 - <company profile>/ediin
 - <company profile>/ediout
 - <company profile>/xmlin
 - <company profile>/xmlout
4. Log off of the EDI Gateway machine.
5. Log in the Interchange Service machine and make sure no password is required for connecting to the shared folders on the EDI gateway machine.

7.5 Configure Interchange Service .INI File

You can configure Interchange Service by changing the items in its initialization (INI) file from the Interchange Mapping interface.

1. Open ESM Mapping.
2. In the Service INI File Setup dialog box, enter the following parameters and click **OK**.

| Field Name | Description |
|---------------------------|--|
| IT E-mail | e-mail address that will be used by Interchange Service in case the transmit time-out occurs (Physical Media or EDI Gateway time-out). |
| Business E-mail | e-mail address where a message can be sent if the Receive ACK time-out value is reached. |
| User E-mail | e-mail address where a message can be sent if the user does not process the E2B Report within the time-out value. |
| EDI Software Name | EDI Software name used i.e. Axway B2Bi |
| EDI Database Name | Database name for the EDI software |
| EDI User ID | User name for EDI database |
| EDI Password | Password for the User ID |
| EDI Client Software | Type of database used by the EDI software |
| DTD Path | Path to the location of the DTD file |
| Log File Path | Path where Interchange Service will write the log files |
| Multiple Database Section | Displays all the configured databases for Interchange Service. |
| Delete Button | Removes the entire database configuration from the Interchange Service INI file. |

Configure the Argus Insight Application

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

8.1 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.
-

8.2 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)

8.2.1 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 8.2.4, "Set Up the Attributes Specific ONLY to Argus Mart"](#).

8.2.2 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 8–1 *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 8–1 (Cont.) Populate Data Attribute-Value set

| Attribute | Value |
|------------------------------|---|
| LEGACY REPORTS CONFIGURATION | <p>0 — Configuration items are not visible.</p> <p>1— Configuration items are visible.</p> <p>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:</p> <ul style="list-style-type: none"> ■ 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 <p>To configure these switches, refer to Argus Insight 7.0.2 Installation Guide.</p> |

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 8–1, "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.

8.2.3 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 8–2 Email Specific Attribute-Value set

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

Table 8–2 (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 8–2, "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*.

8.2.4 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 8–3 Argus Mart Specific Attribute-Value set

| Attribute | Value |
|---------------------------------------|--|
| Argus Insight Application Data Source | <p>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.</p> <p>Argus Mart — Enable queries on Argus Mart data source only.</p> <p>Insight Mart — Enable queries on Argus Insight data source only.</p> <p>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.</p> |
| 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 | <p>Note: Use Argus Safety Console to enable this profile switch.</p> <p>This profile switch must be set to Yes to link Argus Insight database to Argus Mart database.</p> <p>Yes — Enable Argus Insight Processing for Argus Mart.</p> <p>No — Disable Argus Insight Processing for Argus Mart.</p> |

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 8–3, "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**.

8.2.5 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.

8.2.6 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.

8.3 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 8.2.4, "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 (\geq) 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 (\geq)** 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.

8.4 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**.

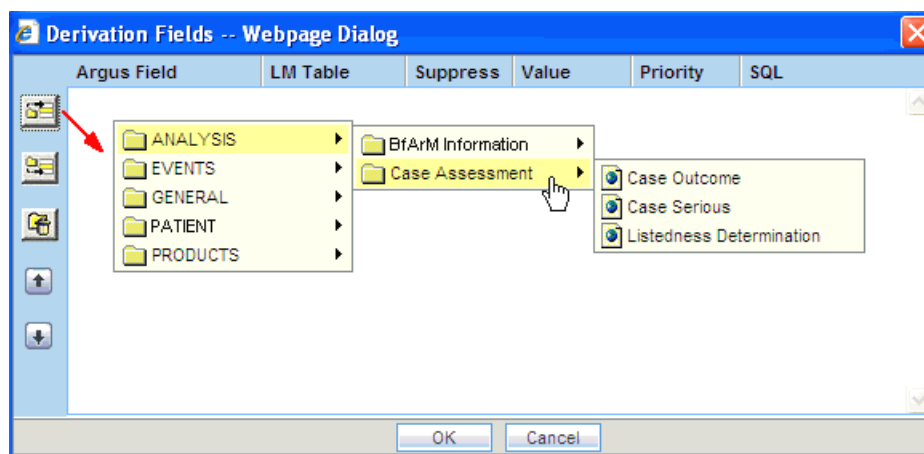
Note: There can be situations where two different List Maintenance items you create contain similar attributes in the SQL criteria. In this case, you can assign a priority level to individual List Maintenance items. The priority level determines which List Maintenance item SQL executes first.

8.4.1 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.



8.4.2 Icons in the Derivation Fields Dialog Box

Table 8–4 describes the icons in the Derivation Fields dialog box that you can use to add, delete, and reorder derivation field elements (rows).

Table 8–4 *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 8–4 (Cont.) Icons in the Derivation Fields Dialog Box

| Click... | To... |
|---|----------------------------|
|  | Move the selected row down |

8.4.3 Field Mapping Derivation Rules

Table 8–5 lists the available field mapping derivation rules for Argus Insight.

Table 8–5 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.

8.4.4 Fields and Check Boxes in the Derivation Fields Dialog Box

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

8.4.4.1 LM Table

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

8.4.4.2 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.

8.4.4.3 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

8.4.4.4 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.

8.4.4.5 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...

8.5 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.

8.6 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**.

8.6.1 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**.

8.7 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.

8.7.1 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.

8.7.2 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.

8.8 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**.

8.9 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

Upgrade the Argus Application

You can upgrade the Argus application from the following versions:

- 8.2.1
- 8.2.1.1
- 8.2.1.2
- 8.2.1.3

9.1 Upgrade Argus Application on the Web Server

1. Log in as an administrator.
2. Stop Microsoft IIS (Internet Information Server).
3. Stop the **Argusvr2.exe** and **Argusvr2a.exe** services.
Alternatively, make sure these processes are not running.
4. Copy the build contents to your local server for upgrade, and run the <Software Path>\Argus Safety\Setup.exe utility.
The setup auto-detects a previous compatible version of the application.
5. When a compatible version is detected, click **Next**.
6. Restart the server after the upgrade process is complete.

9.2 Upgrade Argus Application on the Transaction Server

1. Log in as an administrator.
2. Stop the Argus Safety and Argus Interchange services.
3. Wait for the following processes to shut down:
 - **AGProc.exe**
 - **ESMMapping.exe**
 - **E2BReceive.exe**
 - **ESMProc.exe**
4. Copy the build contents to your local server for upgrade, and run the <Software Path>\Argus Safety\Setup.exe utility.
The setup auto-detects a previous compatible version of the application.

5. When a compatible version is detected, click **Next**.
6. Restart the server after the upgrade process is complete.

Set Up the Client Browser

10.1 Prerequisite

Set the screen resolution for the client workstation to a minimum of 1280 x 1024 for an optimal view of the application. If the screen resolution is less than this, the field labels may appear truncated.

10.2 Install Files Required to View Reports

Install Windows Supplemental Language Support for East Asian languages and Japanese font pack for Adobe Reader on all Argus Web client machines to view reports in Argus Safety due to common fonts used between Argus English and Argus Japanese.

Make sure that you have sufficient free disk space for installing the language packs.

10.3 Configure Internet Explorer

To configure Internet Explorer on clients that access Argus Safety Web, Affiliate, Dossier, and Interchange Web:

1. Open Internet Explorer v11.
2. Select **Tools > Internet Options**.
3. Locate Browsing History and click **Settings**.
4. Locate Check for newer versions of stored pages, select **Automatically** and click **OK**.
5. Click the Advanced tab and do the following:
 - a. Locate the Multimedia section.
 - b. Uncheck the **Show image download placeholders** checkbox.
 - c. Check the **Show Pictures** checkbox.
 - d. Uncheck the **Enable Automatic Image Resizing** checkbox.
 - e. Click **Apply**.
6. Click **OK**.

Note: Make sure cookies are enabled on the client machine.

If password encryption is required between Internet Explorer Client and the Web Server, HTTPS must be utilized. Refer to the [Section 3.3, "Configure Load Balancer in Argus Web."](#)

When logged into Argus Safety, having multiple internet browsers open may cause the user to receive a login screen when opening certain parts of the application such as opening E2B Report dialog box. It is recommended to close all other non-Argus Safety Sessions if this problem occurs on an end user machine.

Certain requirements within the Argus Safety System open file attachments within a separate internet browser window however based on client machine settings this may not occur. Each application is configured differently as to how it handles files within Internet Explorer. Refer to the application documentation to correctly configure it.

It is not recommended to utilize the IP Address of the Web Server from the client machines within Internet Explorer. Using the IP Address forces Internet Explorer to use a high security mode which may restrict certain functionality from Argus to run.

10.4 Post Application Install or Upgrade

You must clear your local Internet Explore cache after installation or upgrade of the Argus application.

10.5 Add the Argus Site as a Local Intranet Site

1. Open Internet Explorer and from the menu select **Tools > Internet Options**.

The Internet Options dialog box appears.

2. Select the Security tab.
3. Select **Local Intranet** and click **Sites > Advanced**.

The Local intranet dialog box appears.

4. In the **Add this website to the zone** field, enter the Argus Safety website URL.

Note: Contact your System Administrator for the Argus site URL.

5. Click **Add** and click **Close**.
6. Click **OK**.
7. Click **Custom level...**

The Security Settings dialog box appears.

8. Scroll-down to **Miscellaneous**, for **Allow script-initiated windows without size or position constraints**, select **Enable**.
9. Click **OK**.

Note: You must enable the Argus Safety website to run in the Enterprise Mode, if adding to Local Intranet site is not desired.

For more information on how to [Add Argus Site to the Enterprise Mode](#).

10.6 Add Argus Site to the Enterprise Mode

If you do not want to add the Argus Safety website to the Local Intranet site, you must enable the Argus Safety website to run in the Enterprise Mode.

1. Go to
<https://docs.microsoft.com/en-us/internet-explorer/ie11-deploy-guide/turn-on-enterprise-mode-and-use-a-site-list>.
2. Follow the instructions in the section **To turn on Enterprise Mode using Group Policy**.
3. When asked to refer to the **Use the Enterprise Mode Site List Manager**, click the specified link.
4. Scroll down to the procedure for **Using the Enterprise Mode Site List Manager** and click **Add sites to the Enterprise Mode site list using the Enterprise Mode Site List Manager (schema v.2)** link.
5. Follow the instruction in the section **Adding a site to your compatibility list > To add a site to your compatibility list using the Enterprise Mode Site List Manager (schema v.2)**.
6. In the following parameters, enter:
 - a. **URL**—Argus Safety Web URL
 - b. **Compat Mode**—IE 5 Document Mode
 - c. **Open In**—IE 11

10.7 Set Up Compatibility View with Internet Explorer

1. Open Internet Explorer, from the menu select Tools > Compatibility View Settings.
2. Enter the Argus Safety website URL.
3. Click **Add** and click **Close**.

Post-installation Checks

This chapter provides checklists and procedures for verifying that Argus Safety is installed correctly.

11.1 Post-Installation Tasks

11.1.1 General Checklist

Verify That:

- the correct modules are installed as follows:
 1. Go to Add/Remove Programs and select **Argus Safety Web**.
 2. Click **Modify** and click **Next**.
 3. Verify that the applications that you have installed are checked.
- the Argus.XML file has the same data across all the Web Servers.
- a single domain user account <Domain User> is running the Argus Web application on all web servers.
- the login page appears when the server name is entered in your browser.
- you can log in successfully.

11.1.2 Configure Worklist Intake on the Web Server

1. Identify the physical folders where the Intake XMLs will be dropped in. There could be one folder for all the available sites, or one folder each for each site. These folders can be on the same machine, or on different machines. Create shares for the folders.
2. Log in to the Argus Console and open the Sites UI under Access Management menu.
3. Configure the UNC paths of the identified physical folders for the required Sites.
4. On the server where Integrations component has been installed, navigate to the path where the **Argus Safety Windows Service** is running.

```
<InterfaceSchemas>
<add InputXSD="..\..\Integrations\XSD\v1.0\Base.xsd" />
<add InputXSD="..\..\Integrations\XSD\v1.0\DataOperation.xsd" />
<add InputXSD="..\..\Integrations\XSD\v1.0\Dictionary.xsd" />
```

```
<add InputXSD="...\Integrations\XSD\v1.0\Case_Intake.xsd"
OutputXSLT="...\Integrations\XSLT\v1.0\CaseIntake_Transform.xml"/>
</InterfaceSchemas>
```

In the above tag, mention full Argus Install Path. Typically, the Argus Install Path is, *<Argus Install Path>\Argus Safety*. For example:

```
<InterfaceSchemas>
<add InputXSD="<Argus Install Path>\Argus
Safety\Integrations\XSD\v1.0\Base.xsd" />
<add InputXSD="<Argus Install Path>\Argus
Safety\Integrations\XSD\v1.0\DataOperation.xsd" />
<add InputXSD="<Argus Install Path>\Argus
Safety\Integrations\XSD\v1.0\Dictionary.xsd" />
<add InputXSD="<Argus Install Path>\Argus
Safety\Integrations\XSD\v1.0\Case_Intake.xsd" OutputXSLT="<Argus Install
Path>\Argus Safety\Integrations\XSLT\v1.0\CaseIntake_
Transform.xml"/>
</InterfaceSchemas>
```

5. Edit the following files:

- [RelsysWindowsService.exe.config](#)
- [Service.config](#)
- [Intake.config](#)

11.1.2.1 RelsysWindowsService.exe.config

1. Uncomment the following entries under the *<RelsysConfigFilesSection>/<RelsysConfigFiles>*
 - Relsys.InterfaceComponents.ProcessorsConfiguration
 - Relsys.CaseIntake.FolderConfiguration
2. Make sure that the DatabaseConfiguration section is configured for the following attributes:

| Attribute | Description |
|-----------------------|--|
| DBName (Mandatory) | TNS of the database to which the RelsysWindowsService should connect to. Example: DBName="GOLDDemo" |
| DBUser | AGService Username. The RelsysWindowsService logs into the database using this login name. This has to be a user of type AGSERVICE. Example: DBUser="agservice_user1" |
| GeneralEmailTo | The e-mail address to which the e-mails will be sent by the Intake Service, using the General Email feature of Argus. Example: GeneralEmailTo =" recepient@oracle.net " |
| GeneralEmailFrom | The email address from which the e-mails will be sent by the Intake Service, using the General Email feature of Argus. Example: GeneralEmailFrom =" admin@oracle.net " |

| Attribute | Description |
|-----------------|---|
| GeneralEmailCc | This email address will be added to the Cc line when e-mails are sent by the Intake Service, using the General E-mail feature of Argus. Example: GeneralEmailCc ="recepient@oracle.net" |
| GeneralEmailBcc | The email address will be added to the Bcc line when e-mails are sent by the Intake Service, using the General E-mail feature of Argus. Example: GeneralEmailBcc ="recepient@oracle.net" |

11.1.2.2 Service.config

1. Uncomment the entries for "Case Intake" and "Case Intake Ack" in the `<ServiceConfiguration>/<ServiceComponents>` section
2. The following configuration changes are optional:
 - "Recurrence": The value for this attribute specifies the frequency of instantiation of the associated Service Component. The value is specified in seconds. For example:

```
<add Name="Case Intake Ack" Assembly="CaseIntakeServiceComponent"
Type="Relsys.CaseIntakeServiceComponent.IntakeAckGenerator"
Recurrence="600" Metadata="InvokeDirect=true" />
```

The value of 600 for Recurrence above means, the "Case Intake Ack" service is instantiated every 600 seconds (10 minutes) to perform the job.

11.1.2.3 Intake.config

The following configuration changes are optional:

```
<FolderConfiguration>
<MonitorFolders MonitorAllConfiguredFolders="true">
<add FolderPath="\\172.16.38.154\Intake\US" Monitor="true"
AlternatePath="C:\Intake\US" />
</MonitorFolders>
</FolderConfiguration>
```

The FolderConfiguration enables you to have more granular control over what folders are monitored on what machines. This is particularly useful when the Intake folders are distributed across multiple machines and in many cases if these machines are not accessible from one server.

If the server machine on which Integrations component has been installed, has to monitor only a subset of the configured folders (configured in Argus Console), then set the attribute MonitorAllConfiguredFolders = "false"

When the value is set to false, each folder in the subset of folders that need to be monitored should be added as shown in the example above, using multiple `<add />` entries. More info on each of the attributes:

FolderPath: The configured folder path, as specified in Sites UI in Argus Console

Monitor: true means this folder should be monitored, false means this folder should not be monitored.

AlternatePath: Alternate way of accessing the same folder path.

11.1.3 Verify and Update Network Proxy Settings

1. Verify the value of PROXY_AUTO_DETECT:
 - a. Log into SQL session on the database <database_name> and set up the enterprise context.
 - b. To verify that the value of PROXY_AUTO_DETECT, execute:

```
select value from CMN_PROFILE_ENTERPRISE where key = 'PROXY_AUTO_DETECT'
```

If this value is set to a character value, True or False, then update this value to a numeric value, 1 or 0.
2. To update the Network Proxy settings:
 - a. Log in to Argus Console.
 - b. From the **System Configuration** menu, select **System Management**.
 - c. Expand the **Network Settings** folder and click **Proxy** folder.
 - d. Check or uncheck the **Auto Detect Proxy?**, click **Save**.
 - e. Verify the Network Proxy settings again as mentioned in step 1. The value should be set to 1 or 0.

11.2 Verify Files Installed on Middle Tier Servers

Verify the files installed on the server have not been modified or deleted from original installation.

1. Log in to the server as an Admin user.
2. Select Start > Control Panel.
3. Click **Programs and Features**.
4. Hover Argus Suite and right-click.
5. From the drop-down menu, click **Change**.

The Preparing Setup dialog box appears.
6. Click **Modify** and click **Next**.
7. Select **Verify the current installation** and click **Next**.
8. In the File Verification dialog box, click **Next**.

12.1 Configure Argus.xml File

The Argus.xml file is generated during installation on the Argus Safety Web, but you can update this file after installation to add, update, or delete database entries. The file resides in the following directory:

<Argus Install Path>/ArgusWeb/ASP

The Argus.xml file contains the following type of xml tags:

| XML Tag | Description |
|------------|--|
| <ARGUS_DB> | Contains all databases supported by the Argus Web application. Each database is specified as a separate XML tag - <DBNAME> with <ARGUS_DB> as parent tag. For example, for a database that is recognized as "Testing Database" in the Argus Web Login screen and whose alias in the Oracle TNSNAMES.ORA file is "TESTDB", the entry will be <DBNAME id="TESTDB">Testing Database</DBNAME>. |

If you update the Argus.xml file, you must restart the Internet Information Services (IIS) on the server for the changes to take effect.

12.2 Configure Argus.ini File

The Argus.ini file is generated during installation on Argus Web and Transaction (AG) Server, but the user can update this file after installation.

To configure Argus.ini:

1. Select Start > Run.
2. In the Open field, enter **argus.ini**, and click **OK**.
3. Set the entries in the file as described in the [Section 12.2.1, "Argus.ini Parameters"](#).
4. Save the file.
5. Restart the Internet Information Services (IIS) on the server to reflect the changes.

12.2.1 Argus.ini Parameters

With some exceptions, the parameters listed in the table are used by Argus Web as well as Argus Safety Service (AG Service or Transaction Server).

Parameters specific to the Web Server are:

- MessageCachePath
- Upload
- Template
- ArgusInstallPath
- Pooling parameters

The Argus.ini File Parameters are described in the following table:

| Section | Parameter | Sample Value | Description |
|--------------|-------------------|--|---|
| Workstation | ArgusInstallPath | C:\Program Files\Oracle\ArgusWeb\ASP\ | Path of the location where the ASP files are placed. For use with Web Server. |
| Workstation | ArgusLogPath* | C:\Temp\ArgusLogs\ | Path of the root folder for ArgusLogs. |
| Workstation | Cache* | C:\ArgusReports\PDFReports\ | Path for PDF Reports (Expedited/Periodic/Screen Prints etc.). In case of multiple Web Servers, this is a shared path on the network. |
| Workstation | MessageCachePath* | C:\ArgusReports\MessageCache\ | Shared path to save the system level cache such as data for LM tables, CMN Fields, etc. In case of multiple Web Servers, this is a shared path on the network. For use with Web Server. |
| Workstation | Upload* | C:\ArgusReports\UploadedLetters\ | Shared path for uploaded letters. In case of multiple Web Servers, this is a shared path on the network. For use with Web Server. |
| Workstation | Template | C:\Program Files\Oracle\E2BViewer\Templates\ | Location that stores the template and report files used to display CIOMS and MedWatch views. For use with Web Server. |
| Argus Server | SQLTimes | 1 | Enables the Argus Web application to start creating log files for all the SQLs that are fired. These log files are created in C:\Temp folder and can be used for debugging. |

| Section | Parameter | Sample Value | Description |
|--------------|----------------------|--------------|---|
| Argus Server | Pool_Initial_Size | 3 | Refers to the DB Connection Pool Initial Size. For use with Web Server. |
| Argus Server | Pool_Maximum_Size | 120 | Refers to the DB Connection Pool Maximum Size. For use with Web Server. |
| Argus Server | Connection_Wait_Time | 3 | Refers to the connection wait time in seconds. An exception occurs if the system cannot obtain a DB connection in the given time. For use with Web Server. |

Note: * If any anti-virus software is running on Argus Web or Transaction (AG) server(s), it must be configured not to scan these Argus temp folders. Otherwise, it can lead to slower performance or unexpected errors on screens under heavy user load due to file locks by the anti-virus software.

12.3 Installation Maintenance Tasks

You may need to perform certain installation maintenance tasks on the installed Argus Suite Solution Components.

12.3.1 Install New Components

1. Select Start > Control Panel.
2. Click Add or Remove Programs/Uninstall or change a program.
3. Right-click Argus Suite and from the drop-down menu, click **Change**.
The Argus Suite Solutions InstallShield Wizard opens the Preparing Setup dialog box.
4. Select **Modify** and click **Next**.
5. Select **Update installed Argus Components** and click **Next**.
6. In the Select Features dialog box, check the components to install and click **Next**.

Note: Make sure the checkboxes for components that are already installed contain a checkmark. If the checkmark is cleared from the checkbox for an existing component, the component will be uninstalled.

Refer to the relevant chapters in this Installation Guide for instructions for installing individual components.

7. When the installation process is complete, the Argus Suite Setup- Maintenance Complete dialog appears.

8. Click **Finish**.

12.3.2 Uninstall Components

1. Select Start > Control Panel.
2. Click Add or Remove Programs.
3. Right-click Argus Suite and from the drop-down menu, click **Change/Remove**.
The Argus Suite Solutions InstallShield Wizard opens the Preparing Setup dialog box.
4. Select **Modify** and click **Next**.
5. In the Select Features dialog box, uncheck the components to uninstall and click **Next**.
The Argus Safety Components Installer will uninstall the selected components.
6. Follow the on-screen instructions to uninstall the components.

12.3.3 Remove All Components

1. Select Start > Control Panel.
2. Click Add or Remove Programs.
3. Right-click Argus Suite and from the drop-down menu, click **Change/Remove**.
The Argus Suite Solutions InstallShield Wizard opens the Preparing Setup dialog box.
4. Select **Remove** and click **Next**.
5. In the Confirm Uninstall dialog box, click **OK**.
The Argus Safety Components Installer uninstalls the required component(s).
6. Follow the on-screen instructions to uninstall the components.

12.4 Argus Configuration Files

By default, the Argus Safety logs files are placed in the “C:\temp” folder (default temp directory of Argus Safety). You must make sure that the user under which the Argus Safety applications are running has access to this directory.

If you have a different “Temp” directory, change the temp directory path in the following files:

Background Processes (AG Server)

1. <Argus Install Path>/Argus Safety/AGProc.config
2. <Argus Install Path>/Argus Safety/Service.config
3. <Argus Install Path>/Argus Safety/RelsysWindowsService.exe.config

Argus Web Server:

1. <Argus Install Path>/ArgusWeb/ASP/Web.config
2. <Argus Install Path>/ArgusWeb/Bin/Argussvr2.config
3. <Argus Install Path>/ArgusWeb/ASP/Argus.Net/Web.config

4. <Argus Install Path>/ArgusWeb/ASP/Argus.Net/Bin/RelsysWindowsService.exe.config
5. <Argus Install Path>/ArgusWeb/ASP/Argus.Net/Bin/Service.config
6. <Argus Install Path>/ArgusWeb/ASP/Integrations/Web.config

Note: It is recommended that you use the local server path rather than the network share path.

12.4.1 Backup Configuration Files

You must back up the following configuration files before proceeding with the application upgrade. All system configuration (.config) files will be overwritten by this upgrade and your manual configuration changes will be lost. These files may be stored on multiple servers, depending on components selected at the time of the Argus installation (Web Server, integration server, transaction server, and so on). The directory structure of the file, however, remains constant.

Commonly modified configuration files are:

- .\ArgusWeb\ASP\Argus.NET\bin\Intake.config
- .\ArgusWeb\ASP\Argus.NET\bin\RelsysWindowsService.exe.config
- .\ArgusWeb\ASP\Argus.NET\bin\Service.config
- .\ArgusWeb\ASP\Argus.NET\web.config
- .\ArgusWeb\ASP\ArgusConsole\web.config
- .\ArgusWeb\ASP\Integrations\Service.config
- .\ArgusWeb\ASP\Integrations\Web.config
- .\ArgusWeb\ASP\web.config
- .\ArgusWeb\Bin\Argusvr2.config
- .\ArgusWeb\Bin\Argusvr2a.config
- .\Argus Safety\AGProc.config
- .\Argus Safety\Intake.config
- .\Argus Safety\RelsysWindowsService.exe.config
- .\ArgusSafety\Service.config
- .\DBInstaller\ArgusDBInstall.exe.config
- .\ESMMapping\ESMapping.exe.config

Part III

Install or Upgrade Argus Database Tier

You may install or upgrade Argus Safety and Argus Insight database, and upload dictionaries.

Note: To upload dictionaries, refer to the *Oracle Argus Safety Administration Guide*.

Install Argus Safety Database

13.1 Create Argus Safety Database Schema

1. For Windows—To use the interactive user interface, execute the **dbinstallerUI.bat** file.

For silent installation—execute the **dbinstaller.bat** file.

2. Create the tablespaces and schemas using the **dbinstallerUI.bat** or **dbinstaller.bat** file available at *<Argus Release Media>\Database\Argus Safety*.
 - Argus Safety database schemas:
 - Argus Schema
 - Interchange Service Schema
 - ESM Query Schema
 - DLP Schema
 - DLP ESM Query Schema

Note: The mapping SQLs for ESM Generation and Import can be executed only through restricted database user account that have access only to Argus and ESM Schemas (ESM Query Schema and DLP ESM Query Schema).

These DB users does not have access to create or execute anything that would result in change or alteration of the schema or database.

DLP Schema and DLP ESM Query Schema are part of Argus Database, but DLP setup can be enabled or disabled by executing separate batch files shipped with the software.

Besides, features like Factory Data, DB Upgrade, and Oracle Text are merged with the Create Schema option.

- BI Publisher Schema—This schema holds the Flexible Aggregate Reporting (FAR) objects and the Japanese PMDA R3 Paper Reports related objects. This schema must always be created.

Note: When creating new users in Oracle, the password can only contain any ASCII Character, 0-9, or any of the following special characters _ # \$.

3. Create Axway B2Bi or Oracle B2B Database Instance (Optional)—Required only for respective gateway being integrated with Argus Safety.

13.1.1 Prepare to execute the DBInstaller

13.1.1.1 Prerequisites

Before you execute the **dbinstallerUI.bat** or **dbinstaller.bat** file on a server, verify that:

- an Oracle client with Administrator option is installed on the server.
- database TNS entry should be added in the TNSNAMES.ora file.
- Java JRE 1.8 or higher must be installed and Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8 is applied.
- login machine user should have administrative privileges.

13.1.1.2 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>
2. Unzip the **jce_policy-8.zip**.
3. Replace **local_policy.jar** and **US_export_policy.jar** files present in all Java JRE installation security folders with **local_policy.jar** and **US_export_policy.jar** shipped in **jce_policy-8.zip**.

For example, the 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 that the environment variable settings and the path system variables have correct the Java installation path.

13.1.1.3 Set Java Install 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 appears.
3. In the Advanced tab > Startup and Recovery section, click **Environment Variables...**
4. From the System variables section, scroll down to the **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.

13.1.1.4 Install XDB Schema for Interchange

Oracle Schema XDB must be present for Interchange packages to load. To create the XDB schema, if already not present:

1. Click **sqlplus.exe**.
2. Connect to **sys** as **sysdba**.
3. Execute the `<Oracle_Home>/rdbms/admin/catqm.sql` script.
4. Enter the following parameters:
 - user password
 - user default tablespace
 - user temporary tablespace

For example:

```
SQL>@?/rdbms/admin/catqm.sql SYSTEM SYSAUX TEMP
```

13.1.2 Run Create DBA User Script

You must run the Create DBA User scripts to create a new DBA user or grant required privileges to the existing DBA or SYSTEM user. Use this new DBA user account when running the **DBInstaller** to create the Argus Safety schema.

The DBA user created by this script can perform the actions as done by the SYSTEM user. All the manual grants which used to be assigned to the SYSTEM user (prior to the Argus Safety 8.1 release), are now part of this script. The term SYSTEM mentioned in this chapter can be replaced with the new DBA user.

If you use the newly created DBA User to execute the **DBInstaller**, then the validation file might display extra or missing privileges for the SYSTEM or the newly created DBA user.

If you do not wish to create a new DBA user, you may enter SYSTEM when running the script.

To create the DBA user:

1. From the command prompt, run the batch file:


```
<Argus Release Media>\Database\Argus Safety\Utilities\Create_Dba_User\create_dba_user.bat
```
2. Enter the following parameters:
 - a. TNSName of the database
 - b. SYSDBA username
 - c. Password for SYSDBA account
 - d. Name for the new DBA User account that will be created
 - e. Password for the new account

3. Follow the remaining steps to complete the script.
4. You may also run the script:
 - For Windows—execute the script from <Argus Release Media>\Database\Argus Safety\Utilities\Create_Dba_User\create_dba_user.bat
 - For Linux—execute the script from <Argus Release Media>/Database/Argus Safety/Utilities/Create_Dba_User/create_dba_user

13.1.3 Create Tablespaces (Optional)

The **DBInstaller** creates the tablespaces if they do not exist with default parameter settings.

You can create tablespaces as per your parameter requirements before installing Argus Safety. The following is the list of tablespaces that is required for the Argus Safety installation:

| Tablespaces for Argus Safety | Tablespaces for DLP |
|------------------------------|---------------------|
| ARGUS_AEXP_DATA_01 | DLP_DATA_01 |
| ARGUS_AEXP_INDEX_01 | DLP_DATA_02 |
| ARGUS_AL_DATA_01 | DLP_DATA_03 |
| ARGUS_AL_INDEX_01 | DLP_DATA_04 |
| ARGUS_DATA_01 | DLP_DATA_05 |
| ARGUS_DATA_02 | DLP_DATA_06 |
| ARGUS_DATA_03 | DLP_INDEX_01 |
| ARGUS_DATA_04 | DLP_INDEX_02 |
| ARGUS_DATA_05 | DLP_INDEX_03 |
| ARGUS_INDEX_01 | DLP_INDEX_04 |
| ARGUS_INDEX_02 | DLP_INDEX_05 |
| ARGUS_INDEX_03 | DLP_INDEX_06 |
| ARGUS_INDEX_04 | DLP_LOB_01 |
| ARGUS_INDEX_05 | |
| ARGUS_INDEX_06 | |
| ESM_DATA_01 | |
| ESM_INDEX_01 | |

13.1.4 Prerequisites to Create the Schema

- Create the Cryptographic Key, refer to the chapter [Argus Password Management—Cryptography Tool](#).
- A blank Oracle database instance is available.
- A DBA-privileged or a SYSTEM user account is available.
- The Oracle database is available from the machine where the DBInstaller is installed.
- Java is installed and JCE policy is applied. See [Section 13.1.1.2, "Install Java."](#)

- Set database semantics to CHAR.

The Argus Safety Database requires the database semantics to be CHAR and not BYTE. Follow the steps below:

1. Log in to the database as the SYS user.
2. Execute: ALTER SYSTEM SET NLS_LENGTH_SEMANTICS=CHAR SCOPE=BOTH;
3. Shutdown and startup the database after applying the above statement.

13.1.5 Configure the Database Setup Properties File

Make sure the **dbinstaller.properties** file that contains the information for the Argus Safety Database setup has correct data. If not, edit the file.

The file is located on the database server at <Argus Release Media>\Database\Argus Safety.

Note: In case you are creating the schema on windows from the User Interface, you MUST update only the following parameter:

- argus_securekey_path=<path of the ArgusSecureKey.ini file>
The default value is C:/windows
- tablespace_encryption=<blank> or <text>, where
- blank = no encryption
- text like: encryption using 'AES256' default storage (encrypt)

You may ignore other parameters.

- #DB Connection Details
 - db_connect_string=<host name>:<port>/<service name>
 - dba_user=<argus dba user or system user>
- #Application Type
 - application_type=MULTI (for a multi-tenant setup) or SINGLE (for a single-tenant setup)
 - enterprise_name=DEFAULT
 - enterprise_short_name=DEFAULT
- #Complete path of Argus Secure Key ini file
 - argus_securekey_path=<path of the ArgusSecureKey.ini file>
The default value is C:/windows
 - url—URL for the database connection
 - dbaUser—SYSTEM or DBA privileged user
- #Argus DB Schemas—Schema Name and Password (optional). If the password is left blank, it will be prompted at run-time.
 - To prompt for each password on the screen:
 - * appSchema_argus_schema=argus_app

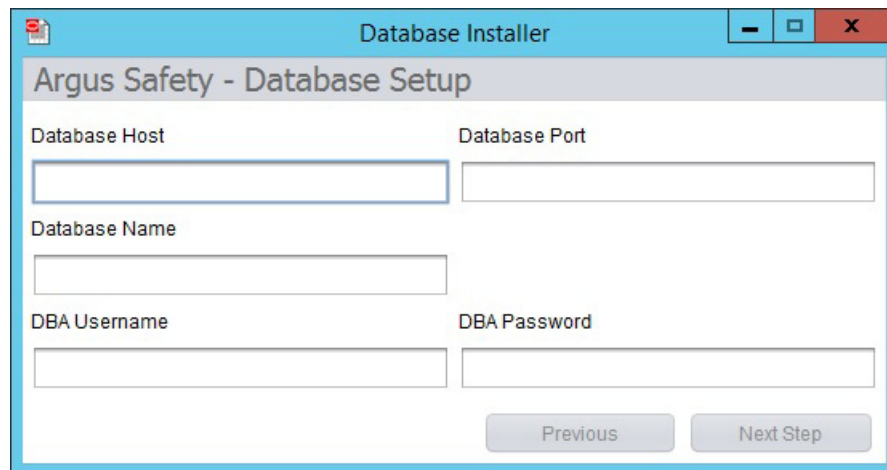
- * appSchema_argususer=argususer
- * appSchema_argus_login=argus_login
- * appSchema_vpd_schema=vpd_owner
- * appSchema_bip_schema=bip_owner
- * appSchema_esm_login=esm_login
- * appSchema_esm_schema=esm_owner
- * appSchema_esmquery_schema=esm_query
- * appSchema_dlp_schema=dlp_owner
- * appSchema_dlp_esmquery_schema=dlp_esm_query
- To avoid prompt for each password on the screen, set up the password as the login password for each user:
 - * appSchema_argus_schema=argus_app/<password>
 - * appSchema_argususer=argususer/<password>
 - * appSchema_argus_login=argus_login/<password>
 - * appSchema_vpd_schema=vpd_owner/<password>
 - * appSchema_bip_schema=bip_owner/<password>
 - * appSchema_esm_login=esm_login/<password>
 - * appSchema_esm_schema=esm_owner/<password>
 - * appSchema_esmquery_schema=esm_query/<password>
 - * appSchema_dlp_schema=dlp_owner/<password>
 - * appSchema_dlp_esmquery_schema=dlp_esm_query/<password>
- #Argus DB Roles—Enter the names of the database roles you need to be required. If this is an upgrade, list the roles under **For upgrade**. If this is a fresh installation, enter the roles under **For the new setup** in the file.
- #Argus Data Tablespaces—Define the tablespace and datafile details. Similarly ESM and DLP sections Define Data and Index datafiles.
- #Default and Temporary table spaces
 - default_ts=USERS
 - temp_ts=TEMP
- #TableSpace parameters
 - tablespace_encryption=<blank> or <text>, where
 - blank = no encryption
 - text like: encryption using 'AES256' default storage (encrypt)
 - tablespace_initial_size=10M
 - tablespace_autoextend=ON
 - tablespace_next_size=10M
 - tablespace_block_size=8K
- #Logging level parameters

- log_level=info
Logs the entire history of changes applied to the database. This is the default value.
- log_level=debug
Logs the entire history of changes applied to the database along with additional debug information.

13.1.6 Create the Schema on Windows from the User Interface

1. Run the **dbinstallerUI.bat** file to invoke the user interface. You must run the file as an administrator.

The Database Installer dialog box appears.



The screenshot shows a Windows-style dialog box titled "Database Installer" with a subtitle "Argus Safety - Database Setup". Inside the dialog, there are four input fields arranged in a 2x2 grid: "Database Host", "Database Port", "Database Name", and "DBA Username". The "DBA Password" field is a password box. At the bottom right of the dialog are two buttons: "Previous" and "Next Step".

2. Enter the parameters and click **Next Step**.

Argus Safety - Database Setup screen appears.

3. Enter the parameters, select the Application Type, and click **Next**.
 - Single Tenant—Select this option to allow the database to support only single tenant. The options to create multiple tenants in the safety system is disabled.
 - Multi-Tenant—Select this option to allow the database to support multiple tenants. Users are able to create multiple tenants using the Global Enterprise setup screens.
4. Create new tablespaces or use the existing tablespaces.

- Under Complete Path and Data File Name, enter the database server path (complete path including the filename) where the data file is placed.

Instead of entering path for each tablespace, you can set up a common folder path. To do so, in the text box, enter the datafile folder path, and click **Set Datafile Folder**.

- If the data file does not exist, the system creates a data file.
- If the data file exists, to use the current data file, click **Yes** in the confirmation dialog box.

Note: When you have existing tablespaces, you may use them; you are not required to create new ones. The system will not regenerate the tablespaces.

- Click **Next**.
- 5. Verify the **Setup Parameters** and click **Execute**.
When execution is complete, a message appears in the Execution Log on screen 3 - *Liquibase Update Successful*.
- 6. To view the execution status or errors, open the schema creation log file with the latest timestamp from <Argus Release Media>\Database\Argus Safety\logs.

13.1.7 Create the Schema on Windows from a Batch file

1. Make sure the **dbinstaller.properties** are set up correctly. (See [Configure the Database Setup Properties File](#).)
2. From Start menu, select Run, type **cmd**, and click **OK**.
3. In the command prompt, go to the following path:

```
cd <Argus Release Media>\Database\Argus Safety
```
4. Type **dbinstaller.bat** and press **Enter**.
5. Monitor the execution log and progress on the running window.
6. To view the log file, go to <Argus Release Media>\Database\Argus Safety\logs.

13.1.8 Create the Schema on Linux or Unix

1. Make sure the **dbinstaller.properties** are set up correctly.
(See, [Configure the Database Setup Properties File](#).)
2. Copy the <Argus Release Media>\Database\Argus Safety folder in the Linux directory.
You must have privileges to execute and create files in this directory and /tmp directory.
3. Open a terminal, log in as the Argus Safety DBA user, and execute the following command:

```
cd <Argus Release Media>/Database/Argus Safety
```
4. Type **dbinstaller** and press **Enter**.
5. Type the DBA user password and press **Enter**.
6. View logs in <Argus Release Media>/Database/Argus Safety/logs.

13.2 Post Fresh Install Steps

1. Log in to ARGUS_APP schema.
2. Verify that the common profile switch DATABASE_TIMEZONE is not empty by executing the following script:

```
select key, value from cmn_profile where key = 'DATABASE_TIMEZONE';
```

13.3 Validate Argus Safety Database

You must validate the database after installation.

Note: If you are creating a fresh Argus Safety database, be sure the factory data is loaded before running the Schema Validation tool.

13.3.1 Validate Argus Safety Database on Windows

1. From Start menu, select Run, type **cmd**, and click **OK**.
2. In the command prompt, go to the following location:
`<Argus Release Media>\Database\Argus Safety\SchemaValidation`
3. Type **SchemaValidation.bat** and press **Enter**.
4. Enter the following parameters:
 - a. TNSNAMES entry to connect to the Argus database: `<ASDB>`
 - b. DBA username in the Argus database: `<argus_dba>`
 - c. Password for the DBA user
 - d. Validation CTL file [Default VLDN_822.CTL]
 - e. Schema difference log file [Default SV_Schema_Diffs_asdb.log]
 - f. CTL loader log file [Default SV_CTLFile_asdb.log]
5. Check the log file for errors.

13.3.2 Validate Argus Safety Database on Linux or Unix

1. Copy the `<Argus Release Media>\Database\Argus Safety` folder in your Linux or Unix directory.
 You must have privileges to execute and create files in this directory and /tmp directory.
2. Open a Linux or Unix terminal, and execute the following command:
`cd <Argus Release Media>/Database/Argus Safety`
3. Type **SchemaValidation** and press **Enter**.
4. Type the DBA user password and press **Enter**.
5. View logs in `<Argus Release Media>/Database/Argus Safety/logs`.

13.4 Enable and Disable Data Lock Point (DLP)

DLP allows a periodic report to use case data as it looked as of a certain date in the past. DLP is a specific type of *point-in-time query* which runs against the Argus History schema in the Argus Safety database. Argus History, once it is enabled at the system level, records all revisions of all cases, allowing point-in-time queries such as DLP to retrieve case data as it was captured at a previous date.

13.4.1 Prerequisites

Before enabling or disabling DLP, make sure that:

- no one is logged on to the Argus Safety database before beginning the enable or disable DLP procedure.
- an Oracle Argus database instance is available.

- a DBA-privileged user or a SYSTEM user account is available.
- the **dlpsetup.properties** file is correctly updated.

13.4.2 Enable DLP

- For Windows, execute the **enableDLP.bat** file from *<Argus Release Media>\Database\Argus Safety\Utilities\DLP_Setup*.
- For Linux or Unix, execute the **enableDLP** shell script.

13.4.3 Disable DLP

- For Windows, execute the **disableDLP.bat** file from *<Argus Release Media>\Database\Argus Safety\Utilities\DLP_Setup*.
- For Linux or Unix, execute the **disableDLP** shell script.

Note: Argus Case Save will not function in case any DLP trigger (s) starting with T_DLP_CASE exists in Argus application schema. This fail safe is to prevent any case data corruption in DLP Schema, in case any trigger is disabled.

- To check if DLP trigger is disabled, use the following SQL from Argus Application Login:

```
SELECT trigger_name FROM user_triggers WHERE trigger_name LIKE
'T_DLP_CASE%' AND status='DISABLED';
```

- If all the triggers are enabled, check the value of CMN Profile Global Switch DLP_TRIGGER_ENABLED and update the value if it is 0:

```
SELECT key,value FROM cmn_profile_global WHERE key ='DLP_
TRIGGER_ENABLED' ;
```

```
UPDATE cmn_profile_global SET value = 1 WHERE key ='DLP_
TRIGGER_ENABLED' AND value != 1;
COMMIT;
```

13.5 Enable DLP on a Specific Enterprise

You can enable DLP for:

- a specific enterprise merged from a non-DLP system to a DLP enabled multi-tenant Argus Safety system.
- delta cases merged into an existing enterprise of a DLP enabled multi-tenant or single-tenant Argus Safety system.

13.5.1 Set Up the Base Database

1. Set up an Argus Safety 8.2.2 multi-tenant or single-tenant database.
Enable DLP on the Argus Safety 8.2.2 database by executing the **enableDLP.bat** file. This sets up the initial DLP infrastructure on the Argus database for all existing enterprises.
2. Validate the schema by executing the **SchemaValidation.bat** file. Use the compatible CTL file.

If any MISSING object exists in schema validation log, fix it before proceeding to the next step.

3. Populate new Argus Safety cases into the existing enterprise of a DLP enabled multi-tenant or single-tenant Argus Safety system from a non-DLP system.

Or, create new enterprise in a DLP enabled multi-tenant Argus Safety system using data migration or merge to multi-tenant utility.

13.5.2 Enable DLP on Specific Enterprise or Delta Cases

To enable DLP on a specific enterprise or delta cases in a specific enterprise, make sure that you use the correct login credentials and set up the appropriate enterprise context.

1. Extract the custom DLP Enable Enterprise Specific script from the following location into a machine's local folder where Argus Safety 8.2.2 is installed:

<Argus Release Media>\Database\Argus Safety\Utilities\DLP_Enable_Enterprise_Specific

2. Double-click DLP_Enable_Enterprise.bat from:

<Argus Release Media>\Database\Argus Safety\Utilities\DLP_Enable_Enterprise_Specific\Argus\DLP\

This batch file execution handles the following scenarios to populate DLP data on newly created Argus Safety cases:

- process all cases merged in Argus Safety system due to creation of new enterprise by merge process
 - process of delta cases merged in an enterprise due to any migration activity
3. Enter a name and location for the log file.

For example, DLP_Enable_Enterprise_Specific.log

4. Enter values at the prompts.

A confirmation message appears.

5. Press **Enter**.

The values you entered are displayed.

6. Verify that the details entered are correct and press **Enter**.

7. Check the log file for errors. If there are errors, the execution process pauses. Fix the errors and continue the process from another SQL window.

8. Check the log file to see if there are any Argus Safety cases missing in DLP.

<Argus Release Media>\Database\Argus Safety\Utilities\DLP_Enable_Enterprise_Specific\Argus\DLP\DLP_ENABLE_Missing_Cases_in_DLP_log.log

13.5.3 Validate the Schema

After enabling DLP Enterprise Specific to Argus Safety 8.2.2, validate the schema by double-click on the SchemaValidation.bat file located in the *<Argus Release Media>*\Database\Argus Safety\SchemaValidation folder.

Extra objects related to table DLP_ENABLE_CASE_HISTORY are ignored in schema validation log file.

The following table and related objects are ignored in Schema Validation if Argus Safety 8.2.2 DLP Enabled system with DLP_Enable_Enterprise_Specific scripts is applied:

- Owner—DLP
- Table—DLP_ENABLE_CASE_HISTORY
- Index—PK_DLP_ENABLE_CASE_HISTORY
- Reason for extra object—Objects are part of Enable DLP Enterprise Specific implementation.

13.6 Copy Configuration Data (Optional)

The Copy Configuration Tool allows you to copy configuration data from one Argus Safety database to another.

13.6.1 Set Up the Copy Configuration Tool

1. The Copy Configuration Tool creates a database directory in order to execute. Make sure to create a physical directory on the database server where export and import dump files are created and copied respectively. The physical path of these directories is required while performing the export and import.
2. Validate Schema on the source database using **SchemaValidation.bat** file.
Make sure that there are no extra or missing objects exist in Schema Validation log file. Messages for extra custom objects created should be ignored.
3. Copy the **Copy Configuration Tool** utility files recursively from <Argus Release Media>\Database\Argus Safety\Utilities\Copy_Config to the C:\CONFIG_EXP_IMP folder.

13.6.2 Use the Copy Configuration Tool

1. Export the source database by running the batch file and following the prompts:
C:\CONFIG_EXP_IMP\Data_ExportConfigOnly.bat
2. Copy ArgusSecureKey.ini (working with source database) from the .\Windows folder, and save it with generated source database file.
In case you do not have ArgusSecureKey.ini, follow the steps listed in the [Section 26.2.6, "Reset the Environment if ArgusSecureKey.ini is Lost."](#)
3. Move the dump files generated on the source Database Server (physical path provided while performing the export) to the target Database Server (physical path where import will be done).
4. To perform the import on the client machine, in the **Directory Path on DB Server where dump files are placed for import** parameter, use the same folder as entered in the **DB Directory Path for export dump files** while executing the export process for logs.
Or move the contents of the export logs folder provided to the **Directory including full path for log/script files** parameter while executing the export process, in the folder being used for the import process for log generation.
5. Create a new database (with or without TDE enabled) using the **dbinstallerUI.bat** or **dbinstaller.bat** file.

6. Import into the target database by running the batch file, and follow the prompts:
C:\CONFIG_EXP_IMP\Data_ImportConfigOnly.bat
Ignore any "ORA-28101: policy already exists" errors.
7. Validate Schema on the target database executing the **SchemaValidation.bat** file.
8. Copy ArgusSecureKey.ini from the source database folder and paste it in the .\Windows folder of application server(s) which are intended to be used with the target database.

13.7 Create Argus Safety Read-only Database Account (Optional)

1. From the command prompt, run the batch file:
`<Argus Release Media>\Database\Argus Safety\Utilities\Create_Readonly_User`
2. Enter the following parameters and follow the instructions provided in the script.
 - a. TNS name of Safety database.
 - b. DBA user in the above specified database.
 - c. Password of the DBA user.
 - d. New read-only user to be created.
 - e. Password for the read-only user.
 - f. New read-only role to be created.

Note: This is not a requirement to install and run Argus Safety. This is an optional script that can be used to create the read-only account for any external interface you may have that needs read-only access to the data.

Upgrade Argus Safety Database

The space requirements for the upgrade are determined by the upgrade script. This requirement is mostly for new objects created during the upgrade. It is a fair estimate of space requirements.

14.1 Prerequisites for Database Upgrade

- The Oracle Database Server version should be upgraded as per the technology stack (see [Section 1.2.2, "Oracle Components"](#)).
- Verify that JRE 1.8 or above is installed, and JCE policy is applied.
- Verify that the Oracle TNSNAMES have been configured.
- To avoid errors during upgrade, do either of the following:
 - Keep datafiles AUTOEXTEND ON, or
 - Monitor free space and add more space, if required
- Create one large rollback segment or size 20 GB for LARGE size model.
Keep all other rollback segments, except SYSTEM, offline.
- The source Argus Safety database must be AL32UTF8 character set.
- The database semantics must be CHAR and not BYTE.

14.2 Argus Safety Database Upgrade

Note: You will need to generate a key prior to the database upgrade or you can use ArgusSecureKey.ini from the existing setup.

You must also make sure that the password information specified in the database is consistent with the information provided in the **ArgusSecureKey.ini** file.

Note: To execute the database creation and setup on a Linux server, copy the build folder from the <Argus Release Media>\Database\Argus Safety on the server.

You may be prompted to press **Enter** at screens that are not included in the procedure. This does not hinder the upgrade procedure. Where applicable, press **Enter** to continue with the upgrade process.

1. Make sure the **dbinstaller.properties** are set up correctly. (See [Section 13.1.5, "Configure the Database Setup Properties File"](#).)
2. Validate the existing Argus Safety using the **SchemaValidation.bat** file. Use the validation file of the existing installed version from the Schema Validation folder:
`<Argus Release Media>\Database\Argus Safety\SchemaValidation`
3. View the validation log file to make sure that the existing database has no errors, missing and invalid objects.
4. To create a new DBA user and refresh the existing DBA user grants, [Run Create DBA User Script](#).
5. From the `<Argus Release Media>\Database\Argus Safety` folder, run the **dbinstallerUI.bat** file as an administrator, to invoke the user interface and enter the parameters.

The Argus Safety - Database Setup screen appears.

You cannot modify any details on this screen. In case, any of the information is incorrect, then you must re-create the schema.

For a silent upgrade, from the `<Argus Release Media>\Database\Argus Safety` folder, run the **dbinstaller.bat** file as an administrator.

6. In case of upgrade, all the schema details will be auto-populated based on the schema selection logic. Before proceeding further, you must confirm that all the schema details are correctly populated.

Note: You must not create any Argus Safety objects in custom schema.

7. Click **Next**.
8. Enter the path for Tablespace and click **Next**.
9. Verify the Setup Parameters and click **Execute**.
10. To ignore any error due to customization, check **Ignore Error** checkbox in the DBInstaller user interface, and analyze it later when the upgrade is done.
11. To validate the schema, from the `<Argus Release Media>\Database\Argus Safety\Schema Validation` folder, run the **SchemaValidation.bat** file.

See [Section 13.3, "Validate Argus Safety Database"](#).

14.3 Post Upgrade Steps

1. Log in to ARGUS_APP schema.
2. Verify that the common profile switch DATABASE_TIMEZONE is not empty by executing the following script:

```
select key, value from cmn_profile where key = 'DATABASE_TIMEZONE';
```

14.4 Enable Local Locking in Argus Safety

Before enabling Local Locking in Argus Safety, you must make sure that you have upgraded your database to this release successfully.

1. Execute the batch file **Enable_local_lock.bat** from <Argus Release Media>\Database\Argus Safety\Utilities\Enable_local_lock directory.
2. Enter the response for *Do you wish to turn on the Local Locking feature for one or more enterprises (Yes/No)?*, enter **Yes** to continue.
3. Enter the log file name to record the results.

This is the execution log that is created on the client workstation under the Enable_local_lock directory mentioned above.

4. Enter TNSNAMES Entry to Connect to the source SAFETY Database.
5. Enter SAFETY schema owner name in source Database.
6. Enter the password for safety schema name in source Database.
7. Enter comma separated list of enterprises where local locking feature is to be enabled or enter ALL for all enterprises in Source safety Database.

If no value is entered script will run for enterprise 1 by default.

8. Enter the Agency name for PMDA reporting destination as configured in **Reporting Destination** codelist.
9. To enable local locking privileges for the Argus J users, enter **Yes**.

Follow the prompts for confirmation.

Note: If the agency entered is invalid for any of the enterprises, the utility will abort and no changes will be committed.

In case of a multi-tenant environment, if this utility is re-run for any of the enterprises, it will display a list of the enterprises for which it has already executed and will continue to process rest of the enterprises.

14.5 Merge a Single Enterprise Safety Database into a Multi-tenant Database

14.5.1 Prerequisites to Run the Merge Export Step

- The end user should not use the source database during the export process.
- Install Argus Safety 8.2.2 on a computer where Oracle database is installed. Make sure the Oracle database is installed as per the [Chapter 1, "System Requirements."](#)
- The source databases should be schema validated at Argus Safety 8.2.2.
- The source database should only be a single-tenant database.
- The source database data must contain only one ENTERPRISE.

14.5.2 Merge Export

1. From the Start menu, navigate to the following path:

<Argus Release Media>\Database\Argus Safety\Utilities\Merge_to_Multitenant

2. Double-click the **merge_export.bat** file and follow the instructions on the sqlplus screen.

- a. Enter Log File Name to record results.

This is the execution log that is created on the client workstation:

Log file path: <Argus Release Media>\Database\Argus
Safety\Utilities\Merge_to_Multitenant

- b. Enter TNSNAMES Entry to Connect to the Source SAFETY Database.
- c. Enter SYSTEM or DBA user name in source Database.
- d. Enter password for SYSTEM or DBA user in source Database.
- e. Enter SAFETY schema owner name in source Database.
- f. Enter password for Safety schema owner in source Database
- g. Enter Interchange schema owner name in Safety Database
- h. Enter password for Interchange schema owner in source Database.
- i. Enter the full directory Path to create the Source Safety database export dump file:

This is the Path on the **Source Database Server** where the Argus Safety Database resides. The batch file will create an export dump file (SAFETY.DMP) and an export log file (SAFETY_EXPORT.LOG) in the directory.

Make sure that SAFETY.DMP file does not exist prior to the export.

3. Make sure that no error has occurred during the database export, by checking the following log files:
 - Log file name entered as parameter 1 during export step execution.
 - Following Oracle Export log files are created on database server. The path is the value entered on "Enter Directory including full Path to create Source safety database export dump file" during export step:

SAFETY_EXPORT.log

14.5.3 Export the dmp File Copy to the Target Database Server

Move the export dmp file created in [Merge Export](#) from the source database server to the target database server.

14.5.4 Prerequisites to Run the Merge Import Step

- Create a cold backup of the target database before starting the Merge Import step.
- The end user should not use the target database during the import process.
- Only one Merge Import process can run on the target database at a time.
- Auto extend should be set on for all database files in the target database.
- Sufficient space should be available on the target database server to import the new enterprise data. The amount of space depends on the number of cases in source Argus Safety database.

- Install the Argus 8.2.2 application. Make sure that Oracle Client version is same as the database server.
- The target databases should be Schema Validated at Argus 8.2.2.
- The target database must be a multi-tenant database.
- All source database dictionaries should be available in target database. If the dictionary does not exist then install missing dictionaries on the target database.
- All existing AG service users on the source database must exist on the target database.
- All source database LDAP configured server names should be available in target database.

14.5.5 Merge Import

1. From the Start menu, navigate to the following path:
`<Argus Release Media>\Database\Argus Safety\Utilities\Merge_to_Multitenant`
2. Click **merge_import.bat** and enter the following parameters for the target database:
 - a. Log File Name to record results.
 This is the execution log that will be created on the client workstation.
 Log file path: `<Argus Release Media>\Database\Argus Safety\Utilities\Merge_to_Multitenant`
 - b. TNSNAMES entry to connect to the target Safety database.
 - c. SYSTEM or DBA user name.
 - d. Password of the DBA user.
 - e. VPD schema owner name.
 - f. Password of the VPD schema owner.
 - g. SAFETY schema owner name.
 - h. Password of the Safety schema owner.
 - i. Interchange schema owner name.
 - j. Password of the Interchange schema owner.
 - k. Directory location where the export dmp file is copied for the import process.
 This is the path on the Target Database Server where the Argus Safety database is installed. The batch file creates an import log file in this directory.
 - l. Name of the new enterprise.
 - m. Abbreviation of the new enterprise.
 - n. SAFETY schema owner name in the source database.
 - o. Interchange schema owner name in source database.
3. This batch file imports the data from the dump file into the target database.
4. Make sure that no error has occurred during import by checking the following log files:
 - Log file name entered as parameter 1 during Import step execution.

- The following Oracle Import log files are created on database server. The path is the value entered in “Enter Directory including full Path on target database server where export dmp file copied for import process” during import step.
 - SAFETY_IMPORT_safety.log
 - SAFETY_IMPORT_interchange.log
 - SAFETY_IMPORT_SAFETY_DUP_SEARCH_DATA.log
 - SAFETY_IMPORT_SAFETY_DUP_LAM_SEARCH_DATA.log
- 5. Validate the schema of the database using the **SchemaValidation.bat** file.

14.5.6 Synchronize Dictionary Manually

The merge process synchronizes the dictionary information based on the dictionary name in the source and target database. If the source dictionary name is not available in target database, then manual synchronization is required.

To synchronize the dictionary data manually on the target database:

1. Log in as the Safety schema owner using sqlplus on the target safety database.
2. Locate the new ENTERPRISE_ID value created from import process using the following sql:

```
SELECT VALUE
FROM cmn_profile_global
WHERE section = 'DATABASE' AND KEY = 'MERGING_TO_MULTITENANT';
```
3. Set the context value to new Enterprise_id

```
Exec pkg_rls.set_context('admin', < Value of New Enterprise ID>, 'ARGUS_SAFETY');
```
4. Locate the list of Dictionaries ID's where Dictionary synchronization pending due to missing Dictionaries on Target database. If the following sql results in NO ROWS, then no further action is required.

```
Select dict_id
From cfg_dictionaries_enterprise
Where enterprise_id = <Value of New Enterprise ID>
And global_dict_id = -1;
```
5. Log in as the Safety schema owner using sqlplus on the source safety database.
6. Locate the dictionary name of each Dictionary ID where the dictionary does not exist on the target database using the following sql:

```
Select name from cfg_dictionaries_global
where dict_id in (<List of Dict ID values (comma separated) from Step 4);
```
7. Load the missing dictionaries on the target database.
8. Set the context to new enterprise_id using following sql on target database.

```
Exec pkg_rls.set_context('admin', <Value of new ENTERPRISE_ID> , 'ARGUS_SAFETY');
```
9. Update GLOBAL_DICT_ID data in the target database using the following SQL:

```
UPDATE CFG_DICTIONARIES_ENTERPRISE
SET GLOBAL_DICT_ID = <Dictionary Global Dict ID value from target database>
WHERE ENTERPRISE_ID = <New ENTERPRISE_ID created in Target Database>
AND DICT_ID = <Value of Dict ID in New ENTERPRISE with Dictionary name>
AND GLOBAL_DICT_ID = -1;
```

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 [Chapter 1, "System Requirements."](#)

15.1 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**
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 Argus Insight Database Server (and vise-versa) > tnsnames.ora file at the following path:

... \network\admin\tnsnames.ora

- 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:

<Build path>\Database\Argus Insight\Utilities\Create_Dba_User\ai_create_dba_user.bat

For more details on creating this user, see [Section 15.3.3, "Create the DBA User."](#)

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

15.2 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 | Yes | db_connect_string =<host>:<port>/<service name> |
| 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: <ul style="list-style-type: none"> 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_LOGIN/pwd |
| 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 |

| Parameter | Description | Modify | Default or Sample Value |
|--------------------------------------|---|--------|---|
| ai_link_role | Argus Insight Mart Link Role | Yes | ai_link_role=LINK_ROLE |
| safety_db | Argus Safety database instance name | Yes | <ul style="list-style-type: none"> ■ safety_db=SAF822DB, or ■ safety_db=SAF822DB.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/822DB> |
| #Insight Stage Normal Datafiles | Location of Argus Insight normal datafiles. | Yes | <ul style="list-style-type: none"> ■ 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 | <ul style="list-style-type: none"> ■ 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 | <ul style="list-style-type: none"> ■ stage_who_01_datafile=APR_SWHOC_DATA_01.DBF |
| #Insight Mart Case/Rpt Datafiles | Location of Insight Mart case and report datafiles. | Yes | <ul style="list-style-type: none"> ■ 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 | <ul style="list-style-type: none"> ■ 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 | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> mart_who_01_datafile=APR_MWHOC_DATA_01.DBF |
| #Insight Hist Case/Rpt Datafiles | Location of Argus Insight case or report History datafiles | Yes | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> default_ts=USERS temp_ts=TEMP |
| Tablespace Encryption | Specifies the logic used for default encryption | Yes | tablespace_encryption=<blank> or <text>, where <ul style="list-style-type: none"> blank—No encryption text—like encryption using 'AES256' default storage (encrypt) |
| Tablespace Parameters | Specifies the details of the tablespace | Yes | <ul style="list-style-type: none"> tablespace_initial_size=10M tablespace_autoextend=ON tablespace_next_size=10M tablespace_block_size=8K |

15.3 Create Argus Insight Database Schema

15.3.1 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.

15.3.2 Create Users in the Argus Safety Database

1. To create the Safety Read-only user for Insight, execute the following script from the folder <Argus Release Media>\Database\Argus Insight\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
 - 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.

<Argus Release Media>\Database\ArgusInsight\Utilities\Create_Safety_Ro_User\AI_AS_RO_User_MMDDYYYY_HH24MISS.log

15.3.3 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 *<Argus Release Media>\Database\ArgusInsight\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, 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:

<Argus Release Media>\Database\ArgusInsight\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;
```

15.3.4 Create Fresh Argus Insight Schema

1. Log in to the Argus Insight Transaction Server.
2. Navigate to *<Argus Release Media>\Database\Argus Insight*.
3. Open the **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>/<service name>
For example, server.us.xx.com:1521/AI822MT
 - dba_user—specifies the name of the DBA user to run Argus Insight Liquibase Install.
See [Section 15.3.3, "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 15.2, "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 INSIGHT_RO_USER of Safety
- From MART_USER of Argus Insight to INSIGHT_RO_USER of Safety

- From MART_APP_USER of Insight to INSIGHT_RO_USER 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 |
| 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.

15.3.5 Validate the Schema

1. Navigate to <Argus Release Media>\Database\ArgusInsight\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:
<VLDN_APR_AI_8.2.2.CTL>
 - Enter the destination where the log file is to be placed:
<Argus Release Media>\Database\ArgusInsight\ValidateSchema>
 - Enter the log file name for recording the schema differences:
<VLDN_APR_AI_8.2.2_diff.log>
 - Enter Validation Output File Name: The validation output file name to record the validation progress:

<VLDN_APR_AI_8.2.2.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:

<Argus Release Media>\Database\ArgusInsight\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.
-

15.3.6 Create Argus Insight Read-only User

1. Open <Argus Release Media>\Database\ArgusInsight\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:

<Argus Release Media>\Database\Argus Insight\Utilities\Create_Insight_Ro_User\AI_RO_User_MMDDYYYY_HH24MISS.log

15.4 Create Database Links

15.4.1 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 *<Argus Release Media>\Database\Argus Insight\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, for example: ARGUS_APP>*
 - 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 user in Safety Database: *<Insight Read-only user, created in Argus Safety>*
For example, *<INSIGHT_RO_USER>*
 - Enter the Argus Insight Database Tns Name: *<Argus Insight database>*
 - Enter the name of link user in Insight Database.: *<link user of Argus Insight, for example: APR_LINK_USER>*
 - 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:
<Argus Release Media>\Database\Argus Insight\Utilities\Database_Links\argus_to_mart\ ARGUS_TO_MART_DB_LINK_MMDDYYYY_HH24MISS.log

15.4.2 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 *<Argus Release Media>\Database\Argus Insight\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, for example: INSIGHT_RO_USER>
 - 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: <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:

- SAF822DB@DB_LINK_ARGUS
 - SAF822DB.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:

<Argus Release Media>\Database\Argus Insight\Utilities\Database_Links\db_link_argus\DB_LINK_ARGUS_MMDDYYYY_HH24MISS.log

15.5 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 25, "Extract, Transform, and Load Data."](#)

15.6 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 *<Argus Release Media>\Database\Argus Insight\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:

<Argus Release Media>\Database\Argus Insight\DBInstaller\Utilities\am_grants\AM_GRANTS_MMDDYYYY_HH24MISS.log

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

Upgrade the Argus Insight Data Mart Structure

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

16.1 Prepare for Database Upgrade

Before upgrading, make sure:

1. Take the latest Liquibase build for 8.2.2.
2. Recreate the DBA User.
(See [Section 15.3.3, "Create the DBA User."](#))
3. Recreate the Safety RO User of Argus Insight.
4. Recreate the DB_LINK_ARGUS from Argus Insight to Argus Safety.
(See [Section 15.4.2, "From Argus Insight to Argus Safety \(manually\)"](#))

16.2 Upgrade Database

1. Log in to Argus Insight Transaction Server.
2. Navigate to <Argus Release Media>\Database\Argus Insight.
3. Open the **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>/<service name>`
For example, `db_connect_string=Dbname.us.xx.com:1521/AI822MT`
Or, `db_connect_string=Dbname.us.xx.com:1521/AI822MT.us.xx.com`
 - **dba_user**—specifies the name of the DBA user to run Argus Insight Liquibase Install.
See [Section 15.3.3, "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 15.2, "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_8.2.2.CTL.

See [Section 15.3.5, "Validate the Schema."](#)

Part IV

Configure Other Products

This part lists the other products that are installed and configured through Argus Safety or Argus Insight, and are required to complete the installation.

During the installation, the information in this manual may differ from what you see on your monitor if additional modules were selected during the Argus Safety Web Installation.

Prerequisites:

- Obtain a domain account with Local Administrator privileges.
- In case of application upgrade, make sure to [Backup Configuration Files](#) of the existing Argus Safety application before setting up the machines.

Configure and Enable Argus Dossier

17.1 Prerequisites

1. [Set Up Argus Middle and Client Tiers.](#)
2. [Install or Upgrade Argus Database Tier.](#)

17.2 Configure Dossier

1. On the server where Dossier is installed, from the installation folder, open the file **service.config**. By default, the installation folder is:
C:\Program Files\Oracle\ArgusWeb\ASP\Argus.NET\bin
2. Uncomment the entries for **DossierBuilder** in the section:
`<ServiceConfiguration>/<ServiceComponents>`
3. From the installation folder, open the file **RelsysWindowsService.exe.config**.
4. Make sure that the `<DatabaseConfiguration>` section is configured for the following attributes:

| Attribute | Description |
|-----------------------|---|
| DBName (Mandatory) | TNS of the Database to which the RelsysWindowsService should connect to. Example: DBName="GOLDDemo" |
| DBUser | AGService Username. The RelsysWindowsService logs into the database using this login name. This has to be a user of type AGSERVICE. Example: DBUser="agservice_user1" |
| GeneralEmailTo | The e-mail address to which the e-mails will be sent by the Intake Service, using the General Email feature of Argus. Example: GeneralEmailTo ="recepient@oracle.net" |
| GeneralEmailFrom | The email address from which the e-mails will be sent by the Intake Service, using the General Email feature of Argus. Example: GeneralEmailFrom =" admin@oracle.net " |

| Attribute | Description |
|--------------------------|--|
| GeneralEmailCc | <p>This email address will be added to the Cc line when e-mails are sent by the Intake Service, using the General E-mail feature of Argus.</p> <p>Example: GeneralEmailCc ="recepient@oracle.net"</p> |
| GeneralEmailBcc | <p>The email address will be added to the Bcc line when e-mails are sent by the Intake Service, using the General E-mail feature of Argus.</p> <p>Example: GeneralEmailBcc ="recepient@oracle.net"</p> |
| Recurrence (Optional) | <p>The value for this attribute specifies the frequency of instantiation of the associated Service Component. The value is specified in seconds.</p> <p>For example:</p> <pre><add Name="DossierBuilder" Assembly="DossierServiceComponent" Type="DossierBuilder" Recurrence="600" Metadata="InvokeDirect=true" /></pre> <p>The value of 600 for Recurrence above means, the "DossierBuilder" service is instantiated every 600 seconds (10 minutes) to perform the job.</p> |

17.3 Enable Dossier

1. Go to Argus Safety > Argus Console > System Configuration > Enabled Modules.
2. Select **Dossier**.
3. Click **Save**.

Install and Configure Axway B2Bi

This chapter describes the steps required to install and configure the Axway B2Bi EDI (Electronic Data Interchange) Gateway so it can operate correctly with Argus Interchange.

Note: Either B2B or Axway B2Bi is required for E2B reports exchange. You can choose any one of the software, as required.

You may install EDI Gateway and Interchange Service in any order.

18.1 Create an Axway B2Bi Database Instance

1. Log in to the database server as an Admin user.
2. Create a blank Axway B2Bi instance, if it does not already exist.
3. Connect to the Axway B2Bi instance created in Step 2.
4. Create an Axway B2Bi DB User identified by the Axway B2Bi DB password.
5. Provide the following grants to the Axway B2Bi DB user:
 - Grant CREATE PROCEDURE
 - Grant CREATE SESSION
 - Grant CREATE TABLE
 - Grant CREATE VIEW
 - Grant UNLIMITED TABLESPACE (Optional)
 - Grant CREATE SEQUENCE
 - Alter user Axway B2Bi DB User default tablespace USERS.
 - Grant CONNECT
 - Grant RESOURCE

18.2 Install Axway B2Bi

For more information, see the *Axway B2Bi installation documentation*.

18.3 Configure Axway B2Bi

1. Log in to a client computer.

2. From the browser, go to (Sender or Receiver) `http://<AxwayB2BiServer>:6080/ui/`.
3. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
4. In the Getting Started screen, hover over the **Trading Configuration** icon and select **Recent Communities > Manage Trading Configuration** from the menu.
5. In the Pick a community screen, click **Add a community**.
6. In the Choose the source screen:
 - a. Click **Next** to continue.
 - b. Click the **Manually create a new community profile** option button.
 - c. Enter the parameters.
 - d. Click **Yes** to add a certificate.

Note: This information is entered for both the sender and the receiver, but initially for the sender.

- e. Click **Finish**.
7. In the Add a certificate screen, click **Create a self-signed certificate** and click **Next**.
8. In the Enter the certificate information screen, click **Next**.
9. In the Review request screen, click **Next**.
10. In the View certificate details screen:
 - a. Check **Make this the default encryption certificate**.
 - b. Check **Make this the default signing certificate**.
 - c. Click **Finish**.
11. Hover over the **Trading Configuration** icon, from the drop-down menu, select the recent **Communities > <community>**.
12. In the **Summary** screen, click the **Setup up a pickup for receiving messages from partners**.
13. In the **Choose message protocol** screen, select the **EDIINT AS2 (HTTP)** option and click **Next**.
14. In the **Choose HTTP transport type** screen, click **Next**.
15. In the Configure URL screen, click **Next**.
16. In the Exchange Name screen, enter the **Exchange Name** and click **Finish**.
17. In the Summary screen, click **Application Delivery** and add an application delivery.
18. In the **Choose transport protocol** screen, select the **File system** option and click **Next**.
19. In the **Configure the file system settings** screen, click **Next**.
20. In the Exchange Name screen, enter the **Exchange Name** and click **Finish**.
21. Go to the Summary Page and click **Configure the settings for application delivery**.

22. In the Select application delivery screen, select **Name**, enter **Friendly Name**, and click **Finish**.

18.3.1 Configure Axway B2Bi for Binary File Transmission

You can configure transmission for binary files such as PMDA zip files and E2B attachments.

To configure Axway B2Bi for binary file transmission:

1. Log in to a client computer.
2. From the browser, go to (Sender or Receiver): `http://<AxwayB2BiServer>:6080/ui`.
3. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
4. In the Getting Started screen, hover over the **Trading Configuration** icon and from the drop-down menu, select **Recent Communities > <community>**.
5. In the Summary screen, click the **Application Pickup** icon and add an application pickup.
6. In the Choose transport protocol screen, click **File system** option and click **Next**.
7. In the From address and To address screens, click **Next**.
Address must be determined by either message attribute configuration or by protocol address only.
8. In the **Configure the file system settings** screen, on the Sender's Axway B2Bi Server, locate Common/Out folder and create the following folder structure:
Common\Out\Sender's Routing ID\Receiver's Routing ID
9. In the Exchange Name screen, enter the **Exchange Name** and click **Finish**.
10. In the **Change this application pickup exchange** screen, click the **Message attributes** tab.
11. In the Message attribute directory mapping tab:
 - a. The system moves them to the **Selected attributes** list.
 - b. Select **From routing ID** and **To routing ID** and click **Add**.
 - c. Locate the **Available Attributes** list.
 - d. Click the **From address** tab.
12. Click **To address** tab, select the **Address determined by message attribute configuration** option or by protocol address only and click **Save Changes**.
13. On the Sender's Axway B2Bi Server, locate Common/Out folder and create the following folder structure:
Common\Out\Sender's Routing ID\Receiver's Routing ID

Note: This completes the folder configuration for outgoing binary transmissions. Since binary file transmission configuration is based on these folder names, each combination of Sender and Receiver Routing ID must be unique for binary file transmission to different trading partners.

The Binary file should be dropped in the RECEIVER's Routing ID Folder which is the last folder. Although in the Axway B2Bi GUI the Application Pickup folder will show up only `..\common\out`.

14. For incoming binary transmissions, repeat steps 5 - 8 for Application Delivery.
Repeat steps 1 - 12 for setting up the Receiver Axway B2Bi.

18.3.2 Configure Axway B2Bi Community

18.3.2.1 Register with the Axway B2Bi Community

1. From the browser, go to `http://<Receiver Axway B2BiServer>:6080/ui/`.
2. In the **Axway B2Bi Login** screen, enter Axway B2Bi User ID and Password, and click **Login**.
3. In the Getting started screen, hover over the **Trading Configuration** icon and from the drop-down menu, select **Recent Communities > <community>**.
4. In the Summary screen, click **Export this community as a partner profile** at the bottom of the page.
5. Enter the password and save the file to your local hard drive and close the **Save** dialog box.
6. Click **Logout** in the upper right corner of the page.

18.3.2.2 Add a Partner to the Axway B2Bi Community

1. From the browser, go to `http://<Sender AxwayB2BiServer>:6080/ui/`.
2. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
3. In the Getting Started screen, hover over the **Trading Configuration** icon and select **Recent Communities > <community>** from the menu.
4. In the Summary screen, click the **Add a Partner to this community** link.
5. In the **Choose the source** screen, select the **Import the profile information from a file** option and click **Next**.
6. In the **Enter profile path** screen, click **Browse** to navigate to the saved file, enter the same password used at the time of exporting this community as a partner profile, and click **Finish**.
7. In the **Successful profile import** screen, click **Close**.

Note: If you receive a summary where the Routing ID is not displayed, you must add the sender's Routing ID manually, as listed from Steps 9 - 12.

8. In the Summary screen:
 - a. Click the **Partners** menu item and select the newly imported partner.
 - b. Click the **Routing IDs** icon.
9. In the Routing IDs screen:
 1. Click **Add**.
 2. Type the partner (sender) routing ID in the **Routing ID** field.
 3. Verify that the partner **does not** have a routing ID.
The new routing ID is added to the page.
 4. Hover over the **Trading Configuration** icon.
 5. Select **Recent Communities** > <community> from the menu.
10. In the Summary screen, select the sender partner.
11. In the Summary: Sender screen, click the **Default delivery exchange** link.
12. In the **Change this delivery exchange** screen, click the **HTTP Settings** tab, and verify that the URL is correct and that the correct routing ID for the send is appended to the end of the URL

18.3.2.3 Register the Receiver's Community on the Sender Server

Repeat the procedures of the [Section 18.1, "Create an Axway B2Bi Database Instance"](#).

18.3.3 Add a Node

1. From the browser, go to `http://<Sender Axway B2BiServer>:6080/ui/`.
2. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
3. In the Getting started screen, click the **System Management** icon.
4. In the System Management screen, click **Add a Trading engine node**.
5. In the Add a node screen:
 - a. Click **Add**.
 - b. Select the machine to add the node to from the **Computer name** drop-down.
 - c. Click the **Trading Engine** option.
6. When the System management page opens with the newly created node:
 - Click **Start** to start the trading engine node.
The system updates System management page.
The status of the node changes to **Starting**.
The system updates the System management page.
The status of the node changes to **Running**.
7. Click **Home** and verify that the node status is **Running**.
8. Repeat the procedure to set up the Receiver Axway B2Bi.

18.3.4 Configure Axway B2Bi Certificates

18.3.4.1 Configure Receiver Axway B2Bi Certificates

1. From the browser, go to `http://<Receiver Axway B2BiServer>:6080/ui/`.
2. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
3. In the Getting Started screen, hover over the **Trading Configuration** icon and select **Manage trading configurations** from the menu.
4. In the Community screen, click the **Community name**.
5. In the Summary screen, click the **Certificates** link.
6. In the Certificate screen, click the **Certificate** listed on the **Personal certificates** tab.

Note: Click the Trusted root certificates tab to verify that no certificates exist for the Sender or Receiver Axway B2Bi.

Skip this section if a valid trusted root certificate already exists in the Name section on the Trusted root certificates tab.

7. In the View certificate screen, in the General tab, locate the **Related task** section and click **Export this certificate**.
8. In the **Choose the format you want to use for the certificate export** screen, retain the default configurations.
 - a. Click **Export certificate**.
 - b. Click the **Cryptographic Message Syntax Standard PKCS #7** option button.
 - c. Select the **Include all certificates in the certification path if possible** checkbox.
9. Save the file to the Sender's local hard drive and click **Logout** in the upper right corner of the page.

18.3.4.2 Configure Sender Axway B2Bi Certificates

1. From the browser, go to `http://<Sender Axway B2BiServer>:6080/ui/`.
2. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
3. In the Getting Started screen, hover over the **Trading Configuration** icon and select **Manage trading configurations** from the menu.
4. In the Community screen, click the **Community name**.
5. In the Summary screen, click the **Certificates** link.
6. In the Certificate screen, click the **Trusted root certificates** tab and click the **Add a trusted root certificate** link.

Note: It is possible that the Trusted Root Certificates for the Receiver Axway B2Bi Server may already be on the Sender Axway B2Bi Server.

7. In the Add a certificate screen, click **Next**.
8. In the Locate the certificate file screen, click **Browse** to locate the P7B certificate file saved for the Receiver Axway B2Bi Server and click **Next**.
9. In the View certificate details screen, click **Finish**.
10. In the Pick a certificate screen, click the **Trusted root certificates** tab.
11. Verify that the certificate you added appears on the list.
12. Log out of the Sender Server.

Repeat the procedure to register the Sender's certificate on the Receiver Server as a Trusted Root Certificate.

18.3.5 Configuring EVENTS.XML

To configure Event.xml on Client machine:

1. Log in to a client computer.
2. Using Windows Explorer, go to the local directory containing the Argus Safety installation files and navigate to `..\DBInstaller\Utilities\Cyclone`.
3. Locate and double-click the **cyclone_setup.bat** file to open a DOS command prompt window.
4. In the Oracle SQL+ screen:
 - a. Enter the Axway B2Bi instance in the **TSNAMES** entry.
 - b. Enter the Axway B2Bi DB User Name in the **Axway B2Bi User Name**.
 - c. Enter the Axway B2Bi User Password in the **Password for User Axway Synchrony_USER**.
 - d. Enter the Axway B2Bi Schema User in the **[USERS]**.
5. When SQL+ connects to the specified database, enter the Directory name and the log file name.

When the process is complete, the SQL+ window and DOS command prompt window close.

To configure Event.xml on Receiver machine:

1. Log in to the Receiver Server.
2. Using Windows Explorer, navigate to `<Axway B2Bi Install Folder>\conf folder\`.
3. Take a backup of the Events.xml file and rename it Events.xml.bak.
4. Right-click the Events.xml file and select **Edit** to display it in **Notepad**.
5. Locate the `<EventRouters>` section and add the following code:

```
<EventRouter id="ARGUS Events" class =
"com.cyclonecommerce.relsys.router.GetEventInfo" active="true">
<Parameters file="../../logs/ARGUS.log" rollOnStart= "true" autoFlush="true"
maxFileSize="2M" maxBackupFiles="5"/>
<MetadataProcessorListRef ref="Messaging"/>
<EventFilterRef ref="ARGUS"/>
</EventRouter>
```

6. Add the following section in the Events.xml file in the `<EventFilters>` section:

```
<EventFilter id="ARGUS">
<OrFilter>
<EventFilterRef ref="Message Milestones"/>
<EventLevelFilter level="Warning"/>
<EventLevelFilter level="Error"/>
<EventLevelFilter level="High"/>
</OrFilter>
</EventFilter>
```

7. Copy the ArgusRouter.jar file from Argus local directory:
\\SUPPORT\\AxwayB2Bi\\2.6 to Axway B2Bi directory: <Axway B2Bi Install folder>\\Interchange\\jars\\.

Note: Make sure that the ArgusRouter.jar available from the previous versions is removed before replacing with new one. There must only be the latest ArgusRouter.jar present.

In case Axway Interchange is upgraded to Axway B2Bi, then the old ArgusRouter.jar can be found at <Axway Install Folder>\\jars\\.

8. From the browser, go to <http://<Receiver Axway B2BiServer>:6080/ui/>.
9. In the Getting Started screen, hover over the **Trading Configuration** icon and from the drop-down menu select **Recent Communities > Community**.
10. In the Summary screen and click the **Application Pickup** icon.
11. In the Application pickup exchange screen, click the link in the **Name** column.
12. Click the **Inline Processing** tab.
13. In the Inline processing rules screen, enter the following parameters:
 - a. **Class name**—com.cyclonecommerce.relsys.router.GetMessageInfo
 - b. **Parameter**—Relsys Argus
 - c. **Description**—GetMessagesInformation
14. Click **Save changes**.
15. When the Pick an integration pickup exchange screen appears, click **Logout**.
16. Repeat the preceding steps for the Sender Server.

18.3.6 Configure Message Processing Settings

1. From the browser, go to <http://<Sender Axway B2BiServer>:6080/ui/>.
2. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
3. In the Getting Started screen, hover over the **Trading Configuration** icon and select **Recent Communities > <community>** from the menu.
4. In the Summary screen, click the **Application Pickup** icon.
5. In the Application pickup exchange screen, click a link in the **Name** column.
6. Click the **Advanced** tab and from **Message processing**, select **Limited - only use message handler and collaboration settings**.
7. In the Getting Started screen, hover over the **Trading Configuration** icon and select **Recent Communities > <community>** from the menu.

8. In the Summary screen and click the **Trading Pickup** icon.
9. In the Trading pickup exchange screen, click a link in the **Name** column.
10. Click the **Advanced** tab, and from **Message processing**, select **Limited - only use message handler and collaboration settings**.
11. Go to <AxwayB2Bi Install folder>\B2Bi, and execute the following command to stop the server:
./B2Bi stop
12. Go to <AxwayB2Bi Install Folder>\B2Bi, and execute the following command to start the server:
./B2Bi start
13. To verify that the Trading engine node in Running state and the Integration engine node in Started state, and the Trading engine node is assigned to the Integration engine node:
 - a. From the browser, go to <http://<Sender Axway B2BiServer>:6080/ui/>
 - b. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
 - c. In the Getting started screen, click the **System Management** icon.

Note: If the **Trading engine node** is not in **Running** state then click **Start**.

18.4 Test Communication

1. From the Sender Axway B2Bi Server, configure an XML file to transmit from the Sender server to the Receiver server.

Note: The file must be an E2B file that contains the correct routing IDs for the sender and the receiver.

2. Make sure that the Axway B2Bi servers on both sender and receiver are running.
3. Drop the E2B XML file into the out bound folder of the Axway B2Bi Sender server.
4. Log in to a machine where Axway B2Bi is installed.
5. From the browser, go to <http://<Sender Axway B2BiServer>:6080/ui/>.
6. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
7. In the Getting started screen, hover over the **Message Tracker** icon and select the **Message Searches > All Messages** from the menu.

From the Search results screen, verify that the transmission is in progress by locating the Custom Search section and click **Find** until Delivered appears on the screen.

Note: The system does not display this screen if it has already transmitted the file.

8. When the file is transmitted successfully, click **Logout**.
9. Go to the Axway B2Bi Receiver server and verify that the E2B file has been received.
10. To verify that the file has been transmitted:
 - a. Log in to the receiver Axway B2Bi server.
 - b. Select the All Messages option.
 - c. View the message payload.
11. Compare the E2B file on the receiving machine (payload version displayed) with the file from the sending machine.

These files should be identical.
12. To verify delivery on the Receiver Server, repeat the procedure.

Verify that the E2B XML file is configured with proper routing IDs for both the send and the receiver before dropping the file into the Axway B2Bi outbound folder.

Install and Configure Oracle B2B

You can install either Oracle B2B or Axway B2Bi for E2B reports exchange.

19.1 Install Oracle B2B

Refer to *Oracle B2B Installation Guide*.

19.2 Integrate Oracle B2B with Argus Safety

The entire integration process can broadly be categorized under the following steps:

1. Creation of integration tables in B2B Schema through provided scripts
2. Oracle B2B UI Configuration
 - a. General Configuration
 - b. Document Configuration
3. Enterprise Manager Configuration
 - a. SOA Composites Deployment
 - b. SOA Composites Configuration
4. Web Logic Console Configuration
 - a. Data Sources and JNDI Configuration
5. Large Payload Configuration
6. Configuration on Argus Safety side

19.3 Create Integration tables in B2B Schema

There are a few database objects which are created in the ESM Schema for outbound file integration as part of the Argus Safety installation. However, a few database objects need to be created in B2B Schema for inbound files integration.

After Argus Safety is installed, locate DB Script B2B_setup.bat under <Argus Install Folder>\Oracle\Argus\DBInstaller\Utilities\B2B_Setup\.

Double-click it to provide database details of B2B. This is recommended to be installed under SOA_INFRA Schema of B2B database instance.

This script creates the following database objects required to integrate incoming files data:

1. B2B_ARGUSSAFETY_INBOUND (table)

2. S_B2B_ARGUSSAFETY_INBOUND (sequence)

19.4 Configure Oracle B2B User Interface

Log in to Oracle B2B UI as an admin user.

19.4.1 General Configuration > Administration > Configuration

1. Under the **Non Purgeable** section, set **Use JMS Queue as default** to **True**.
2. Under the **Miscellaneous** section, set **Additional MIME Types** to **application/octet-stream : application/pdf**.
3. Under the **Performance** section, set **Large Payload Directory** to the desired location.
It is recommended to set it, even if large payloads are not likely to be received.

19.4.2 Document Configuration > Administration > Document

There can be one document type configured for each of the following categories, as transmitted and received from Argus Safety:

1. XML—for E2B Message and Acknowledgments
 - a. SGML files with no EDI Header and Footer are also categorized under this category.
2. Zip—for PMDA E2B Message files
3. PDF—for E2B R2 Attachments
 - a. The Zip and PDF may be combined together under one category since both are binary documents. One common doc type may be sufficient for them.
4. EDI files—for those E2B Reporting Destinations in Argus Console for which EDI Header and footer is checked. If there is no such Reporting Destination, this document type need not be created. Identification Types for EDI Files can be given as:
 - a. Identification Start Position = 1
 - b. Identification End Position = 3
 - c. Identification Value = UNB

Besides this, XML, EDI, and Binary should be created as separate document types rather than as different document definitions under one document type.

19.5 Configure Enterprise Manager

19.5.1 Deploy SOA Composite

The Argus Safety build provide the following composites to integrate Oracle B2B:

- **sca_AS_BPEL_Outbound_rev1.0.jar**—for all outbound traffic from Argus Safety
- **sca_AS_BPEL_Inbound_rev1.0.jar**—for all inbound traffic from Argus Safety

The files are available in <Install Directory>\Support\OracleB2B.

To deploy SOA composites:

1. Log in to Enterprise Manager as Admin user.
2. Locate the domain under which composites are to be deployed.
3. Right-click and select SOA Deployment > Deploy To This Partition.
4. Select the path of the JAR file and click **Next** to deploy the JAR file.
5. Repeat the above process to deploy the other JAR file.

19.5.2 Configure SOA Composite

There are certain parameters for the deployed composites which need to be modified as per the Customer Environment.

19.5.2.1 AS_BPEL_Outbound Composite

1. In the Enterprise Manager, under deployed domain, right-click AS_BPEL_Outbound and click **Service/Reference Properties**.
2. Select AS_FileAdapter.
 - a. Change PhysicalDirectory and PhysicalArchiveDirectory to the desired location.
Do not change other properties.
 - b. Argus Safety may create outbound files under the same or under any of the child directories of the above specified directory.
3. B2B_DBAdapter should NOT be changed for any of the properties.
4. B2B_JMSAdapter can be changed, but only if required.

19.5.2.2 AS_BPEL_Inbound Composite

In the Enterprise Manager, under deployed domain, right-click AS_BPEL_Inbound and click **Service/Reference Properties**.

1. Select AS_FileAdapter.
 - a. Set PhysicalDirectory as the top level folder under which all the incoming files are dropped by B2B.
Do not change other properties.
2. Select LargeFileReader.
 - a. The PhysicalDirectory should be the same as Large Payload Directory under Oracle B2B UI > Administration > Configuration > Performance section.
Do not change other properties.
3. B2B_DBAdapter should NOT be changed for any of the properties.
4. B2B_Inbound can be changed, but only if required.

19.6 Configure Web Logic Console

Log in to Web Logic Console to create the following data sources and JNDI configuration.

19.6.1 Data source with JNDI Name as 'eis/DB/ArgusSafety_Outbound'

This is hard coded JNDI Identifier being used inside AS_BPEL_Outbound SOA Composite for outbound files. This should point to a data source which has all access to the Argus Safety database table **B2B_ARGUSSAFETY_OUTBOUND** under ESM Schema. This table is available as part of the Argus Safety installation.

The configuration is validated with xADatasource property filled with a data source using database driver as 'Oracle's Driver (Thin XA) for instance connection; Version: 9.0.1 and later'.

19.6.2 Data source as 'jdbc/ArgusSafety_Inbound'

This is a hard coded data source being used inside AS_BPEL_Inbound SOA composite for inbound files. This should point to a data source which has access "all access" on the integration database table B2B_ARGUSSAFETY_INBOUND and the sequence S_B2B_ARGUSSAFETY_INBOUND. These are created as part of the script.

Besides, the same data source can be used as an underlying data source under the following:

The configuration is validated with database driver chosen as "Oracle's Driver (Thin XA) for instance connection; Version:9.0.1 and later".

19.6.3 Data source with JNDI Name as 'eis/DB/ArgusSafety_Inbound'

This is hard coded JNDI Identifier being used inside sca_AS_BPEL_Inbound_rev1.0.jar for inbound files. This should point to a data source which has access "all access" on the B2B database table B2B_ARGUSSAFETY_INBOUND and for Sequence S_B2B_ARGUSSAFETY_INBOUND created under the step above "Creation of integration tables in B2B Schema".

The data source created in the above section "jdbc/ArgusSafety_Inbound" can be used as a data source here.

The configuration is validated with xADatasource property filled with a data source using database driver as "Oracle's Driver (Thin XA) for instance connection; Version: 9.0.1 and later".

19.6.4 DB Adapters for Data Source

Navigate to Deployments > Summary of Deployments > DbAdapter > Configuration > Outbound Connection Pools, and verify that the DB Adapters are present for the data sources created in the previous sections.

Make sure that the data source name (JNDI Name) has been configured in the property 'XADatasourceName'. If not present, then create a data source with the name 'eis/DB/ArgusSafety_Outbound' and 'eis/DB/ArgusSafety_Inbound' respectively for the corresponding data sources name populated in 'XADatasourceName'.

19.7 Configure Large Payload Exchange

For B2B, a large payload is a file bigger than the configured size in B2B UI > Administration > Configuration > Performance section.

Argus Safety can send large files if E2B R2 Attachments are configured or E2B R3 or eVAERS files are exchanged. With other scenarios, generally, large payloads may not be applicable.

19.7.1 Outbound Files

Select Trading Partner > Channel > Channel Attributes > Ack Mode to be Async.

This configuration is good even if large payloads are not supposed to be exchanged.

19.7.2 Inbound Files

1. Log in to the Enterprise Manager.
2. Go to SOA > (Domain) > SOA Administration > B2B Server Properties.
3. On the right side, under the Operation tab, click **addProperty** to add a new property called **b2b.setisLargePayloadPropertyForSmallMsg** with value as **True**.
4. The Large Payload Directory configuration should be the same for B2B Web UI > Administration > Configuration > Performance section, and also for Enterprise Manager > SOA > (Domain) > AS_BPEL_INBOUND > LargeFileReader PhysicalDirectory property.

Both these configurations are required, even if large payloads are not expected to be exchanged.

19.7.3 Transaction Time

Log in to Web Logic Console > (Domain) > Services > JTA > Timeout Seconds. Set the time to 720 seconds to allow processing of large pay loads. This has been tested with 20 MB files.

This may have to be tuned if transaction time-out errors occur for the same size or larger size files.

19.7.4 General B2B Settings for Large Payloads

If required, go through other general Oracle B2B configuration for large payload, available with Oracle B2B documentation.

19.8 Configurations for Argus Safety

19.8.1 Configure Oracle B2B

1. Log in to ESM Mapping Utility as an ESM Admin user.
2. Go to Administrator Menu > Setup INI file > EDI Section.
3. Select Oracle B2B as the EDI Gateway.

The Oracle B2B database details should be provided for a User who has all access on the following:

- B2B_ARGUSSAFETY_INBOUND table (all access)
- B2B_INSTANCEMESSAGE table (read access)

19.8.2 Update for B2B Documents

Manually update document in the Argus Safety database table **B2B_ARGUSSAFETY_DOC** under ESM Schema as mentioned in Oracle B2B UI > Configuration > Document.

The following table list the sample factory data:

| Doc_ID | Doc_Type | Doc_Revision | Comments (Not a column) |
|--------|--------------|-----------------|---|
| 1 | AS_XmlDoc | ArgusSafety_1.0 | Xml for E2B Message and Acknowledgments |
| 2 | AS_BinaryDoc | ArgusSafety_1.0 | Zip for PMDA E2B Message files |
| 3 | AS_BinaryDoc | ArgusSafety_1.0 | PDF for E2B Attachments |
| 4 | AS_EDIDoc | ArgusSafety_1.0 | EDI files |

- The Admin should update only Doc_Type and Doc_Revision columns from B2B UI.
- The Doc ID column must not be updated as new Doc ID is not supported.
- the mapping between Doc ID and other columns is assumed to be exactly as provided in the sample above. For example:
 - Doc_ID = 1 should not point to Binary Docs.
 - Doc ID = 2 and Doc ID = 3 can point to the same or different doc type and doc version but neither of these should be left blank.
 - Doc_ID=4 may be left blank, if there is no Reporting Destination with EDI Header and Footer configuration.

This information is picked up by outbound SOA Composite at run time to dynamically attach Document Type and Document Version properties to outgoing file via JMS.

19.8.3 Argus Console > Reporting Destination Code List

The Company Identifier under EDI Tab should contain Name Identifier as configured in Oracle B2B UI > Partners > Trading Partner > Profile > Identifier.

Configure OBIEE or BI Publisher

The OBIEE or BI Publisher Server is needed when Flexible Aggregate Reporting (FAR) or Japanese PMDA R3 Paper Forms is generated through Argus Safety. This chapter elaborates the steps needed to integrate the OBIEE or BI Publisher with Argus Safety.

In the Argus Enterprise Edition, OBIEE or BI Publisher Server is also required for Argus Analytics and BI reporting on Argus Mart.

20.1 Prepare BI Publisher Server

To execute PMDA R3 Paper Forms or BI Publisher Periodic Reports, a standalone BI Publisher Server or BI Publisher on an OBIEE Server must be prepared.

Note: BIP Standalone Server is applicable only for the Argus Standard Edition users. The Argus Enterprise Edition users must install OBIEE integrated with BIP only.

When the BI Publisher Server/OBIEE Server is successfully installed, make a note of:

- TNS Names details of the database where BI Publisher repository is created
- BI Platform User ID and Password
- BI Publisher Console login credentials
- BI Publisher Console URL along with the Port Number

20.2 Set Up BI Publisher for Argus Safety

20.2.1 Enable a Local Superuser

BI Publisher enables you to define an administration Superuser. Using the Superuser credentials you can directly access the BI Publisher administrative functions without logging in through the defined security model. Set up this Superuser to ensure access to all administrative functions in case of failures with the configured security model. It is highly recommended that you set up a Superuser.

To enable a local superuser:

1. Click **Administration**.
2. Under **Security Center**, click **Security Configuration**.

3. Under Local Superuser, select the **Enable Local Superuser** checkbox and enter the credentials.
4. Restart the BI Publisher service.

20.2.2 Create a Database Connection

To establish a database connection with the Argus Safety database, create a new JDBC connection named **asbip** in the BI Publisher.

Note: It is recommended to provide the JDBC connection name, user name and database connection information in the lower case.

1. Log in to BI Publisher using the administrator credentials. This displays the BI Publisher Home Page.
2. Click **Administration**.
3. Click **JDBC Connection** under **Data Sources**.
This displays the **Data Sources** screen.
4. Click **Add Data Source**.
5. In the **Add Data Source** section:
 - a. Enter **asbip** in the **Data Source Name** field.
Make sure that you enter this data source name in lowercase only.
 - b. Select the database from the **Driver Type** drop-down.
This auto-populates the **Database Driver Class** field.
 - c. Enter either of the following connection strings in the **Connection String** field.
- `url="jdbc:oracle:thin:@[host]:[port]/[sid]"`
- `url="jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=host.com)(PORT=<port number>)))(CONNECT_DATA=(SID=orcl)))"`
 - d. Enter the Argus BIP schema username (for example, bip_owner) and the password.
This user is created as part of the Argus Safety database installation.
 - e. Click **Test Connection**.
If successful, this displays a confirmation message.
6. Click **Apply**. This displays the **asbip** Data Source in the list of already existing data source names.

This successfully creates a connection between BI Publisher and the Argus Safety database.

20.2.3 Set Up Runtime BI Publisher Time-out

1. Log in to BI Publisher.
2. Click **Administration**.
3. From Runtime Configuration section, click **Properties**.

4. Modify the following parameter values to **5000** seconds from 600 seconds:
 - Memory Guard > Process timeout for online report formatting
 - Data Model > SQL Query Timeout
5. Click on **Apply**.

These values can be increased as needed, for any BIP custom reports that take longer to complete.

20.2.4 Configure Oracle Fusion Middleware Security Model

Note: If you are using the BI Publisher Security model, it is recommended to move to Oracle Fusion Middleware Security model.

When moving from BI Publisher Security model, you must re-create the users, roles and policies through the Enterprise Manager.

20.3 Manage Users and Roles

20.3.1 Configure Users, Groups and Roles

This section describes the steps to create users, groups and roles in Oracle Fusion Middleware Security model (recommended security model).

In case you are using the BI Publisher Security Model, refer to [Appendix A, "Configure BI Publisher Security Model."](#)

20.3.1.1 Create a Group

Note: For detailed information, refer to section 2.5.2 *Managing Users and Groups Using the Default Authentication Provider* of <https://docs.oracle.com/middleware/1221/bip/BIPAD.pdf>.


1. Log in to Fusion Middleware Enterprise Manager.
2. Navigate to WebLogic Domain > Security > Security Realms > myrealm > Users and Groups.
3. From the Groups section, click **New**.
The Create a New Group dialog box appears.
4. Create the following groups for Flexible Aggregate Reports by entering the **Name** and **Description**:
 - FARAdminGroup
 - FARSafetyAuthorGroup
 - FARSafetyConsumerGroup
5. Create the following groups for Expedited Reports by entering the **Name** and **Description**:
 - EXPAdminGroup

- EXPSafetyAuthorGroup
- EXPSafetyConsumerGroup

20.3.1.2 Create a User

1. Log in to Fusion Middleware Enterprise Manager.
2. Navigate to WebLogic Domain > Security > Security Realms > myrealm > Users and Groups >.
3. From the Users section, click **New**.
The Create a New User screen appears.
4. Enter the parameters and click **OK**.
5. Assign a group to the user and click **Save**.

20.3.1.3 Create an Application Role

1. Log in 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, 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 **FARAdminRole**.
6. From the Members section, click **+Add**.
The Add Principal dialog box appears.
7. From the **Type** drop-down, select **Group** and click **Search**.
A list of principals appears.
8. From the list of Searched Principals, select **FARAdminGroup** and click **OK**.
9. From the Members section, click **+Add**.
The Add Principal dialog box appears.
10. From the **Type** drop-down, select **User** and click **Search**.
A list of principals appears.
11. From the list, search Users, select **Weblogic** and click **OK**.
12. Repeat from Step 4 to Step 11 to create other FAR and Expedited Reports role and add Member to these roles as listed in the table below.

Besides, make sure to add EXP Roles only for Expedited Reports (and not the FAR roles).


| Role | Application Roles |
|---------------------|-----------------------|
| FARAdminRole | FARAdminGroup |
| | Weblogic |
| FARSafetyAuthorRole | FARSafety AuthorGroup |

| Role | Application Roles |
|-------------------------|------------------------|
| | FARAdminGroup |
| FARSafetyConsumerRole | FARSafetyConsumerGroup |
| | FARSafetyAuthorGroup |
| | FARAdminGroup |
| EXPAdminRole | EXPAdminGroup |
| | Weblogic |
| EXPSafety Author Role | EXPSafetyAuthorGroup |
| | EXPAdminGroup |
| EXPSafety Consumer Role | EXPSafetyConsumerGroup |
| | EXPSafetyAuthorGroup |
| | EXPAdminGroup |

Note: For more details, refer to *Section 2.8.2.2.1 Creating Application Roles Using Fusion Middleware Control* from <https://docs.oracle.com/middleware/1221/bip/BIPAD.pdf>

20.3.2 Create Application Policies and Set Up Folder Privileges (BI Publisher Standalone only)

20.3.2.1 Create Application Policies

1. Log in 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, select **Application Role** and click **Search** .
6. From the list of Searched Principals, select **FARAdminRole** 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, 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 FAR 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:

| Policy Name/Principal | Resource Type | Resource Name | Permission Actions |
|-----------------------|--------------------------------|--|--------------------|
| FARAdminRole | oracle.bi.user | oracle.bi.user | impersonate |
| | oracle.bi.publisher.permission | oracle.bi.publisher.administerServer | _all_ |
| FARSafetyAuthorRole | oracle.bi.publisher.permission | oracle.bi.publisher.developDataModel | _all_ |
| | oracle.bi.publisher.permission | oracle.bi.publisher.developReport | _all_ |
| FARConsumerRole | oracle.bi.publisher.permission | oracle.bi.publisher.accessExcelReportAnalyzer | _all_ |
| | oracle.bi.publisher.permission | oracle.bi.publisher.accessReportOutput | _all_ |
| | oracle.bi.publisher.permission | oracle.bi.publisher.accessOnlineReportAnalyzer | _all_ |
| | oracle.bi.publisher.permission | oracle.bi.publisher.scheduleReport | _all_ |

14. Similarly, create roles and policies for Expedited Reports for the following groups:

- EXPAdminRole
- EXPSafetyAuthorRole
- EXPSafetyConsumerRole

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>

20.3.2.2 Manage Folder Privileges

To set Catalog Folder-level permissions:

1. Log in to BI Publisher application as a privileged user.
For example, log in to `http://<hostname.domainname>:<port>/xmlpserver`, as WebLogic.
2. Go to Catalog > Shared Folders > Argus Safety > Tasks > Permissions.
The Permissions dialog box appears.
3. Set the Permissions as follows and click **OK**.

| Accounts | Permissions |
|--------------------------|---|
| FAR Admin Role | Write, Delete, Run Report Online, Schedule Report, View Report Output |
| FAR Safety Consumer Role | Read, Run Report Online |
| FAR Safety Author Role | Read, Write, Delete, Run Report Online, Schedule Report, View Report Output |

Note: Make sure to select the **Apply permissions** option for the items within this folder.

4. Go to Catalog > Shared folders > AS_Expedited > Tasks > Permissions.
The Permissions dialog box appears.
5. Set the Permissions as follows and click **OK**.

| Accounts | Permissions |
|--------------------------|---|
| EXP Admin Role | Write, Delete, Run Report Online, Schedule Report, View Report Output |
| EXP Safety Consumer Role | Read, Run Report Online |
| EXP Safety Author Role | Read, Write, Delete, Run Report Online, Schedule Report, View Report Output |

Note: Make sure to select the **Apply permissions** option for the items within this folder.

6. To add the Data Sources to Roles in BI Publisher:
 - a. Log in to the BIP with Administrator credentials.
 - b. Go to Administration > Roles and Permissions.
The Roles and Permissions screen appears.
 - c. From the list of roles, select **FARAdminRole** and click the corresponding **Add Data Sources** icon.
The Add Data Sources screen appears.
 - d. From the Available Data Sources section, select **asbip** and click the **Move (>)** icon to move the **asbip** data source to the Allowed Data Sources section.
 - e. Click **Apply**.
 - f. Repeat the steps to add **asbip** data source for the following roles as well:
 - FARSafetyAuthorRole,
 - FARSafetyConsumerRole,
 - EXPAdminRole,
 - EXPSafetyAuthorRole
 - EXPSafetyConsumerRole

20.3.3 Create Application Policies and Set Up Folder Privileges (OBIEE and BI Integrated Installation only)

20.3.3.1 Create Application Policies


1. Log in to Fusion Middleware Control Enterprise Manager.
 2. Go to WebLogic Domain > Security > Application Policies.
The Application Policies screen appears.
 3. From the **Application Stripe** drop-down, select **OBI**.
 4. Click **Create**.
The Create Application Grant dialog box appears.
 5. From the Grantee section, click **+Add**.
The Add Principal dialog box appears.
 6. From the **Type** drop-down, select **Application Role** and click **Search** .
 7. From the list of Searched Principals, select **FARAdminRole** and click **OK**.
 8. From the Permissions section, click **+Add**.
The Add Permission dialog box appears.
 9. Select the **Resource Types** radio button.
 10. From the **Resource Type** drop-down, select **<Resource Type>** and click **Search**.
 11. From the Search Results, select **<Resource Name>** and click **Continue**.
The Add Permission dialog box appears.
- Note:** If the Resource Name field is blank, enter it manually.
For Principal, Resource Type, and Resource Name, see [Table 20–1](#).
12. For **Permission Actions**, select **All (_all_)** and click **Select**.
 13. When all the permissions are added, click **OK**.
 14. Repeat Steps 5-13 for other principals and their permissions. (See [Table 20–1](#))

Table 20–1 List of Policies and their Permissions

| Policy Name/Principal | Resource Type | Resource Name | Permission Actions |
|--|--|---|--------------------|
| FARAdminRole/EXPAdminRole | oracle.bi.catalog | * | manage |
| | oracle.bi.server.permission | oracle.bi.server.manageRepositories | _all_ |
| | oracle.bi.presentation.catalogmanager.permission | oracle.bi.presentation.catalogmanager.manageCatalog | _all_ |
| | oracle.bi.delivers.job | oracle.bi.delivers.job | manage |
| | oracle.bi.publisher.permission | oracle.bi.publisher.administerServer | _all_ |
| | oracle.bi.publisher.permission | oracle.bi.publisher.developReport | _all_ |
| | oracle.bi.publisher.permission | oracle.bi.publisher.developDataModel | _all_ |
| | oracle.bi.repository | oracle.bi.repository | manage |
| FARSafetyAuthorRole/EXPSafetyAuthorRole | 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_ |
| | oracle.bi.tech.visualanalyzer.permission | oracle.bi.tech.visualanalyzer.generalAccess | _all_ |
| FARSafetyConsumerRole/EXPSafetyConsumerRole | oracle.bi.delivers.job | * | schedule |
| | 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>

20.3.3.2 Manage Folder Privileges

1. Log in to the OBIEE application as a privileged user.

For example: Log in to <http://acme.oracle.com:port/analytics> with WebLogic user credentials.

2. Go to Administration > Security > Manage Privileges.
3. Add the following Catalog Roles:

Note: Do not remove any existing privileges, only append the additional privileges.

| Component | Privilege | Default Role Granted |
|----------------|--|--|
| Access | Access to Dashboards | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Access | Access to Answers | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Access | Access to BI Composer | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Access | Access to Delivers | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Access | Access to Briefing Books | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Access | Access to Mobile | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Access | Access to Administration | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Access | Access to Segments | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Access | Access to Segment Trees | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Access | Access to List Formats | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Access | Access to Metadata Dictionary | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Access | Access to Oracle BI for Microsoft Office | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Access | Access to Oracle BI Client Installer | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Access | Catalog Preview Pane UI | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Access | Access to Export | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Access | Access to KPI Builder | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Access | Access to Scorecard | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Actions | Create Navigate Actions | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Actions | Create Invoke Actions | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Actions | Save Actions containing embedded HTML | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: Catalog | Change Permissions | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |

| Component | Privilege | Default Role Granted |
|-----------------|---------------------------|--|
| Admin: Catalog | Toggle Maintenance Mode | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: General | Manage Sessions | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: General | Create Dashboards | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Admin: General | See sessions IDs | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: General | Change Log Configuration | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: General | Issue SQL Directly | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: General | View System Information | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: General | Performance Monitor | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: General | Manage Agent Sessions | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: General | Manage Device Types | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: General | Manage Map Data | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: General | See privileged errors | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: General | See SQL issued in errors | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Admin: General | Manage Global Variables | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: General | Diagnose BI Server Query | Denied: Authenticated User |
| Admin: General | Manage Marketing Jobs | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Admin: General | Manage Marketing Defaults | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: Security | Manage Catalog Accounts | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |

| Component | Privilege | Default Role Granted |
|-----------------|--|--|
| Admin: Security | Manage Privileges | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: Security | Set Ownership of Catalog Objects | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Admin: Security | User Population - Can List Users | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Admin: Security | User Population - Can List Catalog Groups | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Admin: Security | User Population - Can List Application Roles | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role, |
| Admin: Security | Access to Permissions Dialog | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Briefing Book | Add To or Edit a Briefing Book | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Briefing Book | Download Briefing Book | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Briefing Book | Add to Snapshot Briefing Book | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Catalog | Personal Storage (My Folders and My Dashboard) | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Catalog | Reload Metadata | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Catalog | See Hidden Items | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Catalog | Create Folders | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Catalog | Archive Catalog | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Catalog | Unarchive Catalog | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Catalog | Upload Files | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Catalog | Perform Global Search | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Catalog | Perform Extended Search | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Conditions | Create Conditions | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Dashboards | Save Customizations | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |

| Component | Privilege | Default Role Granted |
|-----------------|---------------------------------------|--|
| Dashboards | Assign Default Customizations | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Dashboards | Create Bookmark Links | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Dashboards | Create Prompted Links | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Dashboards | Export Entire Dashboard To Excel | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Dashboards | Export Single Dashboard Page To Excel | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Formatting | Save System-Wide Column Formats | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Home and Header | Access Home Page | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Home and Header | Access Catalog UI | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Home and Header | Access Catalog Search UI | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Home and Header | Access Rapid Search UI | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Home and Header | Simple Search Field | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Home and Header | Advanced Search Link | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Home and Header | Open Menu | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Home and Header | New Menu | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Home and Header | Help Menu | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Home and Header | Dashboards Menu | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Home and Header | Favorites Menu | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Home and Header | My Account Link | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Home and Header | Custom Links | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| 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 | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| My Account | Change Preferences | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |

| Component | Privilege | Default Role Granted |
|------------|--|--|
| My Account | Change Delivery Options | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Answers | Create Views | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Answers | Create Prompts | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Answers | Access Advanced Tab | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Answers | Edit Column Formulas | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Answers | Save Content with HTML Markup | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Answers | Enter XML and Logical SQL | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Answers | Edit Direct Database Analysis | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Answers | Create Analysis From Simple SQL | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Answers | Create Advanced Filters and Set Operations | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Answers | Save Filters | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Answers | Save Column | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Answers | Add EVALUATE_PREDICATE Function | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Answers | Execute Direct Database Analysis | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Answers | Upload Images | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Delivers | Create Agents | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Delivers | Publish Agents for Subscription | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Delivers | Deliver Agents to Specific or Dynamically Determined Users | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Delivers | Chain Agents | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Delivers | Modify Current Subscriptions for Agents | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Proxy | Act As Proxy | Denied: Authenticated User |
| RSS Feeds | Access to RSS Feeds | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |

| Component | Privilege | Default Role Granted |
|--------------|--|--|
| Scorecard | Create/Edit Scorecards | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Scorecard | View Scorecards | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Scorecard | Create/Edit Objectives | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Scorecard | Create/Edit Initiatives | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Scorecard | Create Views | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Scorecard | Create/Edit Causes And Effects Linkages | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Scorecard | Create/Edit Perspectives | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Scorecard | Add Annotations | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Scorecard | Override Status | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Scorecard | Create/Edit KPIs | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Scorecard | Write Back to Database for KPI | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Scorecard | Add Scorecard Views To Dashboards | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| List Formats | Create List Formats | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| List Formats | Create Headers and Footers | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| List Formats | Access Options Tab | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| List Formats | Add/Remove List Format Columns | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Segmentation | Create Segments | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Segmentation | Create Segment Trees | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Segmentation | Create/Purge Saved Result Sets | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Segmentation | Access Segment Advanced Options Tab | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Segmentation | Access Segment Tree Advanced Options Tab | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Segmentation | Change Target Levels within Segment Designer | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |

| Component | Privilege | Default Role Granted |
|-----------|---|---|
| Mobile | Enable Local Content | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| Mobile | Enable Search | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access SOAP | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Impersonate as system user | BI System |
| SOAP | Access MetadataService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access ScorecardAssessmentService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access MsgdbService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access ReportEditingService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access KPIAssessmentService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access ConditionEvaluationService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access SecurityService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access Tenant Information | BI System |
| SOAP | Access SchedulerService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access DashboardService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access ScorecardMetadataService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access JobManagementService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access CatalogIndexingService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access UserPersonalizationService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access AnalysisExportViewsService Service | BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role |

| Component | Privilege | Default Role Granted |
|-------------------------|--|---|
| SOAP | Access CatalogService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access AdministrationSOAPService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access HtmlViewService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access XmlGenerationService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| SOAP | Access IBotService Service | BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role |
| View Canvas | Add/Edit Canvas View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Column Selector | Add/Edit Column Selector View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Compound Layout | Add/Edit Compound Layout View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Contribution Wheel | Add/Edit Contribution Wheel View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Graph | Add/Edit Graph View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Funnel | Add/Edit Funnel View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Gauge | Add/Edit Gauge View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Micro Chart | Add/Edit Micro Chart View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Filters | Add/Edit Filters View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Dashboard Prompt | Add/Edit Dashboard Prompt View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Performance Tile | Add/Edit Performance Tile View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Heat Matrix | Add/Edit Heat Matrix View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Static Text | Add/Edit Static Text View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Javascript view | Edit Javascript View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Legend | Add/Edit Legend View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Map | Add/Edit Map View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Narrative | Add/Edit Narrative View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |

| Component | Privilege | Default Role Granted |
|--------------------------|-----------------------------------|--|
| View No Results | Add/Edit No Results View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Pivot Table | Add/Edit Pivot Table View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Generic Plugin View | Add/Edit Generic Plugin View View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Report Prompt | Add/Edit Report Prompt View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Create Segment | Add/Edit Create Segment View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Selection Steps | Add/Edit Selection Steps View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Logical SQL | Add/Edit Logical SQL View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Table | Add/Edit Table View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Create Target List | Add/Edit Create Target List View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Ticker | Add/Edit Ticker View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Title | Add/Edit Title View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Treemap | Add/Edit Treemap View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View Trellis | Add/Edit Trellis View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| View View Selector | Add/Edit View Selector View | BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role |
| Write Back | Manage Write Back | BI Service Administrator, EXP Administrator Role, FAR Administrator Role |
| Write Back | Write Back to Database | Denied: Authenticated User |

4. To set Catalog Folder-level Permissions:

- a. Log in to Analytics with WebLogic user credentials.
For example, Log in to *http://acme.oracle.com:port/analytics*.
- b. Go to Catalog > Shared Folders > Tasks > Permissions.
The Permissions dialog box appears.
- c. To set the permissions, select **Apply Permissions** to sub-folders, select **Permission to items within folder**, and click **OK**.

| Accounts | Permissions |
|---|--------------|
| FAR Administrator Role/EXP Administrator Role | Full Control |
| FAR Safety Author Role/EXP Safety Author Role | Full Control |

| Accounts | Permissions |
|---|---------------------------|
| FAR Safety Consumer Role/EXP Safety Consumer Role | Open (Read, and Traverse) |
| BI Service Administrator (Owner) | Full Control |

5. To add the Data Sources to Roles in BI Publisher:
 - a. Log in to the BIP with Administrator credentials.
The BIP home page appears.
 - b. Go to Administration > Roles and Permissions.
The Roles and Permissions screen appears.
 - c. From the list of roles, select **FARAdminRole** and click the corresponding **Add Data Sources** icon.
The Add Data Sources screen appears.
 - d. From the Available Data Sources section, select **asbip** and click the **Move (>)** icon to move the **asbip** data source to the Allowed Data Sources section.
 - e. Click **Apply**.
 - f. Repeat the steps to add **asbip** data source for the following roles as well:
 - FARSafetyAuthorRole
 - FARSafetyConsumerRole
 - EXPAdminRole
 - EXPSafetyAuthorRole
 - EXPSafetyConsumerRole

20.4 Upload BI Publisher Reports

20.4.1 Flexible Aggregate Reports

To upload the **Argus Safety.xdrz** file to BI Publisher, execute the following steps:

1. Copy the Argus Safety.xdrz file from the following location on the Argus Safety Web Server to the local file system:
<Argus Install Media>\SUPPORT\BIP
2. Log in to BI Publisher using BI Admin User credentials.
3. From the left pane, click **Catalog**.
This displays the **Catalog** screen with the **Folders** and **Tasks** sections.
4. Click **Shared Folders** under **Folders**.
5. Click **Upload** under **Tasks**.
This displays the **Upload** dialog box.
6. Click **Browse** and navigate to the location where you have saved the **Argus Safety.xdrz** file on the local file system.

7. Click **Upload**. When done, an **Argus Safety** folder is created in **Shared Folders**.
8. Expand the **Argus Safety** folder to verify whether the data model and reports are present.

To set permissions for Argus Safety Shared Folders:

1. Log in to Analytics.
2. Go to Shared folders > Argus Safety > Tasks > Permissions.
The Permissions dialog box appears.
3. To set the permissions, select **Apply Permissions** to sub-folders, select **Permission to items within folder**, and click **OK**.

| Accounts | Permissions |
|---|---|
| FAR Administrator Role/EXP Administrator Role | Full Control |
| FAR Safety Author Role/EXP Safety Author Role | Full Control |
| FAR Safety Consumer Role/EXP Safety Consumer Role | Custom (Read, Traverse, Run Publisher Report, Schedule Publisher Report, and View Publisher Output) |
| BI Service Administrator (Owner) | Full Control |

20.4.2 PMDA R3 Paper Reports

For the Expedited Reports, log in to BI Publisher with WebLogic user credentials, and upload the AS_Expedited.xdrz file.

The steps to upload the file remains the same as [Section 20.4.1, "Flexible Aggregate Reports"](#).

20.5 Integrate Argus Safety with BI Publisher

20.5.1 Configure AG Service

1. Log in to the server that hosts the AGService and the Batch Periodic Reports process.
2. Navigate to the ArgusInstallPath in the filesystem.
3. Open the file AGProc.exe.config for editing.
4. Navigate to the <system.serviceModel> tag in this file.
5. In the endpoint element that lies within the client element, enter the following text in the Address attribute:

http://<host>:<port>/xmlpserver/services/v2/SecurityService where the *name* attribute is set to *SecurityService*

http://<host>:<port>/xmlpserver/services/v2/ScheduleService where the *name* attribute is set to *SchedulingService*

http://<host>:<port>/xmlpserver/services/v2/ReportService where the *name* attribute is set to *ReportService*

In the above instances, <host> refers to the IP address or the Fully Qualified Domain name of the BI Publisher server and <port> refers to the BI Publisher port number.

If the BI Publisher Server has been configured over an OAM/SSO controlled port, then that port number to be used here.

20.5.2 Configure Web Service (Expedited Reports only)

1. Log in to the Argus Safety Web Server.
2. Navigate to the ArgusInstallPath in the filesystem.
3. Open the file Argusvr2.exe.config for editing.
4. Navigate to the <system.serviceModel> tag in this file.
5. In the endpoint element that lies within the client element, enter the following text in the Address attribute:

http://<host>:<port>/xmlpserver/services/v2/SecurityService where the *name* attribute is set to *SecurityService*

http://<host>:<port>/xmlpserver/services/v2/ScheduleService where the *name* attribute is set to *SchedulingService*

http://<host>:<port>/xmlpserver/services/v2/ReportService where the *name* attribute is set to *ReportService*

In the above instances, <host> refers to the IP address or the Fully Qualified Domain name of the BI Publisher server and <port> refers to the BI Publisher port number.

If the BI Publisher Server has been configured over an OAM/SSO controlled port, then that port number to be used here.

20.5.3 Add AG Service user to BI Publisher (Expedited Reports only)

This section is applicable for Expedited Reports only.

To auto-schedule the Expedited Reports through AG Services:

1. Navigate to the Argus Safety Transaction Server.
2. Open the AG Proc and note down the AG Service user, which is used for Batch Report Generation Service.
3. Create the same user (AG Service user) in the BI Publisher.

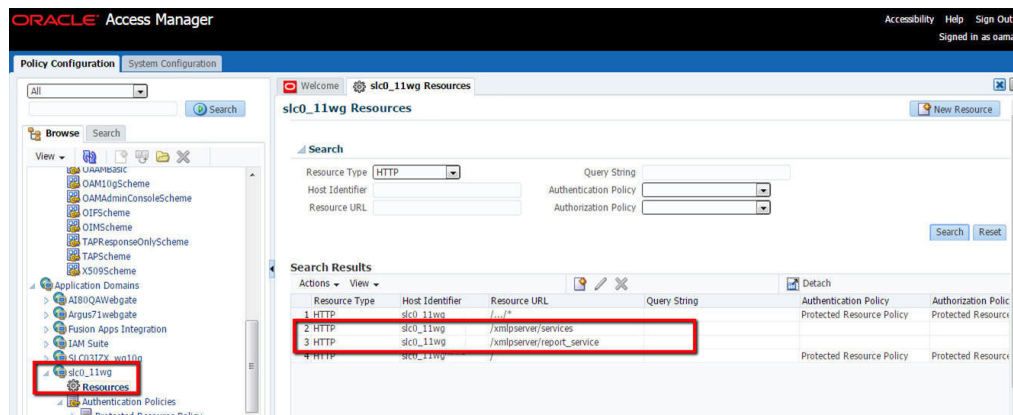
20.5.4 Update SSO Exclusion List

If SSO is enabled, exclude the following URLs from SSO:

- *http://<host>:<port>/xmlpserver/services/v2/ScheduleService* where the *name* attribute is set to *SchedulingService*
- *http://<host>:<port>/xmlpserver/services/v2/SecurityService* where the *name* attribute is set to *SecurityService*
- *http://<host>:<port>/xmlpserver/services/v2/ReportService* where the *name* attribute is set to *ReportService*

If OAM is the SSO being used, perform the following configuration:

1. Add excluded resource (/xmlpserver/services and /xmlpserver/report_service) on OAM Server for the OBIEE/BIP server application domain.



2. Copy mod_osso.conf from the disabled directory to the moduleconf directory for editing. For example:

From: ORACLE_INSTANCE/config/OHS/<ohs_name>/disabled/mod_osso.conf

To: ORACLE_INSTANCE/config/OHS/<ohs_name>/moduleconf/

3. Add the following Web services in the mod_osso.conf file:

```
<Location /xmlpserver/services/>
require valid-user
AuthType Basic
Allow from All
Satisfy any
</Location>
```

4. Save the file and restart OHS Service.

20.6 Argus Console—BIP Common Settings

20.6.1 Configure BIP Reporting Admin User

1. Navigate to Argus Console > System Configuration > System Management (Common Profile Switches).
2. Expand the **Reporting** node on the tree that appears on the left pane.
3. Click **BIP Reporting**.
4. In **Common Settings** section, enter the BIP Common username and password.
This user is created in BI Publisher with administrator privileges. This user could be an actual Argus Safety user or a user who has No Access to Argus Safety.
5. Save the changes.

20.6.2 Enable BIP Aggregate Reports and Configure Persistence Data (Flexible Aggregate Reporting only)

1. Navigate to Argus Console > Enabled Modules.
2. Enable the **BIP Aggregate Reports** module.

3. Navigate to **Argus Console > System Configuration > System Management (Common Profile Switches)**.
4. Expand the **Reporting** node on the tree that appears on the left pane.
5. Click **BIP Reporting**.
6. Set the Persist data in BIP Aggregate Temp tables to **Yes** or **No**.
The default value is **No**.
7. Set the Number of days to persist the BIP Aggregate Temp table data. Defaulted to null.
8. Perform **iisreset** on Webserver to make sure that the changes made to enable the BIP Aggregate Reports module are visible in the periodic report configuration.

Note: The Persist data parameters are used to logically retain the data from the BIP temp tables and purge them after the specified number of days.

20.6.3 Configure Code Lists

20.6.3.1 Flexible Aggregate Reporting Code Lists

The REPORT_TEMPLATE Code list to be updated for executing Flexible Aggregate Reports through BI Publisher. Execute the following steps to configure the REPORT_TEMPLATE code list.

1. Navigate to **Argus Console > Code Lists > Flexible Data Re-categorization**.
2. Under the **Flexible Data Re-categorization** tree, navigate to **Flexible Re-categorization**.
3. Select the **Code List Name** as **REPORT_TEMPLATE** and click **Search**.
4. Update the **REPPATH** as follows:
 - For PBRER - /Argus Safety/PBRER/Reports/pbrer.xdo
 - For PMAR - /Argus Safety/PMAR/Reports/pmar.xdo
 - For DSUR - /Argus Safety/DSUR/Reports/dsur.xdo
5. Click **Save**.

Note: As the REPPATH is case sensitive, in Unix based Operating System, it must be same as that provided in Report.

For example, in PBRER > Code List, the REPPATH is */Argus Safety/PBRER/Reports/pbrer.xdo*

The same path must be provided in the Reports and vice-versa.

20.6.3.2 PMDA R3 Paper Forms Code lists

1. Navigate to **Argus Console > Code Lists > Flexible Data Re-categorization**.
2. Under the **Flexible Data Re-categorization** tree, navigate to **Flexible Re-categorization**.

3. Select the **Code List Name** as **LM_REPORT_FORMS_EXPEDITED**, and click **Search**.
4. Check the **REPPATH** that is pre-configured with the report path of all the PMDA reports.

Note: Update this REPPATH only if the PMDA R3 reports are uploaded to a different folder than the one that is configured.

20.7 Configure Flexible Aggregate Reporting Database

Note: This section is applicable only if Flexible Aggregate Reporting is enabled.

Some database configurations need to be handled in order to enable the Flexible Aggregate Reporting in Argus. These steps need to be handled from a machine where the Argus database can be accessed (preferably the Argus Safety Web Server or the Argus Safety Transaction Server).

20.7.1 Execute Argus_BIP_Enable

1. From the command prompt, navigate to *<Argus Release Media>\DBInstaller\Utilities\BIP_Enable*.
2. Execute the batch file **Argus_BIP_Enable.bat**.
3. Enter the following parameters:
 - a. TNSNAMES entry to connect to the Argus Safety database
For example, Argus Safety database SID.
 - b. SYSTEM or DBA user name in Argus database
 - c. Password for SYSTEM or DBA user
 - d. Argus schema owner name
For example: ARGUS_APP.
 - e. Argus schema password
 - f. BI Publisher Schema user
The BI Publisher Schema owner name created during the Argus Safety database installation. For example, BIP_OWNER.
 - g. Password for the BIP Schema user
 - h. BIP Repository Service name
This is the database SID of the BI Publisher metadata repository.
 - i. BIP Repository user name (Default DEV_BIPLATFORM)
This is the BIPLATFORM user created in BI Publisher metadata repository.
 - j. BIP Repository password
 - k. Host name of the BIP Repository instance
For example, <hostname>.<domain name>

I. BIP Repository instance listener port

When the execution is complete, the database objects needed for enabling and integrating the Flexible Aggregate Reporting are created

Note: If you are using Argus Mart with BI Publisher enabled in Argus Safety, make sure that you re-create the Safety RO user.

20.8 Upgrade BIP Reports to 8.2.2

If you have enabled the Argus Flexible Aggregate Reporting and you are upgrading from 8.1, 8.1.1, 8.1.2, or 8.1.3:

Note: You can upgrade BIP reports only from Argus Safety 8.1. Upgrade from previous versions of Argus Safety is not supported. Besides, any customization done to the Aggregate Reports must be taken care after upgrading.

1. For BI Publisher Flexible Aggregate Reporting, repeat the instructions of [Section 20.7.1, "Execute Argus_BIP_Enable"](#) to recreate the AS_TO_BIPREP DB link.

Note: Skip this step, if you are using ONLY PMDA R3 Paper reports.

2. Log in to the BI Publisher console as administrator (or any user who has BI Admin User access).
3. Back up the existing .xdrz files.
 - a. From the left pane, click **Catalog**.
The Catalog screen with the Folders and Tasks sections appears.
 - b. Click Folders > **Shared Folders**.
 - c. Click Tasks > **Download**.
 - d. Click **Browse** and navigate to the location where the backup will be saved.
4. To upload the latest xdrz files (Argus Safety.xdrz and AS_Expedited.xdrz), see [Section 20.4.1, "Flexible Aggregate Reports"](#).
While uploading, click **Overwrite existing files**.

Configure the BIP Environment for Argus Insight

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.

21.1 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.

21.2 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.

21.2.1 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.

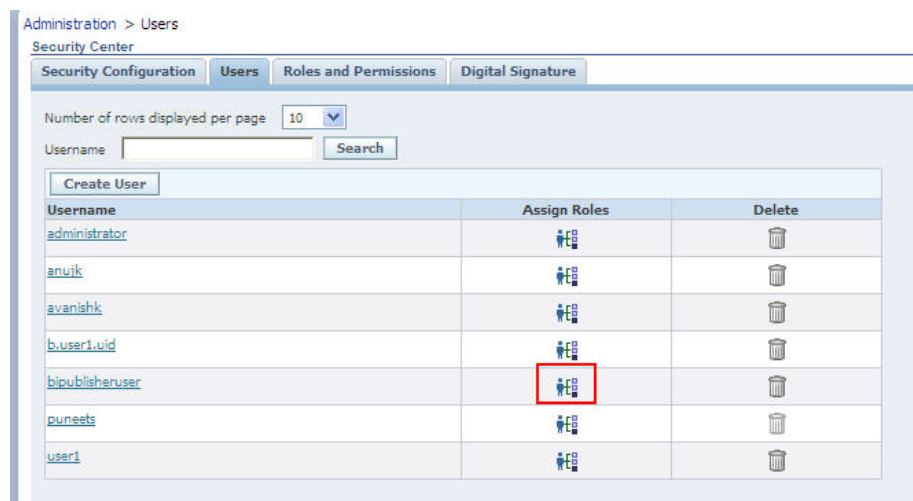
6. In the **Password** field, enter the password.

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 21.2.2, "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 21.4, "Configure BIP Users and Roles: Oracle Fusion Middleware Security Model"](#).

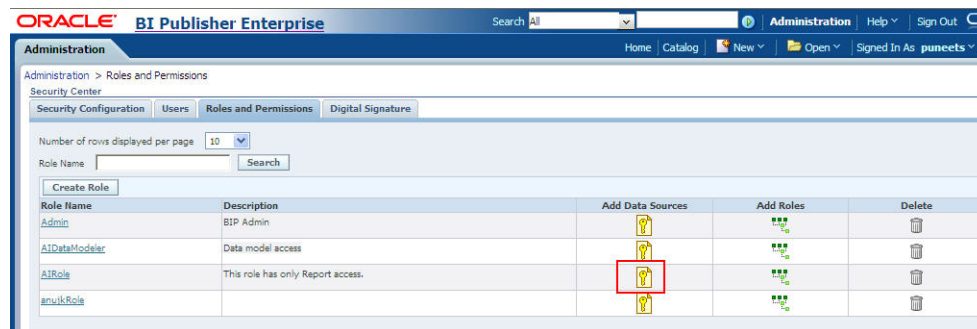
21.2.2 Create Roles, Add Data Sources, and Assign Roles

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.

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



The Add Data Sources screen appears.

- From Available Data Sources section, select **PRMART**, and click **Move(>)** to move it to the Allowed Data Sources section.
- Click **Apply** to save the changes.

The Roles and Permissions screen appears.

See [Section 21.1, "Create PRMART JDBC Connection"](#) for the steps to create the JDBC connection.

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

The Add Roles screen appears.

- 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.
- 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 21.4, "Configure BIP Users and Roles: Oracle Fusion Middleware Security Model"](#).

21.3 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.

21.3.1 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 21.4, "Configure BIP Users and Roles: Oracle Fusion Middleware Security Model"](#).

21.3.2 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.

21.3.2.1 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>.

21.3.2.2 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>.

21.3.3 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.

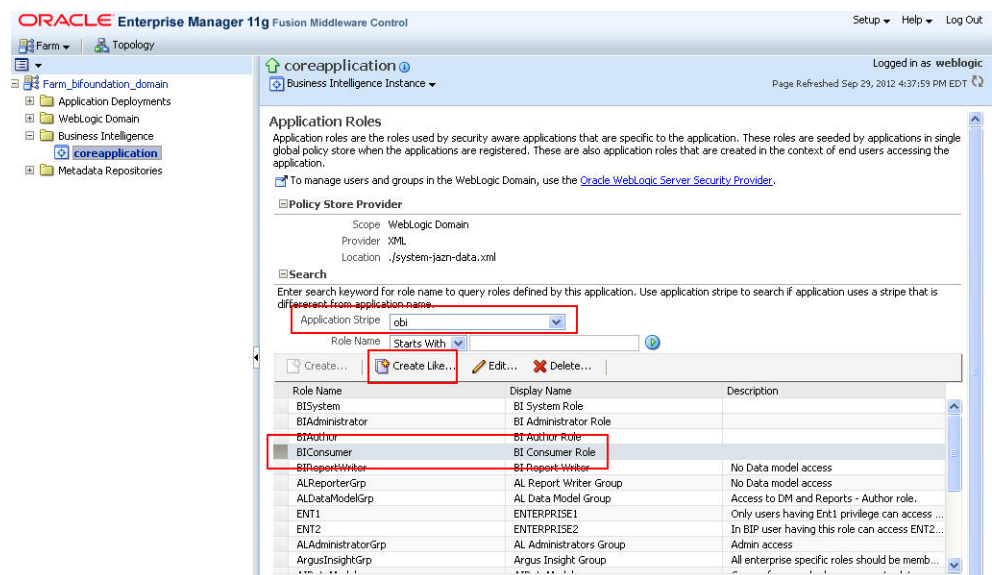
2. In the left pane, expand the **Business Intelligence** folder, and click **coreapplication**.

The Coreapplication screen appears in the right pane.

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

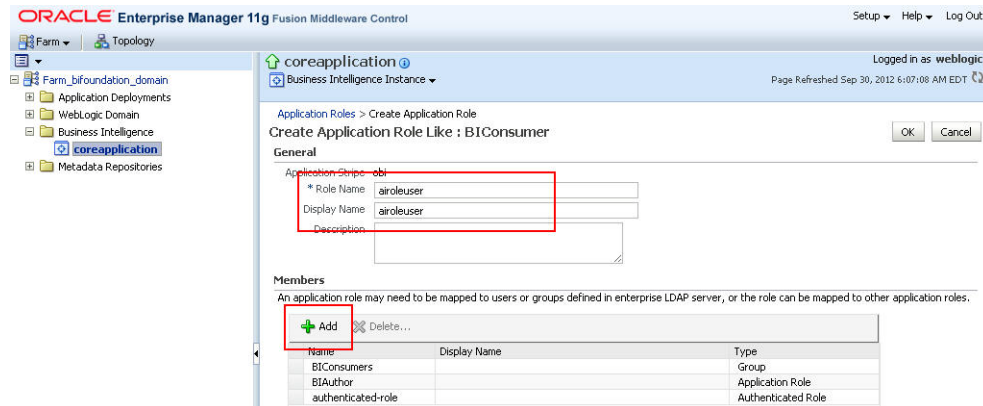
The Application Roles screen appears.

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 21.4, "Configure BIP Users and Roles: Oracle Fusion Middleware Security Model"](#).

21.3.4 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.

21.3.5 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 release media to the local file system:
<Argus Install Media>\SUPPORT\BIP
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. Navigate to Shared Folders > Argus Insight > General > Reports > Remove/Delete Generic Line Listing Report – LE.
6. From Folders section in the left pane, click **Shared Folders**.
7. From Tasks section in the left pane, click **Upload**.

The Upload dialog box appears.

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

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

10. 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 **RTF** format exists in the **Reports** sub-folder.

21.4 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 21.2, "Manage Users and Roles: BI Publisher Standalone Installation with BI Publisher Security"](#) and [Section 21.3, "Manage Users and Roles: BI Publisher Standalone Installation with OFM Security"](#).

Table 21–1 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 | <p>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.</p> <p>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.</p> |
| Users | <p>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.</p> <p>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.</p> |

Table 21–1 (Cont.) Configuring BIP Users: Oracle Fusion Middleware Security Model

| User | Description |
|--------------------|--|
| 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). |

21.4.1 Configure BIP Roles

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

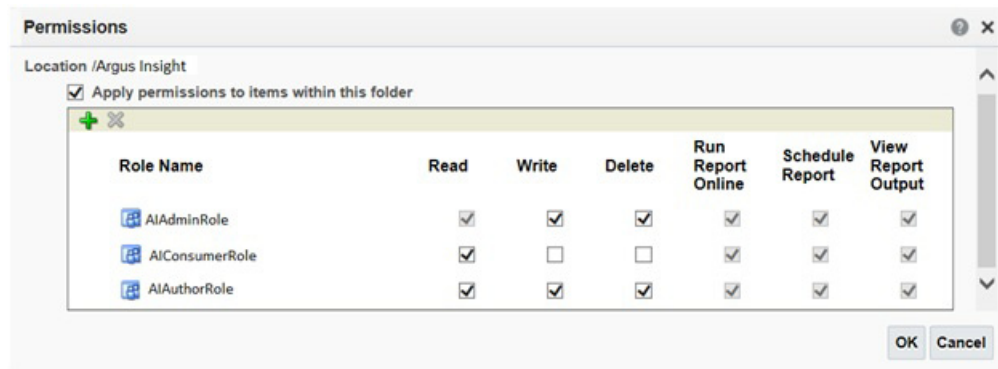
Table 21–2 Configuring BIP Roles

| 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 |

21.4.2 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 |

Configure the OBIEE Environment for Argus Insight

22.1 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*.

22.2 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.

22.2.1 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:\ai822\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 22.6, "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 B, "Create ODBC Connection for OBIEE Administration Tool for Argus Insight."](#)

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 22.4, "Create Users and Groups in OBIEE"](#))
5. Go to Catalog, and set the folder level permissions for the OBIEE Groups. (See [Section 22.5, "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 22.6, "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.

22.2.2 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 22.4, "Create Users and Groups in OBIEE"](#))
7. Go to Catalog, and set the folder level permissions for the OBIEE Groups. (See [Section 22.5, "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 22.6, "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.

22.3 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 22.4.1, "Create Users and Groups in WebLogic Server."](#)).
15. Create Roles and policies manually in Enterprise Manager. (See [Section 22.4.2, "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 22.6, "OBIEE Default Application Roles."](#)
18. Go to Catalog, and set the folder level permissions for the OBIEE Groups. (See [Section 22.5, "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

22.4 Create Users and Groups in OBIEE

22.4.1 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**.

22.4.2 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 22.3, "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.catalogmanager.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 | * |
| AI Consumer Role | oracle.bi.delivers.job | * | schedule |
| | 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 22.6, "OBIEE Default Application Roles."](#)

22.5 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\bi\data\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**.

22.6 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 |

Install Argus Unblinding

23.1 Prerequisites

1. [Set Up Argus Middle and Client Tiers.](#)
2. [Install or Upgrade Argus Database Tier.](#)
3. Tablespace with free space of 500 MB on the Database Server to create Argus Unblinding schema.
4. (Optional) To enable the audit trail, set the INIT.ORA parameters as AUDIT_TRAIL=DB.

23.2 Install Argus Unblinding Utility

Note: When Argus Unblinding is installed alone, you must provide a temporary path and update the Argus.ini 'UploadedLetters' parameter. This parameter uses this same path that is entered as the temporary path.

1. Log in as the Administrator on the system where Argus Safety is being installed.
2. Copy the installation package to the local directory of the target machine.
3. Open the Argus Safety folder and click **setup.exe**.
4. In the Argus Suite Solution Components Installation Wizard, click **Next**.
5. Enter the User Name and Company Name, and click **Next**.
6. In the Argus Suite Solution Components screen, select **End of Study Unblinding Module** and click **Next**.
7. In the Setup Completed dialog box, click **Finish**.
8. You can now run the Argus Unblinding Interface utilities.
9. To set up the Argus Cryptography Key, refer to the section [Section 26.1.3, "Argus Safety Application Servers"](#).

Configure Argus Centralized Coding

You must execute the following batch files to set up the Argus Centralized Coding Interface schema and to migrate encoded terms for all cases to the Interface schema.

24.1 `setup_centralized_coding_interface_schema.bat`

This batch file creates the schema objects for the Argus Centralized Coding Interface schema.

This script also updates the coding status field with the current status for existing cases for the following fields. The code status fields displays whether all events are encoded and are in a coding state or if the case has items that can be coded but are not coded.

- LM_LAB_TEST_TYPES.CODE_STATUS
- LM_LABELED_TERMS.CODE_STATUS
- LM_PRODUCT.IND_CODE_STATUS
- CASE_EVENT.CODE_STATUS
- CASE_DEATH_DETAILS.CAUSE_CODE_STATUS
- CASE_PROD_INDICATIONS.IND_CODE_STATUS
- CASE_PAT_HIST.ITEM_CODE_STATUS
- CASE_ASSESS.DIAGNOSIS_CODE_STATUS

To execute the batch file:

1. Double-click the `setup_centralized_coding_interface_schema.bat` file and enter:
 - a. Log folder name
 - b. Database name
 - c. DBA user credentials, such as system and password
 - d. RLS schema owner name and password

Execute the following query to get the RLS schema owner name:

```
SELECT owner
FROM all_objects
WHERE object_name = PKG_RLS AND object_type = PACKAGE;
```

- e. Argus schema owner name, such as ARGUS_APP and password
- f. Argus Safety role name

The script creates two users, ARGUS_DMS and DMS_LOGIN, and their tablespaces.

The Interface schema object is present in the ARGUS_DMS schema.

2. Enter the following:
 - a. Password for user ARGUS_DMS.
 - b. Password for user DMS_LOGIN.
 - c. Temporary tablespace name.

If no input is provided, TEMP tablespace is taken by default.

The script creates two tablespaces: DMS_DATA_01.DBF, and DMS_INDEX_01.DBF.
 - d. Path and data file name of the tablespaces, such as:

C:\APP\ORADATA\DBNAMD\DMS_DATA_01.DBF

C:\APP\ORADATA\DBNAMD\DMS_INDEX_01.DBF
 - e. A log file name
3. Press Enter when the Users and Roles are located.
4. Check the log file to validate the successful completion of the script.
5. Log in to the application and enable the Centralized Coding module.

Configure Centralized Coding from the dictionary selection page in the Console.

24.2 dms_migration.bat

Execute this script to populate the already encoded terms from all cases to the Interface schema table. This script supports two types of migration:

- [Single Enterprise Migration in One Execution](#)
- [All Enterprise Migration in One Execution](#)

24.2.1 Single Enterprise Migration in One Execution

To migrate encoded terms for case data for a particular enterprise, enter an enterprise_id such as 1.

24.2.2 All Enterprise Migration in One Execution

When you have multiple enterprises in the Argus Safety multi-tenant environment:

- To migrate encoded terms of case data for one enterprise only, enter only one enterprise_id such as 1 when prompted.
- To migrate encoded terms of case data for all enterprises in one go, enter input as ALL when prompted.
- To migrate encoded terms of case data for some enterprises (but not all), the number of executions of *dms_migration.bat* = Migration of encoded terms of case data for the number of enterprises.

Note: This migration script does not check whether the Argus Centralized Coding module is enabled for any specific enterprise. You must verify that module is enabled and then migrate data for enterprises.

To populate terms to the Interface table, you must load MedDRA into the Argus schema.

The migration script populates already encoded terms from all cases to the Interface table. Any open cases in the application are processed during migration.

Execute the batch file **dms_migration.bat** and enter the following:

1. Log folder name
2. Log file name
3. TNSNAMES of the Argus Safety database when the Interface schema was created
4. Argus Safety schema owner name and password
5. Based on whether you want to migrate coded terms for all cases, one enterprise or for multiple enterprises:
 - i. Enter the `enterprise_id` of one enterprise to migrate data for that particular enterprise.
 - ii. Enter ALL as Input to migrate data for all enterprises.
 - iii. To migrate coded terms of cases for more than one enterprise, execute step (i) multiple times and provide different `enterprise_ids`.
6. Application user name

If no input is provided, *admin* is taken as user input.
7. Check the log file to validate successful completion of the script.

Extract, Transform, and Load Data

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

25.1 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.

25.2 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 **Oracle > Argus Insight**, and then select **Insight ETL 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 Insight ETL 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 25.2.3, "Stop the Execution of ETL."](#)

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

25.2.1 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

25.2.2 Close the Initial ETL Status Dialog Box

1. Click **Close**.

A message to confirm that you want to close the Insight ETL Tool application appears.

2. Click **OK**.

25.2.3 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 Insight ETL Tool application, click **Close**.

25.3 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.

25.4 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:

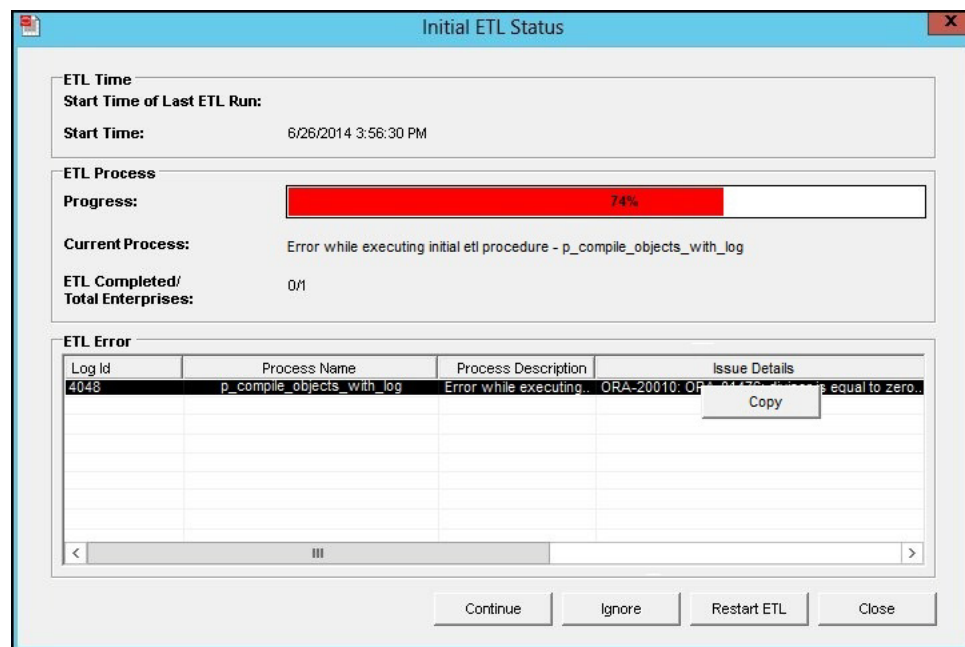
- To continue the failed Initial ETL process, click **Continue**.
- To ignore the failed Initial ETL process, click **Ignore**.
- For ETL Data Exclusion, click **Modify Attributes**, if PRE_REQ_CHECK_FLAG switch is set to ABORT.

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

25.4.1 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.



- 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.
- Click **OK**.
The ETL process continues (if no errors are found).

25.4.2 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).

25.4.3 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.

25.5 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**.

Part V

Secure Oracle Argus

Argus Password Management—Cryptography Tool

Argus Safety uses dynamically generated encryption keys for passwords within the system. The Cryptography Key Editor allows you to generate a dynamic key and then encrypt passwords using the said key. The generated key must be installed on each application server and must be common to allow all servers to communicate with the Argus Safety database.

The key is stored in the ArgusSecureKey.ini file located in the .\Windows folder.

IMPORTANT: During a new environment installation, a key will need to be generated **prior to** creating a database.

During an upgrade, a key will need to be generated prior to upgrading or an existing key from the existing setup can be used to perform the database upgrade. Make sure that the password information specified in the database is consistent with the information provided in the ArgusSecureKey.ini file.

Note: When the ArgusSecureKey.ini file is generated, there is no need to run this tool again while launching the Argus Crypto Tool. The tool should only be run again if you are resetting passwords, keys or have lost the ArgusSecureKey.ini file.

When the key file is created, copy it to the .\Windows folder on all application servers (web, transaction, etc.).

Note: Do not run the Cryptography Key Editor on each application server to generate passwords. It need only be run once during the initial system setup. Subsequent server installations must have the key manually copied to each .\Windows folder.

26.1 Install or Upgrade to Argus Safety 8.2.2

Whether you are upgrading to Argus Safety 8.2.2 or installing a fresh instance of it, you must generate new key using the Cryptography Key Editor.

Recommendation: Install the Argus Crypto Tool and Argus Insight Crypto Tool on the Transaction Server.

26.1.1 Generate New Cryptography Key

You must generate the ArgusSecureKey.ini key file before running the Argus Crypto Tool.

1. Launch the **Cryptography Key Editor**.
The Key Editor Utility screen appears.
2. Click **New**.
The Generate Key screen appears.
3. In the **Note to be added as comment** field, enter a comment that will be saved in the ArgusSecureKey.ini.
This can be any form of metadata, such as the reason why this key was generated or for what environments it is used.
4. Enter ARGUSUSER password and Confirm password.
5. (Optional) Enter APR_USER password and Confirm password.
This field applies to the Argus Insight user. If Argus Insight is not installed along with Argus Safety, leave this field blank.
6. Click **OK**.
The ArgusSecureKey.ini file is created in the *<Install folder>\CryptoKeyEditor\output\<DateTimeStamp>*.
7. Click the link in the **Argus Secure Key Path** dialog box to open the folder in Windows Explorer.
8. Click **Close, I will copy it manually** and copy the file manually from the window that gets opened by clicking on the link mentioned above.
9. To move the generated ArgusSecureKey.ini file to the *.\Windows* folder, click **Copy to windows folder**.

26.1.2 Argus Safety Database

Run the Argus Crypto Tool to create or upgrade the database. If you run the Argus Crypto Tool before creating the key, a warning message appears that the cryptography key is required.

26.1.3 Argus Safety Application Servers

After the application servers are set-up:

1. From the server where the database is created or upgraded, go to the *.\Windows* folder, and copy the **ArgusSecureKey.ini** file.
2. Paste this file in the *.\Windows* folder of each installed application server.

26.2 Reset Password or Change the Cryptography Key

26.2.1 Reset the ARGUSUSER Password

If the password for the database user ARGUSUSER has changed, you will need to reset the password in the ArgusSecureKey.ini file on all the servers.

1. Launch the **Cryptography Key Editor**.
The Key Editor Utility screen appears.
2. Click **Existing**.
The Key Editor Login or Re-encrypt ARGUSUSER screen appears.
3. Enter the ARGUSUSER password.
4. Enter the APR_USER password.
This field appears only when you have installed Argus Insight along with Argus Safety.
5. Enter the database name.
6. Click **Re-encrypt**.
A confirmation dialog appears.
7. Click **Yes**.
8. Copy the updated ArgusSecureKey.ini File from the .\Windows folder to all the .\Windows folder of all the application servers.
9. Verify that you can Log in to the Argus Safety application.

26.2.2 Edit Keys

An administrator might want to change a key due to various reasons like a policy to change key every few days, or to avoid network compromise, etc.

1. Launch the **Cryptography Key Editor**.
The Key Editor Utility screen appears.
2. Click **Existing**.
The Key Editor Login or Re-encrypt ARGUSUSER screen appears.
3. Enter the ARGUSUSER password.
4. Enter the APR_USER password.
This field appears only when you have installed Argus Insight along with Argus Safety.
5. Enter the database name.
6. Click **Login**.
The Key Editor Options for Existing Installation screen appears.
7. Enter the DBA User Name and User Password.
8. Click **Validate**.
9. Select the **Edit Key** checkbox.
This enables the child checkboxes of **User Key** and **Cookie Key**.
The User Key is used for all the encrypted strings which are persisted in the database or file server.
The Cookie Key is only used to encrypt and decrypt the key.
The user has the option to change either one or both keys.
10. Select the checkboxes in front of the key that you want to change.

11. Change the Key Size drop-down value, if you wish to change the key size. Key Size is measured in bits of the key used in a cryptographic algorithm.
12. Click **Re-Generate**.

This will change the value of the checked items and the new value will be visible in the textbox.
13. Click **Execute**.

The Reason for this Action dialog box appears, prompting the user to add a reason for his action.

The text entered here is visible in the Audit Log in the Argus Safety application.
14. Click **OK**.
15. Check the status box to verify if the operation has been successful.
16. If the operation is successful and the Cryptography key is checked, then the changed key is now stored in the ArgusSecureKey.ini.

You should now copy this file from the .\Windows folder of the current machine and paste it to the .\Windows folder of all web servers.
17. When the user key is changed, all the encrypted strings in the database are re-encrypted using the new key.

However, there are still some other file server locations where this key change must also be applied manually. The following is a list of places where the changes must be done manually:
18. Items to be changed from the User Interface:

| String | Description |
|-----------------|---|
| Argus Services | Open Argus Safety Service Configuration: Open all the processes and enter password again. |
| Cyclone | Open ESM Mapping utility and re-enter the Cyclone password. |
| ESM Common User | Open ESM Mapping utility and re-enter the ESM Common User password. |

26.2.3 Re-encrypt Common User Passwords

The **Key Editor Options for Existing Installation** screen can also be used to change the common user (ARGUS_LOGIN, ARGUS_LOGIN_I, and ARGUS_LOGIN_IPS) passwords.

1. Launch the **Cryptography Key Editor**.

The Key Editor Utility screen appears.
2. Click **Existing**.

The Key Editor Login or Re-encrypt ARGUSUSER screen appears.
3. Enter the ARGUSUSER password.
4. Enter the APR_USER password.

This field appears only when you have installed Argus Insight along with Argus Safety.
5. Enter the database name.

6. Click **Login**.

The Key Editor Options for Existing Installation screen appears.

7. Enter the DBA User Name and User Password.

8. Click **Validate**.

9. Check the **Re-encrypt** checkbox.

10. Enter the passwords for the common users.

11. Click **Execute**.

The Reason for this Action dialog box appears, prompting the user to add a reason for his action.

12. The text entered here is visible in the Audit Log in the Argus Safety application.

13. Click **OK**.

14. Check the status box to verify if the operation has been successful.

26.2.4 Generate Encrypted String

Generate the encrypted string from clear text, using the configured UserCryptoKey in ArgusSecureKey.ini.

1. Launch the **Cryptography Key Editor**.

The Key Editor Utility screen appears.

2. Click **Existing**.

The Key Edit Login screen appears.

3. Enter the ARGUSUSER password.

4. Enter the APR_USER password.

This field appears only when you have installed Argus Insight along with Argus Safety.

5. Enter the database name.

6. Click **Login**.

The Key Editor Options for Existing Installation screen appears.

7. Enter the DBA User Name and User Password.

8. Click **Validate**.

9. Check the **Generate Encrypted** checkbox.

10. Enter the password in the **Clear text** field.

11. Click **Execute**.

The Reason for this Action dialog box appears, prompting the user to add a reason for his action.

12. The text entered here is visible in the Audit Log in the Argus Safety application.

13. Click **OK**.

14. Check the status box to verify if the operation has been successful. If the operation is successful, the encrypted script gets displayed in the **Encrypted String** field.

26.2.5 Reset Administrator and System Application User Password

1. Launch the **Cryptography Key Editor**.
The Key Editor Utility screen appears.
2. Click **Existing**.
The Key Editor Login screen appears.
3. Enter the ARGUSUSER password.
4. Enter the APR_USER password.
This field appears only when you have installed Argus Insight along with Argus Safety.
5. Enter the database name.
6. Click **Login**.
The Key Editor Options for Existing Installation screen appears.
7. Enter the DBA User Name and User Password.
8. Click **Validate**.
9. Check the **Reset password for the default Administrator and System Accounts** checkbox.
10. To set **Administrator** password, select the respective checkbox, and enter the parameters.
11. To set **System** user password, select the respective checkbox and enter the parameters.
12. Click **Execute**.
The Reason for this Action dialog box appears, prompting the user to add a reason for his action.
The text entered here is visible in the Audit Log in the Argus Safety application.
13. Click **OK**.
14. Check the status box to verify if the operation has been successful.

26.2.6 Reset the Environment if ArgusSecureKey.ini is Lost

1. To generate a new key and copy it to the Windows folder, follow the steps listed in the [Section 26.2.1, "Reset the ARGUSUSER Password."](#)
2. To re-encrypt common user passwords, follow the steps listed in the [Section 26.2.3, "Re-encrypt Common User Passwords."](#)
3. Re-encrypt strings in the following locations:

| String | Description |
|--------|--|
| LDAP | Clear column LDAP_SEARCH_PASSWORD in all rows from table CFG_LDAP_SERVERS. Now open Argus Console > System Configuration > System Management > LDAP and re-enter passwords for all configurations. |
| SMTP | Clear column USER_PASSWORD in all rows from table CFG_SMTP. Now open Argus Console > System Configuration > SMTP Configuration and re-enter passwords for SMTP account. |

| String | Description |
|-----------------|---|
| Documentum | Clear column VALUE for row where SECTION='SYSTEM' AND KEY='DOCUMENTUM_PASSWORD' from table CMN_PROFILE_ENTERPRISE. Now open Argus Console > System Configuration > Common profile Switches to re-enter Documentum password. |
| Argus Services | Open Argus Safety Service Configuration: Open all the processes and enter password again. |
| Cyclone | Open ESM Mapping utility and re-enter the Cyclone password. |
| ESM Common User | Open ESM Mapping utility and re-enter the ESM Common User password. |

26.3 Manage Argus Insight Cryptographic Key

26.3.1 Update APR_USER Password

When Argus Insight is installed and you have an If you have the ArgusSecureKey.ini file, updated the APR_USER password in ArgusSecureKey.ini

1. Log in to Argus Insight Client.
2. Click **Start**.
3. Navigate to **Programs > Oracle > Argus Crypto Tool**.
Or, go to: *C:\Program Files\Oracle\Argus\ArgusCrypto*
The Argus Key Editor Utility screen appears.
4. Click **Existing**.
5. Select the **Re-encrypt** option.
6. From the drop-down list, select APR_USER, enter the parameters, and click **Re-encrypt**.

The system updates the password for APR_USER.

26.3.2 Copy Initialization Files to Other Servers

After you change the cryptography key using the Key Management tool, you must manually copy the **Argus SecureKey.ini** initialization file 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 Argus SecureKey.ini file 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.

26.3.3 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.

Configure BI Publisher Security Model

Oracle recommends to use the Oracle Fusion Middleware Security model. In case you prefer to use the BI Publisher Security Model, follow the subsequent sections for the set up.

Create Custom Roles and Assign Data Sources

1. Log in to BI Publisher with the administrator credentials.
The BI Publisher Home Page appears.
2. Click **Administration**.
3. Under Security Center, click **Roles and Permissions**.
The Roles and Permissions screen appears.
4. Click **Create Role**.
The Create Role screen appears.
5. Enter a role **Name** and **Description**, and click **Apply**.
A new custom role is created.
6. To assign data sources to the created role, click the **Add Data Sources** icon .
7. From the Available Data Source section, select a data source (for example, **asbip**) and click **Move (>)** to add it to the Allowed Data Sources section.
8. Click **Apply**.
9. To assign the required roles to the custom role, click **Add Roles** icon .
10. From the Available Roles, select the roles to be included and click **Move (>)** to add the selected roles to Included Roles.
11. Click **Apply**.

Create Users and Assign Roles

1. Log in to BI Publisher with the administrator credentials.
The BI Publisher Home Page appears.
2. Click **Administration**.
The Administration screen appears.

3. Under **Security Center**, click **Users**.

The Users screen appears.

4. Click **Create Users**.

The Create User screen appears.

5. Enter a **Username** and **Password** and click **Apply**.

A new user is created.

6. To assign roles to the user, click the **Assign Roles** icon corresponding to the new user.



The Assign Roles screen appears with the BI Publisher system roles as the following:

- BI Publisher Administrator
- BI Publisher Excel Analyzer
- BI Publisher Online Analyzer
- BI Publisher Developer
- BI Publisher Scheduler
- BI Publisher Template Designer

These roles are available by default along with the custom roles you create.

In the above figure, ASAdmin and BIAdmin are custom roles.

7. From the Available Roles section, select a role and click **Move (>)** to move the selected role to the Assigned Roles section.
8. Click **Apply**.

The selected role is assigned to the user.

Create ODBC Connection for OBIEE Administration Tool for Argus Insight

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**.

