### Oracle® Argus Safety

Installation Guide Release 8.1 **E71757-01** 

September 2016



Oracle Argus Safety Installation Guide, Release 8.1

E71757-01

Copyright © 2016 Oracle and/or its affiliates. All rights reserved.

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, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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

| reface  | xi   |
|---|------|
| Intended Audience   | xi   |
| Documentation Accessibility                               | xii  |
| About This Book   | xii  |
| Related Documents   | xiii |
| Checking My Oracle Support                                | xiv  |
| Conventions   | xiv  |
| Introduction  |      |
| General Installation and Software Requirements            | 1-1  |
| Pre-Requisite Installation Order                          | 1-2  |
| Software Requirements for Argus Safety                    | 1-3  |
| Argus Safety Hardware Topology                            |      |
| Recommended Hardware Topology for a Small Company         | 1-7  |
| Recommended Hardware Topology for a Mid-sized Company     |      |
| Recommended Hardware Topology for a Large Company         |      |
| Hardware Requirements for Argus Safety                    |      |
| General Pre-Installation Tasks                            |      |
| Installation Process Overview                             | 1-10 |
| Converting Argus Safety Report Server to Argus Web Server | 1-11 |
| Starting the Installation                                 |      |

#### 2 Starting the Installation

| Getting Started                                     | 2-1 |
|---|-----|
| Installing the Files Required to View Japanese Text | 2-1 |

### 3 Installing the Argus Safety Database

| Overview                                     | 3-1 |
|--|-----|
| Schemas Required for Database Instances      | 3-2 |
| Argus Safety Instance Database Schemas       | 3-2 |
| Axway Synchrony Database Instance (Optional) | 3-3 |
| Setting up Oracle Parameters                 | 3-3 |
| Oracle Database Settings                     | 3-3 |
| Argus Safety Database Instance Parameters    | 3-3 |
| Additional Database Setup Information        | 3-4 |
| GMT Offset Calculation                       | 3-4 |
|  |     |

| Prerequisites for New Schema Creation                                       |
|---|
| Creating the Argus Safety Read Only Database Account (Optional)             |
| Creating the Argus Safety Database Schema 3-                                |
| XDB Schema Installation Requirement for Interchange                         |
| Installing the Schema Creation Tool 3-                                      |
| Creating the Tablespaces 3-   |
| Creating the Schema   |
| Creating the Argus Safety Read Only Database Account (Optional)             |
| Loading Factory Data  |
| Enabling and Disabling Oracle Text  |
| Enabling Oracle Text  |
| Disabling Oracle Text   |
| Implementing Table Partitioning   |
| Working with the MedDRA and MedDRA J Dictionaries                           |
| Loading the MedDRA Dictionary   |
| Overwriting an Existing MedDRA Dictionary                                   |
| Recoding Events   |
| Loading the J Drug Dictionary   |
| Overwriting an Existing J Drug Dictionary                                   |
| Loading the WHO-DRUG Dictionary   |
| Loading the WHO-Drug Dictionary to New Tables                               |
| Loading the WHO-Drug Dictionary Using the Overwrite Option                  |
| To Load the WHO-Drug Dictionary using the Format C Option                   |
| Validating the Argus Safety Database  |
| Enabling and Disabling DLP 3-29   |
| Creating the Tablespaces  |
| Enabling DLP 3-30   |
| Disabling DLP 3-3   |
| Enabling DLP on a Specific Enterprise                                       |
| Upgrading the Argus Safety Database   |
| Prerequisites for Database Upgrade  |
| DLP Data Correction Script to be Run Before Upgrading the Database          |
| Data Migration Logic for New Fields   |
| Database Upgrade Procedure (with or without DLP) from AS 8.0 to AS 8.1 3-40 |
| Post-Upgrade Steps 3-44   |
| Enabling Local Locking in Argus Safety                                      |
| Merging a Single Enterprise Safety Database into a Multi-tenant Database    |
| Prerequisites to Running the Merge Export Step 3-4                          |
| Prerequisites to Running the Merge Import Step                              |
| Completing the Merge Process  |
| Merge Export  |
| Exporting the dmp File Copy to the Target Database Server                   |
| Merge Import  |
| Manual Dictionary Synchronization 3-4                                       |
| Copy Configuration Tool   |

### 4 Installing Argus Safety Web

5

6

7

| Installing Argus Safety Web                               |   |
|---|---|
| Configuring the IIS Manager for Windows 2012              |   |
| Connecting to a Domain Account on Windows 2012            |   |
| Enabling SSL Support for Windows 2012                     |   |
| Configuring Load Balancer in Argus Web                    |   |
| Set up Argus Web Load Balancer IP Address                 | ۷ |
| Set up Load Balanced Folders                              |   |
| Set up Shared Network Directory                           | 4 |
| Securing Sensitive Configuration and Operational Data     |   |
| Configuring Identity in the IIS Application Pools         | ۷ |
| Resetting IIS   | 4 |
| Setting up Client Browser                                 |   |
| Adding the Argus Site as a Local Intranet Site            |   |
| Setting up Compatibility View with Internet Explorer      |   |
|   |   |
| Installing Argus Safety Service                           |   |
| Starting Argus Safety Service                             |   |
| Setting up RightFax                                       |   |
| Installing and Configuring EDI Gateway                    |   |
| Creating an Axway Synchrony Database Instance             |   |
| Installing Axway Synchrony Interchange                    |   |
| Starting the Axway Synchrony Server                       |   |
| Configuring Axway Synchrony Interchange for Axway 5.10    |   |
| Configuring Axway Synchrony Interchange                   |   |
| Configuring Axway Synchrony for Binary File Transmission  |   |
| Configuring Axway Synchrony Community                     |   |
| Registering with the Axway Synchrony Community            |   |
| Adding a Partner to the Axway Synchrony Community         |   |
| Registering the Receiver's Community on the Sender Server |   |
| Adding a Node   |   |
| Configuring Axway Synchrony Certificates                  |   |
| Configuring Receiver Axway Synchrony Certificates         |   |
| Configuring Sender Axway Synchrony Certificates           |   |
| Configuring EVENTS.XML                                    |   |
| Configuring Axway Synchrony Interchange for Axway 5.12    |   |
| Configuring Axway Synchrony for Binary File Transmission  |   |
| Configuring Axway Synchrony Community                     |   |
| Registering with the Axway Synchrony Community            |   |
| Adding a Partner to the Average Sunchrony Community       |   |

| Configuring Receiver Axway Synchrony Certificates | 7-19 |
|---|------|
| Configuring Sender Axway Synchrony Certificates   | 7-20 |
| Configuring EVENTS.XML                            | 7-21 |
| Testing Communication                             | 7-23 |

### 8 Configuring Oracle B2B

| Integrating Oracle B2B with Argus Safety                    | 8-1 |
|---|-----|
| Creation of integration tables in B2B Schema                | 8-1 |
| Oracle B2B UI Configuration                                 | 8-2 |
| General Configuration > Administration > Configuration      | 8-2 |
| Document Configuration > Administration > Document          | 8-2 |
| Enterprise Manager Configuration                            | 8-2 |
| SOA Composite Deployment                                    | 8-2 |
| SOA Composite Configuration                                 | 8-3 |
| AS_BPEL_Outbound Composite                                  | 8-3 |
| AS_BPEL_Inbound Composite                                   | 8-3 |
| Web Logic Console Configuration                             | 8-3 |
| Data source with JNDI Name as 'eis/DB/ArgusSafety_Outbound' | 8-3 |
| Data source as 'jdbc/ArgusSafety_Inbound'                   | 8-4 |
| Data source with JNDI Name as 'eis/DB/ArgusSafety_Inbound'  | 8-4 |
| DB Adapters for Data Source                                 | 8-4 |
| Large Payload Exchange Configuration                        | 8-4 |
| Outbound Files  | 8-4 |
| Inbound Files   | 8-5 |
| Transaction Time  | 8-5 |
| General B2B Settings for Large Payloads                     | 8-5 |
| Configuration on Argus Safety side                          | 8-5 |
| Configure Oracle B2B  | 8-5 |
| Update for B2B Documents                                    | 8-5 |
| Argus Console > Reporting Destination Code List             | 8-6 |
|   |     |

### 9 Installing and Configuring Interchange

| Installing Interchange Service               | 9-1 |
|--|-----|
| Configuring Interchange Service              | 9-5 |
| Transmitting E2B Attachments                 | 9-6 |
| Accessing EDI Gateway Shared Folders         | 9-6 |
| Configuring the Interchange Service.INI File | 9-6 |

### 10 Performing Post-installation Checks

| Post-Installation Tasks  | 10-1 |
|--|------|
| General Checklist  | 10-1 |
| Configuring Argus Safety Windows Service to run as a Domain User | 10-2 |
| Configure Worklist Intake  | 10-2 |
| RelsysWindowsService.exe.config                                  | 10-3 |
| Service.config   | 10-3 |
| Intake.config  | 10-4 |

| IIS Checklist  | 10-4 |
|--|------|
| .INI File Checklist  | 10-5 |
| Service Checklist  | 10-5 |
| Verifying the Web Server Installation and IIS Configurations | 10-6 |
| Verifying IIS Configuration                                  | 10-6 |
| Configure and Verify the Dossier Installation                | 10-6 |
| Configuring the Dossier Application                          | 10-6 |
| Verifying the Dossier Installation                           | 10-7 |
| Verify Files installed on Middle Tier Servers:               | 10-8 |
| Verifying the Documentum Installation                        | 10-8 |

### 11 Enabling IIS HTTP Compression

| IIS Web Page Compression                             | 11-1 |
|--|------|
| HTTP Compression                                     | 11-1 |
| Known Effects of Enabling Compression                | 11-1 |
| How to Enable HTTP Compression                       | 11-2 |
| IIS Caching Settings                                 | 11-2 |
| IIS Caching  | 11-2 |
| Known Effects of Enabling Caching                    | 11-2 |
| How to Enable Caching                                | 11-2 |
| Local Internet Explorer (IE) Client Caching Settings | 11-3 |
| IE Client Caching                                    | 11-3 |
| IE Client Caching Tab Options                        | 11-3 |
| How to Enable IE Caching                             | 11-4 |

### 12 Configuring E-mail

| About E-mail Configuration           | 12-1 |
|--------------------------------------|------|
| Configuring SMTP                     | 12-1 |
| Using the SMTP Configuration Utility | 12-1 |
| Functions Affected by SMTP           | 12-2 |
| Bulk Report Transmit E-mail          | 12-2 |
| Autosignal E-mail                    | 12-3 |
| Fax E-mail                           | 12-3 |
| Fax Status E-mail                    | 12-3 |
| Priority E-mail                      | 12-3 |
| Dossier Notification E-mail          | 12-3 |
| E-mail Sent by Interchange Service   | 12-3 |

### 13 Enabling and Configuring BI Publisher Periodic Reports

| Preparing BI Publisher Server                                  | 13-1 |
|--|------|
| TNS Names Configuration  | 13-2 |
| Database Configuration   | 13-2 |
| Setting up the BI Publisher for Argus Safety                   | 13-3 |
| Enabling a Local Superuser for BI Publisher Standalone Install | 13-3 |
| Configuring the Security Model                                 | 13-3 |
| Creating ASBIP JDBC Connection                                 | 13-4 |

| Setting-up Runtime BI Publisher Memory  | 13-6  |
|---|-------|
| Managing Users and Roles in BI Publisher Security Model [BI Publisher Standalone] | 13-6  |
| Creating Users and Assigning Roles  | 13-7  |
| Creating Custom Roles   | 13-9  |
| Managing Users and Roles in Oracle Fusion Middleware [BI Publisher Standalone]    | 13-10 |
| Creating Users and Assigning Groups   | 13-10 |
| Creating Roles and Policies   | 13-14 |
| Managing Privileges and Folder Rights   | 13-21 |
| Managing Users and Roles for BI Publisher [OBIEE and BI Integrated Installation]  | 13-22 |
| Creating Users and Assigning Groups   | 13-22 |
| Creating Roles and Policies   | 13-22 |
| Managing Privileges and Folder Rights   | 13-26 |
| Uploading the Argus Safety.xdrz file to BI Publisher                              | 13-33 |
| Integrating Argus Safety with BI Publisher  | 13-35 |
| Argus Console-level Configurations  | 13-36 |
| Configuring Code Lists  | 13-37 |
| Creating the Database Jobs  | 13-38 |
| Upgrading Flexible Aggregate Reports from 8.0 to 8.1                              | 13-39 |
| Upgrading Argus Safety Database from 8.0 to 8.1 for FAR                           | 13-39 |
| Upgrading BI Publisher Periodic Reports from 8.0 to 8.1 for FAR                   | 13-39 |
|   |       |

### 14 Installing End of Study Unblinding

| EOSU Hardware/Software Requirements | 14-1 |
|-------------------------------------|------|
| How to Install the EOSU Utility     | 14-1 |

### 15 Other Tasks

| Configuring the Argus.xml File   | 15-1  |
|--|-------|
| Configuring the Argus.ini File   | 15-2  |
| Increasing the Internet Explorer Timeout Setting to Run Reports          | 15-4  |
| Deploying a Portlet on Oracle WebLogic Server                            | 15-5  |
| Deploying the Global Home Application on a WebLogic Server               | 15-8  |
| Configure Global Homepage Properties File                                | 15-8  |
| Update Global Homepage Properties File                                   | 15-8  |
| Deploy Company Logo  | 15-8  |
| Pre-Deployment Configuration   | 15-8  |
| Configuring SSO in Oracle Access Manager 11g                             | 15-12 |
| Installation and Configuration of Oracle Web Tier Suite                  | 15-15 |
| Installing Oracle Web Tier   | 15-15 |
| Configuring Oracle Web Tier  | 15-18 |
| Oracle Http Server Administration  | 15-22 |
| Configuring Oracle Http Server as Reverse Proxy Server for WebLogic      | 15-22 |
| Configuring the WebCenter Security Provider for Identity Assertion       | 15-24 |
| Configuring the Oracle Internet Directory Authenticator                  | 15-24 |
| Configuring the OAM Identity Asserter                                    | 15-26 |
| Configuring the Default Authenticator and Setting the Order of Providers | 15-28 |
| Setting EXTRA_JAVA_PROPERTIES for WebLogic Domain                        | 15-28 |
|  |       |

| Installation Maintenance Tasks | 15-29 |
|--------------------------------|-------|
| Installing New Components      | 15-29 |
| Uninstalling Components        | 15-30 |
| Removing All Components        | 15-30 |
| Web Client Tips                | 15-31 |
| Clearing Oracle Temp Files     | 15-32 |
| Configuring easyPDF            | 15-33 |
| Setting Up easyPDF             | 15-33 |
| Setting up Microsoft Office    | 15-34 |
| Using Display PDF in Browser   | 15-34 |
| Setting Printer Defaults       | 15-35 |
| Argus Configuration Files      | 15-35 |

### 16 Argus Integrations

| Installing Argus Integrations          | 16-1  |
|--|-------|
| Resetting IIS                          | 16-2  |
| Overview: Argus Web Service Interface  | 16-3  |
| Argus Web Service Interface Framework  | 16-4  |
| Basic Configuration Overview           | 16-4  |
| Outbound Interface                     | 16-4  |
| Inbound Interface                      | 16-4  |
| Safety Message Overview                | 16-5  |
| MedDRA Interface                       | 16-5  |
| Overview                               | 16-5  |
| MedDRA Encoding Safety Message Example | 16-5  |
| Request (V 1.1)                        | 16-5  |
| Response (V 1.1)                       | 16-7  |
| Request (V 1.0)                        | 16-9  |
| Response (V 1.0)                       | 16-10 |
| MedDRA Dictionary: XML Schema          | 16-12 |
| Request: MEDDRA_Request                | 16-12 |
| Request: MEDDRA_Response               | 16-13 |
| Flow of MedDRA Auto Encoding           | 16-14 |
| Configuration                          | 16-14 |
| Product License Study Interface        | 16-15 |
| WHO Drug Coding Interface              | 16-16 |
| Overview                               | 16-16 |
| WHO Drug Coding Safety Message Example | 16-17 |
| Request                                | 16-17 |
| Response                               | 16-18 |
| WHO Drug Coding: XML Schema            | 16-20 |
| Request: WHODrug_Request               | 16-21 |
| Response: WHODrug_Response             | 16-21 |
| Flow of Drug Dictionary Coding         | 16-21 |
| Configuration                          | 16-22 |
| Lot Number Interface                   | 16-22 |
| Overview                               | 16-22 |

| Lot Number Safety Message Example                     | 16-23 |
|---|-------|
| Request   | 16-23 |
| Response  | 16-24 |
| Lot Number: XML Schema                                | 16-25 |
| Request: Lot_Request                                  | 16-25 |
| Response: Lot_Response                                | 16-26 |
| Flow of Lot Validation                                | 16-27 |
| Configuration   | 16-27 |
| Transformation  | 16-28 |
| Worklist Intake                                       | 16-29 |
| Flow of Worklist Intake                               | 16-29 |
| Worklist Intake Safety Message Example                | 16-30 |
| Configuration   | 16-34 |
| Literature Intake                                     | 16-35 |
| Flow of Literature Intake                             | 16-35 |
| Configuration   | 16-35 |
| Metadata Configuration                                | 16-36 |
| Extended E2B Interface                                | 16-37 |
| E2B Mapping Updates                                   | 16-37 |
| Adding Extension Elements to DTD                      | 16-37 |
| Prepare Factory Data for Extension Elements           | 16-38 |
| Create Business Logic for Extension Elements          | 16-40 |
| Configure Reporting Destination for Extension Profile | 16-40 |
| Extension Elements Sample XML                         | 16-41 |
| Extension Elements Sample Import PL/SQL Block         | 16-41 |

### 17 Argus Password Management - Cryptography Tool

| Cryptography Tool Overview  | 17-1  |
|---|-------|
| Installing or Upgrading to Argus Safety 8.1                                     | 17-1  |
| The Argus Safety 8.1 Database   | 17-2  |
| The Argus Safety 8.1 Application Servers  | 17-2  |
| Generating a New Cryptography Key   | 17-2  |
| Resetting Password / Changing the Cryptography Key                              | 17-3  |
| Resetting the ARGUSUSER Password  | 17-4  |
| Editing Keys  | 17-5  |
| Re-encrypting Common User Passwords   | 17-8  |
| Generating Encrypted String from Clear Text on Configured User Cryptography Key | 17-12 |
| Resetting the Environment if ArgusSecureKey.ini is Lost                         | 17-15 |

### 18 Argus Centralized Coding

| setup_centralized_coding_interface_schema.bat | 18-1 |
|---|------|
| setup_dsnav_centralized_coding.bat            | 18-3 |
| dms_migration.bat                             | 18-4 |
| Single Enterprise Migration in One Execution  | 18-4 |
| All Enterprise Migration in One Execution     | 18-4 |

# Preface

This guide describes installing or upgrading to Oracle Argus Safety 8.1. Keep this guide; you would perform some of these tasks only once, while you might need to repeat some others as your system changes or grows.

### Intended Audience

We wrote this manual assuming your organization has the expertise to perform the job functions listed in this section. If your staff needs help with these skills, we recommend that you engage Oracle Consulting.

#### **Oracle Database Administrators**

Installing Oracle Argus Safety requires a level of knowledge equivalent to having mastered the material in Oracle's DBA Architecture and Administration course. You must be able to read SQL\*Plus scripts and edit them. You must be able to run SQL scripts and review logs for Oracle errors. For ongoing administration, additional training as a DBA is essential.

#### System Administrators

Installing and maintaining an Oracle Argus Safety network requires mastery of the following skills:

- Microsoft Windows operating systems, in general
  - creating and managing user accounts and groups
  - installing Oracle software
  - managing settings through the Control Panel
  - managing network printers
  - creating services
  - installing and configuring OBIEE and OAM
- UNIX:
  - creating and managing user accounts and groups
  - installing Oracle RDBMS software and patches
  - identifying space on a file system for Oracle database tablespaces
  - setting and using environment variables
  - installing and configuring OBIEE and OAM

### **Documentation Accessibility**

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

#### Access to Oracle Support

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

### About This Book

This guide contains these chapters:

#### Chapter 1, "Introduction"

This chapter provides an overview of the hardware and software requirements for Oracle Argus Safety.

#### Chapter 2, "Starting the Installation"

This chapter provides information about starting the installation.

#### Chapter 3, "Installing the Argus Safety Database"

This chapter describes the steps in creating, upgrading, and validating the Argus Safety Database schema.

#### Chapter 4, "Installing Argus Safety Web"

This chapter describes how to install Argus Safety Web, and how to configure IIS Manager and Load Balancer.

Chapter 5, "Setting up Client Browser"

This chapter describes how to set up Client Browser.

Chapter 6, "Installing Argus Safety Service" This chapter provides instructions on installing Argus Safety Service.

#### Chapter 7, "Installing and Configuring EDI Gateway"

This chapter describes how to install and configure the EDI Gateway.

**Chapter 8, "Configuring Oracle B2B"** This chapter provides information about configuring B2B.

#### Chapter 9, "Installing and Configuring Interchange"

This chapter describes how to install and configure Interchange.

#### Chapter 10, "Performing Post-installation Checks"

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

#### Chapter 11, "Enabling IIS HTTP Compression"

This chapter describes how to enable IIS HTTP Compression on Windows 2012 Server.

**Chapter 12, "Configuring E-mail"** This chapter provides information about configuring E-mail.

Chapter 13, "Enabling and Configuring BI Publisher Periodic Reports" This chapter provides information about configuring BI Publisher.

**Chapter 14, "Installing End of Study Unblinding"** This chapter describes how to install the EOSU Utility.

Chapter 15, "Other Tasks"

This chapter provides information for performing other installation and configuration tasks.

**Chapter 16, "Argus Integrations"** This chapter provides information about the Argus Integrations.

**Chapter 17, "Argus Password Management - Cryptography Tool"** This chapter provides information about the Cryptography Tool.

Chapter 18, "Argus Centralized Coding"

This chapter provides information about Argus Centralized Coding.

### **Related Documents**

This section lists the manuals for Oracle Argus products. You can order printed manuals from the Oracle iStore.

#### **Oracle Argus Documentation**

The *documentation set* includes:

- Argus Affiliate User Guide
- Argus Console User Guide
- Argus Dossier User Guide
- Argus Interchange User Guide
- Argus Safety Service Administrator Guide
- Argus Safety BI Publisher Periodic Reporting Extensibility Guide
- Argus Safety BIP Aggregate Reporting User's Guide
- Argus Safety User Guide
- Argus Unblinding User Guide
- Minimum Security Configuration Guide
- Third Party Licenses and Notices

(A new Technical Reference Manual (TRM) is added to Oracle Argus TRM set).

### **Checking My Oracle Support**

The Oracle Argus Safety product suite continues to grow and evolve. To help you use it and stay abreast of updates we provide between releases, it is a good practice to check My Oracle Support for information that enhances our released documentation.

To open the Oracle Argus Safety product page on My Oracle Support, complete the following steps:

- 1. Open a Web browser to http:/support.oracle.com.
- 2. Click Sign In and enter your user information.

The My Oracle Support portal opens, displaying general news from several categories. If you do not yet have an account, click **Register here** and follow the instructions given on the registration page.

- 3. Click Knowledge.
- 4. In the Browse any Product, by Name field, enter Oracle Argus Safety.
- **5.** Click **Go**. My Oracle Support loads the Oracle Argus Safety Knowledge Browser Product Page.

### Conventions

The following text conventions are used in this document:

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

# Introduction

This section includes the following information:

- General Installation and Software Requirements
- Pre-Requisite Installation Order
- Argus Safety Hardware Topology
- General Pre-Installation Tasks
- Installation Process Overview

### **General Installation and Software Requirements**

This section contains table that show the software installation requirements for small, mid-sized, and large companies for the following:

Argus Safety Database Server

**Note:** Argus Safety 8.1 both Standard and Enterprise Editions support the CDB/PDB as well as Non-CDB database formats of the Oracle Database 12.1.0.2.

Argus Safety Web Server

#### Note:

- The ArgusSecureKey.ini file should be placed under the .\Windows folder. Refer to the Generating a New Cryptography Key section to create a cryptography key.
- Report Server is not required for the Argus Safety installation.
   Existing customers can convert the Report Server to an Argus Web Server. Refer to the Converting Argus Safety Report Server to Argus Web Server section for details.
- Argus Transaction Server

#### Note:

We do not recommend that AG/ESM Service runs on the Web Server, because the agproc.exe and argusvr2.exe services might conflict with each other when running together.

Argus Interchange Server

The Argus Interchange Server is an optional component meant to off-load Interchange Service from the Argus Transaction Server. Alternatively, Interchange Service can be installed on the Transaction Server itself.

- Argus Safety Web Client
- Argus End of Study Unblinding Tool
- Argus Safety OBIEE/BI Publisher Server

The OBIEE/BIP Server installation is optional, and required only if Argus Safety Flexible Aggregate Reporting (FAR) through BI Publisher is enabled.

Argus 8.1 supports OBIEE/BI Publisher 12.2.1.

Refer to the OBIEE 12c Installation Guide for Hardware and Software requirements.

See Hardware Requirements for Argus Safety for hardware requirements.

### **Pre-Requisite Installation Order**

When installing the pre-requisites for the servers, the following order should be followed for installing each component. Depending on the server being installed, some of the pre-requisites may not be needed and can be skipped. After these are installed, you can install the rest of the pre-requisites (if any are needed) in any order prior to installing Argus.

- Windows Operating System
- Internet Information Services
- Microsoft .NET Framework
- Oracle Client 12.1.0.2 (32-bit)
- Oracle ODP.NET

**Note:** If you install Windows and run Windows Updates without installing IIS first, Microsoft.NET will be installed first without correctly setting up ASP.NET. In the event this occurs where IIS is installed after Microsoft .NET, 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 V2.0.50727 folder.

1) Manually modify Machine.config

Path: "%windir%\Microsoft.NET\Framework\v2.0.50727\CONFIG

To modify the default .NET Transaction Scope time, the following change should be made in the configuration file:

</system.serviceModel>

<system.transactions>

<machineSettings maxTimeout="01:00:00" />

</system.transactions>

</configuration>

The value specified in **maxTimeout** is applicable for all Argus servers.

#### Software Requirements for Argus Safety

The following table show the software installation requirements for small, mid-sized, and large companies:

| Software Requirements                                    | Argus<br>Safety<br>Database<br>Server | Argus<br>Safety<br>Web<br>Server | Argus<br>Transacti<br>on Server | Argus<br>Interchan<br>ge Server | Argus<br>Safety<br>Web<br>Client | Argus End<br>of Study<br>Unblindin<br>g Tool<br>(EOSU) +<br>Schema<br>Creation<br>Tool ** +<br>Interchang<br>e Mapping<br>Tool |
|--|---------------------------------------|----------------------------------|---------------------------------|---------------------------------|----------------------------------|--|
| OPERATING SYSTEM   |                                       |                                  |                                 |                                 |                                  |  |
| Microsoft Windows 2012 Standard                          | Yes                                   | Yes                              | Yes                             | Yes                             |                                  | Yes  |
| Microsoft Windows 2012 R2 Standard                       | Yes                                   | Yes                              | Yes                             | Yes                             |                                  | Yes  |
| Windows Client Machines and Internet                     | Explorer                              |                                  |                                 |                                 |                                  |  |
| Microsoft Windows 7 (32/64-bit)                          |                                       |                                  |                                 |                                 | Yes                              | Yes  |
| Microsoft Windows 8.1 (32/64-bit)                        |                                       |                                  |                                 |                                 | Yes                              | Yes  |
| Microsoft Windows 10 (32/64-bit)**                       |                                       |                                  |                                 |                                 | Yes                              | Yes  |
| Microsoft Internet Explorer, Version 11.0<br>(32/64-bit) |                                       |                                  |                                 |                                 | Yes                              |  |
| ΟΡΑ ΟΙ Ε ΠΑΤΑΡΑ ΕΕ ΕΕΡΙΤΕΡ                               |                                       |                                  |                                 |                                 |                                  |  |

#### **ORACLE DATABASE SERVER**

(Enterprise/Standard over CDB/PDB or non-CDB format)

| Software Requirements   | Argus<br>Safety<br>Database<br>Server | Argus<br>Safety<br>Web<br>Server   | Argus<br>Transacti<br>on Server | Argus<br>Interchan<br>ge Server | Argus<br>Safety<br>Web<br>Client | Argus End<br>of Study<br>Unblindin<br>g Tool<br>(EOSU) +<br>Schema<br>Creation<br>Tool ** +<br>Interchang<br>e Mapping<br>Tool |
|---|---------------------------------------|------------------------------------|---------------------------------|---------------------------------|----------------------------------|--|
| Microsoft Windows 2012 Standard   | Yes                                   |                                    |                                 |                                 |                                  |  |
| Microsoft Windows 2012 R2 Standard  | Yes                                   |                                    |                                 |                                 |                                  |  |
| Oracle Linux 6.7/7.1  | Yes                                   |                                    |                                 |                                 |                                  |  |
| Oracle RAC  | Yes                                   |                                    |                                 |                                 |                                  |  |
| Sun Solaris 10/11   | Yes                                   |                                    |                                 |                                 |                                  |  |
| Other Oracle Database Components  |                                       |                                    |                                 |                                 |                                  |  |
| Oracle Advanced Security Transparent<br>Data Encryption (TDE)***                                    | Optional                              |                                    |                                 |                                 |                                  |  |
| Oracle Advanced Security Network<br>Encryption  | Optional                              |                                    |                                 |                                 |                                  |  |
| ORACLE CLIENT   |                                       |                                    |                                 |                                 |                                  |  |
| Oracle 12c Release 1 Client 12.1.0.2<br>(32-bit only), Oracle Call Interface,<br>ODAC, MTS, ODP.NET |                                       | Yes                                | Yes                             | Yes                             |                                  | Yes  |
| OTHER MANDATORY SOFTWARE'S  |                                       |                                    |                                 |                                 |                                  |  |
| Microsoft Visual C++ 2005 SP1<br>Redistributable Package MFC Security<br>Update (32 bit)            |                                       | Yes                                | Yes                             | Yes                             |                                  | Yes  |
| Microsoft Visual C++ 2012 Runtime   |                                       | Yes                                | Yes                             | Yes                             |                                  | Yes  |
| Microsoft Visual Basic Power Packs 10.0   |                                       |                                    |                                 |                                 |                                  | Required<br>for<br>Interchang<br>e Mapping<br>Tool   |
| Microsoft .NET 3.5 SP1 Framework  |                                       | Yes                                | Yes                             | Yes                             |                                  | Yes  |
| Microsoft Word + Excel 2010/2013<br>(64-bit)  |                                       | Required<br>for<br>Dossier<br>only | Yes                             | Yes                             | Yes                              | Required<br>for Schema<br>Creation<br>MedDRA<br>Recode and<br>End of<br>Study only   |
| Adobe Acrobat Reader DC/XI with East Asian Fonts  |                                       |                                    |                                 |                                 | Yes                              |  |
| OPTIONAL SOFTWARE   |                                       |                                    |                                 |                                 |                                  |  |
| Documentum DFC 7.2/6.7 SP2 (64-bit)   |                                       | Yes                                | Yes                             | Yes                             |                                  |  |
| RightFax 10.5/10.6 -Required files only   |                                       |                                    | Yes                             |                                 |                                  |  |
| OPTIONAL SUPPORTED FEATURES   |                                       |                                    |                                 |                                 |                                  |  |
| Oracle Components   |                                       |                                    |                                 |                                 |                                  |  |

| Software Requirements  | Argus<br>Safety<br>Database<br>Server | Argus<br>Safety<br>Web<br>Server |  | Argus<br>Interchan<br>ge Server |                         | Argus End<br>of Study<br>Unblindin<br>g Tool<br>(EOSU) +<br>Schema<br>Creation<br>Tool ** +<br>Interchang<br>e Mapping<br>Tool |
|--|---------------------------------------|----------------------------------|--|---------------------------------|-------------------------|--|
| Oracle Identity Manager (OIM) 11.1.2.2 -<br>WebGate 10.1.4.3 (32-bit only) | Required o<br>Manager.                | nly for Sing                     | le Sign-On ir  | ntegration w                    | ith Oracle 1            | ldentity   |
| Oracle WebCenter - 11g (11.1.1.7)  | Required o                            | nly for mult                     | ti-tenant inst   | allations                       |                         |  |
|  | Ideally, the<br>Web Server            | WebCenter<br>Alternativ          | nly to deploy<br>Portal Serve<br>ely, the Glob<br>ety Web Serv | r should be<br>al Applicatio    | deployed c<br>on module | n a separate   |
| Reporting Solutions  |                                       |                                  |  |                                 |                         |  |
| Oracle Business Intelligence Enterprise<br>Edition (OBIEE) 12.2.1          |                                       | Yes^                             |  |                                 |                         |  |
| Oracle BI Publisher 12.2.1   |                                       | Yes^                             |  |                                 | Yes                     |  |
|  |                                       | (For<br>Argus SE<br>only)        |  |                                 |                         |  |
| Third Party Integrations   |                                       |                                  |  |                                 |                         |  |
| LDAP/LDAPS Protocol Version 3.0  | LDAP auth                             | entication s                     | upport   |                                 |                         |  |
| SMTP Protocol  | E-mail sup                            | port                             |  |                                 |                         |  |
| Documentum DFC, Version 6.7 SP2<br>(64-bit), or 7.2                        | Required o                            | nly when D                       | ocumentum  | is used for S                   | torage.                 |  |
| RightFax 10.5/10.6   | Required o                            | nly for faxir                    | ng Expedited   | Reports.                        |                         |  |
| Gateway for E2B Reporting  |                                       |                                  |  |                                 |                         |  |
| Oracle B2B - 12.2.1  |                                       |                                  | 1 and AS2 pr<br>and pharmad                                    |                                 |                         | ges between  |
| Axway Interchange 5.12 SP8 (64-bit)  | Required for                          | or E2B Repo                      | rt Exchange.   |                                 |                         |  |

#### \* Note:

\_

\* Database Instance is required to be AL32UTF8 Character Set.

\*\* Refer to **Note 1** for Oracle Client Patch required for Schema Creation Tool.

\*\*\* Refer to **Note 2** for Oracle Database TDE feature.

^ Refer to **Note 3** for WebLogic 12.2.1 patch details.

#### \*\* Note 1: Oracle Client Patch required for the Schema Creation Tool

Download the patch 19720843: WINDOWS DB BUNDLE PATCH 12.1.0.2.1 through Oracle Support.

Apply the following workaround after successfully installing this patch:

1. Set oracle\_home to your client home location

For example:

SET ORACLE\_HOME=C:\app\client32\product\12.1.0\client\_1

Go to %oracle\_home%\bin\ of the client

Copy file "oranfsodm12.dll" present in "\p19720843\_121020\_ WINNT\19720843\files\bin\" and paste it under %oracle\_ home%\bin

2. Run sqlldr help=y or sqlldr.exe.

**\*\*\* Note 2:** Oracle Database TDE feature is part of the Oracle Advanced Security option available for Oracle Database Enterprise Edition 12c

(https://docs.oracle.com/database/121/ASOAG/asotrans\_ config.htm#ASOAG10275, or

http://www.oracle.com/technetwork/database/options/advanced-s ecurity/index-099011.html).

TDE provides the capability to encrypt sensitive data in the Oracle Database in a manner that is transparent to applications.

Argus Safety product has been functionally certified with tablespace level encryption using the Oracle Database TDE feature.

**^ Note 3:** For Argus Safety Web Server, you need Oracle Business Intelligence Enterprise Edition (OBIEE) 12.2.1 + Patch 22248372 for CVE-2015-4852 for WebLogic 12.2.1

### Argus Safety Hardware Topology

This section provides information about the recommended hardware topology and hardware requirements for small, mid-size, and large companies.

The size of your company and licensed Argus components determines the distribution of the software among the servers.

The following are the definitions for small, mid-sized, and large companies.

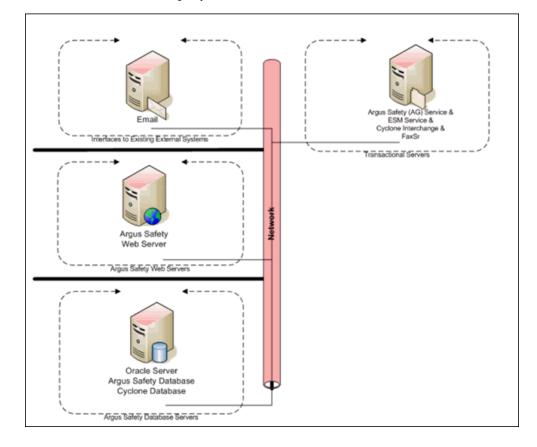
**Small Company:** A small company is a company that has from 1 to 50 concurrent users and fewer than 200 new cases reported each month.

**Mid-Sized Company:** A mid-sized company is a company with 51 to 100 concurrent users and 300 to 600 new cases reported each month.

**Large Company:** A large company is a company with more than 100 concurrent users and approximately 1000 to 5000 new cases reported each month.

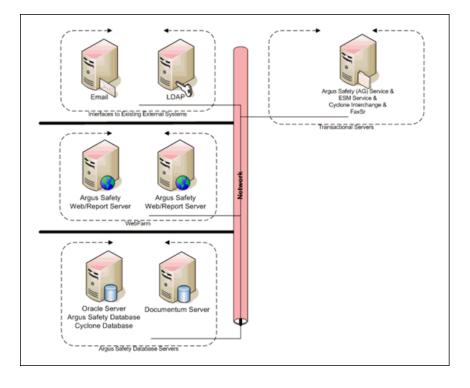
#### **Recommended Hardware Topology for a Small Company**

The following image shows the recommended hardware topology for the Argus Safety Hardware for a small company.



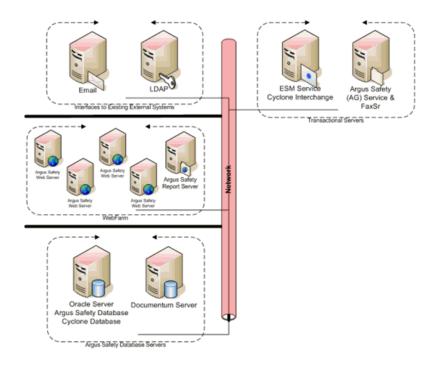
### **Recommended Hardware Topology for a Mid-sized Company**

The following image shows the recommended topology for the Argus Safety Hardware for a mid-sized company.



### **Recommended Hardware Topology for a Large Company**

The following is an illustration of the recommended topology for a large company.



#### Hardware Requirements for Argus Safety

The following table show the hardware requirements for Argus Safety installation for small, mid-sized, and large companies:

|   |           | ıs Saf<br>base   |     | er                    |           | is Safe<br>Serve  |     | Argu<br>Tran<br>Serv | sactic            | on  | Argu<br>Inter<br>Serv | chang             | ge  | Argus         |     |
|---|-----------|------------------|-----|-----------------------|-----------|-------------------|-----|----------------------|-------------------|-----|-----------------------|-------------------|-----|---------------|-----|
| Hardware<br>Requirements                          |           |                  |     |                       |           |                   |     |                      |                   |     |                       |                   |     | Safety<br>Web |     |
|   | Sma<br>ll | Mid<br>-Siz<br>e |     | Ver<br>y<br>Lar<br>ge | Sma<br>ll | Mid<br>-Siz<br>ed |     | Sma<br>ll            | Mid<br>-Siz<br>ed |     | Sma<br>ll             | Mid<br>-Siz<br>ed |     |               |     |
| RAM   |           |                  |     |                       |           |                   |     |                      |                   |     |                       |                   |     |               |     |
| 2 GB  |           |                  |     |                       |           |                   |     |                      |                   |     |                       |                   |     | Yes           |     |
| 4 GB  |           |                  |     |                       | Yes       | Yes               | Yes | Yes                  | Yes               | Yes | Yes                   | Yes               | Yes |               | Yes |
| 4 - 8 GB  | Yes       |                  |     |                       |           |                   |     |                      |                   |     |                       |                   |     |               |     |
| 8 - 16 GB   |           | Yes              |     |                       |           |                   |     |                      |                   |     |                       |                   |     |               |     |
| 16 - 32 GB  |           |                  | Yes | Yes                   |           |                   |     |                      |                   |     |                       |                   |     |               |     |
| CPU/Processor                                     |           |                  |     |                       |           |                   |     |                      |                   |     |                       |                   |     |               |     |
| 1 Dual Core<br>CPU X 3 GHz                        |           |                  |     |                       | Yes       |                   |     | Yes                  |                   |     | Yes                   |                   |     |               | Yes |
| 2 Dual Core<br>CPUs X 3 GHz                       |           |                  |     |                       |           | Yes               | Yes |                      | Yes               | Yes |                       | Yes               | Yes |               |     |
| Equivalent to 2 -<br>4 Dual Core X<br>3GHz        | Yes       |                  |     |                       |           |                   |     |                      |                   |     |                       |                   |     |               |     |
| Equivalent to 4 -<br>8 Dual Core X<br>3GHz        |           | Yes              |     |                       |           |                   |     |                      |                   |     |                       |                   |     |               |     |
| Equivalent to 16<br>Dual Core X<br>3GHz           |           |                  | Yes | Yes                   |           |                   |     |                      |                   |     |                       |                   |     |               |     |
| Pentium IV X 3<br>GHz                             |           |                  |     |                       |           |                   |     |                      |                   |     |                       |                   |     | Yes           |     |
| Fail Support Plat                                 | form      |                  |     |                       |           |                   |     |                      |                   |     |                       |                   |     |               |     |
| Dataguard<br>(physical<br>standby option)         | Yes       |                  |     |                       |           |                   |     |                      |                   |     |                       |                   |     |               |     |
| Virtualization                                    |           |                  |     |                       |           |                   |     |                      |                   |     |                       |                   |     |               |     |
| Physical Server                                   |           |                  |     |                       | Yes       |                   |     | Yes                  |                   |     | Yes                   |                   |     |               |     |
| Oracle Virtual<br>Machine (OVM<br>3.2.10, 64-bit) | Opti      | onal             |     |                       | Yes       |                   |     | Yes                  |                   |     | Yes                   |                   |     |               |     |
| Others  |           |                  |     |                       |           |                   |     |                      |                   |     |                       |                   |     |               |     |
| Exadata 12c R1<br>(with 12.1.0.2)                 | Opti      | onal             |     |                       |           |                   |     |                      |                   |     |                       |                   |     |               |     |

| Hardware<br>Requirements                | Argus Safety<br>Database Server | Argus Safety<br>Web Server | Argus<br>Transaction<br>Server | Argus<br>Interchange<br>Server | Argus<br>Safety<br>Web<br>Client | Argus<br>End of<br>Study<br>Unblindi<br>ng Tool<br>(EOSU) |
|---|---------------------------------|----------------------------|--------------------------------|--------------------------------|----------------------------------|---|
| Oracle RAC 12c<br>R1 (with<br>12.1.0.2) | Optional                        |                            |                                |                                |                                  |   |
| Minimum<br>Resolution                   |                                 | 1280X1024                  | 1280X1024                      | 1280X1024                      | 1280X<br>1024                    | 1280X10<br>24   |

### **General Pre-Installation Tasks**

Before installing the Argus Safety software, be sure to do the following:

- Set the resolution for the client workstation to a minimum of 1280 X 1024 for optimum viewing of the application. If the screen resolution is less than 1280 X 1024, some of the field labels may appear truncated.
- Make sure that the regional settings on the web server are American settings.
- Install East Asian languages on the following:
  - Argus Web Server
  - Argus Service Server
  - Interchange Transaction Server
  - Argus Web client machines
  - Install the Japanese font pack for Adobe Reader on the Argus Web client machines. If you fail to install this font pack, you will be unable to view the Japanese data correctly.

### **Installation Process Overview**

The following is the recommended order for installing the Argus Safety solution components:

- **1.** Install the Schema Creation Tool
- 2. Create/Upgrade Argus Safety Database Schema
- 3. Load the Factory Data
- 4. Execute the Argus Safety Database Schema Validation
- 5. Install the Argus Safety Web Component
- 6. Load MedDRA
- 7. Load WHO-Drug
- **8.** Load J Drug (if you are using Argus J)
- 9. Install the Argus Safety Services / Interchange Service / Interchange Mapping
- 10. Configure the Argus Safety Service
- **11.** Configure the Interchange Service
- 12. Install and Configure Axway Synchrony

**13.** Maintain Installation

**Note:** In this release, merging of databases into a Multi-Tenant Database does not support merging of DLP data.

### **Converting Argus Safety Report Server to Argus Web Server**

Execute the following steps to convert Argus Safety Report Server to Argus Web Server:

- 1. Navigate to the Argus Safety Report Server.
- 2. Go to C:\Windows and open the argus.ini file.
- **3.** Delete references to the **ReportServerUser**, **ReportServerPassword** and **ReportServerPriority**.
- 4. Update the entry for **ReportServer** to **HTTP://Localhost**

# Starting the Installation

This chapter provides information about starting the installation. It includes discussions of the following:

- Getting Started
- Installing the Files Required to View Japanese Text

### **Getting Started**

Argus Safety is a configurable system and, based on user needs, administrators may install all or only some of the components. If you choose to install multiple components, the installation steps may vary from what is described in this documentation. In such cases, refer to the installation instructions for each component.

Before starting the installation procedure do the following:

- 1. Log on 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 run Setup.exe.

**Note:** If Terminal Services are enabled, use the Add or Remove Programs utility in the Control Panel to install Argus Safety Solution components. Go to Control Panel > Add or Remove Programs > Add New Programs, open the setup.exe in your local directory.

**4.** Follow the setup screens to continue the installation.

To perform any database upgrade, refer to the chapter 3 – Installing the Argus Safety Database. To install Argus Safety application, refer to Chapter 4 and subsequent chapters for detailed installation instructions for each component.

### Installing the Files Required to View Japanese Text

If your Argus Web client machine is on an English operating system, and you are using the Argus J version of Argus Safety, you must install Windows Supplemental Language Support for East Asian languages and Japanese font pack for Adobe Reader in order to view Japanese text correctly. Make sure that you have sufficient free disk space for installing the language packs.

# **Installing the Argus Safety Database**

This chapter describes the steps in creating, upgrading, and validating the Argus Safety Database schema. The following topics are contained in the chapter:

- Overview
- Schemas Required for Database Instances
- Setting up Oracle Parameters
- Creating the Argus Safety Database Schema
- Loading Factory Data
- Enabling and Disabling Oracle Text
- Working with the MedDRA and MedDRA J Dictionaries
- Loading the WHO-DRUG Dictionary
- Validating the Argus Safety Database
- Enabling and Disabling DLP
- Upgrading the Argus Safety Database
- Merging a Single Enterprise Safety Database into a Multi-tenant Database
- Copy Configuration Tool

#### **Overview**

Argus Safety installation requires a database instance. To set up Axway, a separate database instance is required.

- The Argus Safety database can be set up using the Schema Creation Tool.
- If DLP is to be set up, use the Enable DLP option in the Schema Creation Tool. The DLP Schema is created in the Argus instance only. No separate instance is required for DLP setup
- Axway Synchrony Database Instance (Optional)

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

**Note:** The Create DB User script provided with this release is meant as an alternative to the SYSTEM user. 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 Argus Safety Schema Creation Tool functionalities (such as Schema Creation, Upgrade), then the Validation File might display some extra or missing privileges for the system and/or for the newly created DBA user.

### Schemas Required for Database Instances

The following sections outline the schemas you must create for each database instance.

#### Argus Safety Instance Database Schemas

The Argus Safety instance requires you to create database schemas. The Argus schema and the Interchange Service schema are required for all systems. The other schemas you create are MedDRA or WHO.

Argus Schema:

Use the Argus Safety Schema Creation Tool to create this database schema. This is a required schema.

Interchange Service Schema:

Use the Argus Safety Schema Creation Tool to create this database schema. This is a required schema.

ESM Query Schema:

Use the Argus Safety Schema Creation Tool to create this database schema. This is a required schema.

BI Publisher Schema:

You must create this schema to hold the BI Publisher Periodic Reporting related objects. This schema must be created even though BI Publisher Periodic Reporting is an optional component.

DLP Schema:

This is optional. You can create this schema if DLP is to be enabled.

DLP ESM Query Schema:

This is optional and required when DLP is enabled. You can create this schema from Argus Safety Schema Creation tool while DLP is enabled.

MedDRA Schema:

You must create this schema if MedDRA is to be enabled. This schema is created by the MedDRA Loader Tool when MedDRA is loaded to the new database tables.

J Drug Schema:

You must create this schema if J Drug is to be enabled.

WHO Schema:

You must create this schema if WHO is to be enabled. This schema is created by the WHO Loader Tool when WHO is loaded to the new database tables.

**Note:** Argus Safety 8.1 provides a security regime much stricter than the previous releases.

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.

#### Axway Synchrony Database Instance (Optional)

The Axway Synchrony Database Instance is optional and is applicable only if Axway Synchrony is required.

### Setting up Oracle Parameters

This chapter provides the recommended Oracle parameter values for Argus Safety databases.

#### Oracle Database Settings

The tables in this section list the suggested parameters, configurations, and/or settings for an Oracle database for various sized companies as follows:

- Small refers to companies with less than 30,000 cases in the database.
- Mid-sized refers to companies with 30,000 to 200,000 cases in the database.
- Large refers to companies with 200,000 to 1 million cases in the database.
- Very Large refers to companies with more than 1 million cases in the database.

#### **Argus Safety Database Instance Parameters**

Oracle Database parameters are recommendations only, and may differ based on various factors including company's policy, database server needs, configuration and data load. These recommended values should be evaluated for each specific site based on the intended use of the application, business needs, performance testing and adjusted accordingly.

| # | Database<br>Parameters                | Small                                 | Mid-Sized                             | Large                              | Very Large                         |
|---|---------------------------------------|---------------------------------------|---------------------------------------|------------------------------------|------------------------------------|
| 1 | MEMORY_<br>TARGET                     | 2 GB                                  | 3 GB                                  | 10 GB                              | >10 GB                             |
| 2 | PROCESSES                             | Expected<br>concurrent users +<br>100 | Expected<br>concurrent users +<br>100 | Expected concurrent<br>users + 100 | Expected concurrent<br>users + 100 |
| 3 | MEMORY_                               | >= value set                          | >= value set                          | >= value set                       | >= value set                       |
|   | MAX_TARGET                            | for MEMORY_<br>TARGET                 | for MEMORY_<br>TARGET                 | for MEMORY_<br>TARGET              | for MEMORY_TARGET                  |
| 4 | OPTIMIZER_<br>SECURE_VIEW_<br>MERGING | FALSE                                 | FALSE                                 | FALSE                              | FALSE                              |

| -  | <b>-</b>                     |        |           |       |            |
|----|------------------------------|--------|-----------|-------|------------|
| #  | Database<br>Parameters       | Small  | Mid-Sized | Large | Very Large |
| 5  | CURSOR_<br>SHARING           | EXACT  | EXACT     | EXACT | EXACT      |
| 6  | WORKAREA_<br>SIZE_POLICY     | AUTO   | AUTO      | AUTO  | AUTO       |
| 7  | JOB_QUEUE_<br>PROCESSES      | 25     | 25        | 25    | 25         |
| 8  | SHARED_<br>POOL_SIZE         | 500 MB | 500 MB    | 1 GB  | 2 GB       |
| 9  | DB_CACHE_<br>SIZE            | 500 MB | 500 MB    | 1 GB  | 2 GB       |
| 10 | DB_BLOCK_<br>SIZE (bytes)    | 8192   | 8192      | 8192  | 8192       |
| 11 | PGA_<br>AGGREGATE_<br>TARGET | 500 MB | 500 MB    | 1 GB  | 2 GB       |

#### **Additional Database Setup Information**

| # | Setting                              | Small                | Mid-Sized            | Large                | Very Large        |
|---|--------------------------------------|----------------------|----------------------|----------------------|-------------------|
| 1 | Number and Size of Redo<br>Log Files | 5 Groups * 100<br>MB | 5 Groups * 100<br>MB | 5 Groups * 100<br>MB | 5 Groups * 100 MB |
| 2 | TEMP Tablespace Size                 | 8 GB                 | 16 GB                | 32 GB                | 64 GB             |
| 3 | Undo Tablespace Size                 | 8 GB                 | 16 GB                | 32 GB                | 64 GB             |

#### **GMT Offset Calculation**

For column level description, refer to the *Oracle Argus DBA Guide*. Verify that the value stored in the TABLE is accurate for GMT\_DIFF and other columns related to Day Light Saving.

Be aware of the following:

- Argus is using function gss\_util.gmt\_offset to derive the GMT OFFSET which impacts the calculation of GMT date and time.
- Use the following SQL queries to verify the GMT offset returned by the database function:
  - Query to get the current GMT Time offset
  - Query to get the current Timestamp and GMT Timestamp.
- Daylight Savings Time. Assume that Daylight Savings Time starts on First Sunday of April at 2:00 AM and it ends on Last Sunday of October at 2:00 AM.
  - Query to get GMT Time Difference just before the starting of Day Light Saving.
  - Query to get GMT Time Difference One Second After Day Light Savings started.
  - Query to get GMT Time Difference just before the End of Day Light Saving.
  - Query to get GMT Time Difference just After Day Light Savings ended.

### **Prerequisites for New Schema Creation**

Before creating a new schema, make sure that you run the "Create DBA User" scripts. This script asks the user to connect as an existing DBA User SYS to create a new DBA User with the proper granted access that will be used while running the Schema Creation Tool.

Note: It is mandatory to run this script when creating a new schema.

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

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 DBA User script.

If you use the newly created DBA User to execute the Argus Safety Schema Creation Tool functionalities (such as Schema Creation, Upgrade), then the Validation File might display some extra or missing privileges for the system and/or for the newly created DBA user.

To perform the above-mentioned action, go to the Start menu, run the Create DBA User script, and follow the steps given below:

- 1. Enter a new log file name to store the output of the script execution.
- 2. Enter the TNSName of the database where the Schema Creation Tool will be run.
- 3. Enter the Password for SYS account.
- 4. Enter the name for a new <DBA User account> that will be created.
- 5. Enter the <password> for the new account.
- 6. Follow the remaining steps to complete the script.

After the script has successfully run, use the new DBA user account entered in Step 4 when running the Schema Creation Tool to create the Argus Safety Schema.

#### Creating the Argus Safety Read Only Database Account (Optional)

If you required a database account that can connect to the Argus Safety Schema with Read Only Privileges, a script has been provided that you can run to create this account.

**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.

From the Start menu, run the script "Create Read-only Database User" and follow the steps provided in the script.

#### Creating the Argus Safety Database Schema

Two (2) required steps and one (1) optional step are involved in creating Argus Safety database schema as follows:

Installing the Argus Safety schema creation tool

- Creating the Tablespace (optional)
- Creating the Argus schemas using the schema creation tool

**Note:** The source Argus Safety Database must have AL32UTF8 character set. When DLP is enabled, DLP Schema will be a part of the Argus Safety database.

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

- Log in to the Database as the SYS user.
- Execute: ALTER SYSTEM SET NLS\_LENGTH\_ SEMANTICS=CHAR SCOPE=BOTH;
- Shutdown and Startup the database after applying the above statement.

#### XDB Schema Installation Requirement for Interchange

Oracle Schema XDB must be present for Interchange packages to load.

If Schema XDB does not exist, use the following procedure to create it:

- 1. Click sqlplus.exe
- **2.** Connect to **sys** as **sysdba**.
- 3. Execute the ?/rdbms/admin/catqm.sql script.
- 4. Provide the following required parameters
- user password
- user default tablespace
- user temporary tablespace

For example: SQL>@?/rdbms/admin/catqm.sql SYSTEM SYSAUX TEMP

#### Installing the Schema Creation Tool

**Note:** Make sure that you disable the UAC (User Account Control) in order to run the schema creation tool.

Before installing the **Schema Creation Tool** on a server, verify that an Oracle client with Administrator option is installed on the server.

- 1. When Argus Safety Setup opens the Argus Safety Solution Components dialog box:
  - Select the Schema Creation Tool.
  - Click Next.
- 2. The system begins the installation procedure and displays the Setup Status screen.
  - The system displays installation progress.
- 3. When the system displays the Setup Completed screen:

- Click Finish.
- **4.** When the system copies the required files to the system and displays the following message:
  - Click **OK** to reboot the system.

#### Creating the Tablespaces

If you wish to create tablespaces before installing Argus Safety, the following information shows the different tablespaces. However, this step is optional.

| # Tablespace Name |
|-------------------|
|-------------------|

- 1 ARGUS\_AEXP\_DATA\_01
- 2 ARGUS\_AEXP\_INDEX\_01
- 3 ARGUS\_AL\_DATA\_01
- 4 ARGUS\_AL\_INDEX\_01
- 5 ARGUS\_DATA\_01
- 6 ARGUS\_DATA\_02
- 7 ARGUS\_DATA\_03
- 8 ARGUS\_DATA\_04
- 9 ARGUS\_DATA\_05
- 10 ARGUS\_INDEX\_01
- 11 ARGUS\_INDEX\_02
- 12 ARGUS\_INDEX\_03
- 13 ARGUS\_INDEX\_04
- 14 ARGUS\_INDEX\_05
- 15 ARGUS\_INDEX\_06
- 16 ESM\_DATA\_01
- 17 ESM\_INDEX\_01

The schema creation tool creates the tablespaces if they do not exist.

#### Creating the Schema

**Note:** Refer to the chapter Argus Password Management -Cryptography Tool to create the Cryptographic key before creating the new schema.

Before creating the schema, verify that:

- A blank Oracle database instance is available
- A SYSTEM user account is available
- The Oracle database is available from the machine where the schema creation tool is installed

Use the following procedure to create the schema.

- **1.** Open the schema creation tool.
  - Click Create Schema.
- **2.** When the system displays the Oracle Database Connect dialog box, enter the Password associated with the system user and the Database.
  - Enter the password associated with the system user in the Password field and the database name in the Database field.
  - Click OK.
- **3.** When the system displays the Argus Safety Schema Creation Options dialog box:

| Schema Options                 |                 |                     |                  |   |
|--------------------------------|-----------------|---------------------|------------------|---|
| Database <u>S</u> ize:         |                 | Time Zone:          |                  |   |
| Small                          | •               | India               |                  | • |
| Password:                      |                 | Verify Password:    |                  |   |
| ******                         |                 |                     |                  |   |
| Credentials for VPD Admin User |                 |                     |                  |   |
| VPD Admin Schema Owner:        | Password:       |                     | Verify Password: |   |
| VPD_OWNER                      | ******          |                     | ******           |   |
| Schema Owner                   | 1               | ESM Support         |                  |   |
| Argus Safety Schema Owner:     |                 | ESM Schema Own      | er:              |   |
| ARGUS_APP                      | •               | ESM_OWNER           |                  | • |
|                                | ESM Login User: |                     |                  |   |
| Access Privileges              |                 | ESM_LOGIN           |                  | * |
| Argus Safety Role:             | ESM Role:       |                     |                  |   |
| ARGUS_ROLE                     | -               | ESM_ROLE            |                  | - |
| Argus Safety Grantees:         |                 | ESM Query User:     |                  |   |
| APEX 030200                    |                 | ESM_QUERY           |                  | • |
| APEX_030200                    | ^               |                     |                  |   |
| APEX_PUBLIC_USER               |                 | BIP                 |                  |   |
| APPQOSSYS                      |                 | BIP Schema Owne     | er.              |   |
| ARGUS_LOGIN_I                  | ×               | BIP_OWNER           |                  | • |
|                                |                 |                     |                  |   |
| Application Type               |                 |                     |                  |   |
| Single-tenant     Mult         | i-tenant        |                     |                  |   |
| Default Enterprise Details     |                 |                     | 015              |   |
| Enterprise Name: ENTERPRISE1   |                 | Enterprise Short Na | ame: ENT1        |   |
|                                | 1950            |                     |                  |   |

- Enter the user name in the VPD Admin Schema Owner field.
- Enter the user's password in the **VPD Admin Schema Owner Password** field.
- Reenter the user's password in the **Verify Password** field.
- 4. When the system displays the New User dialog box:
  - Enter the user name in the **New User Name** field.
  - Enter the user's password in the New User Password field.
  - Reenter the user's password in the **Re-enter Password** field.

- Verify that the Default Tablespace and Temporary Tablespace values are correct.
- Click **OK**.
- **5.** When the system displays the Argus Safety Schema Creation Options dialog box, repeat Steps 3 and 4 until you have created all the users.
- 6. When the system displays the Argus Safety Schema Creation Options dialog box:
  - Click New Role to create the following roles as appropriate:
    - Argus Role
    - Interchange Role
- 7. When the system displays the New Role dialog box:
  - Type the role name in the **New Role** field.
  - Click OK.
- **8.** When the system redisplays the Argus Safety Schema Creation Options dialog box:
  - Locate the Argus Safety Schema Owner drop-down list and select the Argus Schema Owner you created.
  - Locate the Schema Options and select the appropriate Database Size and the Time Zone.
  - Select the appropriate Argus Role from the Argus Safety Role drop-down list.
  - Locate Argus Safety Grantees and select the appropriate Argus Login account.
  - Locate the Interchange Support section and do the following:
    - Select the Interchange Schema Owner from the drop-down list.
    - Select the Interchange Role from the drop-down list.
    - Select the Interchange Login User from the drop-down list.
    - Select the Interchange Query User from the drop-down list.
  - Enter password for the ARGUSUSER user.
  - Under BI Publisher, create a new BI Publisher Schema by clicking New User, and select the created schema from the BI Publisher Schema Owner drop-down list.
  - Select an Application Type from the following two radio buttons:
    - Single Tenant Selecting this option allows the database to only support a single tenant. The options to create multiple tenants in the safety system is diabled.
    - Multi-Tenant Selecting this option allows the database to support multiple tenants. Users are able to create multiple tenants using the Global Enterprise setup screens.
  - Select the Default Enterprise from the following:
    - Enterprise Name
    - Enterprise Short Name
  - Click Generate.

**9.** If the Tablespace Creation dialog box displays, you may create new tablespaces or use existing tablespaces as follows:

| Tablespaces        | Small<br>Model | Medium<br>Model | Large<br>Model | Complete Path and Data File Name         |
|--------------------|----------------|-----------------|----------------|--|
| ARGUS_AEXP_DATA_01 | 667M           | 1213M           | 2272M          | C10RADATA\ASDOCDB\ARGUS_AEXP_DATA_01.dbf |
| ARGUS_AEXP_NDEX_01 | 60M            | 994             | 142M           | C10RADATA\ASDOCDB\ARGUS_AEXP_NDEX_01.dbf |
| ARGUS_AL_DATA_01   | 76M            | 238M            | 580M           | C:\ORADATA\ASDOCDB\ARGUS_AL_DATA_01.dbf  |
| ARGUS_AL_NDEX_01   | 76M            | 125M            | 206M           | C:\ORADATA\ASDOCDB\ARGUS_AL_NDEX_01.dbf  |
| ARGUS_DATA_01      | 1035M          | 3029M           | 3248M          | C.\ORADATA\ASDOCDB\ARGUS_DATA_01.dbf     |
| ARGUS_DATA_02      | 751M           | 4644M           | 2829M          | C.\ORADATA\ASDOCDB\ARGUS_DATA_02.dbf     |
| ARGUS_DATA_03      | 4771/          | 650M            | 1228M          | C:\ORADATA\ASDOCDB\ARGUS_DATA_03.dbf     |
| ARGUS_DATA_04      | 483M           | 775M            | 1460M          | C:IORADATA\ASDOCDB\ARGUS_DATA_04.dbf     |
| ARGUS_DATA_05      | 285M           | 456M            | 855M           | C:\ORADATA\ASDOCDB\ARGUS_DATA_05.dbf     |
| ARGUS_NDEX_01      | 764M           | 1526M           | 3216M          | C:\ORADATA\ASDOCDB\ARGUS_NDEX_01.dbf     |
| ARGUS_NDEX_02      | 1283M          | 9516M           | 5526M          | C:\ORADATA\ASDOCDB\ARGUS_NDEX_02.dbf     |
| ARGUS_NDEX_03      | 572M           | 722M            | 1243M          | C\ORADATA\ASDOCDB\ARGUS_NDEX_03.dbf      |
| ARGUS_NDEX_04      | 279M           | 377M            | 623M           | C10RADATA\ASDOCDB\ARGUS_NDEX_04.dbf      |
| ARGUS_NDEX_05      | 466M           | 733M            | 2032M          | C:\ORADATA\ASDOCDB\ARGUS_NDEX_05.dbf     |
| ARGUS_NDEX_06      | 169M           | 2961            | 803M           | C:10RADATA\ASDOCDB\ARGUS_NDEX_06.dbf     |
| ESM_DATA_01        | 362M           | 591M            | 1016M          | C:\ORADATA\ASDOCDBIESM_DATA_01.dbf       |
| ESM_NDEX_01        | 373M           | 483M            | 673M           | C10RADATA\ASDOCDBIESM_NDEX_01.dbf        |

- Under Complete Path and Datafile, enter the complete path (including the filename) under which the data file is located on the database server.
- If the data file does not exist, the system automatically creates it. It will automatically be created.
- If the data file exists, the system prompts you to use the current data file.
   Select Yes in the dialog box.

**Note:** The Tablespace Creation dialog box appears if the Database Size was selected as **Small**, **Medium**, or **Large**. It will not appear if the database size was selected as **Default**.

When you have existing tablespaces, you may use them; you are not required to create new ones. The system will not regenerate the tablespaces. If a tablespace already exists the Argus Schema Creation tool will warn you to select **Yes** to use an existing tablespace.

- 10. When the system opens the Argus Safety Database Installation dialog box:
  - Select Pause on error.
  - Select Continue to start the Schema Creation Process. It may take some time to complete the schema creation process.

**Note:** Select Pause on Error to pause the system when an error occurs. This is essential for troubleshooting Schema creation problems. You can also select the Show All box to display the SQL statements the system is executing. However, to create the database schema more quickly, we recommend clearing the Show All check box. The system enters all executed SQL statements in a log file.

- **11.** When the schema creation process is complete:
  - Click Open to open the schema creation log file.

Click Finish.

# Creating the Argus Safety Read Only Database Account (Optional)

If you require a database account that can connect to the Argus Safety Schema with Read Only Privileges, a script has been provided that you can run to create this account.

From the Start menu, run the script "Create Read-only Database User" and follow the steps provided in the script.

## Loading Factory Data

Before loading factory data verify that:

- The schema creation tool is installed
- An Oracle database instance is available
- A SYSTEM or DBA user account has been created

To load Factory Data into the Argus Safety database:

- 1. Open the schema creation tool.
  - Click Factory Data.
- When the system opens the Connect to Database dialog box, enter the Argus Schema Owner Name, Password, and the Database name in the appropriate fields and click OK.
  - Enter the name of the Argus Schema Owner and the password.
  - Click OK.
- **3.** When the system opens the Connect to Database dialog box a second time:
  - Enter the name of the Interchange Schema Owner and the password.
  - Click OK.
- 4. Enter the default user passwords for the Admin User and the System User.
  - Verify the passwords for both users in their Password Verify fields.
  - Click OK.
- **5.** The system loads the factory data into the database and displays the following message: *Factory Data has been loaded*. *Please check your factory data folder for "Log" files*.
  - Click OK.
- **6.** Check the .LOG files in the \DB Installer\Factory\_Data\ folder to verify that the factory data loaded without errors.
- **7.** The system displays the following message: *Oracle text is mandatory. Please press the OK button to enable Oracle text.* 
  - Click **OK**.

**Note:** You can disable the following dashboard triggers, if you are not using the Oracle Argus Safety dashboard feature:

- TRG\_CA\_DSHBRD\_ROW\_AFT\_UPD
- TRG\_CMRR\_DSHBRD\_ROW\_AFT\_UPD
- TRG\_CMRR\_DSHBRD\_TBL\_AFT\_UD
- TRG\_CSRR\_DSHBRD\_ROW\_AFT\_UPD
- TRG\_CSRR\_DSHBRD\_TBL\_AFT\_IUD
- TRG\_LPF\_DSHBRD\_ROW\_AFT\_UPD
- TRG\_LPF\_DSHBRD\_TBL\_AFT\_UPD

However, if you enable these triggers again, you should populate the data for the existing cases. Since these triggers get enabled after each upgrade, make sure that you disable these triggers.

Implement these instructions after completing the database upgrade, listed in the Upgrading the Argus Safety Database section.

# **Enabling and Disabling Oracle Text**

Oracle Text search is an index-based querying solution that improves Duplicate Case search performance. This section provides information about enabling and disabling Oracle Text.

**Note:** If you do not use the Schema Creation Tool to install Oracle Text and the Common Profile Switch is enabled, running a search from the Argus Book-in screen can cause the system to display the following error message:

*Oracle Text is not installed correctly. Please install/verify the Oracle Text installation first.* 

### Enabling Oracle Text

Once enabled, Oracle Text performs the following functions:

- DB Installer checks whether Oracle Text is installed. If not, it displays an error message that Oracle Text not installed. Please install Oracle Text before adding this feature.
- Estimates the Tablespace Size Requirements and adjusts as required.
- Populates existing cases in the Oracle Text duplicate Search Table for indexing. This process can take a few hours.
- Creates the Oracle Text Index.
- Creates the PDP job for Delta updates.
- Updates the CMN\_PROFILE Key, ORA\_TXT\_SRCH\_ENABLE, to a value of 1.

Before enabling Oracle Text, there must be enough free space available in the tablespace. If there is not enough free space available, the system displays the following dialog box with the amount of space currently available (in megabytes).

Click **OK** and provide the required free space before enabling Oracle Text.

Use the following procedure to enable Oracle Text:

- **1.** Open the Schema Creation Tool.
  - Click Oracle Text.
- 2. When the system displays the Enable/Disable Oracle Text dialog box:
  - Click Yes.
- **3.** When the system displays the Enable Oracle Text dialog box, enter the connection parameter in the Argus Database Name field and click **Proceed**.

|                                      | E                             | nable Oracle Text                |         |               |
|--------------------------------------|-------------------------------|----------------------------------|---------|---------------|
| Database Connection                  |                               | Argus Schema Password:           |         |               |
| Argus Schema Owner:<br>DBA Username: | SYSTEM                        | Password:                        | [······ |               |
| Log Directory:                       | C:\Program Files (x86)\Oracl  | e\Argus\DBinstaller              | SelectL | og Directory  |
| Status                               |                               |                                  |         |               |
| Enabling Oracle Text 0               |                               |                                  |         |               |
| g File: C:\Program Files             | (x86)\Oracle\Argus\DBinstalle | riOracleTextLog_20160629144536.t | View    | <u>C</u> lose |
|                                      |                               |                                  |         |               |

- Enter the database connection parameter.
- Enter the Oracle Text Log Directory.
- Click Proceed to enable Oracle.
- View Oracle Text Log.
- Click Close to exit.
- 4. Oracle Text is enabled. Click **Close** to exit.
- 5. Run the schema validation tool to validate the schema.

### **Disabling Oracle Text**

After Oracle Text is disabled, the system performs the following functions:

- Updates the CMN\_PROFILE Key, ORA\_TXT\_SRCH\_ENABLE, to a value of 0
- Deletes the PDP Job
- Drops the Oracle Text Index
- Truncates the Duplicate Case Search Table

Use the following procedure to disable Oracle Text.

- **1.** Open the **Schema Creation Tool**.
  - Click Oracle Text.

- 2. When the system displays the Enable/Disable Oracle Text dialog box:
  - Click No.
- 3. When the system displays the Disable Oracle Text dialog box:

| atabase Connection              |                               |                        |                      |
|---------------------------------|-------------------------------|------------------------|----------------------|
| Argus Database Name:            | ASDOCDB                       |                        |                      |
| Argus Schema Owner:             | ARGUS_APP                     | Argus Schema Password: |                      |
| DBA Username:                   | SYSTEM                        | Password               |                      |
| Log Directory:                  | C:\Program Files (x86)\Oracle | a\Argus\DBInstaller    | Select Log Directory |
|                                 | Second also                   |                        | Proceed              |
| atus<br>Disabling Oracle Text ( | Somplete.                     |                        | Proceed              |
|                                 | Complete.                     |                        | Proceed              |

- Enter the database connection parameter in the Argus Database Name field.
- Enter the Oracle Text Log Directory.
- Click Proceed to disable Oracle Text. The system disables Oracle Text.
- View Oracle Text Log.
- Click Close to exit.

## Implementing Table Partitioning

**Note:** Partitioning is an optional module that can be purchased from Oracle database.

Partitioning of CMN\_AUDIT\_LOG table can significantly improve performance of the system on large Argus Safety databases. Range partitioning can be performed on CMN\_AUDIT\_LOG table for LOG\_DATETIME\_STAMP column.

We recommend that you create partitioning on a yearly basis. Partitioning must be performed and maintained by a qualified database administrator.

## Working with the MedDRA and MedDRA J Dictionaries

The minimum space required to install MedDRA and MedDRA J on your system is 50 MB. Verify that you have that amount of space available before loading MedDRA and MedDRA J. You also need to verify that:

- The schema creation tool is installed
- An Oracle database instance is available

A SYSTEM user account has been created

**Note:** If loading MedDRA V8 or V8.1, the smq\_list.asc and smq\_ content.asc files containing SMQ data must be placed in the same folder as the other dictionary files.

### Loading the MedDRA Dictionary

To load the MedDRA dictionary into the database:

- 1. Open the Schema Creation Tool:
  - Click MedDRA Loader.
- 2. When the system displays the Oracle Database Connect dialog box, Click OK.
  - Enter the Password associated with the SYSTEM user and the Database name.
  - Click OK.
- **3.** When the system displays the MedDRA Dictionary Loader dialog box, do the following:
  - Select Load to New Tables if a MedDRA dictionary has not been loaded before.
  - Select MedDRA J if you are loading a MedDRA J dictionary.
  - Locate the Tablespace Information section and select the tablespace and index from the drop-down lists. Select the applicable tablespace from the Tables drop-down list.
  - Click Create User to create a new MedDRA user.
- **4.** When the system displays the New MedDRA User dialog box:, enter the appropriate information in the fields and click **OK**.
  - Enter the name of the user in the New User Name field.
  - Enter the password in the New User Password field.
  - Re-enter the password in the Reenter Password field.
  - Click OK.
- 5. When the system redisplays the MedDRA Dictionary Loader dialog box again:
  - Click **Create Role**.
- **6.** When the system displays the New MedDRA Role dialog box:, enter the New Role name and click **OK**.
  - Enter the new role name in the **New Role** field.
  - Click OK.
- **7.** When the system redisplays the MedDRA Dictionary Loader dialog box:, locate the Dictionary to Load section and o the following:

|  | MedDRA Dictionar                                | y Loader    |
|--|---|-------------|
| Loading Option                             | s 🕞 Load to New Tables                          | MedDRA J    |
| Tablespace Inf                             | ormation  |             |
| Tables                                     | USERS   | <b>•</b>    |
| Indexes                                    | USERS   | ▼           |
| Load to New T                              | ables   |             |
| MedDRA L                                   | Jser MEDDRA151_J                                | Create User |
| MedDRA F                                   | Role MEDDRA151_J_ROLE                           | Create Role |
|  |   |             |
| Dictionary to Lo<br>MedDRA Ve<br>Dictionar | ersion 15.1J                                    | Browse      |
| MedDRA Ve<br>Dictionar                     | ersion 15.1J                                    |             |
| MedDRA Ve<br>Dictionar                     | rsion 15.1J<br>y Files y<br>y SO Non-Primary SO |             |

- a. Select the MedDRA Version to be loaded from the drop-down list.
- **b.** Click **Browse** to go to the directory where the dictionary files reside and select the appropriate dictionary files.
- **c.** Check the **MedDRA Browser** check box if this dictionary version is being used in the Argus Safety MedDRA Browser.
- d. Click Load.
- Select the MedDRA version to be loaded from the MedDRA Version drop-down list.
- 8. The system loads the dictionary and displays the following message.
  - Click **OK**.

#### **Overwriting an Existing MedDRA Dictionary**

If you find it necessary to overwrite an existing MedDRA dictionary, use the following procedure to do so.

- 1. Open the Schema Creation Tool.
  - Click MedDRA Loader.
- 2. When the system displays the Oracle Database Connect dialog box:
  - Enter the SYSTEM user password in the Password field and the database name in the Database field.
  - Click OK.
- **3.** When the system displays the MedDRA Dictionary Loader dialog box: locate the Loading Options section and do the following:

|                 | MedDF             | RA Dictionary Lo     | oader          |       |
|-----------------|-------------------|----------------------|----------------|-------|
| Loading Option  |                   |                      | -              |       |
| (• Overwr       | ite C Load to     | New Tables           | MedDRA J       |       |
| Tablespace In   | formation         |                      |                |       |
| Tables          | USERS             |                      |                | -     |
| Indexes         | USERS             |                      |                | •     |
| Overwrite Cur   | rent Dictionary - |                      |                |       |
| User            | MEDDRA151_J       |                      |                | -     |
| Password        | ******            | Verify Passwo        | rd ******      |       |
| Role            | MEDDRA151_J       | ROLE                 |                | -     |
|                 | Curren            | t Version to Overwri | ite            | -     |
|                 |                   |                      |                |       |
| Dictionary to L | oad               |                      |                |       |
| MedDRAV         | ersion 16.1J      |                      | <b>•</b>       |       |
| Dictiona        | ry Files          |                      | Bre            | owse  |
| C Prima         |                   | n-Primary SO 🔽 N     | fodDRA Browner |       |
| 1               |                   |                      | ACCORA DIOWSCI |       |
|                 |                   |                      |                |       |
|                 |                   |                      | 95100          |       |
| Re-Code         |                   |                      | Load           | Close |
| Status: Rea     | idy               |                      |                |       |
| 0.000           |                   |                      |                |       |
|                 |                   |                      |                |       |

- Select **Overwrite**.
- Select MedDRA J if you are loading a MedDRA J dictionary.
- Select the tablespace and index from the Tablespace and Index drop-down lists.
- Select the user from the **User** drop-down list.
- Enter the user password in the **Password** field; re-enter it in the Verify Password field.
- Select the appropriate role from the Role drop-down list.
- Select the version to overwrite from the Current Version to Overwrite drop-down list.
- Select the MedDRA version to load from the MedDRA Version drop-down list.
- Click Browse to go to the directory where the dictionary files reside and select the appropriate dictionary files.
- Click the MedDRA Browser check box if the dictionary version is being used in the Argus Safety MedDRA Browser.
- Click Load.
- **4.** When the system displays the Oracle Database Connect dialog box: enter the Password associated with the SYSTEM user and the Database name and click **OK**.
  - Enter the SYSTEM user password in the Password field and the database name in the Database field.
  - Click OK.
- **5.** When the system finishes overwriting the dictionary, it displays the Dictionary Load dialog box.

Click OK.

### **Recoding Events**

The following table lists and describes the options in the dialog box.

| Option                             | Point E  |  |  |  |
|------------------------------------|--|--|--|--|
| Argus MedDRA Version to Re-code    | Select the existing MedDRA version to re-code.                             |  |  |  |
| Enterprises                        | Select the enterprises to recode.  |  |  |  |
| Data Update/View Options [Currency | Check one or both of the following options:                                |  |  |  |
| determined at LLT Level Only]      | Process Current Terms (Using Primary SOC Path)                             |  |  |  |
|                                    | Process Non-current Terms (Using Primary SOC Path)                         |  |  |  |
|                                    | Select one of the following options:                                       |  |  |  |
|                                    | Update Data (Updates will be made to cases and to the audit log.)          |  |  |  |
|                                    | View Only (Updates <b>will not</b> be made to cases and to the audit log). |  |  |  |
| Output Log File Options            | Select an output log file option and directory path for the log files.     |  |  |  |
| Status                             | Displays status.   |  |  |  |

### **Event Recoding Dialog Box Options**

If you find it necessary to recode events, use the following procedure to do so:

- **1.** Open the Schema Creation Tool.
  - Click MedDRA Loader.
- **2.** When the system displays the Oracle Database Connect dialog box, enter the Password associated with the SYSTEM user and the Database name.
  - Enter the password for the SYSTEM user in the Password field and the database name in the Database field.
  - Click **OK**.
- 3. When the system displays the MedDRA Dictionary Loader dialog box:

|   | MedDRA Dictionar           | y Loader                   |
|---|----------------------------|----------------------------|
| Loading Option                              | s 📀 Load to New Tables     | MedDRA J                   |
| Tablespace Inf<br>Tables<br>Indexes         | ormation<br>USERS<br>USERS | -                          |
| Load to New T                               |                            | Create User<br>Create Role |
| ⊡Dictionary to Lo<br>MedDRA Vi<br>Dictionar | ersion 15.1J               | Browse                     |
|   | y SO 🔽 Non-Primary SO      |                            |
| Re-Code<br>Status: Rea                      |                            | Load Close                 |

- Click the Re-Code button.
- 4. When the system opens the Event Re-Coding dialog box, do the following:
  - Select the Enterprise to recode.

**Note:** If Argus is setup in Single Tenant Mode, you will only have one option here. If you are setup as a Multi-Tenant Database, you can choose which Enterprises to recode. Multiple enterprises can be selected.

- Select the existing version of MedDRA that needs to be re-coded.
  - Select a specific version to only recode data coded with that version.
  - Select All to recode all existing coded data regardless of the version it is coded with.
- Select either or all of the Process Current Terms, Process Non-Current Terms and/or Update dictionary version check boxes.
- Select Update Data if events are to be updated or select View Only if you are interested is just seeing what events will be coded without making the changes.
- Select the Output File format.
  - Delimited Text
  - Excel Sheet output
- Click on the Execute button to start the recoding process.
- When the system displays the Connect to Database dialog box, enter the Schema Owner name, Password, and Database. Click **OK**.

- Enter the schema owner name in the **Argus Schema Owner** field.
- Enter the password in the **Password** field.
- Enter the database name in the **Database** field.
- The system recodes the following fields from Case Form and Code List.

| Field Location | Name of Recoded Field  |
|----------------|------------------------|
| Case Form      | Death Details          |
|                | Lab Data               |
|                | Other Relevant History |
|                | Product Indications    |
|                | Events                 |
|                | Case Diagnosis         |
| Code List      | Product Indication     |
|                | Lab Test Types         |

### Loading the J Drug Dictionary

The J Drug Dictionary loader in the Schema Creation Tool now supports loading the English name from the English sub file that is part of J Drug Dictionary.

#### Before loading the J Drug Dictionary:

The following is the information necessary to load the J Drug Dictionary data into the Argus Safety Japan application.

- the dictionary distribution organization name and contact
- file to be used
- how the file to be used
- if any necessary file is to be created
- how to understand the current .mdb file that shows only a single drop-down list value for the release version on the J-drug dictionary loader.

**Assumptions:** J-Drug Dictionary distributor organization (MT Kyogikai) is a different organization from Oracle thus there is a possibility that their specification, scheme or procedure may change in future as per their own discretion.

The following is the detailed information:

J-drug dictionary distributor organization information

Organization Name: MT Kyogikai Contact Information: URL: http://www.iyaku.info/ TEL: +81-3-3230-2867 FAX: +81-3-3239-3954 e-mail:mtk@iyaku.info

#### J-drug loader load procedure

J drug loader loads the following files using dictionary loading tool:

- All\_Data.txt
- formulationcode.txt
- drugnameenglish.txt

All the files must be present to load the dictionary, and the file names must be same as mentioned above.

#### To create file All\_Data.txt:

Copy the 全件.txt file received from MT Kyogikai to Al\_Data.txt without character code conversion. This file must be a file which contains all the drug data records. A file that contains only the delta (difference from the previous release) must not be used for All\_Data.txt.

Sample All\_Data.txt'files:

"1114700","","6","外","","麻酔用エーテル","マスイヨウエーテル","麻酔用エーテル", "マスイヨウエーテル","","","350000000000000000","0","0000060","B","9705","3"

```
"1115F01","","4","注","","チアミラールナトリウム!","チアミラールナトリウム]",
"チアミラールナトリウム!","1115403","","31000000000000000000",
"0","0000080","C","9201","3"
```

#### To create formulationcode.txt file:

The file formulationcode.txt is a text file containing the drug formulation code information. You need to create this text file on your own. The drug formulation information is provided from MT Kyogikai on a document titled *Drug Name Data File and English Name Sub File Summary*. The formulation code list section provides the contents information of the formulationcode.txt file.

Format of the file formulationcode.txt:

- Physical file name: formulationcode.txt
- File format: CSV (Comma Separated Value) with 4 fields.
- Character Code: Shift-JIS code. (This file contains Kanji.)
- Field Information:

Field#1: Route of Administration --either of 1,4,6,8 (For example, 1=内用薬, 4=注射薬, 6=外用薬, 8=歯科用薬剤)

Field#2: Code --00, 10, 11, etc.

```
Field#3: Formulation name (Japanese)
(For example, 内服薬, 散剤, 末, etc.)
```

Field#4: Formulation name (English) (For example, medicine, Powders, <null>, etc.)

Sample formulationcode.txt:

1,10,散剤,Powders 1,11,末, 1,12,散, 1,13,細粒,Fine granules ... 8,46,噴霧剤,Spray 8,47,パスタ剤, 8,50,貼付剤,Attach 8,70,注射剤,Injection

The complete formulationcode.txt file as of Feb.2011 is available at:

https://support.oracle.com/epmos/main/downloadattachmentprocessor?parent=DOCUME NT&sourceId=1293240.1&attachid=1293240.1:formulationcode&clickstream=yes

#### To create drugnameenglish.txt file:

Copy the <sup>英名.txt</sup> file received from MT Kyogikai, and rename the file to drugnameenglish.txt. This file is added in order to support English Names in J dictionary

Sample drugnameenglish.txt:

"0000040","111270001","FLUOTHANE","","","","","" "0000060","1114700","ANESTHETIC ETHER","1","",","1010","B" "0000080","1115F01","THIAMYLAL SODIUM","1","","","9806","C"

#### To modify the.MDB file:

1. Open the jdrug.mdb from the following location:

<disk>:\Program Files\Oracle\Argus\DBInstaller

A table appears with J\_Drug table supported versions (second column).

2. To add a new version, modify the Meddra Version column.

For example, if 2015-OCT is the last version added, then to add a new version (2015-Dec) append the column value with a comma.

| Tables   | 48 |    | ID  |     | MeddraVersion  | • | MeddraTableName          |  |
|--|----|----|-----|-----|--|---|--------------------------|--|
| J_DRUG   |    | .0 | 1   |     | ,2007-APR,2012-APR,2014-APR,2014-AUG,2014-OCT,2015-                  |   | JPN_DRUG_DICT            |  |
| J_DRUG_Constraint                                      |    |    |     |     | APR,2015-OCT,2013-DEC.   |   |                          |  |
| J_DRUG_CB<br>J_DRUG_Index<br>J_DRUG_Sqls               |    |    | 4   |     | ,2007-APR,2012-APR,2014-APR,2014-AUG,2014-OCT,2015-<br>APR,2015-OCT, |   | JPN_FORMULATION_CODE_UST |  |
| J_DRUG_Versions     MeddraBrowserSql     SQLLoaderInfo |    |    | -   | 231 | ,2007-APR,2012-APR,2014-APR,2014-AUG,2014-OCT,2015-<br>APR,2015-OCT, |   | JPN_DRUG_DICT_ENG_SUB    |  |
| WHO_82_AFTER_LOAD                                      |    | *  | (Ne | ew) |  |   |                          |  |

**3.** Similarly, modify other rows, and for other tables wherever the previous version number exists.

#### To load the J Drug dictionary into the database:

- **1.** Open the Schema Creation Tool:
  - Click J Drug Loader.
- 2. When the system displays the Oracle Database Connect dialog box, Click OK.
  - Enter the Password associated with the SYSTEM user and the Database name.

- Click **OK**.
- **3.** When the system displays the J Drug Dictionary Loader dialog box, do the following:
  - Select Load to New Tables if a J-Drug dictionary is not loaded before.
  - Locate the Tablespace Information section and select the tablespace and index from the drop-down lists.
  - Click Create User to create a new J-Drug user
- **4.** When the system displays the New J-Drug User dialog box:, enter the appropriate information in the fields and click **OK**.
  - Enter the name of the user in the **New User Name** field.
  - Enter the password in the New User Password field.
  - Reenter the password in the Reenter Password field.
  - Click OK.
- 5. When the system redisplays the J-Drug Dictionary Loader dialog box again:
  - Click Create Role.
- **6.** When the system displays the New J-Drug Role dialog box:, enter the New Role name and click **OK**.
  - Enter the new role name in the New Role field.
  - Click OK.
- **7.** When the system redisplays the J-Drug Dictionary Loader dialog box:, locate the Dictionary to Load section and the following:
  - a. Select the J-Drug Version to be loaded from the drop-down list.
  - **b.** Click **Browse** to go to the directory where the dictionary files reside and select the appropriate dictionary files.
  - **c.** Check the **J-Drug Browser** check box if this dictionary version is being used in the Argus Safety MedDRA Browser.
  - d. Click Load.
- **8**. The system loads the dictionary and displays a message.
  - Click **OK**.

**Note:** \*Argus Safety will use and display J drug data from the latest J drug dictionary which is loaded in the database.

For example, if JDrug\_Aug\_2015 dictionary and JDrug\_OCT\_2015 dictionary are loaded in the database, then Argus Safety will use data from the latest dictionary i.e., JDrug\_OCT\_2015 dictionary.

#### Overwriting an Existing J Drug Dictionary

This section provides instructions for overwriting an existing J Drug dictionary and for recoding events.

If you find it necessary to overwrite an existing J Drug dictionary, use the following procedure to do so.

- 1. Open the Schema Creation Tool.
  - Click J Drug Loader.
- 2. When the system displays the Oracle Database Connect dialog box:
  - Enter the SYSTEM user password in the Password field and the database name in the Database field.
  - Click OK.
- **3.** When the system displays the J Drug Dictionary Loader dialog box: locate the Loading Options section and do the following:
  - Select Overwrite.
  - Select the tablespace and index from the Tablespace and Index drop-down lists.
  - Select the user from the **User** drop-down list.
  - Enter the user password in the **Password** field; re-enter it in the **Verify Password** field.
  - Select the appropriate role from the **Role** drop-down list.
  - Select the J Drug dictionary version to load from the Dictionary Version drop-down list.
  - Click Browse to go to the directory where the dictionary files reside and select the appropriate dictionary files.
  - Click Load.
- **4.** When the system displays the Oracle Database Connect dialog box: enter the Password associated with the SYSTEM user and the Database name and click **OK**.
  - Enter the SYSTEM user password in the Password field and the database name in the Database field.
  - Click OK.
- **5.** When the system finishes overwriting the dictionary, it displays the Dictionary Load dialog box.
  - Click OK.

# Loading the WHO-DRUG Dictionary

Before loading the WHO-DRUG dictionary, verify the following:

- Windows workstation PC is available to load the WHO-DRUG data on
- The PC has Oracle client installed, including the following:

SQLPLUS (Exe=sqlplusw)

SQL\*Loader (Exe=sqlldr)

- There is an updated TNSNAMES file and Oracle client to connect to the Argus Safety database.
- The following WHO-DRUG dictionary data files are available:

| bna.dd | ccode.dd    |
|--------|-------------|
| dda.dd | ddsource.dd |

| ing.dd | man.dd |  |
|--------|--------|--|
| dd.dd  | ina.dd |  |

 The format of the WHO-DRUG dictionary data files is Text and alternate rows are not blank.

**Note:** WHO-DRUG is loaded using sql\*load with DIRECT=TRUE option. Because of sql\*loader restrictions, **no one should have access** to the Argus Safety system while WHO-DRUG is being loaded.

You can load WHO-Drug dictionary as follows:

- Use the Load to New Tables option to load the dictionary to new tables
- Use the **Overwrite** option to overwrite existing and existing dictionary
- Use the **Format C** option to load the dictionary with a different format

### Loading the WHO-Drug Dictionary to New Tables

Use the following procedure to load WHO-Drug dictionary to new tables:

- **1.** Launch the Schema Creation Tool:
  - Click Who Drug Loader.
- 2. When the system displays the Oracle Database Connect dialog box:
  - Enter the SYSTEM password in the Password field. Enter the database name in the Database field.
  - Click **OK**.
- **3.** When the system opens the WHO-Drug Dictionary Loader dialog box do the following:
  - Click Load New Tables to load the dictionary into a separate schema.
  - Click Create User to open the New WHO-Drug User dialog box to open the New WHO-Drug User dialog box.

Provide the information required to create a new user and click **OK**.

**4.** The system reopens the WHO-Drug Dictionary Loader dialog box, click **Create Role** to open the New WHO-Drug Role dialog box.

| 1                              | WHO-Drug Dictionary Load       | ler         |
|--------------------------------|--------------------------------|-------------|
| Loading Options                |                                |             |
| C Overwrite (                  | Load to New Tables             |             |
| Dictionary Format              |                                |             |
| Format B2                      | C Format C                     |             |
| Tablespace Informat            |                                |             |
| Tables USEF                    | RS                             | -           |
| Indexes USEF                   | 2S                             | •           |
| Load to New Tables             |                                |             |
| Who-Drug User                  | WHODRUG_USER                   | Create User |
| Who-Drug Role                  | WHODRUG_ROLE                   | Create Role |
| Dictionary to Load             |                                |             |
| Dict Version                   | 2014-JUN                       | -           |
| Dictionary File                | C:\Dictionaries\who_dde_b2_jun | 1 2 Browse  |
|                                |                                |             |
| View Log file<br>Status: Ready | _                              | Load Close  |

- In the New WHO-Drug Role dialog box, enter the New Role name and click OK.
- **5.** When the system redisplays the WHO-Drug Dictionary Loader dialog box, locate the Dictionary to Load section and do the following:
  - In the New WHO-Drug Role dialog box, enter the New Role name and click OK.
- **6.** When the system displays the WHO-Drug Dictionary Loader dialog box with the appropriate information: click **Load**.
- **7.** When the system displays the Dictionary Load dialog box to indicate that the dictionary has loaded successfully: click **OK**.
  - Enter the SYSTEM password in the Password field. Enter the database name in the Database field.
  - Click **OK**.

### Loading the WHO-Drug Dictionary Using the Overwrite Option

Use the following procedure to when using the overwrite option to load the WHO-Drug Dictionary:

- **1.** Launch the Schema Creation Tool.
- 2. Click Who Drug Loader.
- 3. When the system opens the Oracle Database connect dialog box:
  - Enter the SYSTEM password in the Password field. Enter the database name in the Database field.
  - Click **OK**.
- **4.** When the system opens the WHO-Drug Dictionary Loader dialog box, do the following:

- Click **Overwrite** to overwrite existing dictionary files.
- Select the dictionary version to load.
- Click Browse to display the Select Folder dialog box and select the appropriate path and click Select.
- Click Load to load the dictionary.
- View WHO-Drug dictionary log.
- **5.** When the system opens the Oracle Database Connect dialog box, enter the SYSTEM User Password and click **OK**.
  - Enter the SYSTEM password in the Password field. Enter the database name in the Database field.
  - Click OK.
- **6.** When the system displays to Dictionary Load dialog box to indicate that the dictionary has loaded successfully:
  - Click **OK**.

### To Load the WHO-Drug Dictionary using the Format C Option

Format C is a WHO-Drug dictionary format. For information about this format, go to http://who-umc.org.

To load the WHO-DRUG dictionary using the Format C option:

- **1.** Launch the Schema Creation Tool.
  - Click Who Drug Loader.
- **2.** When the system displays the Oracle Database Connect dialog box, enter the SYSTEM Password and Database name. Click OK.
  - Enter the SYSTEM password in the Password field. Enter the database name in the Database field.
  - Click OK.
- **3.** When the system opens the WHO-Drug Dictionary Loader dialog box do the following:
  - Click Load New Tables to load the dictionary into a separate schema.
  - Click Create User to open the New WHO-Drug User dialog box When the system opens the New WHO-Drug User dialog box, provide the information required to create a new user and click OK.
  - Select Dictionary Format Format C
- 4. When the system reopens the WHO-Drug Dictionary Loader dialog box:
  - Click **Create Role** to open the New WHO-Drug Role dialog box. Provide the information required to create the new role. Click **OK**.
- 5. When the system redisplays the WHO-Drug Dictionary Loader dialog box:
  - Select the Dictionary Version to load from the drop-down list.
  - Click Browse to display the Select Folder dialog box and select the appropriate path.
- **6.** When the system displays the WHO-Drug Dictionary Loader dialog box with the appropriate information:

- Click Load.
- 7. When the system opens the Oracle Database Connect dialog box:
  - Enter the SYSTEM password in the Password field. Enter the database name in the Database field.
  - Click OK.
- **8.** When the system displays the Dictionary Load dialog box to indicate that the dictionary has loaded successfully, click **OK**.

# Validating the Argus Safety Database

A necessary step in installing Argus Safety is to validate the database after installation. Use the following procedure to validate the Argus Safety database.

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

To validate the Argus Safety database:

- 1. Launch the Schema Creation Tool.
  - Click Schema Validation.
- 2. When the system opens the Connect to Database dialog box:
  - Enter the user **Password**.
  - Enter the name of the database to be validated in the **Database** field.
  - Click OK.
- 3. When the system displays the Schema Validation dialog box:
  - Validate the values in the fields.
  - Locate the Validation CTL File section and click Browse to open the Selection Path for CTL File dialog box.
- 4. When the system opens the Selection Path for CTL file dialog box:
  - Click **OK**.
  - Locate and select the correct folder and CTL file for the database being validated.

| atabase Connection:  | SYSTEM@ASDOCDB                      |             | Validate DLP Schema            |            |                  |
|--|-------------------------------------|-------------|--------------------------------|------------|------------------|
| Isers and Roles  |                                     |             | DLP                            |            |                  |
| Argus Schema Owner:  | ARGUS_APP                           | -           | DLP Schema Owner:              | DLP_OWNER  |                  |
| Argus Role Name:   | ARGUS_ROLE                          | •           | DLP Schema Password:           | ******     |                  |
| Argus Login User.  | ARGUS_LOGIN                         | •           | DLP ESM Query User:            | DLP_ESM_QU | IERY             |
| ESM Schema Owner:  | ESM_OWNER                           | *           | DLP ESM Query Password:        |            |                  |
| ESM Role Name:   | ESM_ROLE                            | •           |                                |            |                  |
| ESM Login User:  | ESM_LOGIN                           | •           |                                |            |                  |
| ESM Query User:  | ESM_QUERY                           | •           |                                |            |                  |
| BIP Schema Owner:  | BIP_OWNER                           | *           |                                |            |                  |
|  |                                     |             |                                |            |                  |
| VPD Admin Schema Owner:  | VPD_ADMIN                           | •           |                                |            |                  |
| Validation CTL File<br>Validation CTL Folder and Fil                         | VPD_ADMN                            | •           | r/SchemaValidation/VLDN_81.CTL |            | Browse           |
| /alidation CTL File  |                                     | •DBinstalle |                                |            | Browse<br>Browse |
| Validation CTL File<br>Validation CTL Folder and Fil<br>Validation Log Files | C:\Program Files (x86)\Oracle\Argus | •DBinstalle |                                |            |                  |

- 5. When the system reopens the Schema Validation dialog box:
  - Locate the Validation Log Files section.
  - Click Browse to open the Selection Path for Creating Log Files dialog box.
- **6.** When the system opens the Selection Path for creating Log files dialog box:
  - Choose the folder where you want the system to create the log files.
  - Click OK.
- **7.** When the system displays the Schema Validation dialog box with the required entries:
  - Click Validate Schema.
- **8.** The system displays the cmd.exe screen to indicate that processing is taking place.
  - Press Enter when the system prompts you to do so.
- 9. When the system opens the Oracle Sql\*Plus window, press Enter.
- **10.** When the system opens another Oracle Sql\*Plus:
  - Note the path of the log files created during processing.
- 11. Exit from the Schema Creation Tool.
- **12.** Check the files for errors.

## Enabling and Disabling DLP

DLP refers to Data Lock Point, a feature that 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.

This section provides information about how to enable and disable DLP.

## Creating the Tablespaces

If you wish to create tablespaces before enabling DLP, the following information shows the different tablespaces. However, this step is optional.

| #  | Tablespace Name |
|----|-----------------|
| 1  | DLP_DATA_01     |
| 2  | DLP_DATA_02     |
| 3  | DLP_DATA_03     |
| 4  | DLP_DATA_04     |
| 5  | DLP_DATA_05     |
| 6  | DLP_INDEX_01    |
| 7  | DLP_INDEX_02    |
| 8  | DLP_INDEX_03    |
| 9  | DLP_INDEX_04    |
| 10 | DLP_INDEX_05    |
| 11 | DLP_INDEX_06    |
| 12 | DLP_LOB_01      |

The schema creation tool creates the tablespaces if they do not exist.

### Enabling DLP

Before enabling DLP (Data Lock Point), do the following:

- Verify that the Schema Creation Tool is installed.
- Make sure an Oracle Argus database instance is available.
- Verify that either a DBA-privileged or a SYSTEM user account has been created.
- Verify that the database contains extra hard disk space to support DLP. It is advised that you should have a separate disk for DLP.
- Invoke SQL/PLUS and connect to the Argus database as a SYS user.

Use the following procedure to enable DLP:

- 1. Open the Schema Creation Tool.
  - Click Argus DLP.
- 2. When the system displays the Enable DLP screen:
  - Click Yes.
- **3.** When the system displays the expanded Enable DLP window:

|                        |               | Enabl | le DLP                    |          |
|------------------------|---------------|-------|---------------------------|----------|
| Argus Database         |               |       |                           |          |
| Argus Database Name    | ASDOCDB       |       |                           |          |
| Argus DBA User         | SYSTEM        |       |                           |          |
| Argus Schema Owner     | ARGUS_APP     | •     | Argus Schema Password     | *****    |
| ESM Schema Owner       | ESM_OWNER     | •     | ESM Schema Password       | ******   |
| Argus Role             | ARGUS_ROLE    | *     | ESM Role                  | ESM_ROLE |
| BIP Schema Owner       | BIP_OWNER     | -     | BIP Schema Password       | ******   |
| OLP Schema Owner       | DLP_OWNER     | •     | DLP Schema Password       | ******   |
| OLP ESM Query User     | DLP_ESM_QUERY | •     | DLP ESM Query Password    | ******   |
| VPD Admin Schema Owner | VPD_OWNER     | •     | VPD Admin Schema Password | ******   |

Click **New User** to create the DLP Schema Owner and DLP ESM Query User in the New User Information dialog box.

| Argus Safety          | Schema Creation Tool |
|-----------------------|----------------------|
| New User Information  |                      |
| Database              | ASDOCDB              |
| New User Name:        | DLP_OWNER            |
| New User Password:    | *****                |
| Re-enter Password:    | ******               |
| Default Tablespace:   | USERS -              |
| Temporary Tablespace: | TEMP                 |
|                       | OK Cancel            |
|                       |                      |

- Enter the required details for the new Owner and click **OK**.
- Enter the required schema information.
- Enter the user's password in the VPD Admin Schema Password field.
- **4.** The system redisplays the Enable DLP window with the DLP Schema Owner and DLP ESM Query User.
- 5. Enter the required user information.

Enter the user name in the VPD Admin Schema Owner field and click OK to proceed.

- **6.** In the Enable DLP window:
  - Locate the Local Folder name to create DLP Process Log and DMP files [No Spaces].
  - Click Browse to select a local folder (without spaces) for the temporary path.
- 7. When the system updates and displays the Enable DLP window:
  - Click OK.
- **8.** When the system opens the Enable DLP: Create Tablespace, the following screen is displayed:

| Tablesp | aces  | Small<br>Model | Medium<br>Model | Large<br>Model | Complete Path and Data File Name     |  |
|---------|-------|----------------|-----------------|----------------|--------------------------------------|--|
| DLP_IND | EX_01 | 59M            | 88M             | 122M           | C:IORADATA/ASDOCDB/DLP_INDEX_01.dbf  |  |
| DLP_IND | EX_02 | 109M           | 164M            | 222M           | C:IORADATA\ASDOCDBIDLP_INDEX_02.dbf  |  |
| DLP_IND | EX_03 | 104M           | 156M            | 211M           | C:IORADATA\ASDOCDBIDLP_INDEX_03.dbf  |  |
| DLP_IND | EX_04 | 54M            | 82M             | 108M           | C::ORADATA'A SDOCDBIDLP_INDEX_04.dbf |  |
| DLP_LOS | 3_01  | 53M            | 80M             | 118M           | C:IORADATA\ASDOCDBIDLP_LO8_01.dbf    |  |
| DLP_DAT | A_01  | 359M           | 906M            | 1491M          | C:IORADATA'A SDOCDBIDLP_DATA_01.dbf  |  |
| DLP_DAT | A_02  | 71M            | 110M            | 204M           | C:IORADATA'A SDOCDBIDLP_DATA_02.dbf  |  |
| DLP_DAT | A_04  | 63M            | 96M             | 165M           | C::ORADATA'A SDOCDBIDLP_DATA_04.dbf  |  |
| DLP_DAT | A_05  | 121M           | 158M            | 217M           | C:IORADATA'A SDOCDBIDLP_DATA_05.dbf  |  |
| DLP_DAT | A_03  | 197M           | 359M            | 1157M          | C:IORADATA'A SDOCD8IDLP_DATA_03.dbf  |  |
| DLP_IND | EX_05 | 133M           | 220M            | 608M           | C:IORADATA'A SDOCDBIDLP_INDEX_05.dbf |  |
| DLP_IND | EX_06 | 86M            | 138M            | 224M           | C:IORADATA'A SDOCDELDLP_INDEX_06.dbf |  |
|         |       |                |                 |                |                                      |  |

**Note:** The Tablespace Creation dialog box appears if the Argus Database Size was created as **Small**, **Medium**, or **Large**. It will not appear if the database size was created as **Default**.

- Enter the tablespace information in the Complete Path and Datafile fields.
- Click Create Tablespace.

**Note:** After creating the DLP datafiles in the Argus database, if the AUTOEXTENSIBLE value is set to NO, set the AUTOEXTENSIBLE value to 'YES' on all DLP tablespaces data files.

- 9. When the system displays the Enable DLP window with a dialog box:
  - Click **OK** to close the dialog box.
  - Click Proceed to start processing.

Before clicking Proceed, verify that the DLP tablespsaces Autoextend property is set to YES.

## **Disabling DLP**

Verify that no one is logged on to the Argus Safety database before beginning the Disable DLP procedure.

- 1. Open the Schema Creation Tool.
  - Click Argus DLP.
- 2. When the system displays the Disable DLP dialog box:
  - Click Yes.
- **3.** When the system displays the expanded Disable DLP dialog box:
  - Click **OK** to close the dialog box.
  - Click **Proceed** to start processing.

**4.** When the system displays the following message, click **OK** and then click **Proceed** in the Disable DLP expanded dialog box.

|                     |               | Disab | le DLP                 |        |
|---------------------|---------------|-------|------------------------|--------|
| Argus Database      |               |       |                        |        |
| Argus Database Name | ASDOCDB       |       |                        |        |
| Argus DBA User      | SYSTEM        |       |                        |        |
| Argus Schema Owner  | ARGUS_APP     | *     | Argus Schema Password  | ****** |
| DLP Schema Owner    | DLP_OWNER     | -     | DLP Schema Password    | ****** |
| DLP ESM Query User  | DLP_ESM_QUERY | -     | DLP ESM Query Password |        |

- Click **OK** to close the dialog box.
- Click **Proceed** to start processing.
- 5. When the system displays the Disable DLP window:
  - Click OK to close the dialog box.
  - The system displays status information regarding the DLP Disable operation in the Disable DLP window.
  - Click Exit.
- 6. When the Disable DLP operation is complete:
  - Click Exit.
- **7.** DLP has been disabled.

# Enabling DLP on a Specific Enterprise

This section provides the steps to:

a) either enable DLP on a specific enterprise merged from a non-DLP system to a DLP enabled multi-tenant Safety system

OR

b) to enable DLP on delta cases merged into an existing enterprise of a DLP enabled multi-tenant or single-tenant Safety system.

This implementation requires the following pre-requisites:

- This script shall be used after Enabling DLP from Schema Creation Tool using the standard Argus DLP option in Schema Creation Tool which setups the initial DLP infrastructure.
- This script is supported on top of Argus DLP infrastructure which setups the initial DLP on the Argus database for all existing enterprises.

Execute the following step to extract the custom scripts:

1. Extract the custom DLP Enable Enterprise Specific from C:\Program Files\Oracle\Argus\DBInstaller\Utilities\DLP\_Enable\_Enterprise\_Specific into a machine's local folder where Argus Safety 8.1 is installed.

Execute the following steps to set up the base database:

- 1. Set up an Argus Safety 8.1 multi-tenant or single-tenant database. Enable DLP on the Argus Safety 8.1 database, using standard Argus DLP option available in the Schema Creation Tool.
- **2.** Validate the schema using the Schema Validation in Argus Safety 8.1 Schema Creation Tool by selecting the compatible CTL file for Schema Validation. If any MISSING object exists in schema validation log, it needs to be fixed before proceeding to the next step.
- **3.** Populate new Argus cases into existing enterprise of a DLP enabled multi-tenant or single-tenant Safety system from non-DLP system or create new enterprise in a DLP enabled multi-tenant Safety system using data migration or merge to multitenant utility.

Execute the following steps to enable DLP on a Specific Enterprise or Delta Cases in a Specific Enterprise:

- Double-click DLP\_Enable\_Enterprise.bat from C:\Program Files\Oracle\Argus\DBInstaller\Utilities\DLP\_Enable\_Enterprise\_ Specific\Argus\DLP\. This batch file execution handles the following scenarios to populate DLP data on newly created Argus cases:
  - Process all cases merged in a Safety system due to creation of new enterprise by merge process
  - Process of delta cases merged in an enterprise due to any migration activity

| C:\Windows\System32\cmd.exe            |                                       | _ 🗆 X    |
|--|---------------------------------------|----------|
|  |                                       | <b>^</b> |
| ###################################### | ##                                    |          |
| Enter Log File Name to record results  | : DLP_Enable_Enterprise_Specific.LOG_ | V        |

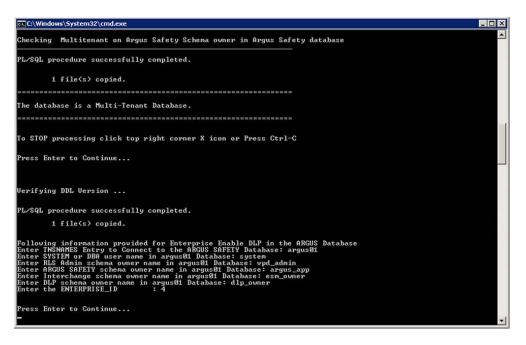
**2.** Provide the name and location for the log file.

| Select C:\Windows\System32\cmd.exe   | _ <b>_ _ _</b> × |
|--|------------------|
| аналынааланынаалынынааланынааланынанаалынынананана   | ** **            |
|  | ##               |
| ## Project Name : Enterprise DLP Enable process on Argus Safety database   | ##               |
| Please provide following information to Enable DLP for Specific Enterprise in Argus Safety d<br>Enter TMSNAMES Entry to Connect to the ARGUS SAFETY Database: argus01<br>Enter SYSTEM or DBA user name in argus01 Database: system<br>Enter password for system in argus01 Database: | atabase          |
| Enter RLS Admin schema owner name in argusØ1 Database: vpd_admin<br>Enter password for vpd_admin in argusØ1 Database:  |                  |
| Enter ARGUS SAFETY schema owner name in argusØ1 Database: argus_app<br>Enter password for argus_app in argusØ1 Database:   |                  |
| Enter Interchange schema owner name in argus01 Database: esm_owner<br>Enter password for esm_owner in argus01 Database:  |                  |
| Enter DLP schema owner name in argus01 Database: dlp_owner<br>Enter password for dlp_owner in argus01 Database:  |                  |
| Enter the ENTERPRISE_ID : 4  |                  |
| Enter Tablespace name to create DLP Tables : dlp_data_04<br>Enter Tablespace name to create DLP Indexes: dlp_index_04  |                  |
| Connecting as system@argus01   |                  |
| Connected.   | -                |

**3.** Follow the prompt messages on the screens and proceed by entering the required parameters and continue with the Enable DLP Enterprise Specific process.

| as C:\Windows\System32\cmd.exe   | _ 🗆 X |
|--|-------|
|  | -     |
| Connecting as argus_app@argus01  |       |
| Connected.   |       |
| Checking Multitenant on Argus Safety Schena owner in Argus Safety database |       |
| PL/SQL procedure successfully completed.                                   |       |
| 1 file(s) copied.  |       |
| The database is a Multi-Tenant Database.                                   |       |
|  |       |
| To STOP processing click top right corner X icon or Press Ctrl-C           |       |
| Press Enter to Continue<br>-   | •     |

**4.** A message is prompted to display whether the database is single-tenant or multi-tenant.



**5.** The above screen shows the details entered for the Enable DLP Enterprise Specific process. The process shall only be continued further if the details displayed in this screen are correct.

In case of any error during the Enable DLP process, the execution gets paused.

The process should be continued once the error is corrected and executed from another sql window.

While executing the above, make sure that you use the correct login credentials and set up the appropriate enterprise context.

Once the process is completed the log files shall be verified for any errors.

For any missing cases between Argus and DLP, the log file DLP\_ENABLE\_Missing\_ Cases\_in\_DLP\_log.log shall be verified in \DLP\_Enable\_Enterprise\_ Specific\Argus\DLP\ folder.

After applying the Enable DLP Enterprise Specific to Argus Safety 8.1, the DLP Enabled system performs the Schema Validation, as listed below:

- 1. Double-click on ArgusDBInstall.exe file that exists in C:\Program Files\Oracle\Argus\DBInstaller.
- **2.** Click Schema Validation and continue the Schema Validation on Argus Safety 8.1 database.

Extra objects related to table DLP\_ENABLE\_CASE\_HISTORY shall be ignored in schema validation log file.

The following table and related objects shall be ignored in Schema Validation at to Argus Safety 8.1 DLP Enabled system with DLP\_Enable\_Enterprise\_Specific scripts applied on top of it:

| Owner | Туре  | Name                           | Reason for extra<br>object  |
|-------|-------|--------------------------------|---|
| DLP   | TABLE | DLP_ENABLE_<br>CASE_HISTORY    | Objects are part of<br>Enable DLP<br>Enterprise Specific<br>implementation. |
| DLP   | INDEX | PK_DLP_ENABLE_<br>CASE_HISTORY | Objects are part of<br>Enable DLP<br>Enterprise Specific<br>implementation. |

# Upgrading the 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.

### Prerequisites for Database Upgrade

Before upgrading the schema, connect to ARGUS Safety database as a SYS user.

**Note:** If another DBA user is used instead of SYSTEM, then change SYSTEM to the name of DBA user and execute the command below.

The following grants need not be provided if the DBA user has been created through the Argus 8.1 Create DBA User script:

Define user\_dba=SYSTEM

GRANT EXECUTE on SYS.DBMS\_CRYPTO TO &user\_dba. WITH GRANT OPTION;

Before starting the upgrade procedure:

- Verify that the Oracle TNSNAMES have been configured.
- To avoid errors during upgrade, do either of the following:

a) KEEP DATA FILES AUTOEXTEND ON, or

b) Monitor free space and add more space, if required.

- Ensure you have a sort area of approximately 100 MB to avoid disk sort
- Create one large rollback segment or size 20 GB for LARGE size model.

Keep all other, except SYSTEM, rollback segments offline.

**Note:** If the source Argus Safety Database is not AL32UTF8 character set database, then it must be converted to AL32UTF8 character set before performing the database upgrade to version 8.1.

**Note:** The Argus Safety Database requires the Database semantics to be CHAR and not BYTE. Execute the following steps:

- Log in to the Database as the SYSTEM user
- Execute: ALTER SYSTEM SET NLS\_LENGTH\_ SEMANTICS=CHAR SCOPE=BOTH;
- Shutdown and Startup the database after applying the above statement.

### DLP Data Correction Script to be Run Before Upgrading the Database

To correct the case data in **dlp\_case\_rev\_master** table, execute the DLP Data Correction script before upgrading the database.

**Note:** This step is required ONLY for Argus Safety with DLP setup.

**1.** Execute the file DLP\_CASE\_REV\_MASTER\_Correction\_script.sql from the installation folder:

\Oracle\Argus\DBInstaller\Utilities\DLP\_Case\_Rev\_Master\_Correction\_Script\

The SQL file contains the steps for execution.

- 2. When a command prompt screen appears:
  - **a.** For USER, enter the Argus Schema owner.
  - **b.** For USER\_DLP, enter the DLP Schema owner.
- **3.** If followup for a case is present, verify that the following dlp\_case\_rev\_master effective dates are correctly populated:
  - effective\_receipt\_date
  - effective\_receipt\_date\_j
  - effective\_safety\_date
  - effective\_time\_stamp

You can verify the impacted cases from the tmp\_dcrm\_upd\_data table for which correction is done.

**Note:** Ignore any additional objects present in the Schema Validation related to tmp\_dcrm\_upd\_data and dlp\_case\_rev\_master\_bkp tables.

#### Data Migration Logic for New Fields

Execute scripts to copy data from the existing fields to the new fields added in this release. You can modify the Migration Logic based on the Company specific usage of these fields.

If one or more files are updated, Oracle recommends you to test them to make sure that there are no errors. These scripts are executed by the Schema Creation Tool, and it is not required to execute them separately.

The following are the field details where migration logic can be modified:

Migration data can be altered by editing the following scripts:

- For Argus\_app: Argus\_81\_CUSTOM\_UPGRADE\_data\_change1.sql
- For DLP: dlp\_81\_CUSTOM\_UPGRADE\_data\_change1.sql

| Condition   | Source Field                  | Target Field   |
|---|-------------------------------|--|
| If the data is present in the<br>field CASE_VACC_<br>VAERS.ADMIN_BY     | CASE_VACC_<br>VAERS.ADMIN_BY  | CASE_VACC_<br>VAERS.LAST_NAME (Last<br>Name of Best<br>Doctor/Responsible<br>Physician). |
| If the data is NOT present in<br>the field CASE_VACC_<br>VAERS.ADMIN_BY | CASE_VACC_<br>VAERS.PHYSICIAN | CASE_VACC_<br>VAERS.LAST_NAME (Last<br>Name of Best<br>Doctor/Responsible<br>Physician)  |

 If the data is present in the Device Age (Approx.) (CASE\_PROD\_ DEVICES.DEVICE\_AGE) field, then it is copied to CASE\_PROD\_DEVICES. AGE and CASE\_PROD\_DEVICES. AGE\_ID fields.

**Assumptions:** The Device Age is entered in two parts: Age and Units.

To copy the data, the following logic is used:

- The initial numeric value of the Device Age field is populated to the CASE\_ PROD\_DEVICES. AGE field.
- The Unit is derived from the CASE\_PROD\_DEVICES.DEVICE\_AGE by considering the later part of the Device Age field value.

| Unit of value             |                                  |                               |
|---------------------------|----------------------------------|-------------------------------|
| (irrespective of the case |                                  | Mapped to value in            |
| (lower/upper)             | Source Field                     | LM_AGE_UNITS codelist         |
| Hour/Hours/Hr             | CASE_PROD_<br>DEVICES.DEVICE_AGE | ID corresponding to the Hour  |
| Day/Days/Da               |                                  | ID corresponding to the Day   |
| Month/Months/Mo           |                                  | ID corresponding to the Month |
| Year/Years/Yr             |                                  | ID corresponding to the Year  |

Migration data can be altered by editing the following scripts:

- For Argus\_app: Argus\_81\_UPGRADE\_data\_change1.sql
- For DLP: dlp\_81\_UPGRADE\_data\_change1.sql
- If the data is present in the following fields related to the location where the event occurred that is printed in MedWatch Device report, then corresponding ID from LOCATION\_EVENT\_OCCURRED codelist is copied to the CASE\_MEDWATCH\_ DATAEVENT.LOCATION field.

|                             | Mapped to value in      |
|-----------------------------|-------------------------|
| Source Field                | LOCATION_EVENT_OCCURRED |
| CASE_MEDWATCH_DATA.LOC_HOSP | Hospital                |

|                              | Mapped to value in             |  |  |  |
|------------------------------|--------------------------------|--|--|--|
| Source Field                 | LOCATION_EVENT_OCCURRED        |  |  |  |
| CASE_MEDWATCH_DATA.LOC_HOME  | Home                           |  |  |  |
| CASE_MEDWATCH_DATA.LOC_NH    | Nursing Home                   |  |  |  |
| CASE_MEDWATCH_DATA.LOC_OTF   | Outpatient Treatment Facility  |  |  |  |
| CASE_MEDWATCH_DATA.LOC_ODF   | Outpatient Diagnostic Facility |  |  |  |
| CASE_MEDWATCH_DATA.LOC_ASF   | Ambulatory Surgical Facility   |  |  |  |
| CASE_MEDWATCH_DATA.LOC_OTHER | Other                          |  |  |  |

**Assumptions:** Any one of the checkboxes for the **Location Where Event Occurred** option is marked as per the typical business use case.

If multiple checkboxes are selected in a case for the **Location Where Event Occurred** option, then this field is left blank in the upgraded database, and the upgrade log indicates that the users are required to manually select the data for this field.

Migration data can be altered by editing the following scripts:

- For Argus\_app: Argus\_81\_UPGRADE\_data\_change1.sql
- For DLP: dlp\_81\_CUSTOM\_UPGRADE\_data\_change1.sql

Besides modifying the migration logic, the out of the box application upgrade logic populates the data in the new database fields based on the following logic:

- Field Name—CASE\_PROD\_MALFUNCTION.RPT\_MALFUNCTION\_J and CASE\_PROD\_MALFUNCTION.DET\_MALFUNCTION\_J
- Upgrade Logic—Search for PMDA Device Info > Malfunction Name (CASE\_ PROD\_DEVICES\_PMDA.MALFUNCTION\_NAME) field (now marked OBSELETE).

If any data exists, then this data is copied to CASE\_PROD\_MALFUNCTION.RPT\_ MALFUNCTION\_J and CASE\_PROD\_MALFUNCTION.DET\_MALFUNCTION\_J fields.

The upgrade logic splits the existing malfunction names based on the comma in the data, and creates the same number of malfunctions in the new Malfunction Information section.

**Note:** : If the length of the split Malfunction Name is more than 50 characters, then the upgrade logic creates a new malfunction with 50 characters, and log it as *could not fit-in the 50 char length* in the log file. You must modify the migrated malfunction name with appropriate value.

### Database Upgrade Procedure (with or without DLP) from AS 8.0 to AS 8.1

**Note:** The Oracle Database Server version should be upgraded to 12c (12.1.0.2.0) prior to upgrading the database from AS 8.0 to AS 8.1.

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

Use the following procedure to upgrade the database.

- 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. Select Start > Programs > Oracle > Schema Creation Tool.
- **2.** When the system opens the Schema Creation Tool:
  - Click **DB Upgrade**.
- **3.** When the system opens the Connect to Database dialog box:
  - Enter the **DBA username**.
  - Enter the **password**.
  - Enter the Database name.
  - Click OK.
- 4. Select the version-specific upgrade folder and click **OK**.

**Note:** During the upgrade this validation may appear. This is due to a few tables where the column size has been adjusted and the table currently has more data than the new column size.

**5.** When the system opens the Upgrade Parameters screen loaded with default values:

|   | ormatio      | 00  |                    |                                 |        |   |
|---|--------------|---|--------------------|---------------------------------|--------|---|
| Database and Upgrade Inf<br>Database Name:  | -            | OCDB  |                    |                                 |        |   |
| Current Database Version: 8.0   |              |   |                    | Upgrade to Version: 8.1         |        |   |
| Upgrade Directory:  | C:\P         |   |                    | DBInstaller\Upgrades\UPGRADE_TO |        |   |
| Please specify parameter  | s for th     | e Upgrade                                       |                    |                                 |        |   |
| Argus Safety Schema Owne  |              | ARGUS_APP                                       | •                  | Password:                       | ****** |   |
| Argus Role Name:  |              | ARGUS_ROLE                                      | and a second       |                                 | ·      |   |
| ESM Schema Owner:   |              | ESM_OWNER 💌                                     |                    | Password:                       |        |   |
| ESM Role Name:  |              | ESM_ROLE  |                    |                                 | •      |   |
| ESM Query User:   |              | ESM_QUERY                                       | •                  | Password:                       | ****** |   |
| BIP Schema Owner:   |              | BIP_OWNER V                                     |                    | Password:                       | *****  |   |
| MedDRA User Name:   |              | MEDDRAJ   |                    |                                 |        | - |
|   |              | DLP Enabled on ti                               | nis Database       |                                 |        |   |
| DLP Schema Owner:   |              |   |                    | Password:                       |        |   |
| DLP ESM Query User:   |              |   |                    | Password:                       |        |   |
|   |              | 1   | _                  |                                 | ,      |   |
| Credentials for VPD Adr   | min Use      | n   |                    |                                 |        |   |
| VPD Admin Schema Own  | ier:         | VPD_OWNER                                       | •                  | Password:                       | ****** |   |
| Optional Upgrades Avai  | lable        |   |                    |                                 |        |   |
| ▼         Replace factory vers           ▼         Replace factory vers           ▼         Replace factory vers           ▼         Replace factory vers | ion of th    | e function SF_CASE_LIS<br>e function SF_CASE_CA | TEDNESS<br>USALITY | EVENT                           |        |   |
|   |              |   |                    |                                 |        |   |
| Application Type<br>© Single-tenant C 1   | Multi-ter    | ant   |                    |                                 |        |   |
| C Single-tenant C 1   |              | ant   |                    |                                 |        |   |
| C Single-tenant C 1<br>Default Enterprise Detai<br>Enterprise Name:   | IIS<br>DEFAI | ענז   |                    |                                 |        |   |
| © Single-tenant C 1   | ils          | ענז   |                    |                                 |        |   |

In the Upgrade Parameters screen, enter information in the following fields:

- Credentials for VPD Admin User This includes the VPD Admin Schema Owner, Password, and Verify Password.
- Application Type This field is auto-selected based on the existing application type.
  - Single Tenant This option is selected, if you are upgrading this database from a single tenant model.
  - Multi Tenant This option is selected, if you are upgrading this database from a multi-tenant model.
- Default Enterprise Details This includes the Enterprise Name and Enterprise Short Name.

**Note:** The three optional functions SF\_CASE\_SERIOUSNESS, SF\_ CASE\_LISTEDNESS, and SF\_CASE\_CAUSALITY have had their signatures changed. The original functions will be spooled to the log file at .\DBInstaller\Upgrades\UPGRADE\_TO\_80\UPG\_SF\_ FUNCTIONS\_SOURCE.LOG. If custom functions are in use, it will be necessary to re-apply them after the upgrade is complete to conform to the new signatures.

- Enter the Argus Safety Schema Owner password.
- Enter the ESM Schema Owner password.
- Click New User to create a new ESM Query Schema, and select it from the ESM Query Schema drop-down list.
- If DLP is enabled, click New User to create a new DLP ESM Query Schema, and select it from the DLP ESM Query Schema drop-down list.
- Select the BI Publisher Schema Owner from the drop-down list, and enter the BI Publisher Schema Owner password.
- Click Next.

**Note:** If DLP is already enabled, the check box will be checked; otherwise it will be unchecked.

**6.** When the system loads the Tablespace Management window for the Argus databas1

|                        | base and Upgrade Info  | mation       |                                    |               |                   |                 |                            |  |  |
|------------------------|--|--------------|------------------------------------|---------------|-------------------|-----------------|----------------------------|--|--|
| Database Name: ASDOCDB |  | ASDOCDB      |                                    |               |                   |                 |                            |  |  |
|                        |  | 8.0          | 8.0                                |               |                   |                 |                            |  |  |
|                        |  | 8.1          |                                    |               |                   |                 |                            |  |  |
| Upgi                   | rade Directory:  | C:\Program F | Files (x86)\Oracle\Argus\DBInstall | er\Upgrades\l | JPGRADE_TO_81     |                 |                            |  |  |
|                        |  |              |                                    |               |                   |                 |                            |  |  |
|                        | Description  |              | Tablespaces                        |               | Current Size (Mb) | Free Space (Mb) | Free Spaced Needer<br>(Mb) |  |  |
|                        | Argus Data Tablespace Name 01<br>Argus Data Tablespace Name 02 |              | ARGUS_DATA_01                      | •             | 1035              | 536             | 32                         |  |  |
|                        |  |              | ARGUS_DATA_02                      | -             | 751               | 386             | 4                          |  |  |
|                        | Argus Index Tablespace   | e Name 01    | ARGUS_NDEX_01                      | -             | 764               | 458             | 64                         |  |  |
|                        | Argus Index Tablespace   | t Name 02    | ARGUS_NDEX_02                      | -             | 1283              | 814             | 4                          |  |  |
|                        | Argus Index Tablespace   | e Name 04    | ARGUS_NDEX_04                      | •             | 279               | 247             | 1                          |  |  |
|                        | ESM Data Tablespace N  | ame 01       | ESM_DATA_01                        | •             | 362               | 289             | 9                          |  |  |
|                        | ESM Index Tablespace   | Name 01      | ESM_INDEX_01                       | -             | 373               | 343             | 10                         |  |  |

- Select the tablespace name from the drop-down list corresponding to the description.
- Click Recalculate Free Space. Verify that the available free space is greater than the amount of required space. If you have increased the freespace, click this button to recalculate the amount of available free space.
- Click Next.

**7.** If DLP is already enabled on the selected Argus DLP database, the system displays the Tablespace Management DLP window. If Argus does not have DLP, this system does not display this screen.

| Durrent Database Version:     8.0       opgrade to Version:     8.1       Deprade Directory:     C:\Program Files (x86)\OracLe\Argus\DBInstaller\Upgrades\UPGRADE_TO_81       LP Database Name :     ASDOCDB       Description     Tablespace       DLP Data Tablespace Name 01     DLP_DATA_01       DLP Index Tablespace Name 01     DLP_DATA_01       DLP Index Tablespace Name 01     DLP_NDEX_01       DLP Index Tablespace Name 01     DLP_NDEX_01 | Data  | base Name:                  | ASDOCDB |             |   |                   |                 |                           |  |
|--|---|-----------------------------|---------|-------------|---|-------------------|-----------------|---------------------------|--|
| ppgrade to Version:     8.1       ppgrade Directory:     C:\Program Files (x86)\Oracle\Argus\DBInstaller\Upgrades\UPGRADE_TO_81       LP Database Name :     ASDOCDB       Description     Tablespaces     Current Size (Mb)     Free Space (Mb)     Free Space Need (Mb)       DLP Data Tablespace Name 01     DLP_DATA_01     359     341     12       DLP Index Tablespace Name 01     DLP_NDEX_01     194     9     30                               | Current Database Version: 8.0 Upgrade to Version: 8.1 |                             |         |             |   |                   |                 |                           |  |
| LP Database Name :     ASDOCDB       Description     Tablespaces       DLP Data Tablespace Name 01     DLP_DATA_01       DLP Index Tablespace Name 01     DLP_NDEX_01       194     9  |   |                             | 8.1     |             |   |                   |                 |                           |  |
| Description         Tablespaces         Current Size (Wb)         Free Space (Mb)         Free Space Need<br>(Mb)           DLP Data Tablespace Name 01         DLP_DATA_01         359         341         12           DLP Index Tablespace Name 01         DLP_NDEX_01         194         9         30   |   |                             |         |             |   |                   |                 |                           |  |
| Description         Tablespaces         Current Size (Mb)         Pree Space (Mb)         (Mb)           DLP Data Tablespace Name 01         DLP_DATA_011         359         341         12           DLP Index Tablespace Name 01         DLP_NDEX_011         194         9         30  | DLP   | Database Name :             | ASDOCDB |             |   |                   |                 |                           |  |
| DLP Index Tablespace Name 01 DLP_NDEX_01 194 9 30  |   | Description                 |         | Tablespaces |   | Current Size (Mb) | Free Space (Mb) | Free Spaced Neede<br>(Mb) |  |
|  |   | DLP Data Tablespace Name 01 |         | DLP_DATA_01 | - | 359               | 341             | 12                        |  |
| DLP_L08_01535218   |   | DLP Index Tablespace I      | Name 01 | DLP_NDEX_01 | - | 194               | 9               | 30                        |  |
|  | DLP_LOB_01  |                             |         | DLP_LOB_01  | - | 53                | 52              | 18                        |  |
|  |   |                             |         |             |   |                   |                 |                           |  |
|  |   |                             |         |             |   |                   |                 |                           |  |
|  |   |                             |         |             |   |                   |                 |                           |  |
|  |   |                             |         |             |   |                   |                 |                           |  |
|  |   |                             |         |             |   |                   |                 |                           |  |

- Enter the appropriate path of the tablespace and click **Next**.
- 8. When the system prompts for confirmation:
  - Click **OK** and then click **Proceed** on the main screen.
- **9.** When the upgrade is complete:
  - Click OK.
- **10.** When the system opens the Database Upgrade Execution window:
  - Click the log icon to verify any upgrade errors.

The following log files are generated:

UPG\_Argus\_81\_CUSTOM\_UPGRADE\_data\_change1\_<log creation date>.log

UPG\_Argus\_81\_Upgrade\_data\_change1\_<log creation date>.log

UPG\_dlp\_81\_CUSTOM\_UPGRADE\_data\_change1\_<log creation date>.log

UPG\_dlp\_81\_UPGRADE\_data\_change1\_<log creation date>.log

- Click Exit.
- **11.** Upgrade is finished.
- **12.** Run the Schema Validation tool to validate the schema.

**Note:** Make sure that you disable the dashboard triggers after completing the database upgrade, as listed in the Note at the end of the Loading Factory Data section.

## Post-Upgrade Steps

This section provides the following post-upgrade scripts to be executed on the Argus Safety database:

<C>:\Program Files\Oracle\Argus\DBInstaller\utilities\Post\_Upgrade\_Scripts (Optional)

Run the Post\_Upgrade\_Scripts.bat batch file present in the folder mentioned above and follow the ReadMe.txt for details to initiate the Post-Upgrade and execute the following steps:

- 1. Double-click the post\_upgrade\_script.bat file.
- 2. Enter the log file name. This creates a log file in the current working directory.
- **3.** Enter the database TNS details, and log in with the Argus user credentials.
- 4. Press Enter to Continue, if the provided details are correct.
- 5. Press Enter again, if the user could connect successfully to the database.
- 6. Press Enter to initiate the migration script.
- **7.** Review the log file for any errors.

# Enabling Local Locking in Argus Safety

#### **Pre-requisite:**

Before enabling Local Locking in Argus Safety, you must make sure that you have upgraded your database to Argus Safety 8.1 successfully.

Execute the following steps to enable local locking:

- 1. Execute the batch file Enable\_local\_lock.bat under the <C>:\Program Files\Oracle\Argus\DBInstaller\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 enterprise 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.** Enter **Yes** or **No** in case you wish to enable the local locking privileges for Argus J users. 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 nulti-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.

#### Making cases appear in PSUR regardless of past submission:

#### **Pre-requisite:**

Before making cases appear in PSUR regardless of past submission, you must make sure that you have upgraded your database to Argus Safety 8.1 successfully.

Execute the following process to make cases appear in PSUR:

- 1. Delete the data from the cmn\_per\_sub\_child table.
- **2.** Execute the following query to restore the data to factory settings as per upgrade:

INSERT INTO CMN\_PER\_SUB\_CHILD (id,reg\_report\_id,rec\_ type,field,enterprise\_id)

SELECT S\_CMN\_PER\_SUB\_CHILD.NEXTVAL,reg\_report\_id,rec\_ type,field,enterprise\_id FROM (

WITH report\_ids AS (

SELECT crr.reg\_report\_id, crr.report\_form\_id FROM

v\$cmn\_reg\_reports crr,

v\$lm\_report\_forms lrf

WHERE crr.report\_form\_id=lrf.report\_form\_id and crr.enterprise\_ id=lrf.enterprise\_id

AND crr.state\_id=6 AND crr.report\_form\_id>100

```
AND lrf.rpt_type in (2,12)
```

```
)
```

, dataview as (

select distinct ri.reg\_report\_id,cprc.report\_form\_id,cprc.rec\_type,cprc.field, max(cprc.rec\_type) over (partition by cprc.report\_form\_id) max\_rec\_type ,cprc.enterprise\_id

from v\$cfg\_per\_rpt\_child cprc, report\_ids ri

where ri.report\_form\_id=cprc.report\_form\_id

and cprc.rec\_type in (1,8)

)

select reg\_report\_id,rec\_type,field,enterprise\_id

from dataview

where rec\_type=max\_rec\_type

);

**3.** The above query can be used as a base for any custom changes that may be required.

**Note:** The above steps have to be executed after setting the enterprise context using PKG\_RLS.SET\_CONTEXT procedure.

# Merging a Single Enterprise Safety Database into a Multi-tenant Database

## Prerequisites to Running the Merge Export Step

- The end user should not use the Source database during export process.
- Install Argus Safety 8.1 on a computer where Oracle 12c (12.1.0.2.0) is installed.
- The source databases should be schema validated at Argus Safety 8.1.
- The source database should only be a single-tenant database.
- The source database data must contain only one ENTERPRISE.

## Prerequisites to Running 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
- There is only one at the time MERGE Import process allowed to run on the Target database.
- 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 Safety database.
- Install the Argus 8.1 application. Make sure that Oracle Client version is 12c (12.1.0.2.0).
- The Target databases should be Schema Validated at Argus 8.1.
- The target database must be a Multi-tenant database
- All source database dictionaries should be available in target Database. If the dictionary doesn't exist then install missing dictionaries on Target database.
- All existing AG service users on the Source Database must exist on the target Database
- All source database LDAP configured Server name should be available in target database.

## **Completing the Merge Process**

Use the following sections to complete the merge process.

### Merge Export

1. Navigate to the following Path from Start Menu:

All Programs > Oracle > Merge to Multi-tenant

- 2. Click on Export 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:

 $\label{eq:log_file_path: <C>:\Program Files \Oracle \Argus \DBInstaller \Merge_to_ Multitenant$ 

- 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 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.** Check the database export process log and export step log file for any errors. This is critical step to make sure no errors during export step. Check 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

### Exporting 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.

#### Merge Import

1. Navigate to the following path from Start Menu:

All Programs > Oracle > Merge to Multi-tenant

- **2.** Click on Import and follow the instructions on the sqlplus screen.
  - **a.** Enter Log File Name to record results. This is the execution log will be created on the client workstation.

Log file path: <C>:\Program Files\Oracle\Argus\DBInstaller\Merge\_to\_ Multitenant

- **b.** Enter TNSNAMES Entry to Connect to the Target SAFETY Database.
- **c.** Enter SYSTEM or DBA user name in target Database.
- **d.** Enter password for DBA user in target Database.
- **e**. Enter VPD schema owner name in target Database.
- f. Enter VPD schema owner password in target Database.
- **g.** Enter SAFETY schema owner name in target Database.
- h. Enter password for Safety schema owner in target Database
- i. Enter Interchange schema owner name in target Database
- j. Enter password for Interchange schema owner in target Database.

- k. Enter Directory including full Path on target database server where export dmp file copied for import process. This is the Path on the "Target Database Server" where the Argus Safety Database resides. The Batch file creates an import log files file in the directory mentioned.
- I. Enter the name of new ENTERPRISE.
- m. Enter the abbreviation of new ENTERPRISE.
- n. Enter SAFETY schema owner name in source Database.
- **o.** Enter Interchange schema owner name in source Database.
- **3.** This Batch files imports the data from the dump file into the target database.
- 4. Check the database import process log and import step log file for any errors. This is critical step to make sure no errors during import step. Check 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 on "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 Ttget database using Safety Schema Validation tool.

#### Manual Dictionary Synchronization

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.

Use the following steps to synchronize the dictionary data manually on the target database:

- 1. Log in as Safety schema owner using sqlplus on 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 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;

## Copy Configuration Tool

This tool is intended to provide functionality for copying configuration data from one Argus Safety database to another.

**Note:** 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.

The following steps are required to run the tool:

1. Validate Schema on the source database using Schema Validation Tool.

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.

- 2. Copy the Copy Configuration Tool utility files recursively from C:\Program Files\Oracle\Argus\DBInstaller\Copy\_Config to the C:\CONFIG\_EXP\_IMP\_81 folder.
- **3.** Export the Source database by running C:\CONFIG\_EXP\_IMP\_81\Data\_ ExportConfigOnly\_11g.bat and follow the prompts.
- **4.** Copy ArgusSecureKey.ini (working with Source database) from the .\Windows folder and save it with generated source database file.
- **5.** 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).

- 6. Create a new database using Argus Safety 8.1 Schema Creation tool.
- **7.** Import into Target database by running C:\CONFIG\_EXP\_IMP\_81\ Data\_ ImportConfigOnly\_11g.bat and follow the prompts. Ignore any "ORA-28101: policy already exists" error.
- 8. Validate Schema on the target database using Schema Validation Tool.
- **9.** 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.
- **10.** In case you do not have ArgusSecureKey.ini, follow the steps listed in the Resetting the Environment if ArgusSecureKey.ini is Lost section.

# **Installing Argus Safety Web**

This chapter includes the following sections:

- Installing Argus Safety Web
- Configuring the IIS Manager for Windows 2012
- Connecting to a Domain Account on Windows 2012
- Enabling SSL Support for Windows 2012
- Configuring Load Balancer in Argus Web
- Securing Sensitive Configuration and Operational Data
- Configuring Identity in the IIS Application Pools
- Resetting IIS

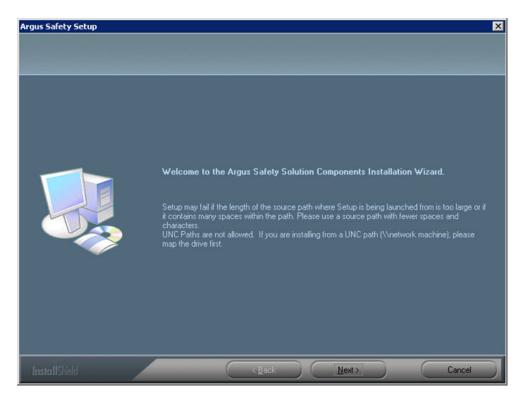
# Installing Argus Safety Web

Before installing Argus Safety Web, be aware of the following:

- During the installation, the information in this document may be different from what you see on your monitor if additional modules were selected during the Argus Safety Web Installation.
- A domain account with Local Administrator privileges to the Web server is required after the Argus Safety Web installation is complete.

Use the following procedure to install Argus Safety Web:

- 1. Open the Argus Safety folder and click setup.exe.
- 2. When the system displays the Argus Safety Setup screen, click Next >.



**3.** When the system displays the Customer Information screen:

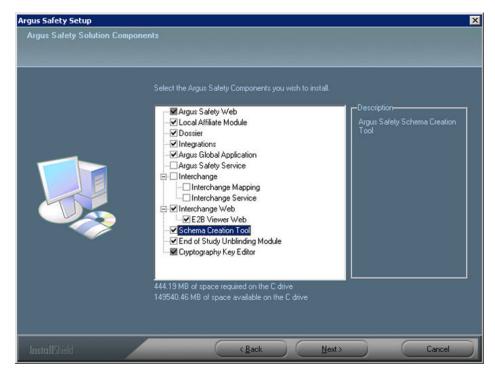
| Argus Safety Setup         |                              | ×      |
|----------------------------|------------------------------|--------|
| Argus Safety Solution Comp | ponents Customer Information |        |
|                            | Enter your name and company, |        |
|                            | User Name:                   |        |
|                            | User                         |        |
|                            | Company Name:<br>Oracle USA  |        |
|                            |                              |        |
| InstallShield              | < Back Next>                 | Cancel |

- 4. Enter the user name in the User Name field.
- 5. Enter the company name in the **Company Name** field.
- 6. Click Next >.

**7.** When the system displays the Default Directory screen, click **Browse** to select the default installation directory where the Argus Safety Solution Components will be installed.

| gus Safety Setup          |  |
|---------------------------|--|
| Argus Safety Solution Com | ponents Default Directory  |
|                           |  |
|                           | Select the default directory where all Argus Safety Solution Components will be installed. |
|                           |  |
|                           |  |
|                           |  |
|                           |  |
|                           |  |
|                           |  |
|                           |  |
|                           | Destination Folder   |
|                           | C:\Program Files\Dracle\Argus  |
|                           |  |
|                           |  |

- **8.** Click **Next** to display the Argus Safety Components list and select the default installation directory where the Argus Safety Solution Components will be installed.
- **9.** When the system displays the component list, you can select **Argus Global Application**.



The **Argus Global Application for Argus Safety Web** option in the Installer module selection screen allows support for the multi-tenancy feature.

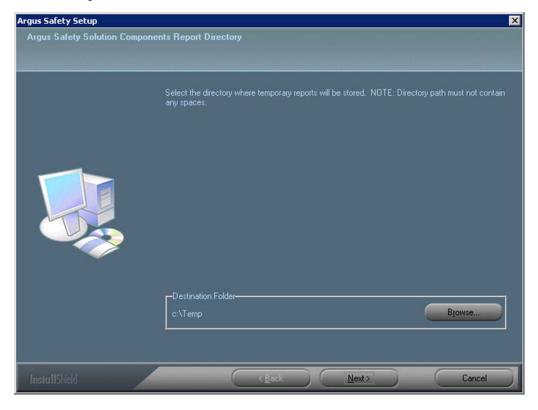
On selecting this option, global modules get installed on the same web server as Argus Safety Web and are accessible as a separate URL from the same web server. Global modules are components of Global Application having the same functionality as Portlets in the Global Homepage for Web Center.

If you have chosen to install the IIS Global Homepage instead of the Webcenter Global Homepage for multi-tenant installations, you must make sure that you access the following URL after installing the IIS Global Homepage:

http://<web server>:<port>/GHP/GlobalHome.aspx

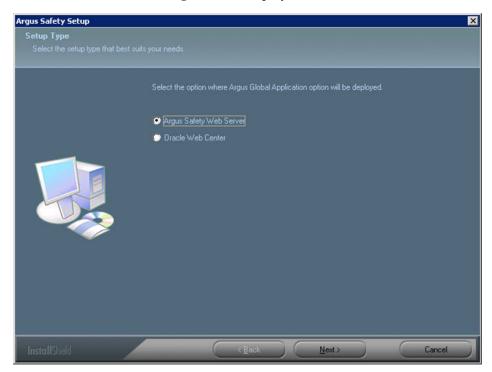
The Argus Global Application for the Argus Safety Web option is enabled only if Argus Safety Web is also selected.

 Select the modules to install and click Next. The Argus Safety Solution Components Report Directory is displayed. Select the directory where temporary reports will be stored. Users can browse through any path or leave this as default (C:\Temp).

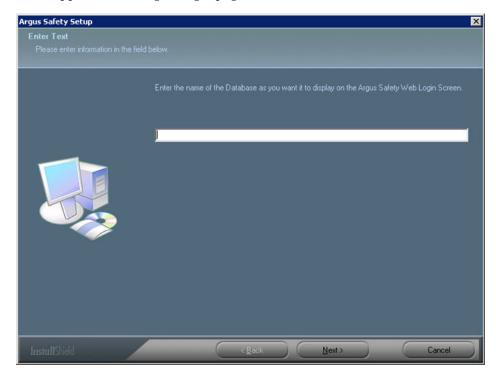


**Note:** It is recommended to install the Cryptography tool on the Web Server.

**11.** Click **Next**. The following screen is displayed.



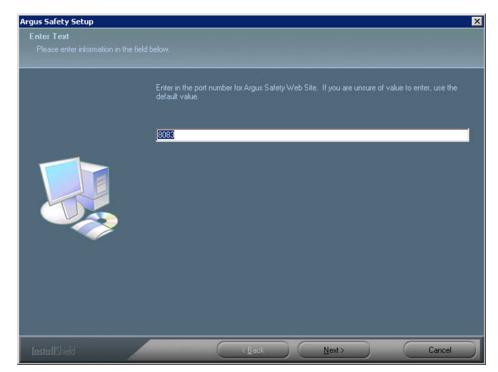
- **12.** Select the applicable **Setup Type** from the listed radio buttons, where the Argus Global Application will be deployed and click **Next** >.
- **13.** When the system asks whether you want to configure a database for Argus, click **Yes** to configure a database.
- **14.** When prompted to enter a database name, enter the database name as you want it to appear on the Argus Login page.



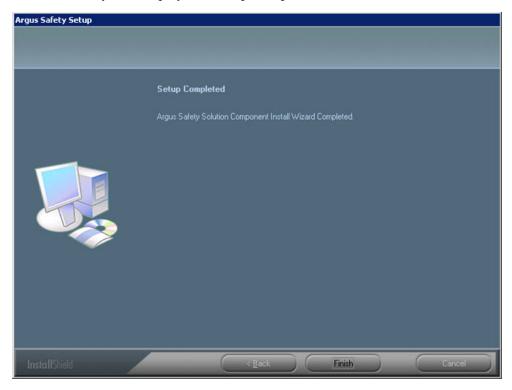
- **15.** Click **Next** > to continue.
- **16.** When prompted to enter the database SID: Enter the database SID.

| Argus Safety Setup<br>Enter Text<br>Please enter information in the | ield below.                    |                    | ×      |
|---|--------------------------------|--------------------|--------|
|   | Enter the Database SID (Oracle | Name) for AS702MTU |        |
| _   | ļ                              |                    |        |
|   |                                |                    |        |
|   |                                |                    |        |
|   |                                |                    |        |
| InstallShield   |                                | ck <u>N</u> ext>   | Cancel |

- **17.** Click **Next** > to continue.
- **18.** When the system ask if you would like to configure database settings for Argus: Click **Yes** to add an additional database to the Argus Login page.
- **19.** When the system prompts you to enter a port number, enter the Port for the Argus website (default is 8083).



- **20.** Click **Next** > to continue.
- **21.** The installer installs the website and it related components and shows the progress of the installation.
- **22.** When the system displays the Setup Completed screen, click Finish.



23. When the system displays the following message: Click OK to reboot the system.



**Note:** After installing Argus Safety Web, refer to the section The Argus Safety 8.1 Application Servers to set up the Argus Cryptography key.

## **Configuring the IIS Manager for Windows 2012**

**Note:** For Windows 2012, IIS 6 Management Compatibility and Application Development > ASP.NET/ASP roles must be installed.

- 1. Select Start > Administrative Tools > Internet Information Services (IIS) Manager.
- 2. Expand the Connection Panel and open Sites.
- **3.** Select Argus Safety Web.

| Services (II                          | S) Manager                |                          |
|---------------------------------------|---------------------------|--------------------------|
| SVMENGIRV001                          | Sites Argus Safety Web    | 🖬 🗠 🔐 🕢 •                |
| File View Help                        |                           |                          |
| Connections                           | Argus Safety<br>Web Home  | Actions                  |
| Start Page                            |                           | Edit Permissions         |
| Application Pools                     | Group by:                 | Edit Site                |
| E- Sites                              | ASP.NET                   | Bindings                 |
| Argus Safety Web     Default Web Site | ۵ 😓                       | Basic Settings           |
|                                       | NET NET                   | View Applications        |
|                                       | Compilation Globalization | View Virtual Directories |
|                                       |                           | Manage Web Site 🔗        |
|                                       |                           | 😂 Restart                |
|                                       | .NET Profile .NET Roles   | ▶ Start                  |
|                                       |                           | Stop                     |
|                                       | A 🕀 🔅                     | Browse Web Site          |
|                                       | .NET Trust .NET Users     | Browse :8083 (http)      |
|                                       | Levels 💌                  | Advanced Settings        |
|                                       | Features View             | Configure 🔻              |
| Ready                                 |                           | • <u>1</u> .:            |

4. On the right panel, click on **Basic Settings**.

| Edit Site  |                                     | ?×     |
|--|-------------------------------------|--------|
|  | Application pool:<br>DefaultAppPool | Select |
| Physical path:<br>C: \Program Files\Oracle\Argus\Arg | usWeb\ASP                           |        |
| Connect as 'abuser' Connect as Test Settings         |                                     |        |
|  | OK                                  | Cancel |

- 5. Click on **Connect as...**
- 6. Click on Specific User and click on Set.
- 7. Enter Domain user name and password and click **OK**.

| tart Page Edit Site                  |            |            | ? ×             |
|--------------------------------------|------------|------------|-----------------|
| Applic Site Connect As               |            |            | ?×              |
| Sites Path credentials:              |            |            |                 |
| E 😌 Ar<br>E 😔 De 🛛 De Specific user: |            |            |                 |
| Set Credentials                      | <u>? ×</u> |            | Set             |
| User name:                           |            | ntication) |                 |
| Argus\user1                          |            |            |                 |
| Password:                            |            | ок         | Cancel          |
| •••••                                |            |            |                 |
| Confirm password:                    |            | OK         | Cancel          |
| •••••                                |            |            | DIOWSE WED :    |
|                                      |            | sers       | Browse :8083 (h |
| ОК                                   | Cancel     | · ·        | Advanced Settin |
|                                      |            |            |                 |

### 8. Click OK.



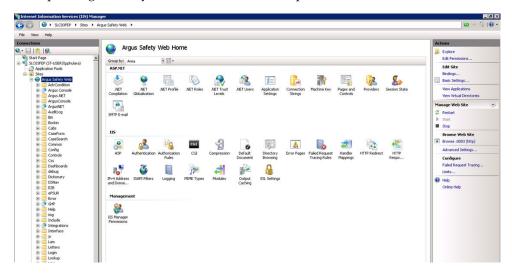
9. Click on **Test Settings** to verify the user credential is valid for the connection.

| dit Site                        |                   | <u>? ×</u> |
|---------------------------------|-------------------|------------|
| Site name:                      | Application pool: |            |
| Argus Safety Web                | DefaultAppPool    | Select     |
| Physical path:                  |                   |            |
| C:\Program Files\Oracle\Argus\A | gusWeb\ASP        |            |
| Connect as 'Argus\user1'        |                   |            |
| Connect as Test Settings.       |                   |            |
|                                 | ОК                | Cancel     |

## Connecting to a Domain Account on Windows 2012

If multiple web servers are configured for Argus in a load-balanced environment, the reports folder must be on a shared path on the network. Connect the PDFReports, UploadedLetters, Integrations, GHP, ArgusNet, Argus Console and Scanned\_Images using the domain account as shown in the following steps:

1. Open Argus Safety Web folder from the left panel.



**2.** Click on **PDFReports** on the left panel, and click on **Basic Settings** on the right panel.

|                                  | nformation Services (IIS) Manag    |                            |                                |               |            |                      |              |                         |                       |               |                       |              |               | _ 6 ×                                     |
|----------------------------------|------------------------------------|----------------------------|--------------------------------|---------------|------------|----------------------|--------------|-------------------------|-----------------------|---------------|-----------------------|--------------|---------------|---|
| 99 0                             | SLC03FEP + Sites + Arg             | us Safety Web              | <ul> <li>PDFReports</li> </ul> | •             |            |                      |              |                         |                       |               |                       |              |               | ₩ × @ 10 •                                |
| Ele Yew                          | Help                               |                            |                                |               |            |                      |              |                         |                       |               |                       |              |               | Actions                                   |
|                                  |                                    | A /PC                      | FReports                       | Home          |            |                      |              |                         |                       |               |                       |              |               |   |
| <mark>€,•     2</mark><br>⊕<br>⊕ | Argus.NET                          | Group by: Ar               | rea                            | • 11 •        |            |                      |              |                         |                       |               |                       |              |               | Edit Permissions     Basic Settings       |
| ۲                                | AuditLog                           |                            | 1                              | [200]         | (E)        | 0                    | 0            |                         |                       | 100           | Contra la             |              | -             | View Virtual Directories                  |
|                                  | 📫 Bin<br>🍯 Bookin                  |                            | <b>e</b>                       |               |            |                      |              | ¥=                      | ab                    |               |                       | 0            | <b>*</b>      | Manage Application                        |
|                                  | Cabs<br>CaseForm<br>CaseSearch     | .NET<br>Compliation        | .NET<br>Globalization          | .NET Profile  | .NET Roles | .NET Trust<br>Levels | .NET Users   | Application<br>Settings | Connection<br>Strings | Machine Key   | Pages and<br>Controls | Providers    | Session State | Browse Application<br>Browse :8083 (http) |
|                                  | Common<br>Config                   |                            |                                |               |            |                      |              |                         |                       |               |                       |              |               | Advanced Settings                         |
|                                  | Controls                           | SMTP E-mail                |                                |               |            |                      |              |                         |                       |               |                       |              |               | Help     Online Help                      |
|                                  | 🧾 debug                            | IIS                        |                                |               |            |                      |              |                         |                       |               |                       |              |               |   |
|                                  | Dictionary<br>DSNav<br>E2B<br>PSUR | ASP                        | Authentication                 | Authorization | CGI        | Compression          | Default      | Directory               | Error Pages           | Faled Request | andler (              | HTTP Redrect | HTTP          |   |
| ۲                                | C Error                            |                            |                                | Rules         |            |                      | Document     | Browsing                |                       | Tracing Rules | Mappings              |              | Respo         |   |
|                                  | 🔮 GHP<br>Help<br>ing               | 1.                         |                                | 1             | al.        |                      |              |                         |                       |               |                       |              |               |   |
| ۲                                | C Include                          | IPv4 Address<br>and Domai  | Logging                        | MIME Types    | Modules    | Output<br>Caching    | SSL Settings |                         |                       |               |                       |              |               |   |
|                                  | Interface                          | Manageme                   | ent                            |               |            |                      |              |                         |                       |               |                       |              |               |   |
| ۲                                | Can Lam                            | <u>88</u>                  |                                |               |            |                      |              |                         |                       |               |                       |              |               |   |
|                                  | Cetters                            |                            |                                |               |            |                      |              |                         |                       |               |                       |              |               |   |
|                                  | Cookup                             | IIS Manager<br>Permissions |                                |               |            |                      |              |                         |                       |               |                       |              |               |   |
| ۲                                |                                    |                            |                                |               |            |                      |              |                         |                       |               |                       |              |               |   |
|                                  | NevronConfig                       |                            |                                |               |            |                      |              |                         |                       |               |                       |              |               |   |
|                                  |                                    |                            |                                |               |            |                      |              |                         |                       |               |                       |              |               |   |
|                                  | C Reconciliation                   |                            |                                |               |            |                      |              |                         |                       |               |                       |              |               |   |
| ۲                                | a Reports                          |                            |                                |               |            |                      |              |                         |                       |               |                       |              |               |   |

- **3.** Change the Physical Path to a shared folder in the Domain.
- 4. Click on Connect as... and select Specific User.
- 5. Enter the Domain User ID and Password and click OK.

**Note:** You can click on Test Settings to verify the user authentication for the connection.

6. Repeat the above-mentioned steps for UploadedLetters, and Scanned\_Images.

## Enabling SSL Support for Windows 2012

Use the following procedure to enable SSL support for Windows 2012:

- **1.** Obtain and install the SSL certificate.
- **2.** Click Argus Safety Web > Bindings.

| Internet Information Services (IIS) Manager  | - 8 × |
|--|-------|
| 🔇 🕒 🗧 SVMENGIRV001 🔸 Sites 🔸 Argus Safety Web 🔸  | 10 -  |
| Vew Heb  |       |
| Connections     Argus Safety Web Home     Actions       Image: Strategy |       |
| Site Bindings  |       |
| Type         Host Name         Port         IP Address         Bind         Add         Manage Web Site           http         8083         Edt         Edt         > Start         > Start             Browse         Browse         Browse Web Site  | •     |
| Close ID83 (http) Advanced Settings SMTP E-mail  |       |
| IIS Content View Ready Ready   | Øj    |

3. Click on Add, then change Type to HTTPS.

| Add Site Binding                                      | <u>?</u> × |
|---|------------|
| Type: IP address:<br>https  All Unassigned Host name: | Port:      |
| SSL certificate:                                      |            |
| Not selected  | ▼ View,.,  |
|   | OK. Cancel |

4. Select SSL Certificate, then click **OK**.

## **Configuring Load Balancer in Argus Web**

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

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

### Set up Argus Web Load Balancer IP Address

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

- 1. Login to Argus Console.
- 2. Select System Management from System Configuration Menu.
- 3. Click the Network Settings Folder.
- 4. Enter the Load Balancer IP Address and click Save.

### Set up Load Balanced Folders

When setting up the load balanced folders, update the network directories for the following virtual directories:

- pdfreports
- uploadedletters
- scannedimages

### 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 the following entries:

- cache=<shared directory for the pdfreports>
- messagecachepath=<shared directory for the message cache>
- upload=<shared directory for the uploaded letters>

**Note:** The Nevron temp file folder on all the Web Servers should point to a common file share such as PDFReports and other folders. The configuration file is present in the ASP\NevronConfig folder. Apart from this, you must also make sure that the client machine has also got access to that share.

## Securing Sensitive Configuration and Operational Data

The following security recommendations should be made to the following files and folders on Argus Safety Web. This ensures that only the IIS User can access these files and local system login accounts outside of the Administrator cannot make changes to the files.

### Windows Directory File

Minimum permission required for file is "Full Control" for the user under which IIS is running:

Argus.ini

### **Shared Folders**

The following folders require minimum permission of "Full Control" for the user under which IIS is running:

- MessageCache
- PDFReports
- Scanned\_Images
- UploadedLetters

## **Configuring Identity in the IIS Application Pools**

- Select Start > Administrative Tools > Internet Information Services (IIS) Manager.
- 2. Select Application Pools.
- 3. Right click on Argus Console Pool and select Advanced settings
- 4. Enter user ID and password in the identity field.
- 5. Reset IIS.
- 6. Repeat same configuration for Argus NET Pool.

**Note:** This configuration will prevent the following error from appearing when filtering data on the Worklist Portal screen:

Error processing your request

## **Resetting IIS**

After changes have been made to the areas listed below, IIS needs to be reset to make the latest data / configurations available to the rest of the system:

1. Changes in config files:

- Argus.ini, Argus.xml
- **2.** Changes in following screens through Console:
  - Common Fields
  - System Management
  - Enabled Modules
- **3.** Loading of MedDRA and WHO Drug dictionaries (J Drug is optional).

# **Setting up Client Browser**

This chapter describes the minimum hardware/software requirements and the installation procedures for the End of Study Unblinding (EOSU) utility. It includes the following sections:

- Adding the Argus Site as a Local Intranet Site
- Setting up Compatibility View with Internet Explorer

## Adding the Argus Site as a Local Intranet Site

To add the Argus site URL as a local intranet site:

- **1.** Open Internet Explorer.
- 2. Select Tools > Internet Options.

The Internet Options dialog box appears.

- **3.** Select the Security tab.
- 4. Select Local Intranet, and click Sites > Advanced.

The Local intranet dialog box appears.

- 5. In the Add this website to the zone field, enter the Argus Safety web site URL.
- 6. Click Add, and click Close.

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

7. Click Custom level...

The Security Settings dialog box appears.

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

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

For more information on how to add a site to Enterprise Mode, refer to

https://technet.microsoft.com/en-us/itpro/internet-explorer/ie11-deploy-guide/ turn-on-enterprise-mode-and-use-a-site-list

# Setting up Compatibility View with Internet Explorer

The URL for Argus Safety can be set to always be displayed in Compatibility View. To do so, execute the following steps:

- **1.** Open Internet Explorer.
- 2. Select Tools > Compatibility View Settings.
- **3.** Enter the Argus Safety web site URL.
- 4. Click Add.
- 5. Click Close.

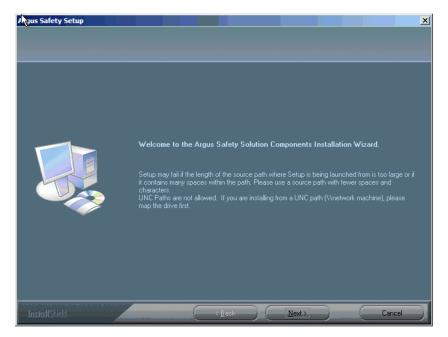
# **Installing Argus Safety Service**

Before installing Argus Safety Service, be sure that a domain account with administrator privileges to the Argus Safety Service box is available after Argus Safety Service has been installed.

See section Setting Up easyPDF to continue installing Argus Safety Service.

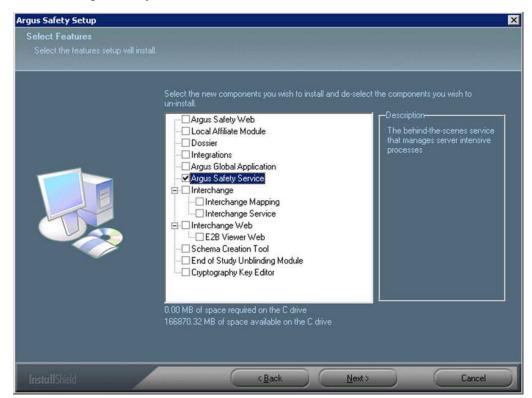
To install Argus Safety Service:

- 1. Click Argus Safety.
- **2.** When the system displays the Argus Safety Solutions Components Installation Wizard: Click **Next** > to continue.

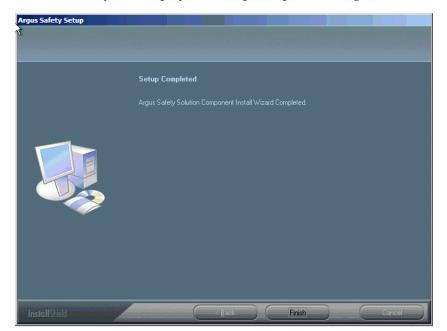


- **3.** When the system displays the Customer Information dialog box:
- 4. Enter the User Name and Company Name.
- 5. Click Next >.
- **6.** When the system opens the Default Directory dialog box, Click Browse to select the default installation directory where the Argus Safety Solution Components will be installed.
- 7. Click Next to open the Argus Safety Components list.
- 8. When the system opens the Argus Safety Components list:

9. Select Argus Safety Service from the list.



- **10.** Click Next >.
- 11. When the system opens the Argus Safety Setup screen dialog box:
- 12. Click Browse, select the folder to store the temporary reports in, and click OK.
- **13.** Click **Next** > to continue.
- 14. Argus installs and shows the progress of the installation.
- **15.** When the system displays the Setup Completed dialog box: Click **Finish**.



**16.** When the system displays the Argus Safety Setup dialog box: Click **OK** to reboot the system.



- **17.** See Chapter 15, "Other Tasks" for information about tasks that must be completed after Argus Safety service has been installed.
- **18.** Oracle creates many temp files that need to be regularly deleted. For information about clearing Oracle temp files, see Clearing Oracle Temp Files.

**Note:** After installing Agus Safety Service, refer to the section The Argus Safety 8.1 Application Servers to set up the Argus Cryptography key and also to the section Generating Encrypted String from Clear Text on Configured User Cryptography Key to configure Argus Safety Service user passwords.

## Starting Argus Safety Service

Before you can start Argus Safety Service, you must configure a single process or it will fail to start.

To start Argus Safety Service:

- 1. Select Start > Control Panel > Administrative Tools.
- 2. Double-click the Component Services shortcut.
- 3. Locate Argus Safety Service in the list of services and select Properties.
- **4.** The following screen is displayed when the system opens the Argus Safety Service Properties dialog box:

| rgus Safety Ser                   | vice Properties (Local Computer)                 | ×          |
|-----------------------------------|--|------------|
| General Log Or                    | Recovery Dependencies                            |            |
| Service name:                     | ArgusSafetyService                               |            |
| Display name:                     | Argus Safety Service                             |            |
| Description:                      |  | *          |
| Path to executa<br>C:\OracleArgus | ole:<br>Argus Safety\AGService.exe               |            |
| Startup type:                     | Automatic  | -          |
| Help me configu                   | re service startup options.                      |            |
| Service status:                   | Stopped  |            |
| Start                             | Stop Pause F                                     | Resume     |
| You can specify<br>from here.     | the start parameters that apply when you start t | he service |
| Start parameters                  | 0  |            |
|                                   |  |            |
|                                   | OK Cancel  | Apply      |

- **5.** Select Automatic from the **Startup type** drop-down list.
- 6. Click the Log On tab.
- **7.** When the system opens the Log On tab:

| Argus Safety Service I | Properties (Local Compute               | r) <u>&gt;</u>           |
|------------------------|---|--------------------------|
| General Log On Red     | covery Dependencies                     |                          |
| Log on as:             |   |                          |
| C Local System acco    | p <b>unt</b><br>o interact with desktop |                          |
| • This account:        | abuser                                  | Browse                   |
| Password:              | •••••                                   |                          |
| Confirm password:      | •••••                                   |                          |
| Help me configure use  | r account log on options.               |                          |
| You can enable or disa | able this service for the hardwar       | e profiles listed below: |
| Hardware Profile       |   | Service                  |
| Undocked Profile       |   | Enabled                  |
| Troubleshooting using  | hardware profiles. Enable               | Disable                  |
|                        | OK Ca                                   | ancel Apply              |

**Note:** Before starting Argus Safety Service, make sure that the service has been installed and at least one process has been configured. Refer to the Argus Safety Service Administrator's Guide for information on configuring Argus Safety Service Process.

- 8. Enter the account log on name in the **This account** field.
- 9. Enter the log on password in the **Password** field.
- **10.** Re-enter the log on password in the **Confirm password** field.
- 11. Click OK.

**Note:** The account you enter must be a domain account with access to the domain printers.

**12.** When the system displays the Services dialog box with the following message: Click **OK**.



- **13.** When the system redisplays the Argus Safety Service Properties dialog box, click **Start**.
- **14.** Click **OK** to close the dialog box.
- **15.** You can view the log file at the following location: <target directory>\Oracle\Log.

For configuration information, refer to the Oracle Argus Safety Service Administration Guide.

## Setting up RightFax

**Note:** The following steps apply only when configuring Argus Safety Service to communicate with RightFax Server.

<ARGUSSAFETY> is the installation folder you selected to install the Argus Safety.

<PROGRAMFILES> is the default Program Files location in your Windows installation.

1. Search for the following files on the Right Fax Server:

RFLanguage.dll (From the English Folder)

rfcomapi.dll (Register)

RFI32RPC.ndr

Rfi32smb.ndr (This file is not required while setting up RightFax 10.5) RFWIN32.DLL

**2.** Copy the RFLanguage.dll File to the following folder on your Argus Safety Service server:

<PROGRAMFILES>\RightFax\Shared Files\English

**3.** Copy the remaining files into the following folder on your Argus Safety Service server:

<ARGUSSAFETY>\Argus Safety

**4.** Register the following files using the following commands:

Rfcomapi.dll

From the command line, browse to the <ARGUSSAFETY>\Argus Safety Folder.

Type in the following:

%WINDIR%\System32\Regsvr32 rfcomapi.dll

**Note:** For 64-bit, type the following command:

%WINDIR%\SysWOW64\Regsvr32 rfcomapi.dll

Click OK in the registration dialog.

RightFax.dll

This file is installed part of Argus Safety and should already exist in the <ARGUSSAFETY>\Argus Safety folder.

From the command line, browse to the <ARGUSSAFETY>\Argus Safety Folder.

Type in the following:

%WINDIR%\Microsoft.Net\Framework\V2.0.50727\RegAsm.exe RightFax.dll /tlb /codebase

7

# **Installing and Configuring EDI Gateway**

This chapter describes the steps required to install and configure the Axway Synchrony EDI Gateway so it can operate correctly with Interchange.

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

This chapter includes instructions on the following topics:

- Creating an Axway Synchrony Database Instance
- Installing Axway Synchrony Interchange
- Starting the Axway Synchrony Server
- Configuring Axway Synchrony Interchange for Axway 5.10
- Configuring Axway Synchrony Interchange for Axway 5.12
- Testing Communication

**Note:** You can install EDI Gateway and Interchange Service in any order.

## Creating an Axway Synchrony Database Instance

Use the following procedure to create an Axway Synchrony database instance.

To create a database instance for Axway Synchrony:

- 1. Log on to the database server as an Admin user.
- 2. Create a blank Axway Synchrony instance, if it does not already exist.
- **3.** Connect to the Axway Synchrony Instance created in Step 2.
- **4.** Create an Axway Synchrony DB User identified by the Axway Synchrony DB password.
- 5. Provide the following grants to the Axway Synchrony DB user:
  - Grant CREATE PROCEDURE
  - Grant CREATE SESSION
  - Grant CREATE TABLE
  - Grant CREATE VIEW

- Grant UNLIMITED TABLESPACE (Optional)
- Grant CREATE SEQUENCE
- Alter user Axway Synchrony DB User default tablespace USERS.
- Grant connect, resource, unlimited tablespace to Axway Synchrony DB User.
- **6.** Log in to cyclone schema and create the following indexes to improve the interface performance between Argus Interchange and Cyclone:
  - create index fbi\_mes\_confilename on messageeventsnapshots (direction, upper(consumptionfilename));
  - create index fbi\_mes\_coreid on messageeventsnapshots (upper(coreid), messageid)

## Installing Axway Synchrony Interchange

Before starting and configuring Axway Synchrony Interchange, you must install Axway Interchange. For more information, see the Axway Interchange installation documentation.

## Starting the Axway Synchrony Server

To start the Axway Synchrony Server:

- 1. Log on to the computer as an Admin user.
- **2.** Go to the Services directory for the local machine.
- **3.** Locate the GatewayInterchageService for the local machine.
- 4. Double click to display the GatewayInterchageService Properties dialog box.
- 5. When the system opens the GatewayInterchageService Properties dialog box:
  - Click Start to start the service if the Service Status is not Started.
  - Once **Service Status** is set to **Started**, Click **OK** to close the dialog box.

An alternative way of starting the Axway Synchrony server is to use the Command Prompt.

- 6. To use the Command Prompt to start the Axway Synchrony Server:
  - Select Start > Programs > Axway Synchrony > Start Server.

The system displays the Start Server dialog box.

**Note:** The first time you perform this task, the system creates tables in the database. This dialog is different on subsequent executions. Do not close this dialog box until the system displays Server Startup Complete.

# Configuring Axway Synchrony Interchange for Axway 5.10

## **Configuring Axway Synchrony Interchange**

Use the following procedure to configure Axway Synchrony Interchange.

To configure Axway Synchrony Interchange:

- **1.** Log on to a client computer.
- 2. Open Internet Explorer.
- **3.** Go to the following URL: (Sender or Receiver) http://<Axway SynchronyServer>:6080/ui/.
- 4. When the system opens the Axway Synchrony Login window:
  - Click Login.

- Type the Axway Synchrony Password in the **Password** field.
- Type the Axway Synchrony User ID in the **User ID** field.
- 5. When the system opens the Getting Started window:
  - Place the mouse over the Trading Configuration icon.
    - Select **Recent Communities > Manage Trading Configuration** from the menu.
- 6. When the system opens the **Pick a community** window:
  - Click Add a community.
- 7. When the Add community wizard opens the Choose the source window:
  - Click Next >> to continue.
  - Click the **Manually create a new community profile** option button.
  - Type the name of the Community in the **Community name** field.
  - Click Finish.
  - Type the routing ID in the **Routing ID** field.
  - Type the e-mail address in the **E-mail address** field.
  - Type the phone number in the **Phone number** field.
  - Type the contact name in the **Contact name** field.
  - Click **Yes** to add a certificate.

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

- 8. When the wizard opens Add a certificate window:
  - Click Next >> to continue.
  - Click Create a self-signed certificate.
- 9. When the wizard opens the Enter the certificate information window:
  - Click Next >> to continue.
- **10.** The wizard opens the **Review request** window:
  - Click **Next** >> to continue.
- 11. When the wizard opens the View certificate details window:
  - Click Finish.
  - Click Make this the default encryption certificate.

- Click Make this the default signing certificate.
- 12. When the wizard opens the Pick a community window:
  - Click the community name link for the newly created community.
- 13. When the Summary window opens:
  - Click the Set up a delivery exchange for receiving messages from partners link.
- 14. When the Choose message protocol window opens:
  - Click **Next** >> to continue.
  - Click the EDIINT AS2 (HTTP) option button.
- 15. When the Choose HTTP transport type window opens:
  - Click **Next** >> to continue.
- **16.** When the **Configure URL** window opens:
  - Click Finish.
- **17.** When the **Summary** window opens:
  - Click the Set up a delivery exchange for routing received messages to integration link.
- **18.** When the **Choose transport protocol** window opens:
  - Click Next >> to continue.
  - Click the **File system** option button.
- **19.** When the **Configure the file system settings** window opens:
  - Click Finish.
  - Type the Axway Synchrony Password in the **Password** field.

### Configuring Axway Synchrony for Binary File Transmission

This section provides a procedure for configuring transmission for binary files such as PMDA zip files and E2B attachments.

To configure Axway Synchrony for binary file transmission:

- **1.** Log on to a client computer.
- **2.** Open the following URL (Sender or Receiver): http://<Axway SynchronyServer>:6080/ui.
- 3. When the Axway Synchrony Login window opens:
  - Type the Axway Synchrony Password in the Password field.
  - Click Login.
  - Type the Axway Synchrony User ID in the User ID field.
- 4. When the Getting Started window opens:
  - Place the mouse over the Trading Configuration icon.
  - Select **Recent Communities** > <**community**> from the menu.
- 5. When the **Summary** screen opens:
  - Click the Integration Pickup icon.

- 6. When the **Pick an integration pickup exchange** window opens:
  - Click the **Other (Plaintext) from File system** link.
- 7. When the Change this integration pickup exchange window opens:
  - Click the **Message attributes** tab.
- 8. When the **Message attribute directory mapping** tab opens:
  - The system moves them to the **Selected attributes** list.
  - Select From routing ID and To routing ID and click Add.
  - Locate the **Available Attributes** list.
  - Click the From address tab.
- 9. When the From address tab opens:
  - Click the **To address** tab.
  - Click the Address determined by message attribute configuration option button.
  - Click Save Changes.
- 10. When the To address tab opens:
  - Click the Address determined by message attribute configuration option button.
  - Click Save Changes.
- **11.** On the Sender's Axway Synchrony 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 Synchrony GUI the Integration Pickup folder will show up only ..\common\out.

**12.** For incoming binary transmissions, repeat steps 5 - 7 for Application Delivery.

Repeat steps 1 - 16 for setting up the Receiver Axway Synchrony.

### Configuring Axway Synchrony Community

Configuring the Axway Synchrony Community includes the following:

- Registering with the Axway Synchrony Community
- Adding a Partner to the Axway Synchrony Community

### **Registering with the Axway Synchrony Community**

Use the following procedure to register with the Axway Synchrony Community.

To register with the Axway Synchrony Community:

- 1. Open this URL: http://<Receiver Axway SynchronyServer>: 6080/ui/.
- 2. When the Axway Synchrony Login window opens.
  - Type the Axway Synchrony Password in the **Password** field.
  - Type the Axway Synchrony User ID in the **User ID** field.
  - Click Login.
- 3. When the Getting started window opens:
  - Place the mouse over the Trading Configuration icon.
  - Select **Recent Communities** > <**community**> from the menu.
- 4. When the Summary page opens:
  - Click the **Export this community as a partner profile** link at the bottom of the page.
- 5. Save the file to your local hard drive and close the Save dialog.
- 6. Click the Logout button in the upper right corner of the page.

### Adding a Partner to the Axway Synchrony Community

Open Internet Explorer.

To add a partner to the Axway Synchrony Community:

- 1. Open the following URL: http://<Sender Axway SynchronyServer>: 6080/ui/.
- 2. When the Axway Synchrony Login window opens:
  - Type the Axway Synchrony User ID in the User ID field.
  - Type the Axway Synchrony Password in the **Password** field.
  - Click Login.
- 3. When the **Getting started** page opens:
  - Place the mouse over the Trading Configuration icon.
  - Select Recent Communities > <community> from the menu.
- 4. When the **Summary** page opens.
  - Click the Add a Partner to this community link.
- 5. When the **Partner Wizard** opens the **Choose the source** window:
  - Click the **Import the profile information from a file** option.
  - Click Next >> to continue.
- 6. When the wizard opens the Enter profile path page:
  - Click Browse to navigate to the saved file.
  - Click Finish.
- 7. When the Successful profile import page opens:
  - 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. When the **Summary** page opens:
  - Click the Partners menu item and select the newly imported partner.
  - Place the mouse over the Trading Configuration icon.
  - Click Set up a routing ID.
- 9. When the Change routing IDs page opens:
  - Click Add.
  - Type the partner (sender) routing ID in the **Routing ID** field.
  - Verify that the partner **does not** have a routing ID.

The system adds the new routing ID to the page.

- Place the mouse over the Trading Configuration icon.
- Select Recent Communities > <community> from the menu.
- **10.** When the **Summary** page opens:
  - Select the sender partner.
- **11.** When the **Summary: Sender** page opens:
  - Click the Default delivery exchange link.
- 12. When the Change this delivery exchange page opens:
  - Verify that the URL is correct and that the correct routing ID for the send is appended to the end of the URL.
  - Click the HTTP Settings tab.

**Registering the Receiver's Community on the Sender Server** Repeat the procedures in sections Creating an Axway Synchrony Database Instance and Starting the Axway Synchrony Server to register the Receiver's community on Sender Server.

### Adding a Node

Use the following procedure to add a node.

To add a node:

- 1. Open Internet Explorer.
- 2. Go to the following URL: http://< Sender Axway SynchronyServer>:6080/ui/.
- 3. When the Axway Synchrony Login window opens:
  - Type the Axway Synchrony User ID in the User ID field.
  - Type the Axway Synchrony Password in the Password field.
  - Click Login.
- **4.** When the Getting started page opens.
  - Click the System Management icon to open the System Management page.

- 5. When the System Management page opens:
  - Click Add a trading engine node.
- 6. When the Add a node page opens:
  - Click Add.
  - Select the machine to add the node to from the Computer name drop-down list.
  - Click the Trading Engine option button.
- 7. When the System management page opens with the newly created node, click **Start**.

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**.

8. Click Home.

When the Welcome page opens, verify that the node status is **Running**.

9. Repeat the preceding steps to set up the Receiver Axway Synchrony.

### Configuring Axway Synchrony Certificates

You can configure Axway Synchrony Certificates on the following:

- Configuring Receiver Axway Synchrony Certificates
- Configuring Sender Axway Synchrony Certificates

#### Configuring Receiver Axway Synchrony Certificates

Use the following procedure to configure Axway Synchrony Certificates on the Receiver Axway SynchronyServer.

To configure Axway Synchrony Certificates on the Receiver Axway Synchrony Server:

- 1. Open Internet Explorer.
- 2. Go to the following URL: http://< Receiver Axway SynchronyServer>:6080/ui/.
- **3.** When the Axway Synchrony Login page opens:
  - Type the Axway Synchrony User ID in the User ID field.
  - Type the Axway Synchrony Password in the **Password** field.
  - Click Login.
- 4. When the Getting Started page opens:
  - Place the cursor on the Trading Configuration icon.
  - Select Manage trading configurations from the menu.
- 5. When the Community page opens:
  - Click the Community name.
- 6. When the Summary page opens:
  - Click the Certificates link.

- 7. When the Certificate page opens:
  - 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 Synchrony.

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

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

### Configuring Sender Axway Synchrony Certificates

Use the following procedure to configure Axway Synchrony Certificates on the Sender Axway SynchronyServer.

To configure Axway Synchrony Certificates on the Sender Axway Synchrony Server

- **1.** Open Internet Explorer.
- 2. Go to the following URL: http://< Sender Axway SynchronyServer>:6080/ui/.
- 3. When the Axway Synchrony Login page opens:
  - Click Login.
  - Type the Axway Synchrony Password in the Password field.
  - Type the Axway Synchrony User ID in the **User ID** field.
- **4.** When the Getting Started page opens:
  - Place the cursor on the Trading Configuration icon.
  - Select Manage trading configurations from the menu.
- 5. When the Community page opens:
  - Click the Community name.
- **6.** When the Summary page opens:
  - Click the Certificates link.
- 7. When the Certificate page opens:
  - Click the **Trusted root certificates** tab.

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

- **8.** When the list of trusted root certificates opens.
  - Click the Add a trusted root certificate link.

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

- **9.** When the Add a certificate page opens in a new window:
  - Click Next >> to continue.
- **10.** When the Locate the certificate file page opens:
  - Click Browse to locate the P7B certificate file saved for the Receiver Axway Synchrony Server.
  - Click Next >> to continue.
- **11.** When the View certificate details page opens:
  - Click Finish.
- **12.** When the Pick a certificate page opens in the original window:
  - Click the Trusted root certificates tab.
- **13.** When the list of Trusted root certificates opens:
  - Verify that the certificate you added appears on the list.
- **14.** Log out of the Sender Server.

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

### Configuring EVENTS.XML

**Note:** JVM argument is not applicable in version 5.12. Hence, just edit the Event.xml.

To configure EVENTS.XML

- **1.** Log on to a client computer.
- **2.** Using Windows Explorer, go to the local directory containing the Argus Safety installation files and navigate to ..\DBInstaller\Cyclone.
- **3.** Locate and double-click the **cyclone\_schema\_Oracle11g.bat** file to open a DOS command prompt window.
- 4. When the Oracle SQL+ window opens:
  - Type the Axway Synchrony instance in the TSNAMES entry.

- Type the Axway Synchrony DB User Name in the Axway Synchrony User Name.
- Type the Axway Synchrony Schema User in the [USERS].
- Type the Axway Synchrony User Password in the **Password for User Axway** Synchrony\_USER.
- 5. When SQL+ connects to the specified database:
  - Enter the log file name in **log file name**.
  - Enter the log directory name in **Directory**.

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

- 1. Log on to the Receiver Server.
- **2.** Using Windows Explorer, navigate to <Axway Synchrony Install Folder>\build\conf folder\.
- **3.** Backup the Events.xml file and rename it Events.xml.bak.
- 4. Right-click the Events.xml file and select Edit to display 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"/>

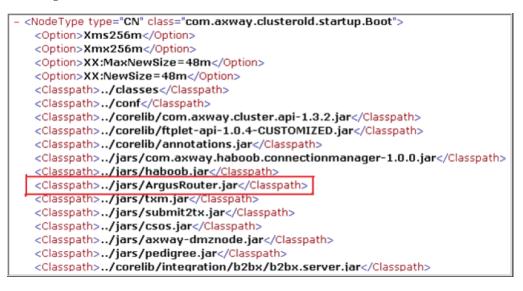
</OrFilter>

</EventFilter>

To re-enable logging into the MESSAGEEVENTSNAPHOTS table, uncomment the following event filter in the events.xml. This was enabled, by default, in Axway Synchrony versions prior to Axway Synchrony 5.4.

<EventRouter id="Message Events to Database" class="com.cyclonecommerce.events2.router.PersistenceRouter" active="true" priority="2147483647"> <EventFilterRef ref="Messaging To Database"/> </EventRouter>.

- **7.** Copy the ArgusRouter.jar file from Argus [local directory] \ SUPPORT \ Axway Synchrony \ Axway Synchrony 5x to Axway Synchrony directory: <Axway Synchrony Install Folder>\jars\.
- **8.** The following file "<Axway Interchange Installation Path>\Synchrony\Interchange\conf\jvmArguments.xml" on the cyclone server must be edited to add the ArgusRouter.jar file entry, as displayed in the following image:



- **9.** Open Internet Explorer.
- **10.** Open the following URL: http://<Receiver Axway SynchronyServer>: 6080/ui/.
- **11.** When the Axway Synchrony Login page opens:
  - Type the Axway Synchrony User ID in the User ID field.
  - Click Login.
  - Type the Axway Synchrony Password in the **Password** field.
- **12.** When the Getting started page opens:
  - Place the cursor on the **Trading Configuration** icon.
  - Select Recent Communities > Community from the menu.
- **13.** When the Summary page appears.
  - Click the Integration Pickup icon.
- **14.** When the Pick an integration pickup exchange page opens:
  - Click the link in the Type column.
- **15.** When the Change this integration pickup exchange page opens:
  - Click the Inline Processing tab.
- **16.** When the Inline processing rules appear:
  - Type **com.cyclonecommerce.relsys.router.GetMessageInfo** in the **Class name** field.
  - Enter **Relsys Argus** in the **Parameter** field.
  - Enter **GetMessagesInformation** in the **Description** field.

- **17.** Click Save changes.
- **18.** When the Pick an integration pickup exchange page opens.
  - Click Logout.
- 19. Repeat the preceding steps for the Sender Server.

# Configuring Axway Synchrony Interchange for Axway 5.12

Use the following procedure to configure Axway Synchrony Interchange.

To configure Axway Synchrony Interchange:

- **1.** Log on to a client computer.
- 2. Open Internet Explorer.
- **3.** Go to the following URL: (Sender or Receiver) http://<*Axway SynchronyServer*>:6080/ui/.
- 4. When the system opens the Axway Synchrony Login window:
  - Click Login.
  - Type the Axway Synchrony Password in the Password field.
  - Type the Axway Synchrony User ID in the User ID field.
- 5. When the system opens the Getting Started window:
  - Place the mouse over the Trading Configuration icon.
  - Select Recent Communities > Manage Trading Configuration from the menu.
- 6. When the system opens the **Pick a community** window:
  - Click Add a community.
- 7. When the Add community wizard opens the **Choose the source** window:
  - Click Next >> to continue.
  - Click the Manually create a new community profile option button.
  - Type the name of the Community in the **Community name** field.
  - Type the full name in the Full Name field.
  - Type the e-mail address in the **E-mail address** field.
  - Type the phone number in the **Phone number** field.
  - Type the routing ID in the Routing ID field.
  - Click **Yes** to add a certificate.

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

- Click Finish.
- 8. When the wizard opens Add a certificate window:
  - Click Next >> to continue.
  - Click Create a self-signed certificate.

- 9. When the wizard opens the Enter the certificate information window:
  - Click Next >> to continue.
- **10.** The wizard opens the **Review request** window:
  - Click Next >> to continue.
- 11. When the wizard opens the View certificate details window:
  - Click Finish.
  - Click Make this the default encryption certificate.
  - Click Make this the default signing certificate.
- **12.** When the wizard opens the **Pick a community** window:
  - Click the community name link for the newly created community.
- **13.** When the **Summary** window opens:
  - Click the Set up a delivery exchange for receiving messages from partners link.
- 14. When the Choose message protocol window opens:
  - Click Next >> to continue.
  - Click the EDIINT AS2 (HTTP) option button.
- 15. When the Choose HTTP transport type window opens:
  - Click Next >> to continue.
- **16.** When the **Configure URL** window opens:
  - Click Next.
- 17. When the Exchange Name window opens:
  - Type the Exchange Name.
  - Click Finish.
- **18.** When the **Summary** window opens:
  - Click Application Delivery.
  - Add an application delivery.
- **19.** When the **Choose transport protocol** window opens:
  - Click Next >> to continue.
  - Click the File system option button.
- 20. When the Configure the file system settings window opens:
  - Click Next.
- 21. When the Exchange Name window opens:
  - Type the Exchange Name.
  - Click Finish.
- **22.** Go to the **Summary Page**.
  - Click Configure the settings for application delivery.
- 23. When the Select application delivery window opens:

- Select Name.
- Click Finish.

## Configuring Axway Synchrony for Binary File Transmission

This section provides a procedure for configuring transmission for binary files such as PMDA zip files and E2B attachments.

To configure Axway Synchrony for binary file transmission:

- **1.** Log on to a client computer.
- **2.** Open the following URL (Sender or Receiver): http://<*Axway SynchronyServer*>:6080/ui.
- 3. When the Axway Synchrony Login window opens:
  - Type the Axway Synchrony Password in the **Password** field.
  - Click Login.
  - Type the Axway Synchrony User ID in the **User ID** field.
- 4. When the **Getting Started** window opens:
  - Place the mouse over the Trading Configuration icon.
  - Select Recent Communities > <community> from the menu.
- 5. When the **Summary** screen opens:
  - Click the **Integration Pickup** icon.
- 6. Add an application pickup.
- 7. When the **Choose transport protocol** window opens:
  - Click Next >> to continue.
  - Click File system option.
- 8. When the From address window opens:
  - Click Next >> to continue.
  - Address must be determined by either message attribute configuration or by protocol address only.
- 9. When the To address window opens:
  - Click Next >> to continue.
  - Address must be determined by either message attribute configuration or by protocol address only.
- 10. When the **Configure the file system settings** window opens:
  - On the Sender's Axway Synchrony Server, locate Common/Out folder and create the following folder structure:

Common\Out\Sender's Routing ID\Receiver's Routing ID

- **11.** When the **Exchange name** window opens:
  - Enter the Exchange Name.
  - Click Finish.
- 12. When the Change this application pickup exchange window opens:

- Click the Message attributes tab.
- **13.** When the **Message attribute directory mapping** tab opens:
  - The system moves them to the Selected attributes list.
  - Select From routing ID and To routing ID and click Add.
  - Locate the Available Attributes list.
  - Click the From address tab.

14. When the From address tab opens:

- Click the **To address** tab.
- Click the Address determined by message attribute configuration option button or by protocol address only.
- Click Save Changes.

**15.** When the **To address** tab opens:

- Click the Address determined by message attribute configuration option button or by protocol address only.
- Click Save Changes.
- **16.** On the Sender's Axway Synchrony 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 Synchrony GUI the Integration Pickup folder will show up only ..\common\out.

17. For incoming binary transmissions, repeat steps 5 - 8 for Integration Delivery.

Repeat steps 1 - 12 for setting up the Receiver Axway Synchrony.

### Configuring Axway Synchrony Community

Configuring the Axway Synchrony Community includes the following:

- Registering with the Axway Synchrony Community
- Adding a Partner to the Axway Synchrony Community

### Registering with the Axway Synchrony Community

Use the following procedure to register with the Axway Synchrony Community.

To register with the Axway Synchrony Community:

- 1. Open this URL: http://<*Receiver Axway SynchronyServer*>: 6080/ui/.
- 2. When the Axway Synchrony Login window opens.

- Type the Axway Synchrony Password in the **Password** field.
- Type the Axway Synchrony User ID in the User ID field.
- Click Login.
- 3. When the Getting started window opens:
  - Place the mouse over the Trading Configuration icon.
  - Select Recent Communities > <community> from the menu.
- 4. When the Summary page opens:
  - Click **Export this community as a partner profile** at the bottom of the page.
- 5. Save the file to your local hard drive and close the **Save** dialog.
- 6. Click **Logout** in the upper right corner of the page.

### Adding a Partner to the Axway Synchrony Community

To add a partner to the Axway Synchrony Community:

- 1. Open the following URL: http://<Sender Axway SynchronyServer>: 6080/ui/.
- 2. When the Axway Synchrony Login window opens:
  - Type the Axway Synchrony User ID in the User ID field.
  - Type the Axway Synchrony Password in the Password field.
  - Click Login.
- 3. When the Getting started page opens:
  - Place the mouse over the Trading Configuration icon.
  - Select Recent Communities > <community> from the menu.
- 4. When the **Summary** page opens.
  - Click the Add a Partner to this community link.
- 5. When the **Partner Wizard** opens the **Choose the source** window:
  - Click the Import the profile information from a file option.
  - Click **Next** >> to continue.
- 6. When the wizard opens the **Enter profile path** page:
  - Click **Browse** to navigate to the saved file.
  - Click Finish.
- 7. When the **Successful profile import** page opens:
  - 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.** When the **Summary** page opens:
  - Click the Partners menu item and select the newly imported partner.
  - Place the mouse over the Trading Configuration icon.

- Click Set up a routing ID.
- 9. When the Routing IDs page opens:
  - Click Add.
  - Type the partner (sender) routing ID in the **Routing ID** field.
  - Verify that the partner does not have a routing ID.
    - The system adds the new routing ID to the page.
  - Place the mouse over the Trading Configuration icon.
  - Select **Recent Communities** > <**community**> from the menu.
- **10.** When the **Summary** page opens:
  - Select the sender partner.
- **11.** When the **Summary: Sender** page opens:
  - Click the Default delivery exchange link.
- 12. When the Change this delivery exchange page opens:
  - Verify that the URL is correct and that the correct routing ID for the send is appended to the end of the URL.
  - Click the **HTTP Settings** tab.

**Registering the Receiver's Community on the Sender Server** Repeat the procedures in sections Creating an Axway Synchrony Database Instance and Starting the Axway Synchrony Server to register the Receiver's community on Sender Server.

### Adding a Node

Use the following procedure to add a node.

- 1. Open Internet Explorer.
- 2. Go to the following URL: http://< Sender Axway SynchronyServer>:6080/ui/.
- 3. When the Axway Synchrony Login window opens:
  - Type the Axway Synchrony User ID in the User ID field.
  - Type the Axway Synchrony Password in the Password field.
  - Click Login.
- **4.** When the Getting started page opens.
  - Click the System Management icon to open the System Management page.
- 5. When the **System Management** page opens:
  - Click Add a node.
- 6. When the Add a node page opens:
  - Click Add.
  - Select the machine to add the node to from the Computer name drop-down list.
  - Click the Trading Engine option button.
- 7. When the System management page opens with the newly created node:

Click Start to start the 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**.

- 8. Click Home.
  - When the Welcome page opens, verify that the node status is Running.
- 9. Repeat the preceding steps to set up the Receiver Axway Synchrony.

### Configuring Axway Synchrony Certificates

You can configure Axway Synchrony Certificates on the following:

- Configuring Receiver Axway Synchrony Certificates
- Configuring Sender Axway Synchrony Certificates

### Configuring Receiver Axway Synchrony Certificates

Use the following procedure to configure Axway Synchrony Certificates on the Receiver Axway Synchrony Server.

- 1. Open Internet Explorer.
- **2.** Go to the following URL: http://<*Receiver Axway SynchronyServer*>:6080/ui/.
- **3.** When the Axway Synchrony Login page opens:
  - Type the Axway Synchrony User ID in the User ID field.
  - Type the Axway Synchrony Password in the **Password** field.
  - Click Login.
- **4.** When the Getting Started page opens:
  - Place the cursor on the Trading Configuration icon.
  - Select Manage trading configurations from the menu.
- 5. When the **Community** page opens:
  - Click the **Community name**.
- 6. When the **Summary** page opens:
  - Click the Certificates link.
- 7. When the **Certificate** page opens:
  - 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 Synchrony.

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

**8.** When the View certificate page opens:

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

### Configuring Sender Axway Synchrony Certificates

Use the following procedure to configure Axway Synchrony Certificates on the Sender Axway Synchrony Server.

- **1.** Open Internet Explorer.
- 2. Go to the following URL: http://<Sender Axway SynchronyServer>:6080/ui/.
- 3. When the Axway Synchrony Login page opens:
  - Click Login.
  - Type the Axway Synchrony Password in the **Password** field.
  - Type the Axway Synchrony User ID in the **User ID** field.
- 4. When the Getting Started page opens:
  - Place the cursor on the **Trading Configuration** icon.
  - Select **Manage trading configurations** from the menu.
- 5. When the Community page opens:
  - Click the **Community name**.
- 6. When the Summary page opens:
  - Click the **Certificates** link.
- 7. When the Certificate page opens:
  - Click the Trusted root certificates tab.

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

- 8. When the list of trusted root certificates opens.
  - Click the **Add a trusted root certificate** link.

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

**9.** When the Add a certificate page opens in a new window:

- Click Next >> to continue.
- **10.** When the Locate the certificate file page opens:
  - Click Browse to locate the P7B certificate file saved for the Receiver Axway Synchrony Server.
  - Click Next >> to continue.
- **11.** When the View certificate details page opens:
  - Click Finish.
- **12.** When the Pick a certificate page opens in the original window:
  - Click the Trusted root certificates tab.
- **13.** When the list of Trusted root certificates opens:
  - Verify that the certificate you added appears on the list.
- 14. Log out of the Sender Server.

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

### Configuring EVENTS.XML

**Note:** JVM argument is not applicable in version 5.12. Hence, only edit the Event.xml.

To configure EVENTS.XML

- **1.** Log on to a client computer.
- 2. Using Windows Explorer, go to the local directory containing the Argus Safety installation files and navigate to ..\DBInstaller\Cyclone.
- **3.** Locate and double-click the **cyclone\_schema\_Oracle11g.bat** file to open a DOS command prompt window.
- 4. When the Oracle SQL+ window opens:
  - Enter the Axway Synchrony instance in the **TSNAMES entry**.
  - Enter the Axway Synchrony DB User Name in the Axway Synchrony User Name.
  - Enter the Axway Synchrony Schema User in the [USERS].
  - Enter the Axway Synchrony User Password in the Password for User Axway Synchrony\_USER.
- 5. When SQL+ connects to the specified database:
  - Enter the log file name in log file name.
  - Enter the log directory name in **Directory**.

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

- **1.** Log on to the Receiver Server.
- Using Windows Explorer, navigate to <*Axway Synchrony 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>
```

To re-enable logging into the MESSAGEEVENTSNAPHOTS table, uncomment the following event filter in the events.xml. This was enabled, by default, in Axway Synchrony versions prior to Axway Synchrony 5.4.

```
<EventRouter id="Message Events to Database"
class="com.cyclonecommerce.events2.router.PersistenceRouter" active="true"
priority="2147483647"> <EventFilterRef ref="Messaging To Database"/>
</EventRouter>
<EventFilterRef ref ="MessgeingToDatabase"/></EventRouter>
```

- **7.** Copy the ArgusRouter.jar file from Argus local directory: \ *SUPPORT* \ *Axway Synchrony* \ *Axway Synchrony 5x* to Axway Synchrony directory: <*Axway Synchrony Install Folder*>\*site*\*jars*\.
- 8. Open Internet Explorer.
- **9.** Open the following URL: http://<*Receiver Axway SynchronyServer>*: 6080/ui/.
- **10.** When the Axway Synchrony Login page opens:
  - Type the Axway Synchrony User ID in the User ID field.
  - Click Login.
  - Type the Axway Synchrony Password in the **Password** field.
- **11.** When the Getting started page opens:
  - Place the cursor on the Trading Configuration icon.
  - Select Recent Communities > Community from the menu.
- **12.** When the Summary page appears.
  - Click the **Application Pickup** icon.
- **13.** When the Application pickup exchange page opens:
  - Click the link in the Name column.
- **14.** When the Application pickup exchange page opens:

- Click the Inline Processing tab.
- **15.** When the Inline processing rules appear:
  - Enter com.cyclonecommerce.relsys.router.GetMessageInfo in the Class name field.
  - Enter Relsys Argus in the Parameter field.
  - Enter **GetMessagesInformation** in the **Description** field.
- **16.** Click **Save changes**.
- **17.** When the Pick an integration pickup exchange page opens.
  - Click Logout.
- 18. Repeat the preceding steps for the Sender Server.

## **Testing Communication**

Use the following procedure to test communication for Axway Synchrony Interchange.

To test communication for Axway Synchrony Interchange:

1. From the Sender Axway Synchrony 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 Synchrony servers on both sender and receiver are running.
- **3.** Drop the E2B XML file into the out bound folder of the Axway Synchrony Sender server.
- 4. Log on to a machine where Axway Synchrony is installed.
- 5. Open Internet Explorer.
- 6. Open this URL: http://<Sender Axway SynchronyServer>:6080/ui/.
- 7. When the Axway Synchrony Login page opens:
  - Click Login.
  - Type the Axway Synchrony Password in the **Password** field.
  - Type the Axway Synchrony User ID in the User ID field.
- **8.** When the Getting started page opens:
  - Place the cursor on the Message Tracker icon.
  - Select Message Searches > All Messages from the menu.

When the Search results page opens verify that the transmission is in progress by locating the Custom Search section and clicking Find until Delivered appears on the screen.

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

- 9. After the system transmits the file it opens the Search results for page:
  - Click Logout.
- **10.** Go to the Axway Synchrony Receiver server and verify that the E2B file has been received.
- **11.** To verify that the file has been transmitted:
  - Log in to the receiver Axway Synchrony server.
  - Select the All Messages option.
  - View the message payload.
- **12.** Compare the E2B file on the receiving machine (payload version displayed) with the file from the sending machine. These files should be identical.
- **13.** Repeat the preceding steps to verify delivery on the Receiver Server.

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 Synchrony outbound folder.

# **Configuring Oracle B2B**

This chapter lists the steps to configure Oracle B2B as per your requirements.

**Note:** Either Oracle B2B or Axway Synchrony is required for E2B reports exchange. Customers can choose any one of the software, as required.

# 8.1 Integrating Oracle B2B with Argus Safety

This section lists the steps to integrate Argus Safety with Oracle B2B, if the latter is selected as the EDI Gateway.

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

## 8.1.1 Creation of integration tables in B2B Schema

There are a few database objects which are created in ESM Schema for outbound files integration as part of 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 Installation 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 2 database objects required to integrate incoming files data:

- 1. B2B\_ARGUSSAFETY\_INBOUND (table)
- 2. S\_B2B\_ARGUSSAFETY\_INBOUND (sequence)

## 8.1.2 Oracle B2B UI Configuration

Log in to Oracle B2B UI as an admin user.

### 8.1.2.1 General Configuration > Administration > Configuration

Follow the steps listed below:

- 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.

### 8.1.2.2 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.

## 8.1.3 Enterprise Manager Configuration

### 8.1.3.1 SOA Composite Deployment

There are 2 composites provided with the Argus Safety build to integrate Oracle B2B, one is for all outbound traffic from Argus Safety, **sca\_AS\_BPEL\_Outbound\_rev1.0.jar**. The other one is for all inbound traffic to Argus Safety, **sca\_AS\_BPEL\_Inbound\_rev1.0.jar**. The location of the files is **\Support\OracleB2B** in the installation directory.

1. Log in to Enterprise Manager with 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.

### 8.1.3.2 SOA Composite Configuration

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

### 8.1.3.2.1 AS\_BPEL\_Outbound Composite

Right-click on AS\_BPEL\_Outbound under the deployed domain in Enterprise Manager and click on Service/Reference Properties.

- 1. Select AS\_FileAdapter.
  - **a.** Change PhysicalDirectory and PhysicalArchiveDirectory to the desired location. The other properties are not supposed to be changed.
  - **b.** Argus Safety may create outbound files under the same or under any of the child directories of the above specified directory.
- **2.** B2B\_DBAdapter should NOT be changed for any of the properties.
- **3.** B2B\_JMSAdapter can be changed, but only if required.

### 8.1.3.2.2 AS\_BPEL\_Inbound Composite

Right-click on AS\_BPEL\_Inbound under the deployed domain in Enterprise Manager and click on Service/Reference Properties.

- **1.** Select AS\_FileAdapter.
  - **1.** PhysicalDirectory should be set as the top level folder under which all the incoming files are dropped by B2B.
  - 2. The other properties are not supposed to be changed.
- **2.** Select LargeFileReader.
  - 1. The PhysicalDirectory should be the same as Large Payload Directory under Oracle B2B UI > Administration > Configuration > Performance section.
  - 2. The other properties are not supposed to be changed.
- **3.** B2B\_DBAdapter should NOT be changed for any of the properties.
- **4.** B2B\_Inbound can be changed, but only if required.

### 8.1.4 Web Logic Console Configuration

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

### 8.1.4.1 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 Argus Safety database table **B2B\_ARGUSSAFETY\_OUTBOUND** under ESM Schema. This table is available as part of Argus Safety installation. The configuration has been 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'.

### 8.1.4.2 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 data source which has access all access on integration database table B2B\_ARGUSSAFETY\_INBOUND and sequence S\_B2B\_ARGUSSAFETY\_INBOUND. These are created as part of script.

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

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

### 8.1.4.3 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 data source which has access all access on 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 has been 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".

### 8.1.4.4 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 Section 8.1.4.1, "Data source with JNDI Name as 'eis/DB/ArgusSafety\_Outbound'," and Section 8.1.4.3, "Data source with JNDI Name as 'eis/DB/ArgusSafety\_Inbound'".

Make sure that 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'.

## 8.1.5 Large Payload Exchange Configuration

For B2B, a large payload is a file bigger than the configured size on 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. Each following point specifies if they are needed even if you are exchanging small files.

### 8.1.5.1 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.

### 8.1.5.2 Inbound Files

Log in to Enterprise Manager.

Go to SOA > (Domain) > SOA Administration > B2B Server Properties.

On the right side, under the Operation tab, click addProperty to add a new property called **b2b.setisLargePayloadPropertyForSmallMsg** with value as **True**.

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 porperty.

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

### 8.1.5.3 Transaction Time

Log in to Web Logic Console > (Domain) > Services > JTA > Timeout Seconds. This can be set 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.

### 8.1.5.4 General B2B Settings for Large Payloads

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

## 8.1.6 Configuration on Argus Safety side

This section comprises the following sub-sections:

- Configure Oracle B2B
- Update for B2B Documents
- Argus Console > Reporting Destination Code List

### 8.1.6.1 Configure Oracle B2B

Log in to ESM Mapping Utility as an ESM Admin user.

Go to Administrator Menu > Setup INI file > EDI Section.

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)

### 8.1.6.2 Update for B2B Documents

Document configuration, as mentioned under Oracle B2B UI > Configuration > Document should be updated in Argus Safety by manually updating the database table **B2B\_ARGUSSAFETY\_DOC** under ESM Schema of Argus Safety.

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

The above is the sample factory data provided. The Admin is expected to update only Doc\_Type and Doc\_Revision columns from Doc Type and Doc Revision information respectively from B2B UI.

The Doc ID column must not be updated and new Doc Id is not supported.

Besides this, the mapping between Doc Id and other columns is assumed to be exactly as provided in the sample above. 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.

If there is no Reporting Destination with EDI Header and Footer configuration, Doc\_ID=4 may be left blank.

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.

### 8.1.6.3 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.

# **Installing and Configuring Interchange**

This chapter provides information about installing and configuring Interchange Service.

**Note:** Microsoft Visual Basic Power Packs 10.0 is required to be installed prior to installing Interchange Mapping.

It includes discussions of the following:

- Installing Interchange Service
- Configuring Interchange Service
- Accessing EDI Gateway Shared Folders
- Configuring the Interchange Service.INI File

# Installing Interchange Service

Before installing Interchange Service, be aware of the following:

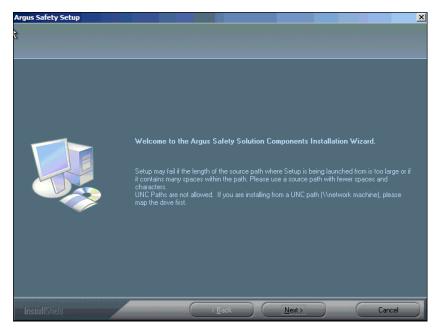
- Since Interchange Mapping has a user interface for configuring Interchange Service, it must be installed on the same system as Interchange Service. If they are not installed on the same system, you will be unable to access the user interface required to configure Interchange Service.
- You must also have the following:
  - A domain account with Local Administrator Privileges. This is required after you finish installing Interchange Service
  - See Setting Up easyPDF to continue installing Argus Web.
- If Interchange Service is already installed on the system, be sure to uninstall it before continuing with the installation.
- Before installing Interchange Service, create a network account to enable Interchange Service to communicate with the e-mail system and access the shared folders on the Axway Synchrony Server.
- The Interchange account must have access to an e-mail account on the Axway Synchrony machine without being prompted for a password.

Use the following procedure to install Interchange Service.

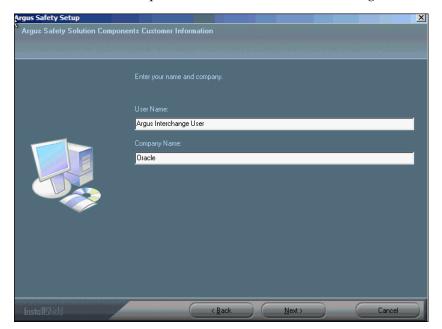
### To install Interchange Service:

1. Start the Argus Safety Setup installation wizard by double-clicking setup.exe.

**2.** When the system displays the Argus Safety Solution Components Install Wizard dialog box, click **Next** > to continue.

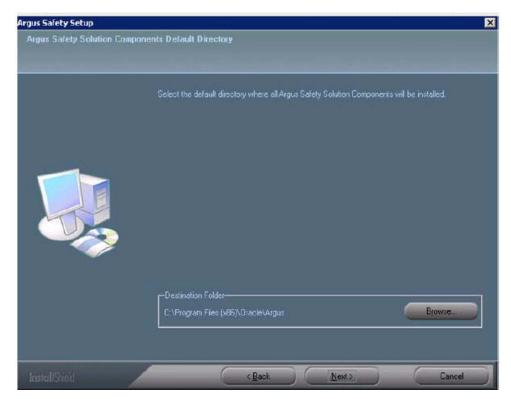


**3.** When the wizard opens the Customer Information dialog box:



- Type the user name in the **User Name** field.
- Type the company name in the **Company Name** field.
- Click Next > to continue.

4. When the wizard opens the Default Directory dialog box:



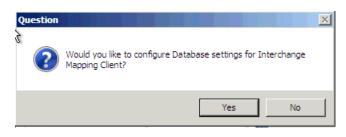
- Click Browse to default installation directory for the Argus Safety Solution components.
- 5. When the wizard opens the dialog box:

|  | elect Features |  |   |
|--|----------------|--|---|
| Un-install  Argus Safety Web  Cocal Affiliate Module  Dossier  Integrations  Argus Global Application  Argus Safety Service  Interchange Mapping  Interchange Service  Content change Web  Cochema Creation Tool  Content of Study Unblinding Module   |                |  |   |
| Argus Safety Web     Local Affliate Module     Local Affliate Module     Integrations     Argus Global Application     Argus Global Application     Argus Safety Service     VInterchange     PVInterchange Service     Interchange Service     Interchange Web     E28 Viewer Web     Schema Creation Tool     End of Study Unblinding Module |                | un-install.  |   |
|  |                | <ul> <li>Local Affiliate Module</li> <li>Dossier</li> <li>Integrations</li> <li>Argus Global Application</li> <li>Argus Safety Service</li> <li>✓ Interchange</li> <li>✓ Interchange Mapping</li> <li>✓ Interchange Web</li> <li>E28 Viewer Web</li> <li>Schema Creation Tool</li> <li>End of Study Unblinding Module</li> </ul> | The solution for electronic<br>transmission of safety reports |
| 74.87 MB of space required on the C drive<br>166868.41 MB of space available on the C drive  |                |  |   |

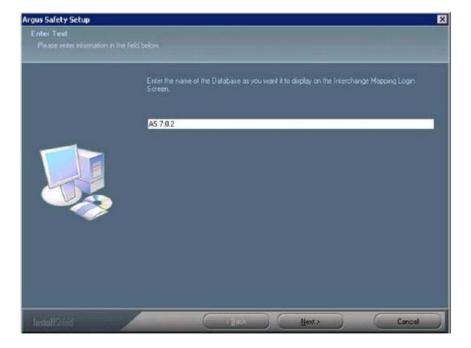
- Select Interchange.
- Click **Next** > to continue.

Argus installs and shows the progress of the installation.

**6.** When the system asks whether you want to configure a database for Argus Interchange:

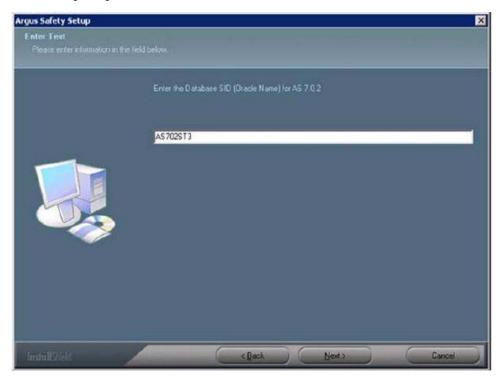


- Click **Yes** to configure a database for Argus Interchange.
- 7. When prompted to enter a database name:

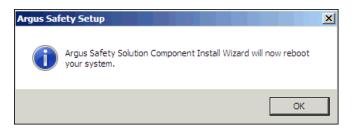


- Enter the database name as you want it to appear in Argus Interchange.
- Click Next > to continue.

**8.** When prompted to enter the database SID:



- Enter the database SID.
- Click Next > to continue.
- **9.** When the system asks if you would like to configure database settings for Argus Interchange:
  - Click Yes to add an additional database to the Argus Interchange.
- **10.** When the following message displays:



11. Click OK to reboot.

**Note:** After installing Interchange Service, refer to the section The Argus Safety 8.1 Application Servers to set up the Argus Cryptography key.

# **Configuring Interchange Service**

Use the following procedure to configure Interchange Service:

- 1. Select Start > Control Panel > Administrative Tools.
- 2. Open Component Services.

- **3.** Locate Argus Interchange Service in the services list, right-click, and select **Properties** from the drop-down menu.
- 4. When the system opens the Electronic Submission Manager Properties dialog box:
  - Select Automatic from the Startup type drop-down list.
  - Click the Log On tab.
- 5. When the Log On tab opens:
  - Select This Account as the Logon as Option
  - Select the user account from the Company domain list.
  - The account must have local admin privileges and access to all site printers.
  - Type the password in the **Password** field.
  - Type the password again in the **Confirm password** field.
  - Click Enable.
  - Click **OK**.

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

### Transmitting E2B Attachments

You must set up the easyPDF before you can transmit E2B attachments.

# Accessing EDI Gateway Shared Folders

Use the following procedure to access EDI gateway shared folders:

- 1. Log on to the machine where Interchange Service is installed.
- 2. Browse to the data folder in the Axway Synchrony 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 on the Interchange Service machine and make sure no password is required for connecting to the shared folders on the EDI gateway machine.

# Configuring the Interchange Service.INI File

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

Use the following procedure to configure Interchange Service:

- **1.** Open ESM Mapping.
- **2.** Select Administrator > Setup INI File from the menu.
- 3. When the Service INI File Setup dialog opens:
  - Type the appropriate values in each field in the dialog box.
- 4. Click OK.

The following table provides the Service.INI File Dialog Box Fields:

| Field Name                | Field Description   |  |
|---------------------------|---|--|
| IT E-mail                 | Enter the 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           | Enter an e-mail address where a message can be sent if the Receive ACK time-out value is reached  |  |
| User E-mail               | Enter an e-mail address where a message can be sent if the user does not process the E2b Report within the time-out value.                      |  |
| Profile Name              | Enter the MAPI Profile name of the mail account used.   |  |
| EDI Software Name         | Enter the EDI Software name used i.e. Axway Synchrony.  |  |
| EDI Database Name         | Enter the Database Name for the EDI software.   |  |
| EDI User ID               | Enter the User Name for EDI database.   |  |
| EDI Password              | Enter the password associated with the User Name to the EDI database.   |  |
| EDI Client Software       | Enter the type of database used by the EDI software   |  |
| DTD Path                  | Enter the path to the location of the DTD file.   |  |
| Log File Path             | Enter the path where Interchange Service will write the log files.  |  |
| Documentum Type           | Enter the Documentum table.   |  |
| Multiple Database Section | Displays all the configured databases for Interchange Service.  |  |
| Delete Button             | Clicking Delete will remove the entire Database Configuration from Interchange Service INI File.  |  |

# **Performing Post-installation Checks**

This chapter provides checklists and procedures for verifying that Argus Safety is installed correctly. It includes discussions of the following:

- Post-Installation Tasks
- Verifying the Web Server Installation and IIS Configurations
- Configure and Verify the Dossier Installation
- Verify Files installed on Middle Tier Servers:
- Verifying the Documentum Installation

# **Post-Installation Tasks**

This section is to verify whether the installation has completed successfully. The post-install checklists include the following:

- General Checklist
- Configuring Argus Safety Windows Service to run as a Domain User
- Configure Worklist Intake
- IIS Checklist
- .INI File Checklist
- Service Checklist

## **General Checklist**

Use this checklist to verify whether the components selected by the user have been configured properly.

### Verify That:

- Oracle 11g/2c is installed.
- The correct modules are installed as follows:
  - Go to Add/Remove Programs and select Argus Safety Web.
  - Click Modify and then click Next.
  - 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 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.
- System performance satisfies the requirement

## Configuring Argus Safety Windows Service to run as a Domain User

Use the following procedure to configure the Argus Safety Windows Service:

- 1. Select Control Panel > Administrative Tools > Services
- 2. Double-click on Argus Safety Windows Service to open the Properties dialog box.
- **3.** When the system opens the Argus Safety Windows Service Properties (Local Computer) dialog box:
  - Click the Log On tab.
  - Click This Account.
  - Enter the proper credentials in the text field.
  - Click OK.
- 4. Right click on Argus Safety Windows Service and select Restart.

### **Configure Worklist Intake**

- 1. Run Argus Installer, and select the option Integrations. Complete the setup.
- **2.** 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.
- 3. Log in to Argus Console and open the Sites UI under Access Management menu.
- 4. Configure the UNC paths of the identified physical folders for the required Sites.
- **5.** On the server where Integrations component has been installed, navigate to the path where **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.xsl"/>

</InterfaceSchemas>

In the above tag, full Argus Install path should be mentioned. Typically, the Argus Install path is, C:\Program Files (x86)\Oracle\Argus\Argus Safety.

For example:

<InterfaceSchemas>

<add InputXSD="C:\Program Files (x86)\Oracle\Argus\Argus Safety\Integrations\XSD\v1.0\Base.xsd" />

<add InputXSD="C:\Program Files (x86)\Oracle\Argus\Argus Safety\Integrations\XSD\v1.0\DataOperation.xsd" />

<add InputXSD="C:\Program Files (x86)\Oracle\Argus\Argus Safety\Integrations\XSD\v1.0\Dictionary.xsd" />

<add InputXSD="C:\Program Files (x86)\Oracle\Argus\Argus Safety\Integrations\XSD\v1.0\Case\_Intake.xsd" OutputXSLT="C:\Program Files(x86)\Oracle\Argus\Argus Safety\Integrations\XSLT\v1.0\CaseIntake\_ Transform.xsl"/>

</InterfaceSchemas>

**6.** Open the following files:

### RelsysWindowsService.exe.config

- Uncomment the following entries under the <RelsysConfigFilesSection>/<RelsysConfigFiles>
  - Relsys.InterfaceComponents.ProcessorsConfiguration
  - Relsys.CaseIntake.FolderConfiguration
- **2.** Make sure that the <DatabaseConfiguration> section is configured. The configuration attributes for DatabaseConfiguration are as described below:
  - DBName: TNS of the Database to which the RelsysWindowsService should connect to. This is a mandatory attribute. 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"
  - DBPassword: Generate new encrypted string, as mentioned in the Generating Encrypted String from Clear Text on Configured User Cryptography Key section. Example: DBPassword="0314F7D9B94FF1F651069E4F36EE517D452537339935F9D7C2FA 04843FA5E486"
  - 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"
  - 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"

### 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.

### 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.

### **IIS Checklist**

Use this checklist to verify whether the IIS Web server is properly configured.

### Verify That:

- The properties in the IIS PDFReports virtual directory are correct.
- For Load Balanced Environments Only
  - The path under the Virtual Directory is set to Share Path.
  - The correct <Domain User> is in the Connect As option.
- The Read and Write options are checked.
- There is no Red X on the PDFReports Folder.

- You can right click PDFReports and select Browse.
- You can create a temp file and delete it after browsing.
- For PDFReports Enable Content Expiration in HTTP Headers is unchecked.
- For PDFReports the Custom HTTP Headers in HTTP Headers does not have a value of Cache-Control.
- The properties in the IIS UploadedLetters virtual directory are correct.
- For Load Balanced Environments Only:
  - The path under the virtual directory is set to Share Path
- The Read and Write options are checked.
- There is not a Red X on the UploadedLetters Folder.
- You can right click UploadedLetters and select Browse.
- You can create a temp file and delete it after browsing.
- For UploadedLetters Enable Content Expiration under HTTP Headers is unchecked.
- For UploadedLetters the Custom HTTP Headers under HTTP Headers does not have a value of Cache-Control.
- The values on the Directory Security tab under Argus Safety Website Properties are correct. Click Edit and verify that:
  - The correct <Domain User> and password are used for Anonymous Access.

**Note:** If you have IIS 7.0, you need to manually add Office 2007 MIME Types on the Web server. IIS 7.0 has these MIME types by default. Refer to the following Microsoft links for required steps:

Register the 2007 Office system file format MIME types on servers:

http://technet.microsoft.com/en-us/library/ee309278.aspx

Configure MIME Types on IIS 7.0:

http://go.microsoft.com/fwlink/?LinkId=158193

## .INI File Checklist

Use this checklist to verify that the .INI file parameters are properly configured.

#### Verify That:

- TempFileDeleteInterval=<Deletetime>
- HoursBeforeDelete= <Hoursbeforeprocess>

## Service Checklist

Use this checklist to verify that services are configured properly. Go to Control Panel > Administrator Tools > Services.

Verify that Argus Report Services is enabled.

# Verifying the Web Server Installation and IIS Configurations

Verifying the web server installation and IIS configurations consists of the following:

- Verifying IIS Configuration
- Configuring the Dossier Application

## Verifying IIS Configuration

Use the following procedure to verify the IIS 7 / 7.5 / 8.0 / 8.5 configuration:

- 1. Open Internet Information Services (IIS) manager from Control Panel > Administrator Tools.
- 2. Browse to the Argus Safety Web website.
- 3. Select the **PDFReports** Folder.
- 4. Double click the HTTP Response Headers option.
- 5. Make sure that there is no value Cache Control header.
- 6. Click the Set Common Headers option.
- 7. Make sure that **Expire Web Content** is unchecked.
- 8. Verify the same settings for the UploadedLetters folder.
- 9. Click Argus Safety Web.
- 10. Click Basic Settings under actions.
- **11.** Make sure that the website is configured to run under a domain account.

# **Configure and Verify the Dossier Installation**

This section provides information about configuring and verifying the Dossier installation.

## **Configuring the Dossier Application**

Use the following procedure to configure the Dossier application.

- 1. Run Argus Installer, and select the option **Dossier**. Complete the setup.
- 2. On the server where Dossier has been installed, open the file service.config under the installation folder. The installation folder, typically is, C:\Program Files\Oracle\ArgusWeb\ASP\Argus.NET\bin
- **3.** Uncomment the entries for **DossierBuilder** in the <ServiceConfiguration>/<ServiceComponents> section.
- 4. Open the file RelsysWindowsService.exe.config under the installation folder.
- **5.** Make sure that the <DatabaseConfiguration> section is configured. The configuration attributes for DatabaseConfiguration are as described below:
  - DBName: TNS of the Database to which the RelsysWindowsService should connect to. This is a mandatory attribute. 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"

- DBPassword: Generate new encrypted string, as mentioned in the Generating Encrypted String from Clear Text on Configured User Cryptography Key section. Example: DBPassword="0314F7D9B94FF1F651069E4F36EE517D452537339935F9D7C2FA 04843FA5E486"
- GeneralEmailTo: The email 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"
- GeneralEmailCc: This email address will be added to the Cc line when e-mails are sent by the Intake Service, using the General Email 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 Email feature of Argus. Example: GeneralEmailBcc ="recepient@oracle.net"

The below mentioned 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="DossierBuilder" Assembly="DossierServiceComponent" Type="DossierBuilder" Recurrence="600" Metadata="InvokeDirect=true" />

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

### Verifying the Dossier Installation

Use the following procedure to verify the Dossier installation:

- 1. Open Internet Explorer.
- **2.** Select Tools > Internet Options.
  - Select Internet Options from the Tools menu.
- 3. When the Internet Options dialog box opens:
  - Click the Advanced tab.
- 4. When the Advanced tab opens:
  - Locate the Multimedia section.
  - Verify that Enable automatic image resizing is cleared.
  - Verify that Show image download placeholders is cleared.
  - Verify that Show pictures is selected
  - Verify that Smart image dithering is cleared.
  - Click the Security tab.
- 5. When the Security tab opens, Click Custom level...
- **6.** When the Security Settings dialog box opens, Verify that Download signed ActiveX controls is enabled.
- **7.** Locate the ActiveX controls and plug-ins.

- Verify that ActiveX controls and plug-ins is enabled.
- Click OK.

**Note:** Make sure there is enough disk space in the drive where your temp files are stored. Check this drive by going to Start > Settings > Control Panel > System. Click the Advanced tab and then click the Environment Variables button. The drive and path are located under the variables for TMP and TEMP.

# Verify Files installed on Middle Tier Servers:

Use the following procedure to 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 the Programs and Features icon.
- **4.** When the Programs and Features window opens, select Argus Safety and click **Change/Remove**.
  - Select Argus Safety and click Change.
- 5. The wizard opens the Preparing Setup dialog box.
- 6. When the wizard opens the Welcome dialog box:
  - Click Modify and click Next
- 7. When the wizard opens:
  - Select Verify the current installation.
  - Click Next > to continue.
- 8. When the wizard opens the File Verification dialog box.
  - Click Next > to continue.

## Verifying the Documentum Installation

Use the following procedure to verify the Documentum installation.

- 1. Log in to Console and verify Documentum is configured in Argus Safety. Refer to the Administrator Guide on setting up Documentum.
- 2. Log in to SQL Session on the database <Database>.
- **3.** Run the following SQL query to verify that you have the value that enables the Periodic Report Documentum interface is set to 1.

select \* from cmn\_profile where key ='ENABLE\_DOCUMENTUM\_PERIODIC'

**4.** Run the following SQL query to verify that the correct user that has been configured in Documentum. This value case sensitive and must match the Documentum login.

select \* from cmn\_profile where key = 'DOCUMENTUM\_LOGIN'

**5.** Run the following SQL to verify that there is password value here that will be encrypted. Set this password again from the Case Form Configuration in Argus

C/S. Make sure the password matches the password for the user identified in Step 4. The password is case sensitive.

select \* from cmn\_profile where key = 'DOCUMENTUM\_PASSWORD'

6. Run the following SQL query to verify that the following information is correct:

**Note:** Rows will only exist if custom attributes are inserted as required by the customer.

select \* from DOCUMENTUM\_PUSH\_INFO

- Verify that the TYPE\_NAME (<DocumentumType>) is the correct name as specified in Documentum (This is the table name in Documentum)
- Verify that all the Attribute names specified here exist in the Documentum table.
- Verify that the SQL\_CONTENT SQLs are correct and run without any error when the parameters are filled in. (No Syntax errors)
- Verify that the ATTRIBUTE\_TYPE matches with the one defined in the Documentum table.
- 7. Log in to the AG Service machine <ServerName>
- **8.** Verify that the Documentum DFC Runtime Environment is installed on the server. This can be verified through Add/Remove Programs.
- **9.** Log in to the Argus Web Server <ServerName>.
- **10.** Verify that the Documentum DFC Runtime Environment is installed on the Server. This can be verified through Add/Remove Programs.
- **11.** Log in to the Interchange Service Server <ServerName>.
- **12.** Verify that Documentum DFC Runtime Environment is installed on the server. This can be verified through Add/Remove Programs.

#### Integrating Documentum Completely

- 1. Open Documentum.
- **2.** Create two Types in Documentum, one for attachments and one for reports.
- **3.** Make sure the Type names are the same as those in the TYPE\_NAME column in the DOCUMENTUM\_DISPLAY\_INFO table in Argus.
- **4.** Create case\_num and user\_fullname as Attributes for both Types.
- 5. Create submission\_succeed as Attribute in the Type being used for reports.
- **6.** Create all values in the ATTRIBUTE\_NAME column in DOCUMENTUM\_ DISPLAY\_INFO table in Argus as corresponding Attributes of the Types through Documentum Administrator.

**Note:** IUSR\_<Machine> Ac/c must be given full access to the shared folder in the DFC installation path where DFC.dll resides.

### Running Documentum on an Argus system

Documentum can be implemented on an Argus system in two ways:

Documentum can be successfully run on an Argus system if the entire environment comprises machines with fully qualified domain names for that environment.

If the actual domains are not present, you can still run Documentum even with minimal security configuration by implementing a workaround, as follows:

Go to the DFC.config file on the Web Server and change its *dfc.registry.mode* setting. Its default setting is: *dfc.registry.mode=windows* 

Change this setting to: *dfc.registry.mode=file* 

Changing this setting ensures that Documentum can run even with minimal security configuration.

# **Enabling IIS HTTP Compression**

This chapter describes how to enable IIS HTTP Compression on a Windows 2012 Server.

This feature is required when the pipeline between the Web Server and the IIS Client have low bandwidth or have high amounts of data usage.

This chapter includes discussions of the following:

- IIS Web Page Compression
- IIS Caching Settings
- Local Internet Explorer (IE) Client Caching Settings

# **IIS Web Page Compression**

This section includes the following sections:

- HTTP Compression
- Known Effects of Enabling Compression
- How to Enable HTTP Compression

# **HTTP Compression**

By default, HTTP compression is disabled in Windows 2012 but can be enabled as necessary. Reasons for enabling compression include the following:

- The bandwidth between the IIS Web Server and the IE Client(s) is of a low speed.
- The bandwidth between the IIS Web Server and the IE Client(s) is high speed but has high utilization.
- Reducing overall traffic between the IIS Web Server and the IE Client(s).

# Known Effects of Enabling Compression

Although implementing IIS Compression proves to be of value to the customer, there is a increase in CPU usage on the Web Server. When compression is enabled, every time a non static page (ASP, ASPX) is requested, the page is compressed on the fly before sending to the client. This puts some overhead on the Web Server CPU however, based on internal testing web server load is usually very minimum. Static Pages such as HTML, JS, HTM pages are compressed only once and then stored in a cache on the Web Server for later requests. Due to the above, the Web Servers should be monitored to prevent a CPU bottleneck from occurring which would decrease performance rather than increasing it.

# How to Enable HTTP Compression

Use the following procedure to enabled HTTP Compression in IIS:

- 1. Open Internet Information Services (IIS) manager from Control Panel > Administrator Tools.
- 2. Browse to the Argus Safety Web website.
- 3. Double click **Compression** in the Features View.
- 4. Check both options:
  - Enable dynamic content compression
  - Enable static content compression

**Note:** To enable compression, the feature option must be installed as part of the Windows installation.

# **IIS Caching Settings**

This section includes discussions on the following:

- IIS Caching
- Known Effects of Enabling Caching
- How to Enable Caching

## **IIS Caching**

IIS Caching is supported in Windows 2012. IIS Caching is required to prevent the web server from having to re-serve certain files to the IE Client when the file has not changed. In other words, files such as Images do not change on a day-to-day basis and once they are sent to the IE client they should not be sent again each time the client requests the file. The local IE client should keep a local cache copy of the file and use the local file instead.

Before IIS Caching will function properly:

- IIS must be set up properly
- The local IE client settings must be set up correctly

#### Known Effects of Enabling Caching

Currently, there are currently no known effects of enabling caching on the Web Server. However, enabling cache should only be used on files / folders where the files are not dynamic or do not change daily. Certain files, such as .ASP and .ASPX files, should never be cached.

# How to Enable Caching

Use the following procedure to enable / verify IIS caching (Default is turned on from Argus Installation):

- 1. Open "Internet Information Services (IIS) manager" from Control Panel > Administrator Tools.
- 2. Browse to the Argus Safety Web website.
- 3. Double click the HTTP Response Headers option.
- 4. Make sure that Cache Control header with value of no-cache exists.
- 5. Click the Set Common Headers option.
- **6.** Make sure that **Expire Web Content** is checked and the option **Immediately**" is selected.
- **7.** Apply and changes.
- 8. Click on the PDFReports Folder.
- 9. Double click the HTTP Response Headers option.
- **10.** Make sure that **Cache Control** header does not exist.
- 11. Click the Set Common Headers option.
- 12. Make sure that Expire Web Content is unchecked.
- 13. Repeat the same steps for UploadedLetters (Steps 9-12).
- **14.** For each of the following folders, the same settings exist (Steps 9-12). In addition, verify on the **Set Common Headers**, the **After** option is selected and configured for the specified number of days as seen next to each folder below:
  - Css 15 Days Expiration
  - Js 1 Day Expiration
  - Img 15 Days Expiration

# Local Internet Explorer (IE) Client Caching Settings

This section includes information about the following:

- IE Client Caching
- IE Client Caching Tab Options
- How to Enable IE Caching

# IE Client Caching

IE Caching works directly with IIS Caching. If IIS Caching is used, you must turn on IE Client Caching otherwise caching will not occur.

# IE Client Caching Tab Options

In IE Client, there are some options on the caching tab that you should be aware of. The following table lists and describes IE Caching Tab Options.

| Option                          | Description   |
|---------------------------------|---|
| Every Time I visit the Web Page | Selecting this option will not cache a single file. Every time a file is requested, IE will request the Server to re-send all files. This option should never be used as performance will suffer severely |

| Option                                  | Description  |
|---|--|
| Every Time I Start Internet<br>Explorer | Selecting this option will cache files only until the browser is closed.<br>Upon closing the IE window, all cache will be expired. This option will<br>provide some performance enhancement when a user visits the same<br>page multiple times within a single browser session   |
| Automatically                           | Selecting this option will allow IE to make a decision if a file should be<br>cached or not. This option automatically performs the same function as<br>"Every Time I Start Internet Explorer". In addition, after a file has been<br>request so many time, IE will automatically cache the file even after the<br>browser is closed. If the file has been cached and a new version of the file<br>exists on the Web Server, the new version will be downloaded to the<br>client. This is the option that should be used for best performance. |
| Never                                   | Selecting this option will cause IE to always cache every file which can<br>cause problem with sites that have dynamic data and so this should not<br>be used. Also, if a file has been updated on the server due to an upgrade,<br>the new file will not be sent to the client.   |

# How to Enable IE Caching

Use the following procedure to enable IE caching:

- **1.** Open Internet Explorer.
- **2.** Select **Tools > Internet Options**.
- 3. When the Internet Options dialog box opens:
  - Select the General Tab.
  - Locate the Browsing history section and click **Settings**.
- 4. When the Temporary Internet Files and History Settings dialog box opens:
  - Select Automatically.
  - Click OK.
- 5. Close the Internet Explorer browser and restart it to begin caching.

# **Configuring E-mail**

This section provides information about configuring e-mail and includes the following sections:

- About E-mail Configuration
- Configuring SMTP

# **About E-mail Configuration**

Argus Safety supports SMTP as an e-mail method.

Argus Safety Service and Interchange Service use SMTP as an e-mail method if it has been enabled and configured in Argus using Argus Console > System Configuration > SMTP Configuration. Case Letters are also sent using SMTP.

# **Configuring SMTP**

This section provides information about configuring SMTP and includes the following:

- Using the SMTP Configuration Utility
- Functions Affected by SMTP

# Using the SMTP Configuration Utility

Use the SMTP Configuration utility to send e-mails using the SMTP protocol from Argus Safety Service to the e-mail server. The following table lists and describes the fields in the SMTP Configuration dialog box.

| Field Name        | Description   |
|-------------------|---|
| Enable SMTP?      | Selecting this check box ensures that the AG Service uses SMTP to send e-mail messages. |
| Server IP or Name | This field contains the SMTP server IP address or name                                  |
| Port              | This field contains the port number. The default port number is 25.                     |

| Field Name                 | Description   |
|----------------------------|---|
| Authentication             | This field enables you to select the authentication type. There are three types of authentication:  |
|                            | No Authentication   |
|                            | In No Authentication, the Username and Password fields are disabled.  |
|                            | Basic Authentication  |
|                            | The user is required to enter the Username and Password fields. This is the default authentication.   |
|                            | NTLM Authentication   |
|                            | The authentication of the OS user logged into the system is automatically passed. The Username and Password fields are disabled in this authentication.   |
| SMTP Username              | This field contains the SMTP username.  |
| SMTP Password              | This field contains the SMTP password.  |
| Custom SMTP Header         | Selecting this check box will allow you to pass a custom header into the SMTP Header when sending e-mails. This is used if you have a SMTP Solution that is depending on specific header information for routing. |
| Custom SMTP Header Textbox | Enter the customer Header to insert into the SMTP Header.   |

Use the following procedure to configure SMTP:

- **1.** Navigate to Argus Safety Console > System Configuration > SMTP configuration.
- **2.** When the SMTP Configuration dialog opens:
  - Enter the SMTP server IP address or name.
  - Enter the port number
  - Enter the user name.
  - Enable SMTP.
  - Click OK.

# **Functions Affected by SMTP**

This section provides information about affected by the use of SMTP and includes discussions of the following:

- Bulk Report Transmit E-mail
- Autosignal E-mail
- Fax E-mail
- Fax Status E-mail
- Priority E-mail
- Dossier Notification E-mail
- E-mail Sent by Interchange Service

#### **Bulk Report Transmit E-mail**

- **1.** Navigate to Argus Console > Code Lists > Argus.
- 2. Select Reporting Destination.

**3.** Enter the e-mail address in the E-mail Address text box under Agency Information.

The Bulk Report Transmit e-mail is sent to this e-mail address.

#### **Autosignal E-mail**

- **1.** Navigate to Argus Console > Code Lists.
- 2. Select Autosignals.
- 3. Enter the e-mail address in the Send E-mail Notification To: text box.

The autosignal e-mail is sent to the specified e-mail address.

#### Fax E-mail

- On the system where Argus Safety Service is installed, select Start > All Programs > Oracle > Argus Safety Service Configuration.
- 2. The Argus Safety Service dialog box opens. Double-click the E-mail process.
- 3. You can enter an e-mail address for Failure E-mail or Notify E-mail.
- **4.** The Notify E-mail field or the Failure E-mail field in the Argus Safety Service Process window indicates the e-mail address of the person receiving the e-mail message.

## Fax Status E-mail

- On the system where Argus Safety Service is installed, select Start > All Programs > Oracle > Argus Safety Service Configuration.
- 2. The Argus Safety Service dialog box opens. Double-click the E-mail Status process.
- 3. You can enter an e-mail address for Failure E-mail or Notify E-mail.
- **4.** The Notify E-mail field or the Failure E-mail field in the Argus Safety Service Process window indicates the e-mail address of the person receiving the e-mail message.

## **Priority E-mail**

From Argus Console > Access Management > Argus > Groups. The E-mail field on the Group Information screen contains the e-mail address of the person receiving the e-mail message.

#### **Dossier Notification E-mail**

For Dossier notification, the E-mail Address on the Groups and Users screen field contains both the sender e-mail address and the receiver e-mail address. However, the sender e-mail address represents the normal AG user and the receiver e-mail address is the owner of the Dossier template. Configure the owner of the Dossier template in Argus Web > Reports > ICH PSUR Reports > Configuration Screen > Template tab.

## E-mail Sent by Interchange Service

- **1.** Log in to ESM Mapping.
- **2.** Select Administrator > Setup INI File.
- **3.** For the e-mail sent by Interchange Service, the IT E-mail, Business E-mail, and User E-mail fields in the Service INI File Setup window contains the e-mail addresses of those receiving the e-mail message.

Sender E-mail is the e-mail address that Argus Interchange Service displays as the 'From' address in the e-mails that it sends.

**Note:** Interchange Service sends e-mail messages to IT, Business, or User e-mail addresses depending on the type of alert/error/warning/information the system encounters.

\_

# Enabling and Configuring BI Publisher Periodic Reports

Argus BI Publisher Periodic Reports are the flexible periodic reporting feature that has been introduced in 8.0. By default, this feature is not enabled in the Safety environment.

This chapter lists the various steps to enable and configure the BI Publisher Periodic reports.

It includes the following sections:

- Preparing BI Publisher Server
- Database Configuration
- Setting up the BI Publisher for Argus Safety
- Managing Users and Roles in BI Publisher Security Model [BI Publisher Standalone]
- Managing Users and Roles in Oracle Fusion Middleware [BI Publisher Standalone]
- Managing Users and Roles for BI Publisher [OBIEE and BI Integrated Installation]
- Uploading the Argus Safety.xdrz file to BI Publisher
- Integrating Argus Safety with BI Publisher
- Argus Console-level Configurations
- Creating the Database Jobs
- Upgrading Flexible Aggregate Reports from 8.0 to 8.1

# 13.1 Preparing BI Publisher Server

A standalone BI Publisher Server or BI Publisher on a OBIEE Server needs to be prepared before enabling the BI Publisher Periodic reporting for Argus Safety.

Once 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

# **13.2 TNS Names Configuration**

During enabling, a database link would be created between the Argus Safety Database and the BI Publisher Metadata repository database.

In order to have this link created, copy the TNS Names of the BI Publisher metadata repository database's TNS Names into the TNS Names.ora file of Argus Safety database server.

# 13.3 Database Configuration

Some database configurations need to be handled in order to enable the BI Publisher reporting in Argus. These steps need to be handled from a machine where the Argus 8.0 database can be accessed (preferably the Argus Safety Web Server).

\* Open a command prompt and navigate to the directory where Argus\_BIP\_Enable.bat file is located.

\* Execute the batch file. The batch file would prompt for few database details. Enter the following information, as prompted:

- Enter TNSNAMES Entry to Connect to the Argus Safety Database: <The database SID of Argus Safety>.
- Enter SYSTEM or DBA user name in Argus Database: <the system or dba user name>.
- Enter password for &user\_dba. in Argus Database: <the system or dba user password>.
- Enter Argus schema owner name: <the argus safety schema owner, typically argus\_app>.
- Enter Argus schema password: cpassword for the argus safety schema owner>.
- Enter BI Publisher Schema which is created: <the BI Publisher Schema owner name created through the schema creation utility during Argus Safety db creation>.
- Enter Password for BIP user: cpassword of the BI Publisher Schema owner>.
- Enter BIP Repository Instance name: <database SID of the BI Publisher metadata repository database>.
- Enter BIP Repository User name (Default DEV\_BIPLATFORM): <the DEV\_ BIPLATFORM user created in BI Publisher metadata repository database>.
- Enter BIP Repository Password: (password for the DEV\_BIPLATFORM user>.

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

With this information, the batch file will execute and create the database objects that are needed for enabling and integrating the BI Publisher Periodic reports to Argus Safety.

A detailed log file called Argus\_BIP\_Enable\_Batchfile\_<datetime>.log will be created in the path of the batch file.

**Note:** The following message can be displayed while installing over the Oracle 12.1.0.2 Database:

Note: ZipUtil uses or overrides a deprecated API.

Note: Recompile with -Xlint:deprecation for details.

creating f\_UnzipBlob

This note about deprecation can be safety ignored.

# 13.4 Setting up the BI Publisher for Argus Safety

This section contains the following topics:

- Enabling a Local Superuser for BI Publisher Standalone Install
- Configuring the Security Model
- Creating ASBIP JDBC Connection
- Setting-up Runtime BI Publisher Memory

## 13.4.1 Enabling a Local Superuser for BI Publisher Standalone Install

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 box and enter the credentials for the Superuser, as shown.
- 4. Restart the BI Publisher service.

| ORACLE BI Publisher Enterprise  | Seech 🔐 🖉 🔤 🖉 🚺 Administration   Hoji -   Sign Cur. 🖸    |
|---|--|
| Advanturation   | Hame   Calaing   💽 New + 🛛 💆 Com + 🛛 Spred In As Johne + |
| Administration > Security Configuration   | 02   |
| Security Center   |  |
| Security Configuration Users Roles and Permissions Digital Signature            |  |
| *TBP Any changes will only take effect after the application is restarted.      | Apply Canod  |
| Local Supervase   |  |
| Lacd segment can be in the action independent from the selected security model. |  |
| Ganst Access  |  |
| FT Allow Guest Access Guest Folder Itarie                                       |  |

## 13.4.2 Configuring the Security Model

BI Publisher supports numerous security models. For Argus Safety 8.0, the following security models are supported:

- BI Publisher Security (default)
- Oracle Fusion Middleware

After setting up the security model, restart the BI Publisher server.

For more information about configuring BI Publisher over different security authentication and authorization models, refer to the BI Publisher Admin Guide.

**Note:** The following sections of the BI Publisher setup are based on the standalone BI Publisher installation with BI Publisher Security mode. For more details about configuring the BI Publisher Security Model or Oracle Fusion Middleware Security set up, refer to *Oracle Argus Safety Extensibility Guide*.

| RACLE BI Publisher Enterprise   | Seath Al  | <ul> <li>Administration   Hop.v   Spr.0.4</li> </ul> |
|---|---|--|
| ferministration   |   | Hana Catalog 🔄 New - 🔛 Open - Signed In As pla       |
| acial suberview can led to to the system independent from the selected security model.<br>P double Local Superviser<br>Superviser name<br>Parameter |   |  |
| Guest Access  |   |  |
| IT Allow Guest Access<br>Quest Folder Harm  |   |  |
| Authentication  |   |  |
| Single Sign Off URL<br>How to get username<br>User Name Parameter   | Over top spr Dr. 2  |  |
| User Locale Parameter   | NTIP Hade   |  |
| nter the value for URL, Administrator Usemanne, Administrator Password, Debriguehed Na<br>T Use LDAP  | the full laters and other required information below  |  |
| URL<br>Administrator Issemant<br>Administrator Passion<br>Detrogalited Name for Using   |   |  |
| 3HDL Cantest Perboy Clear<br>Attribute used for Login Username  | (Initial an Line down the Arean)<br>(Initial 1 (Initial and Antonia Arean)<br>(Initial Value of ) |  |
| Attribute used for user matching with authorization system  | Starrah angul )   |  |
| Authorization   |   |  |
| Security Model [III Publi   | Res Security  |  |
| New Password  | a value Administra Paramet  |  |

# 13.4.3 Creating ASBIP JDBC Connection

**Note:** All the users who have access to run the periodic reports using AS UI should be created in the BI Publisher local as well (applicable for BI Publisher Security model only). The password in BI Publisher local user corresponding to the AS UI need not to be same as that of AS UI.

To connect the BI Publisher and the database, execute the following steps:

- **1.** Log on to BI Publisher using the administrator credentials. This displays the BI Publisher Home Page.
- 2. Click Administration.
- 3. Click JDBC Connection under Data Sources.

| ORACLE BI Publisher Enterprise   |   | Search Al | 6          | O At   | inistration | Help- 1 | ign Car 🖸 |
|--|---|-----------|------------|--------|-------------|---------|-----------|
| Administration   |   |           | Pane Catal | a Brea | Digen -     | Specia  | A ploe-   |
| Data Searces  EXEC Consultor  FOR  FOR  Consultor  FOR  Consultor  FOR  Consultor  FOR  FOR  FOR  FOR  FOR  FOR  FOR  FO   | System Handrauser     elane Charlant Carlory ann     elane Charlant Carlory ann     elane Charlant Carlory ann     elanet New Configuration |           |            |        |             |         |           |
| Security Center  | Runtsmin CanApproxime<br>+ Functions<br>+ Canonyo Promisio<br>- Canonyo Promisio  |           |            |        |             |         |           |
| enderwry<br>* Odiwr y Carliganten<br>* Baran<br>* Baran<br>* Baran<br>* Baran<br>* Strawn<br>* Straw | biogradian<br>+ could thread the section<br>+ could thread  |           |            |        |             |         |           |

This displays the **Data Sources** screen.

4. Click Add Data Source.

| DRACLE BI Put         | blisher Enterprise       |        | Search 44 |                  | Administration rep - Sqn Out 📿 |
|-----------------------|--------------------------|--------|-----------|------------------|--------------------------------|
| Administration        |                          |        |           | Name Catalog She | Den - Signed bille place -     |
| Adversitiation > 208C |                          |        |           |                  | 3                              |
| Data Sources          |                          |        |           |                  |                                |
| 308C 38DE File LDA    | P OLAP Web Services HTTP |        |           |                  |                                |
| Add Data Source       |                          |        |           |                  |                                |
| Data Source Name      | Connection String        | Deleta |           |                  |                                |

- 5. In the Add Data Source section:
  - Enter **asbip** in the **Data Source Name** field.

Make sure that you enter this data source name in lowercase only.

Select the database from the Driver Type drop-down list.

This auto-populates the **Database Driver Class** field.

• Enter either of the following connection string 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=1521)))(CONN ECT\_DATA=(SID=orcl)))"

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

 Enter the username (Argus Safety BIP DB Schema user, for example, bip\_user, which got created during Argus Safety database installation) to connect to the database in the Username field.

#### Click Test Connection.

| DRACLE BI Publisher Enterprise                   |  | Search 👭 💌 🕐 Advantation Help - Sign Dut           |
|--|--|--|
| Administration                                   |  | Hume (Catalog) 🔮 Bern - 🔰 Open - Signed In As Jake |
| Administration > 320C > Update Data Source: addp |  |  |
| Update Clata Source: asbp                        |  |  |
|  |  | Apply Cancel                                       |
| General  |  |  |
| * Cannectan Ring                                 | Alle<br>Once 110<br>Reveal (2015 Chardhow)<br>Reveal with your Chardhow)<br>Reported the Reveal (2015 Section 2) |  |
| tilse System User                                |  |  |
| * Usercarte<br>Reseved                           |  |  |
| Personal<br>Pre Process Function                 | ,  |  |
| Fost Process Function                            |  |  |
|  | T Use Procy Authentication<br>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.

| demandrature .                       |   |        | mee Calific | Ster- Ditte | er- Spelltie plac- |
|--------------------------------------|---|--------|-------------|-------------|--------------------|
| dorabalar. > 28C                     |   |        |             |             | (                  |
| Deta Seurcas                         |   |        |             |             |                    |
| 300C 30CE FBe LDA                    | P OLAP Web Services HITP                                |        |             |             |                    |
| Add Data Source                      |   |        |             |             |                    |
|                                      | Connection String                                       | Delete |             |             |                    |
| Data Source Name                     |   |        |             |             |                    |
| Data Source Name                     | phone through the period streets                        | 0      |             |             |                    |
| Data Source Ranse<br>Artici<br>dette | phonecting are can 1521 areas<br>phonecting 00579047520 | 0      |             |             |                    |

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

# 13.4.4 Setting-up Runtime BI Publisher Memory

- 1. Login to BI Publisher.
- 2. Click Administration.
- **3.** From Runtime Configuration section, click **Properties**.
- 4. Modify the following parameter values to **1800** seconds from 600 seconds:
  - Memory Guard > Process timeout for online report formatting
  - Data Model > SQL Query Timeout

#### Administration

| All Outputs   |          |                          |
|---|----------|--------------------------|
| Hide version number in output   |          | False                    |
| Use 11.1.1.5 compatibility mode   |          | False                    |
| Memory Guard  |          |                          |
| Maximum report data size for online reports                                 |          | 300MB                    |
| Maximum report data size for offline<br>(scheduled) reports                 |          | 500MB                    |
| Free memory threshold   |          | 500MB                    |
| Maximum report data size under the free<br>memory threshold                 |          | free_memory_threshold/10 |
| Minimum time span between garbage<br>collection runs                        |          | 300 (seconds)            |
| Maximum wait time for free memory to come<br>back above the threshold value |          | 30 (seconds)             |
| Process timeout for online report formatting                                | 1800     | 600 (seconds)            |
| Data Model  |          |                          |
| Maximum data size limit for data generation                                 |          | 500MB                    |
| Maximum sample data size limit  |          | 1MB                      |
| Enable Data Model scalable mode   | •        | True                     |
| Enable Auto DB fetch size mode  | T        | True                     |
| DB fetch size   |          | 20                       |
| SQL Query Timeout   | 1800     | 600 (seconds)            |
| Enable Data Model diagnostic  | •        | False                    |
| Enable SQL session trace  | ¥        | False                    |
| Enable SQL Pruning  | <b>T</b> | False                    |

#### 5. Click on Apply.

These changes ensures the out-of-the-box BI Publisher reports to execute successfully.

These values can be increased as needed, for any BIP custom reports that takes longer time-period.

# 13.5 Managing Users and Roles in BI Publisher Security Model [BI Publisher Standalone]

This section contains the following:

- Section 13.5.1, "Creating Users and Assigning Roles"
- Section 13.5.2, "Creating Custom Roles"

# 13.5.1 Creating Users and Assigning Roles

To create users and assign them roles:

1. Log in to BI Publisher with the administrator credentials.

The BI Publisher Home Page appears.

2. Click Administration.

The Administration screen appears.

| ORACLE BI Publisher Enterprise   | Search All 🛛 🔽 🚺 Administration 🛛 Help 🗸 🖉 Sign Out 📿  |
|--|--|
| Administration   | Home   Catalog   🦉 New 🗸   📂 Open 🗸   Signed In As 🛛 <b>jdoe</b> 🗸                             |
| Data Sources  DBC Connection DIADI Connection DIADI Connection Elle DDAP Connection ULAP Connection Web Service Connection HTTP Connection | System Maintenance  Server Configuration  Scheduler Configuration  Report Viewer Configuration |
| Security Center<br>• Security Configuration<br>• Users<br>• Roles and Permissions<br>• Digital Signature                                   | Runtime Configuration  • Properties • Font Mappings • Currency Formats                         |
| Delivery<br>• Delivery Configuration<br>• Printer<br>• Fax<br>• Email<br>• WebDAV<br>• HTTP<br>• FTP<br>• CUPS Server                      | Integration  • Oracle EI Presentation Services • Oracle Endeca                                 |

3. Under Security Center, click Users.

The Users screen appears.

4. Click Create Users.

The Create User screen appears.

| dministration                 |          |                       |                              |                                      |
|-------------------------------|----------|-----------------------|------------------------------|--------------------------------------|
| dministration > Users         |          |                       |                              |                                      |
| Security Center               |          |                       |                              |                                      |
| Security Configuration        | Users    | Roles and Permissions | Digital Signature            |                                      |
| Number of rows displayed      | per page |                       |                              |                                      |
| Username Create User          | per page | 10 Search             | ③ Previous 1-                | -10 of 11 💌 <u>Next 1</u> @          |
| Username                      | per page | Search                | S Previous 1-<br>ssign Roles | 10 of 11 💌 <u>Next 1</u> (<br>Delete |
| Username Create User          | per page | Search                |                              |                                      |
| Username Create User Username | per page | Search                | Assign Roles                 | Delete                               |

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.

| Iministration                 |          |                       |                               |                                  |
|-------------------------------|----------|-----------------------|-------------------------------|----------------------------------|
| ministration > Users          |          |                       |                               |                                  |
| Security Center               |          |                       |                               |                                  |
| Security Configuration        | Users    | Roles and Permissions | Digital Signature             |                                  |
| Number of rows displayed      | per page | ·                     |                               |                                  |
| Username Create User          | per page | 10 Search             | ③ Previous 1-:                | 10 of 11 💌 <u>Next 1</u>         |
| Username                      | per page | Search                | ③ Previous 1-:<br>ssign Roles | 10 of 11 <u>Next 1</u><br>Delete |
| Username Create User          | per page | Search                |                               |                                  |
| Username Create User Username | per page | Search                | ssign Roles                   | Delete                           |

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.

| Administration > Users > Assign Roles: jdoe |  |
|---|--|
|   |  |
| Assign Roles: jdoe                          |  |
|   | Apply Cancel   |
| Available Roles                             | Assigned Roles   |
| ASAdmin<br>BTAdmin                          | BI Publisher Administrator<br>Move<br>Move All<br>S<br>Remove<br>S |

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.

# 13.5.2 Creating Custom Roles

This section describes the steps to create custom roles and assign data sources to them.

**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.

| ORACLE BI Publisher Enterprise  | Search 📶 🚽 🚽 🚱 Administration   Help 🗸   Sign Out 📿   |
|---|---|
| Administration  | Home   Catalog   📑 New 🗸   🐚 Open 🗸   Signed In As jdoe 🗸                                     |
| Data Sources  Disc Connection  Divid Connection  File  DLAP Connection  OLAP Connection  OLAP Service Connection  Web Service Connection  HTTP Connection | System Maintenance   Server Configuration  Scheduler Diagnostics  Report Viewer Configuration |
| Security Center<br>• Security Configuration<br>• Users<br>• Roles and Permissions<br>• Digital Signature  | Runtime Configuration     Properties     Font Mappings     Currency Formats                   |
| Delivery<br>Delivery Configuration<br>Printer<br>Fax<br>Email<br>WebDAV<br>HTTP<br>FTP<br>CUPS Server   | Integration  Oracle BI Presentation Services  Oracle Endeca                                   |

The Roles and Permissions screen appears.

4. Click Create Role.

| Administration                    |                             |                                       |                  |           |        |
|-----------------------------------|-----------------------------|---------------------------------------|------------------|-----------|--------|
| Administration > Roles and Permis | ssions                      |                                       |                  |           |        |
| Security Center                   |                             |                                       |                  |           |        |
| Security Configuration            | Users Roles and Permissions | Digital Signature                     |                  |           |        |
| Number of rows displayed p        | ner nage 10                 |                                       |                  |           |        |
| Role Name                         | Search                      |                                       |                  |           |        |
| Create Role                       | ocuren                      |                                       |                  |           |        |
| Role Name                         | Description                 |                                       | Add Data Sources | Add Roles | Delete |
| ASAdmin                           | Contraction of Contraction  | Develop, Scheduling and Report writer | 8                | E.e.      | Û      |

The Create Role screen appears.

5. Enter a role Name and Description, and click Apply.

A new custom role is created.

| Iministration                |   |                  |           |        |
|------------------------------|---|------------------|-----------|--------|
| ministration > Roles and Per | nissions                                      |                  |           |        |
| ecurity Center               |   |                  |           |        |
| Security Configuration       | Users Roles and Permissions Digital Signature |                  |           |        |
| Number of rows displaye      | per page 10 💌                                 |                  |           |        |
|                              | per page 10 Search                            |                  |           |        |
| Role Name                    | · · · · · · · · · · · · · · · · · · ·         | Add Data Sources | Add Roles | Delete |
|                              | Search  | Add Data Sources | Add Roles | Delete |

- 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 👯 .

The Add Roles screen appears.

**10.** From the Available Roles, select the roles to be included, and click **Move (>)** to add the selected roles to Included Roles.

| Administration  |                            |          |              |
|---|----------------------------|----------|--------------|
| Administration > Roles and Permissions > Add Roles:         | BIAdmin                    |          |              |
| Add Roles: BlAdmin  |                            |          |              |
|   |                            | 1        | Apply Cancel |
| Available Roles   | Included Roles             |          |              |
| -   | BI Publisher Administrator | 3        |              |
| BI Publisher Excel Analyzer<br>BI Publisher Online Analyzer | Move                       | <u> </u> |              |
| BI Publisher Developer<br>BI Publisher Scheduler            | ⊗                          | <b>I</b> |              |
| BI Publisher Template Designer                              | Move All                   | × ×      |              |
| ASAdmin   | 3                          |          |              |
| ·   | Remove                     |          |              |
|   |                            |          |              |

11. Click Apply.

# 13.6 Managing Users and Roles in Oracle Fusion Middleware [BI Publisher Standalone]

This section describes the steps to create roles, policies, users, and groups in Oracle Fusion Middleware (OFM) security in BI Publisher Standalone installation.

# 13.6.1 Creating Users and Assigning Groups

**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.* 

#### To create new groups for FAR periodic:

- 1. Login to Fusion Middleware Console.
- **2.** Navigate to WebLogic Domain > Security > Users and Groups > Groups.

| Change Center   | 🔞 Home Log Out Preferences 🚹   |  |   |  |  |  |
|---|--|--|---|--|--|--|
| View changes and restarts   | Home >Summary of Security Realms   | >myrealm >Users and Groups             |   |  |  |  |
| Click the Lock & Edit button to modify, add<br>or delete items in this domain.  | Source Provide Action Cancelled.   |  |   |  |  |  |
| Lock & Edit   | Settings for myrealm   |  |   |  |  |  |
| Release Configuration   | Configuration Users and Group  | Roles and Policies Credential Mappings | Providers Migration   |  |  |  |
| omain Structure   | Users Groups   |  |   |  |  |  |
| - Domain Partitions<br>- Environment<br>- Deployments<br>- Services<br>- Security Realms<br>- Interoperability<br>- Diagnostics | This page displays information about each group that has been configured in this security realm.  Customize this table  Groups  New Delete |  |   |  |  |  |
|   | 🔽 Name 🗇   | Description                            |   |  |  |  |
|   | AdminChannelUsers  | AdminChannelUsers can                  | access the admin channel.   |  |  |  |
|   | Administrators   | Administrators can view                | Administrators can view and modify all resource attributes and start and stop servers.              |  |  |  |
| w do I  | AppTesters   | AppTesters group.                      | AppTesters group.   |  |  |  |
| Manage users and groups   | CrossDomainConnectors  | CrossDomainConnectors                  | CrossDomainConnectors can make inter-domain calls from foreign domains.                             |  |  |  |
| Create groups<br>Modify groups  | Deployers  | Deployers can view all re              | Deployers can view all resource attributes and deploy applications.                                 |  |  |  |
| Delete groups   | Monitors   | Monitors can view and n                | Monitors can view and modify all resource attributes and perform operations not restricted by roles |  |  |  |
| 11  | Operators  | Operators can view and                 | modify all resource attributes and perform server lifecycle operations.                             |  |  |  |
| stem Status 🗉   | OracleSystemGroup  | Oracle application softwa              | are system group.   |  |  |  |
| ealth of Running Servers  | New Delete   |  | Oracle application software system group.   |  |  |  |
|   | New Delete   |  |   |  |  |  |

3. From the Groups section, click New.

The Create a New Group dialog box appears.

- 4. Create the following groups by entering the Name and Description:
  - FARAdminGroup
  - FARSafetyAuthorGroup
  - FARSafetyConsumerGroup

| OK Cancel                              |  |   |
|--|--|---|
| Group Properties                       |  |   |
| The following properties w             | rill be used to identify your new Group, |   |
| <sup>1</sup> Indicates required fields |  |   |
| What would you like to nar             | me your new Group?                       |   |
| * Name:                                |  |   |
|  | FARAdminGroup                            |   |
| How would you like to des              | cribe the new Group?                     |   |
| Description:                           | FAR Admin Group                          | - |
| Please choose a provider fo            |  |   |
| Please choose a provider to            | and group.                               |   |
| Provider:                              | DefaultAuthenticator                     |   |

#### To create new users in Fusion Middleware Console:

- **1.** Login to Fusion Middleware Console.
- 2. Navigate to WebLogic Domain > Security > Users and Groups > Users.

| Setting | s for my  | realm            |                    |                            |               |                    |                               |
|---------|-----------|------------------|--------------------|----------------------------|---------------|--------------------|-------------------------------|
| Confi   | guration  | Users and Groups | Roles and Policies | Credential Mappings        | Providers     | Migration          |                               |
| User    | s Group   | ps               |                    |                            |               |                    |                               |
| Cus     | tomize th | <i>.</i>         |                    | een configured in this se  | curity realm. |                    |                               |
| Ne      | w De      | elete            |                    |                            |               |                    |                               |
|         | Name 4    | •                | Descriptio         | in                         |               |                    |                               |
|         | LCMUser   | r                | This is the c      | lefault service account fo | or WebLogic   | Server Lifecycle I | Manager configuration updates |
|         | OracleSy  | ystemUser        | Oracle appl        | lication software system   | user.         |                    |                               |
|         | weblogic  | 1                | This user is       | the default administrator  | r.            |                    |                               |

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

The Create a New User screen appears.

| Create a New User                                |  |
|--|--|
| OK Cancel  |  |
| User Properties                                  |  |
| The following properties will be used to identif | y your new User.                         |
| * Indicates required fields                      |  |
| What would you like to name your new User?       |  |
| *Name:   | FARAdminUser                             |
| How would you like to describe the new User?     | anna an an ann an an an ann an ann an an |
| Description:                                     | FAR Administrator User                   |
| Please choose a provider for the user.           |  |
| Provider:  | DefaultAuthenticator                     |
| The password is associated with the login name   | for the new User.                        |
| * Password:                                      | •••••                                    |
| * Confirm Password:                              | •••••                                    |
| OK Cancel  |  |

- **4.** Enter the following fields, and click **OK**.
  - a. Name
  - **b.** Description
  - **c.** Provider
  - d. Password
  - e. Confirm Password
- **5.** Assign role to the user, and click **Save**.

| congs re            | or FARAdmin                | User         |             |                  |
|---------------------|----------------------------|--------------|-------------|------------------|
| General             | Passwords                  | Attributes   | Groups      |                  |
| Save                |                            |              |             |                  |
| Use this            | page to config             | gure group n | embership   | o for this user. |
| Parent G<br>Availab |                            |              |             | hosen:           |
|                     | minChannelU                | sers 🔺       |             | FARAdminGroup    |
| Ad                  | ministrators               |              | >           |                  |
| 1.11.2              | pTesters                   |              | <b>SS</b> : |                  |
| and a second        | ossDomainCo                | nnectors     | 0           |                  |
|                     | ployers                    |              |             |                  |
| I FA                | RSafetyAuth<br>RSafetyCons | 100          | <b>3</b>    |                  |
| E CAL               |                            | umeraro 🔻    |             |                  |

# 13.6.2 Creating Roles and Policies

#### To create new application roles:

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

The Application Roles dialog box appears.

| Ξ                                | bipofm O<br>🚘 WebLogic Domain 💌   |   |   |               |       |
|----------------------------------|---|---|---|---------------|-------|
| Domain_                          | Home  |   |   |               |       |
| Applicati<br>P To mar<br>P Polis | Montoring<br>Disgnostics<br>Control<br>Logs   |   | tions that are specific to t<br>the <u>Oracle WebLook Ser</u> |               |       |
| select ar                        | Environment   |   | name to search for roles                                      | defined by th | s app |
| View                             | Deployments<br>JDBC Data Sources<br>Messaging<br>Cross Component Wiring<br>Web Services |   | Edit X Delete   |               | •     |
| Rol                              | Other Services  | - | e   | Descript      | ion   |
| DISK                             | Administration<br>Refresh WebLogic Domain   |   | ministrator   | This role of  | confe |
| - Me                             | Security  | * | Security Realms   |               | Т     |
| Princip                          | System MBean Browser  |   | Users and Groups  |               |       |
| weblogi                          | WebLogic Server Administration Console  |   | Credentials   |               |       |
|                                  | Target Stemap   |   | Security Provider Co  | nfiguration   |       |
|                                  | Target Information  |   | Application Policies  |               |       |
|                                  |   |   | Application Roles   |               |       |
|                                  |   |   | Keystore  |               |       |
|                                  |   |   | System Policies   |               |       |
|                                  |   |   | Audit Policy  |               |       |

**3.** From the **Application Stripe** drop-down list, select **OBI**, and click **Search**. The default Role available in clean slate installation appears.

| t= WebLogi            | c Domain 👻                                |                                      |  |
|-----------------------|---|--------------------------------------|--|
| /Domain_bipofm/bipofn | n > Application Roles                     |                                      |  |
|                       | ne roles used by secur                    | ity aware applications that are spec | cific to the application. These roles are seeded by applications in single global policy stor<br>aic Server Security Provider. |
| Policy Store Pro      | vider                                     | -                                    |  |
|                       | 1401                                      |                                      |  |
| A Search              |   |                                      | r roles defined by this application. Use the application stripe to search if the application u                                 |
| View 🔹 🎽 Cr           | Application St<br>Role Na<br>eate E Creat | me Starts With                       | ste  |
| 1                     |   |                                      |  |
| Z Dele Name           |   | Diaplay Nama                         | Departmention  |
| Role Name             | trator                                    | Display Name                         | Description  |
| BIServiceAdminis      |   | BI Service Administrator             | Description This role confers privileges required to administer a service instance.  |
| BIServiceAdminis      | for BIServiceA                            | BI Service Administrator             |  |

#### 4. Click Create.

The Create Application Role dialog box appears.

5. In the Role Name field, enter FARAdminRole.

#### Create Application Role

| Role (or Enterprise Role) is the gr          | oup of users designed at the enterprise level and typically used to as | assign a privilege or permission. A role can also contain other roles as members |
|--|--|--|
| General                                      |  |  |
| Application Stripe                           | obi  |  |
| * Role Name                                  | FARAdminRole   |  |
| Display Name                                 | FAR Administrator Role   | Description  |
| Description                                  | FAR BIP Administrator Role   |  |
| Members<br>An application role may need to b | e mapped to users or groups defined in enterprise LDAP server, or th   |  |
| View 👻 🕂 Add 🔀 🛛                             | elete 📑 Detach   |  |
| Name   |  |  |
| No groups or application roles ad            | dded.  |  |

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

The Add Principal dialog box appears.

- From the Type drop-down list, select Group, and click Search.A list of principals appears.
- 8. From the list of Searched Principlals, select FARAdminGroup, and click OK.

| Principal         Display Name         Description           Admin.ChannelUsers         Admin.ChannelUsers can access the admin channel.           AdminolanneuUsers         Admini.ChannelUsers can access the admin channel.           AdminolanneuUsers         Administrators can view and modify all resource attributes and start and stop servers.           AppTesters         AppTesters group.           CossDomainConnectors         CossDomainConnectors can make inter-domain calls from foreign domains.           Deployers         Deployers can view all resource attributes and deploy applications.           FARAdminGroup         FARAdmin Group           FARSafetyAuthorGroup         FAR Safety Author Group           FARSafetyConsumerGroup         FAR Safety Consumer Group           Montors         Genetaris can view and modify all resource attributes and perform operations not restricted by roles.           Operators         Operators can view and modify all resource attributes and perform operations. | cify criteria to search and se<br>Search | lect the application roles that y | ou want to grant permissions to.            |   |  |
|---|--|-----------------------------------|---|---|--|
| Display Name         Display Name           Principal         Display Name         Starts Wth         Image: Construct Name           Principal         Display Name         Description           AdminichannelUsers         AdminichannelUsers can access the admin channel.           Administrators         Administrators can view and modify all resource attributes and start and stop servers.           AppTesters         GeoscomainConnectors         CrossDomainConnectors can make inter-domain calls from foreign domains.           Deployers         Deployers can view all resource attributes and deploy applications.           FARAdminGroup         FAR Safety Author Group           FARSafetyAuthorGroup         FAR Safety Consumer Group           Nontors         Geoscomain Conup           Montors         Geoscomain Conup   |  | Туре                              | Group 👻                                     |   |  |
| Principals           Principal         Display Name         Description           AdminChannelUsers         AdminChannelUsers can access the admin channel.           AdminStrators         Geschiption           AdminStrators         AdminStrators can view and modify all resource attributes and start and stop servers.           ApTesters         CrossDomainConnectors           Deployers         Deployers can view all resource attributes and deploy applications.           FRAdminGroup         FRA damin Group           FARSafetyAuthorGroup         FAR Safety Author Group           FARSafetyConsumerGroup         FAR Safety Consumer Group           Nontors         Geperators an view and modify all resource attributes and perform operations not restricted by roles.  |  | Principal Name                    | Starts With                                 |   |  |
| Price         Display Name         Description           AdminChanneUsers         AdminChanneUsers can access the admin channel.           AdminiStrators         AdminiStrators can view and modify all resource attributes and start and stop servers.           AppTesters         CossDomanConnectors           Deployers         ExaAdmin Group           FARAdminGroup         FAR Admin Group           FARSafetyAuthorGroup         FAR Safety Author Group           FARSafetyConsumerGroup         FAR Safety Consumer Group           Fontors         Goperators can view and modify all resource attributes and perform operations not restricted by roles.           Poprestors         Goperators can view and modify all resource attributes and perform operations.   |  | Display Name                      | Starts With                                 | •   |  |
| Principal         Display Name         Description           Adminichtannet/Jsers         Adminichtannet/Jsers can access the admin channet.           Administrators         Administrators can view and modify all resource attributes and start and stop servers.           AppTesters         GestomainConnectors           Deployers         GestomainConnectors can make inter-domain calls from foreign domains.           Deployers         Beployers can view all resource attributes and deploy applications.           FARAdminGroup         FAR Admin Group           FARSafety/AuthorGroup         FAR Safety Consumer Group           FARSafetyConsumerGroup         FAR Safety Consumer Group           Fontors         Goperators can view and modify all resource attributes and perform operations not restricted by roles.           Operators         Operators can view and modify all resource attributes and perform operations.   | rched Principals                         | 6.0                               | _   |   |  |
| AdminchannelUsers     AdminchannelUsers can access the admin channel.       Adminsharators     Administrators can view and modify all resource attributes and start and stop servers.       AppTesters     AppTesters group.       CrossDomainConnectors     CrossDomainConnectors can make inter-domain calls from foreign domains.       Deployers     Deployers can view all resource attributes and deploy applications.       FARAdminGroup     FAR Admin Group       FARSafetyAuthorGroup     FAR Safety Author Group       FARSafetyConsumerGroup     FAR Safety Consumer Group       Montors     Montors can view and modify all resource attributes and perform operations not restricted by roles.       Operators     Operators can view and modify all resource attributes and perform server lifecycle operations.   | ew 👻 🔤 Detach                            |                                   |   |   |  |
| Administrators     Administrators can view and modify all resource attributes and start and stop servers.       Administrators     AppTesters group.       CrossDomainConnectors     CrossDomainConnectors can make inter-domain calls from foreign domains.       Deployers     Deployers can view all resource attributes and deploy applications.       FARAdminGroup     FAR Admin Group       FARSafetyAuthorGroup     FAR Safety Author Group       FARSafetyConsumerGroup     FAR Safety Consumer Group       Montors     Montors can view and modify all resource attributes and perform operations not restricted by roles.       Operators     Operators can view and modify all resource attributes and perform server lifecycle operations.   | Principal                                | Display Name                      | Description                                 |   |  |
| AppTesters     AppTesters group.       CrossDomainConnectors     CrossDomainConnectors can make inter-domain calls from foreign domains.       Deployers     Deployers can view all resource attributes and deploy applications.       FARAdminGroup     FAR Admin Group       FARSafety/AuthorGroup     FAR Safety Author Group       FARSafety Consumer Group     FAR Safety Consumer Group       Monitors     Monitors can view and modify all resource attributes and perform operations not restricted by roles.       Operators     Operators can view and modify all resource attributes and perform server ilfecycle operations.  | AdminChannelUsers                        |                                   | AdminChannelUsers can access the a          | dmin channel.   |  |
| CrossDomainConnectors     CrossDomainConnectors can make inter-domain calls from foreign domains.       Deployers     Deployers can view all resource attributes and deploy applications.       FARAdminGroup     FAR Admin Group       FARSafety/AuthorGroup     FAR Safety Author Group       FARSafetyConsumerGroup     FAR Safety Consumer Group       Monitors     Monitors can view and modify all resource attributes and perform operations not restricted by roles.       Operators     Operators can view and modify all resource attributes and perform server ilfecycle operations.   | Administrators                           |                                   | Administrators can view and modify all      | resource attributes and start and stop servers.                 |  |
| Deployers         Deployers can view all resource attributes and deploy applications.           FARAdminGroup         FAR Admin Group           FARSafetyAuthorGroup         FAR Safety Author Group           FARSafetyConsumerGroup         FAR Safety Consumer Group           Montors         Montors can view and modify all resource attributes and perform operations not restricted by roles.           Operators         Operators can view and modify all resource attributes and perform server lifecycle operations.  | AppTesters                               |                                   | AppTesters group.                           |   |  |
| FAR Admin Group         FAR Admin Group           FARSa fety Author Group         FAR Safety Author Group           FARSa fety Consumer Group         FAR Safety Consumer Group           Montors         Montors can view and modify all resource attributes and perform operations not restricted by roles.           Operators         Operators can view and modify all resource attributes and perform server lifecycle operations.  | CrossDomainConnectors                    |                                   | CrossDomainConnectors can make inte         | er-domain calls from foreign domains.                           |  |
| FARSafetyAuthorGroup         FARSafetyAuthorGroup           FARSafetyConsumerGroup         FARSafetyConsumer Group           Monitors         Monitors can view and modify all resource attributes and perform operations not restricted by roles.           Operators         Operators can view and modify all resource attributes and perform server lifecycle operations.   | Deployers                                |                                   | Deployers can view all resource attribution | utes and deploy applications.                                   |  |
| FARSafetyConsumerGroup     FAR Safety Consumer Group       Monitors     Monitors can view and modify all resource attributes and perform operations not restricted by roles.       Operators     Operators can view and modify all resource attributes and perform server lifecycle operations.   | FARAdminGroup                            |                                   | FAR Admin Group                             |   |  |
| Monitors         Monitors can view and modify all resource attributes and perform operations not restricted by roles.           Operators         Operators can view and modify all resource attributes and perform server lifecycle operations.  | FARSafetyAuthorGroup                     |                                   | FAR Safety Author Group                     |   |  |
| Operators Operators can view and modify all resource attributes and perform server lifecycle operations.  | FARSafetyConsumerGroup                   |                                   | FAR Safety Consumer Group                   |   |  |
|   | Monitors                                 |                                   | Monitors can view and modify all resou      | arce attributes and perform operations not restricted by roles. |  |
|   | Operators                                |                                   | Operators can view and modify all res       | ource attributes and perform server lifecycle operations.       |  |
| Uracle system group. Uracle application software system group.  | OracleSystemGroup                        |                                   | Oracle application software system gr       | oup.  |  |
|   | Advanced Option                          |                                   |   |   |  |
| Advanced Option   |  |                                   | rom above. This option can be used for a    |   |  |

**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.

| Search                |                |                  | you want to grant permissions to.                                       |
|-----------------------|----------------|------------------|---|
|                       | Туре           | Application Role | le 💌  |
|                       | Principal Name | Starts With      |   |
|                       | Display Name   | Starts With 💌    | •   |
| arched Principals     |                |                  |   |
| iew 🔻 🗐 Detach        |                |                  |   |
| Principal             | Display Na     | ame              | Description   |
| anonymous-role        | Anonymou       | s Role           |   |
| authenticated-role    | Authentical    | ed Role          |   |
| BIServiceAdministrato | BI Service     | Administrator    | This role confers privileges required to administer a service instance. |
|                       | FAR Admin      | istrator Role    | FAR BIP Administrator Role  |

The Membership for FARAdminRole appears as below:

| Role Name                                    | Display                      | Name             | Description  |
|--|------------------------------|------------------|--|
| BIServiceAdministrato                        | BI Servio                    | e Administrator  | This role confers privileges required to administer a service instance |
| FARAdminRole                                 | FAR Adr                      | ninistrator Role | FAR BIP Administrator Role   |
|  |                              |                  |  |
| ▲ Membership for                             |                              | -                |  |
|  | FARAdminRole<br>Display Name | Туре             | Description  |
| Membership for<br>Principal<br>FARAdminGroup |                              | Type<br>Group    | Description<br>FAR Admin Group   |

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

| Role Name                           | Display Na                           | ame              | Description  |  |
|-------------------------------------|--------------------------------------|------------------|--|--|
| BIServiceAdministrator BI Service A |                                      | Administrator    | This role confers privileges required to administer a service instance |  |
| FARAdminRole FAR Adminis            |                                      | strator Role     | FAR BIP Administrator Role   |  |
| FARSafetyAuthorRole                 | FAR BIP Sa                           | fety Author Role | FAR BIP Safety Author Role   |  |
|                                     |                                      |                  |  |  |
| Membership for                      | FARSafetyAuthorRole                  |                  |  |  |
| ✓ Membership for<br>Principal       | FAR SafetyAuthorRole<br>Display Name | Туре             | Description  |  |
|                                     | 1                                    |                  |  |  |

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

|                          | ew 🔻 🎽 Create       | E Create Like                      | 🖋 Edit 🗙 Delete         | han l  |  |
|--------------------------|---------------------|------------------------------------|-------------------------|--|--|
| 1                        |                     |                                    |                         |  |  |
|                          | Role Name           | Display                            | Name -                  | Description  |  |
| BIServiceAdministrator   |                     | BI Service                         | Administrator           | This role confers privileges required to administer a service instance |  |
|                          | FARAdminRole        | FAR Adm                            | nistrator Role          | FAR BIP Administrator Role   |  |
|                          | FARSafetyAuthorRole | FAR BIP S                          | afety Author Role       | FAR BIP Safety Author Role   |  |
| FARSafetyConsumerRole FA |                     | e FAR Safe                         | ty Consumer Role        | FAR BIP Safety Consumer Role   |  |
|                          |                     |                                    |                         |  |  |
|                          |                     | ARSafetyConsumer                   |                         | Description  |  |
| Pri                      | Membership for F    | ARSafetyConsume                    | Role<br>Type            |  |  |
| <b>Pri</b><br>Fai        | Membership for F    | TAR SafetyConsumer<br>Display Name | Role<br>Type<br>o Group | Description  |  |

**Note:** For more details, refer to *Section 2.8.3.1 Creating Application Roles Using Fusion Middleware Control* from 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.

| 6  | Information                       |  |             |
|----|-----------------------------------|--|-------------|
|    | A new security grant has been ad  | Ided successfully.                     |             |
| Do | main_bi/bi > Application Policies |  |             |
|    | Application Stripe                | obi 🗸                                  |             |
|    | Principal Type                    | Application Role                       |             |
|    |                                   |  |             |
|    | Principal Name                    | Starts With                            | •           |
| v  | iew 🔻 🎽 Create 📑 Cre              | eate Like 💉 Edit 🗙 Del                 | lete        |
| 1  |                                   |  |             |
|    | Principal                         | Display Name                           | Description |
|    | ASBIPAdmin                        | AS BIP Admin                           |             |
|    | ASBIPConsumer                     | AS BIP Consumer                        |             |
|    | ASBIPAuthor                       | AS BIP Author                          |             |
|    | BIServiceAdministrator            | BI Service Administrator               |             |
|    | ASBIPReport                       | AS BIP Report                          |             |
|    |                                   | ······································ |             |

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

The Create Application Grant dialog box appears.

|                              | DRACLE Enterprise Manager Fusion Middleware Control 12c |                     |                    |               |               | 🔚 WebLogic Domain 🔻 | weblogic 🔻 🚥         |
|------------------------------|---|---------------------|--------------------|---------------|---------------|---------------------|----------------------|
| bipofm ()                    | nain 👻  |                     |                    |               |               | Apr 14, 20          | 116 4:08:58 AM MDT 👈 |
| /Domain_bipofm/bipofm > Ap   | oplication Policies > Create Application Grant          |                     |                    |               |               |                     |                      |
| Create Application           | n Grant   |                     |                    |               |               |                     | OK Cancel            |
| For managing an application  | policy, select a particular grantee and attach          | a permission to it. |                    |               |               |                     |                      |
| Application Stripe obi       |   |                     |                    |               |               |                     |                      |
| Grantee                      |   |                     |                    |               |               |                     |                      |
| Select the grantees (user, g | group or application role) you want to add to t         | the policy.         |                    |               |               |                     |                      |
| View 🔻 🕂 Add                 | 🗙 Delete 📓 Detach                                       |                     |                    |               |               |                     |                      |
| Name                         | Display Name  | Туре                | Description        |               |               |                     |                      |
| No users or groups added     | 1.  |                     |                    |               |               |                     |                      |
|                              |   |                     |                    |               |               |                     |                      |
| Permissions                  |   |                     |                    |               |               |                     |                      |
| Select from permissions and  | d resources used in this application. Enter se          |                     | right permissions. |               |               |                     |                      |
| View 🔻 🕂 Add                 | 🖉 Edit 🗙 Delete 📰 Detach                                |                     |                    |               |               |                     |                      |
| Permission Class             |   |                     |                    | Resource Name | Resource Type | Permission Actions  | Permission Set       |
| No permissions added.        |   |                     |                    |               |               |                     |                      |

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

The Add Principal dialog box appears.

| Application Stripe obi   Crance   Select the grantese (user, group or application role) you want to dad to the point, where a service instance, or groups added.   View → Add   Permissions Select from permissions and resources used in this application. Enter search or the select the application roles that you want to grant permissions to.   View → Add   Cather   View → Add   Cather   View → Add   Cather   Detech   Permission Class No permissions added.   View → Add   Cather   Display Name   Select.   View → Add Cather Detech View → Detech Secreted Principal Secreted Principal Samplication roles that you want to grant permissions to. Secreted Principal Samplication Role Permission Class No permissions added. Display Name Description anonymous-role Anonymous-role Anonymous-role Anonymous-role Anonymous-role Anonymous-role FAR Administrator Role FAR Sefety Author Role FAR Sefety Consumer Role FAR Se | terra determination            | plicy, select a particular grantee and attach a permission | Add Principal   |                                  |                                 |  |        |  |
|--|--------------------------------|--|---|----------------------------------|---------------------------------|--|--------|--|
| Grante   Select the principal source used in this application. Enter search order   View + Add _ Coluct Column   Name   Display Name   No users or groups added.   Permissions   Select from permissions and resources used in this application. Enter search order   View + Add _ Colum Column   View + Add _ Colum Column   Permissions added.   Principal   Display Name   Select-from permissions added.   Permissions added.   Permissions added.   Principal   Display Name   Description   anonymous-role   Anonymous-role   Anonymous-role   Anonymous-role   BerviceAdministrator   BerviceAdministrator   BerviceAdministrator   BerviceAdministrator   BerviceAdministrator   BerviceAdministrator   BerviceAdministrator Role   FAR Administrator Role   FAR BIP Safety Author Role  | Application Stripe obi         |  |   |                                  |                                 |  |        |  |
| Name Display Name   No users or groups added.     Permissions   Select from permissions and resources used in this application. Enter search orders   View   Add   Edit   Detach     View   Add   Edit   Detach     View              Principal Name   Starts Wth               Permissions added.                     Permissions added.               Permissions added.             Principal Name   Starts Wth   Permissions added.      Principal Display Name  Starts Wth    Permissions added.   Principal Name   Display Name   Display Name   Display Name   Description   anonymous-role   Anonymous-role   Anonymous-role   Anonymous-role   And ministrator   Display Name   Display Name<  |                                | up or application role) you want to add to the policy.     | and the second se | eet me application roles that yo | a want to grant permasions to.  |  |        |  |
| No users or groups added.     Permissions   Select from permissions and resources used in this application. Enter search criters   View + Add   Edit   Detach     View * Add   Character Control     View * Add   Edit   Detach     View * Control         Principal Mame Starts With *   Display Name   Starts With *      Searched Principals   View * Control   Principal   Display Name   Description   anonymous-role   BiService-Administrator   BiService-Administrator   FAR Administrator Role   FAR Administrator Role   FAR Administrator Role   FAR Administrator Role   FAR BIP Safety Author Role   | View 👻 🕂 Add 📉 Delete 🙀 Detach |  |   | Type Application Role            | -                               |  |        |  |
| Permissions     Select from permissions and resources used in this application. Enter search orders     View   Add   Cathing        Detach        View        Detach  Display Name   Description                               Display Name   Display Name   Description      Description <b>Description Description Description</b>   | Name                           | Display Name   | Prin  | cipal Name Starts With 👻         |                                 |  |        |  |
| Permissions   Select from permissions and resources used in this application. Enter search orders   View   Add   Edit   Detect   | No users or groups added.      |  |   |                                  |                                 |  |        |  |
| Permissions       Delach       Detach       Delach       Delach </th <th></th> <th></th> <th>Dis</th> <th>play Name Starts With</th> <th></th> <th>•</th> <th></th>   |                                |  | Dis   | play Name Starts With            |                                 | •  |        |  |
| View         Add         Edit.         Delatech         Principal         Display Name         Description           Permission Class         anonymous-role         Anonymous Role         anonymous-role         Authenticated Role         authenticated Role         authenticated Role         BiService Administrator         BiService Administrator         Biservice Administrator         This role confers privileges required to administer a service instance.           FARAdminRole         FAR Administrator Role         FAR BIP Safety Author Role         FAR BIP Safety Author Role  | Permissions                    |  | Searched Principals   |                                  |                                 |  |        |  |
| Permission Class         Principal         Display name         Description           No permissions added.         anonymous-role         Anonymous Role  | Select from permissions and r  | resources used in this application. Enter search criteri   | View 👻 📄 Detach   |                                  |                                 |  |        |  |
| No permissions added.     Authenticated-role     Authenticated Role       BI Service Administrator     BI Service Administrator     This role confers privileges required to administer a service instance.       FARAdminRole     FAR Administrator Role     FAR BIP Safety Author Role       FARSafetyAuthorRole     FAR BIP Safety Author Role     FAR BIP Safety Author Role   | View 🔹 🕂 Add 🥖                 | Edit 🗙 Delete 📰 Detach                                     | Principal   | Display Name                     | Description                     |  |        |  |
| Bit Service Administrator     Bit Service Administrator     This role confers privileges required to administer a service instance.       FARAdminRole     FAR Administrator Role     FAR BIP Administrator Role       FARSafetyAuthorRole     FAR BIP Safety Author Role     FAR BIP Safety Author Role   | Permission Class               |  | anonymous-role  | Anonymous Role                   |                                 |  |        |  |
| FARAdminRole         FAR Administrator Role         FAR BIP Administrator Role           FARSafetyAuthorRole         FAR BIP Safety Author Role         FAR BIP Safety Author Role   | No permissions added.          |  | authenticated-role  | Authenticated Role               |                                 |  |        |  |
| FARSafetyAuthorRole FAR BIP Safety Author Role FAR BIP Safety Author Role  |                                |  | BIServiceAdministrator  | BI Service Administrator         | This role confers privileges re | quired to administer a service instance. |        |  |
|  |                                |  | FARAdminRole  | FAR Administrator Role           | FAR BIP Administrator Role      |  |        |  |
| FARSafetyConsumerRole FAR Safety Consumer Role FAR BIP Safety Consumer Role  |                                |  | FARSafetyAuthorRole   | FAR BIP Safety Author Role       | FAR BIP Safety Author Role      |  |        |  |
|  |                                |  | FARSafetyConsumerRole   | FAR Safety Consumer Role         | FAR BIP Safety Consumer Rol     | e  |        |  |
|  |                                |  |   |                                  |                                 |  |        |  |
|  |                                |  |   |                                  |                                 | OK                                       | Cancel |  |

- **5.** From the **Type** drop-down list, 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.

| View - + Add Delete 🐨 Detach |   |                               | Add Permission            |                                      | ×   |
|------------------------------|---|-------------------------------|---------------------------|--------------------------------------|---|
| Name                         | Display Name                              | Туре                          | Select from permissions a | and resources used in this applicati | ion. Enter search criteria to search for right permissions. |
| FARAdminRole                 | FAR Administrator Role                    | Application Role              | J Search                  |                                      |   |
|                              |   |                               | C Permissions 📀 R         | Resource Types                       |   |
| Permissions                  |   |                               | Resource T                | ype oracle.bi.publisher.permission   | n 💌   |
|                              | rces used in this application. Enter sear | ch criteria to search for rig | Resource Na               | me Starts With                       | ÷   |
| •                            | I X Delete Detach                         |                               | Search Results            |                                      |   |
| Permission Class             |   |                               | Resource                  |                                      |   |
| No permissions added.        |   |                               | Name                      | Display Name                         | Description   |
|                              |   |                               | oracle.bi.publish         | BIP Access Excel Report Analyzer     |   |
|                              |   |                               | oracle.bi.publish         | BIP Access Online Report Analyze     | r   |
|                              |   |                               | oracle.bi.publish         | BIP Access Report Output             |   |
|                              |   |                               | oracle.bi.publish         | BIP Administer Server                |   |
|                              |   |                               | oracle.bi.publish         | BIP Develop Data Model               |   |
|                              |   |                               | oracle.bi.publish         | BIP Develop Report                   |   |
|                              |   |                               | oracle.bi.publish         | BIP Run Report Online                |   |
|                              |   |                               | oracle bi publich         | BIP Schedule Report                  |   |

- 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.

| Add Permissi          | on                           | ×                |
|-----------------------|------------------------------|------------------|
| Customize res         | ource or actions for selec   | cted permission. |
| 📕 Customize           |                              |                  |
| Permission<br>Class   | oracle.security.jps.Resourc  | cePermission     |
| Resource<br>Type      | oracle.bi.publisher.permissi | ion              |
| Resource<br>Name      | oracle.bi.publisher.administ | erServer         |
| Permission<br>Actions |                              |                  |
|                       | Back                         | Select Cancel    |

- 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.

| Name                           | Display Name   | e                  | Туре                           | Description      |   |                   |  |
|--------------------------------|----------------|--------------------|--------------------------------|------------------|---|-------------------|--|
| FARAdminRole                   | FAR Administra | ator Role          | Application Role               | FAR BIP Administ | rator Role                                      |                   |  |
| rmissions                      |                |                    |                                |                  |   |                   |  |
| elect from permissions and res |                | tion. Enter search | n criteria to search for right | permissions.     |   |                   |  |
| elect from permissions and res |                |                    | criteria to search for right   | permissions.     | Resource Type                                   | Permission Action |  |
| elect from permissions and res | Edit 💢 Delete  |                    |                                |                  | Resource Type<br>oracle.bi.publisher.permission | Permission Action |  |

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              |
|--------------|-----------------------|-----------------------------------|
| FAR Author   | FARSafetyAuthorRole   | BIP Develop Report                |
|              |                       | BIP Develop Data Model            |
| FAR Consumer | FARSafetyConsumerRole | 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

# 13.6.3 Managing Privileges and Folder Rights

To set Catalog Folder-level permissions in BI Publisher:

**1.** Go to Catalog > Shared Folders > Tasks > Permissions.

The Permissions dialog box appears.

2. Set the Permissions as follows, and click OK.

| Accounts                   | Permissions             |
|----------------------------|-------------------------|
| FAR Administrator Role     | Write, and Delete       |
| FAR BIP Safety Author Role | Read, Write, and Delete |
| FAR Safety Consumer Role   | Read                    |
| BI Service Administrator   | Write, and Delete       |

**Note:** Make sure the **Apply permissions** option for the sub-folders and the items is NOT selected.

**3.** Go to Shared folders > Argus Safety > Tasks > Permissions.

The Permissions dialog box appears.

4. Set the Permissions as follows, and click OK.

| Accounts                         | Permissions             |
|----------------------------------|-------------------------|
| FAR Administrator Role           | Write, and Delete       |
| FAR BIP Safety Author Role       | Read, Write, and Delete |
| FAR Safety Consumer Role         | Read                    |
| BI Service Administrator (Owner) | Write, and Delete       |

**Note:** Make sure to select the **Apply permissions** option for the sub-folders and the items.

- 5. To add the Data Sources to Roles in BI Publisher:
  - a. Login to the BIP with Administrator credentials.

For example, login to BIP from *http://acme.com:9502/xmlpserver/* 

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 **asbip** data source to **FARSafetyAuthorRole** and **FARSafetyConsumerRole** as well.

# 13.7 Managing Users and Roles for BI Publisher [OBIEE and BI Integrated Installation]

This section comprises the steps to manage users and their roles for OBIEE and BI Publisher in Oracle Fusion Middleware.

# 13.7.1 Creating Users and Assigning Groups

Refer to Section 13.6.1, "Creating Users and Assigning Groups."

# 13.7.2 Creating Roles and Policies

#### To create new application role and adding members:

See Section 13.6.2, "Creating Roles and Policies" > To create new application roles:

Do NOT copy policies from this reference, and see the following section.

**Note:** As you cannot modify the Catalog Type to BI Publisher File System, you must not use BI Publisher Security for this type of installation. Beside, if you do use BI Publisher Security for this installation, then you will not be able to log-in.

#### To create new application policies:

- 1. Login 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 list, select OBI.

| policies that an application relies upon for<br>bLogic Domain, use the <u>Oracle WebLogi</u> |
|--|
|  |
| WebLogic Domain  |
| LDAP   |
| jdbc/OpssDataSource  |
|  |
| h keyword for principals or permissions  |
| <no application="" selected="" stripe=""></no>   |
| <no application="" selected="" stripe=""></no>   |
| wsm-pm   |
|  |

#### 4. Click Create.

The Create Application Grant dialog box appears.

|   | terprise Manager Fusion Middleware C                                      | Control 12c         |                    |               |               | KebLogic Domain 💌  | weblogic 🔻 🚥        |
|---|---|---------------------|--------------------|---------------|---------------|--------------------|---------------------|
| bipofm ()<br>WebLogic Doma  | ain 💌   |                     |                    |               |               | Apr 14, 20         | 16 4:08:58 AM MDT 👈 |
| /Domain_bipofm/bipofm > App   | plication Policies > Create Application Grant                             |                     |                    |               |               |                    |                     |
| Create Application<br>For managing an application p<br>Application Stripe obi | Grant<br>policy, select a particular grantee and attach                   | a permission to it. |                    |               |               |                    | OK Cancel           |
|   | roup or application role) you want to add to t                            | he policy.          |                    |               |               |                    |                     |
| Name  | Display Name  | Туре                | Description        |               |               |                    |                     |
| No users or groups added.   |   |                     |                    |               |               |                    |                     |
|   | resources used in this application. Enter se<br>Edit Delete <b>Delete</b> |                     | right permissions. |               |               |                    |                     |
| Permission Class  |   |                     |                    | Resource Name | Resource Type | Permission Actions | Permission Set      |
| No permissions added.   |   |                     |                    |               |               |                    |                     |

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

The Add Principal dialog box appears.

- **6.** From the **Type** drop-down list, select **Application Role**, and click **Search**.
- 7. From the list of Searched Principals, select FARAdminRole, and click OK.

| <b>Create Application Gran</b>   | nt   |                                    |                                    |                                 |   |    |        |
|--|--|------------------------------------|------------------------------------|---------------------------------|---|----|--------|
| For managing an application policy, se   | lect a particular grantee and attach a permissi  | Add Principal                      |                                    |                                 |   | -  | -      |
| Application Stripe obi<br>Grantee<br>Select the grantees (user, group or application role) you want to add to the policy.<br>View + Add Delete |  | Specify criteria to search and sel | lect the application roles that yo | u want to grant permissions to. |   |    |        |
|  |  |                                    |                                    |                                 |   |    |        |
| Name Display Name  |  | Prin                               | cipal Name Starts With 💌           |                                 |   |    |        |
| No users or groups added.  |  | Dis                                | play Name Starts With 💌            |                                 | ×   |    |        |
| Permissions  |  | Searched Principals                |                                    |                                 |   |    |        |
| Select from permissions and resource   | es used in this application. Enter search criter | View 🔻 📳 Detach                    |                                    |                                 |   |    |        |
| View 👻 🕂 Add 🥒 Edit  | . 💢 Delete 📄 Detach                              | Principal                          | Display Name                       | Description                     |   |    |        |
| Permission Class   |  | anonymous-role                     | Anonymous Role                     |                                 |   |    |        |
| No permissions added.  |  | authenticated-role                 | Authenticated Role                 |                                 |   |    |        |
|  |  | BIServiceAdministrator             | BI Service Administrator           | This role confers privileges re | equired to administer a service instance. |    |        |
|  |  | FARAdminRole                       | FAR Administrator Role             | FAR BIP Administrator Role      |   |    |        |
|  |  | FARSafetyAuthorRole                | FAR BIP Safety Author Role         | FAR BIP Safety Author Role      |   |    |        |
|  |  | FARSafetyConsumerRole              | FAR Safety Consumer Role           | FAR BIP Safety Consumer Rol     | e   |    |        |
|  |  | 2                                  |                                    |                                 |   |    |        |
|  |  |                                    |                                    |                                 | 0   | ОК | Cancel |

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

The Add Permission dialog box appears.

| Grantee<br>Select the grantees (user, group or | application role) you want to add to the  | policy                        |   |   |
|--|---|-------------------------------|---|---|
| View - + Add Z Del                             |   |                               | Add Permission  | ×   |
| Name   | Display Name                              | Туре                          | Select from permissions and resources used in this application. Enter sea | rch criteria to search for right permissions. |
| FARAdminRole                                   | FAR Administrator Role                    | Application Role              | A Search  |   |
|  |   |                               | C Permissions C Resource Types  |   |
| Permissions                                    |   |                               | Resource Type oracle.bi.publisher.permission 🔻                            |   |
| Select from permissions and resour             | ces used in this application. Enter searc | ch criteria to search for rig | Resource Name Starts With -   | •   |
| View 👻 🕂 Add 🥖 Edit.                           | X Delete Detach                           |                               | Search Results  |   |
| Permission Class                               |   |                               | Resource  |   |
| No permissions added.                          |   |                               | Name Display Name   | Description                                   |
|  |   |                               | oracle.bi.publish BIP Access Excel Report Analyzer                        |   |
|  |   |                               | oracle.bi.publish BIP Access Online Report Analyzer                       |   |
|  |   |                               | oracle.bi.publish BIP Access Report Output                                |   |
|  |   |                               | oracle.bi.publish BIP Administer Server                                   |   |
|  |   |                               | oracle.bi.publish BIP Develop Data Model                                  |   |
|  |   |                               | oracle.bi.publish BIP Develop Report                                      |   |
|  |   |                               | oracle.bi.publish BIP Run Report Online                                   |   |
|  |   |                               | oracle.bi.publish BIP Schedule Report                                     |   |
|  |   |                               | STIP Continue to go to next step if you want to enter policy d            | etails.                                       |

- 9. Select the **Resource Types** radio button.
- **10.** From the **Resource Type** drop-down list, 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 13–1.

**12.** For **Permission Actions**, select **All** (\_all\_), and click **Select**.

| Add Permission        |            |            |            |           |          |
|-----------------------|------------|------------|------------|-----------|----------|
| Customize reso        | ource or a | actions    | for sele   | cted perr | nission. |
| 🖌 Customize           |            |            |            |           |          |
| Permission<br>Class   | oracle.se  | ecurity.jp | s.Resour   | cePermiss | ion      |
| Resource<br>Type      | oracle.bi. | publishe   | r.permiss  | ion       |          |
| Resource<br>Name      | oracle.bi. | publishe   | r.administ | terServer |          |
| Permission<br>Actions | All        |            |            |           |          |
|                       |            |            | Back       | Select    | Cancel   |

**13.** When all the permissions are added, click **OK**.

|  |  |                                    |   |                                   | OK Cance      |
|--|--|------------------------------------|---|-----------------------------------|---------------|
| managing an application policy, select a   | particular grantee and attach a p  | ermission to it.                   |   |                                   |               |
| pplication Stripe obi  |  |                                    |   |                                   |               |
| rantee   |  |                                    |   |                                   |               |
| elect the grantees (user, group or applicat  | tion role) you want to add to the  | policy.                            |   |                                   |               |
| View - + Add X Delete  | Detach   |                                    |   |                                   |               |
| Name   | Display Name   | Туре                               | Description   |                                   |               |
| FARAdminRole   | FAR Administrator Role   | Application Role                   | FAR BIP Administrator Role  |                                   |               |
| elect from permissions and resources use   |  | ch criteria to search for right pe | rmissions.  |                                   |               |
| elect from permissions and resources use   | ed in this application. Enter searc<br>Celete  Celetach<br>Resource Name   | ch criteria to search for right pe | rmissions.<br>Resource Type   | Permission Actions                | Permission Se |
| ielect from permissions and resources use<br>View • + Add / Edit >   | Celete Detach  | th criteria to search for right pe |   | Permission Actions                | Permission Se |
| View  + Add  Centre Edit  Permission Class   | Delete      Detach     Resource Name     *   |                                    | Resource Type   |                                   | Permission Se |
| elect from permissions and resources use<br>View  + Add  Edit Permission Class oracle.security.jps.ResourcePermission  | Celete Cetach Resource Name  | nisterServer                       | Resource Type   | manage                            | Permission Se |
| View + Add Edit<br>Permission Class<br>oracle.security.jps.ResourcePermission<br>oracle.security.jps.ResourcePermission  | Deleter     Detach       Resource Name       *       n     oracle.bi.publisher.admir       n     oracle.bi.scheduler.man   | nisterServer<br>ageJobs            | Resource Type<br>oracle.bi.catalog<br>oracle.bi.publisher.permission  | manage<br>_all_                   | Permission Se |
| View + Add Edit<br>Permission Class<br>oracle.security.jps.ResourcePermission<br>oracle.security.jps.ResourcePermission<br>oracle.security.jps.ResourcePermission                        | Delete     Detach       Resource Name       *       oracle.bi.publisher.admin       oracle.bi.scheduler.man       oracle.bi.scheduler.man                                | nisterServer<br>ageJobs            | Resource Type<br>oracle.bi.catalog<br>oracle.bi.publisher.permission<br>oracle.bi.scheduler.permission  | manage<br>_all_<br>_all_          | Permission Se |
| Permission Class<br>oracle.security.jps.ResourcePermission<br>oracle.security.jps.ResourcePermission<br>oracle.security.jps.ResourcePermission<br>oracle.security.jps.ResourcePermission | Deleter     Detach       Resource Name       *       oracle.bi.publisher.admin       oracle.bi.scheduler.man       oracle.bi.sterver.manage       oracle.bi.delivers.job | nisterServer<br>ageJobs            | Resource Type<br>oracle.bi.catalog<br>oracle.bi.publisher.permission<br>oracle.bi.scheduler.permission<br>oracle.bi.server.permission<br>oracle.bi.delivers.job | manage<br>_all_<br>_all_<br>_all_ | Permission Se |

**14.** Repeat Steps 5-13 for other principals and their permissions. (See Table 13–1)

| Policy Name/Principal | Resource Type                                       | Resource Name  | Permission<br>Actions |
|-----------------------|---|--|-----------------------|
| FARAdminRole          | oracle.bi.catalog                                   | *  | manage                |
|                       | oracle.bi.server.permission                         | oracle.bi.server.manageRepositori<br>es                | _all_                 |
|                       | oracle.bi.presentation.catalogman<br>ger.permission | oracle.bi.presentation.catalogman<br>ger.manageCatalog | _all_                 |
|                       | oracle.bi.delivers.job                              | oracle.bi.delivers.job                                 | manage                |
|                       | oracle.bi.publisher.permission                      | oracle.bi.publisher.administerServ<br>er               | _all_                 |
|                       | oracle.bi.repository                                | oracle.bi.repository                                   | manage                |
|                       | oracle.bi.scheduler.permission                      | oracle.bi.scheduler.manageJobs                         | _all_                 |
| FARSafetyAuthorRole   | oracle.bi.publisher.permission                      | oracle.bi.publisher.developReport                      | _all_                 |
|                       | oracle.bi.publisher.permission                      | oracle.bi.publisher.developDataM<br>odel               | _all_                 |
|                       | oracle.bi.tech.visualanalyzer.perm<br>ission        | oracle.bi.tech.visualanalyzer.gener<br>alAccess        | _all_                 |
|                       | oracle.bi.delivers.job                              | *  | schedule              |

#### Table 13–1 List of Policies and their Permissions

| Policy Name/Principal | Resource Type                  | Resource Name                                      | Permission<br>Actions |
|-----------------------|--------------------------------|--|-----------------------|
| e                     | oracle.bi.publisher.permission | oracle.bi.publisher.scheduleReport                 | _all_                 |
|                       | oracle.bi.publisher.permission | oracle.bi.publisher.runReportOnli<br>ne            | _all_                 |
|                       | oracle.bi.publisher.permission | oracle.bi.publisher.accessReportO<br>utput         | _all_                 |
|                       | oracle.bi.publisher.permission | oracle.bi.publisher.accessOnlineRe<br>portAnalyzer | _all_                 |
|                       | ESSMetadataPermission          | oracle.bip.ess.JobDefinition.EssBip<br>Job         | •                     |
|                       | oracle.bi.publisher.permission | oracle.bi.publisher.accessExcelRep<br>ortAnalyzer  |                       |

 Table 13–1 (Cont.) List of Policies and their Permissions

**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

# 13.7.3 Managing Privileges and Folder Rights

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

For example: Login to *http://obieeapps.us.oracle.com:9502/analytics* with WebLogic user credentials.

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

| Component | Privilege                                | Default Role Granted                                |
|-----------|--|---|
| Access    | Access to Administration                 | FAR Administrator Role, BI Service<br>Administrator |
| Access    | Access to Answers                        | FAR Safety Author Role                              |
| Access    | Access to BI Composer                    | FAR Safety Author Role                              |
| Access    | Access to Briefing Books                 | FAR Safety Consumer Role                            |
| Access    | Access to Dashboards                     | FAR Safety Consumer Role                            |
| Access    | Access to Delivers                       | FAR Safety Author Role                              |
| Access    | Access to Export                         | FAR Safety Consumer Role                            |
| Access    | Access to KPI Builder                    | FAR Safety Author Role                              |
| Access    | Access to List Formats                   | FAR Safety Author Role                              |
| Access    | Access to Metadata Dictionary            | FAR Safety Author Role                              |
| Access    | Access to Mobile                         | FAR Safety Consumer Role                            |
| Access    | Access to Oracle BI Client Installer     | FAR Safety Consumer Role                            |
| Access    | Access to Oracle BI for Microsoft Office | FAR Safety Consumer Role                            |
| Access    | Access to Scorecard                      | FAR Safety Consumer Role                            |

| AccessAccess to Segment TreesFAR Safety Author RoleAccessAccess to SegmentsFAR Safety Consumer RoleAccessCatalog Preview Pane UIFAR Safety Consumer RoleActionsCreate Invoke ActionsFAR Safety Author RoleActionsCreate Navigate ActionsFAR Safety Consumer RoleActionsCreate Navigate ActionsFAR Safety Consumer RoleActionsSave Actions containing embedded HTMLFAR Administrator Role, BI Ser<br>Admini: CatalogAdmin: CatalogChange PermissionsFAR Safety Author RoleAdmin: CatalogToggle Maintenance ModeFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralChange Log ConfigurationFAR Administrator Role, BI Ser<br>Admini: GeneralAdmin: GeneralCreate DashboardsFAR Safety Author RoleAdmin: GeneralDiagnose BI Server QueryDenied: Authenticated UserAdmin: GeneralIssue SQL DirectlyFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Agent SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Agent SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing JobsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: General <th></th>  |      |
|---|------|
| AccessCatalog Preview Pane UIFAR Safety Consumer RoleActionsCreate Invoke ActionsFAR Safety Author RoleActionsCreate Navigate ActionsFAR Safety Consumer RoleActionsSave Actions containing embedded HTMLFAR Administrator Role, BI Ser<br>AdministratorAdmin: CatalogChange PermissionsFAR Safety Author RoleAdmin: CatalogToggle Maintenance ModeFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralChange Log ConfigurationFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralCreate DashboardsFAR Safety Author RoleAdmin: GeneralDiagnose BI Server QueryDenied: Authenticated User<br>AdministratorAdmin: GeneralIssue SQL DirectlyFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Agent SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Agent SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing JobsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage                            |      |
| ActionsCreate Invoke ActionsFAR Safety Author RoleActionsCreate Navigate ActionsFAR Safety Consumer RoleActionsSave Actions containing embedded HTMLFAR Administrator Role, BI Ser<br>AdministratorAdmin: CatalogChange PermissionsFAR Safety Author RoleAdmin: CatalogToggle Maintenance ModeFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralChange Log ConfigurationFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralCreate DashboardsFAR Safety Author RoleAdmin: GeneralDiagnose BI Server QueryDenied: Authenticated UserAdmin: GeneralIssue SQL DirectlyFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Agent SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Agent SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Global VariablesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: General <t< td=""><td></td></t<> |      |
| ActionsCreate Navigate ActionsFAR Safety Consumer RoleActionsSave Actions containing embedded HTMLFAR Administrator Role, BI Ser<br>AdministratorAdmin: CatalogChange PermissionsFAR Safety Author RoleAdmin: CatalogToggle Maintenance ModeFAR AdministratorAdmin: GeneralChange Log ConfigurationFAR AdministratorAdmin: GeneralCreate DashboardsFAR Safety Author RoleAdmin: GeneralCreate DashboardsFAR Safety Author RoleAdmin: GeneralDiagnose BI Server QueryDenied: Authenticated UserAdmin: GeneralJusue SQL DirectlyFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Agent SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Device TypesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Global VariablesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing JobsFAR Safety Author RoleAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>Administrator Role, BI Ser<br>Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>Administrator Role, BI Ser<br>Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing JobsFAR Saf  |      |
| ActionsSave Actions containing embedded HTMLFAR Administrator Role, BI Set<br>AdministratorAdmin: CatalogChange PermissionsFAR Safety Author RoleAdmin: CatalogToggle Maintenance ModeFAR AdministratorAdmin: GeneralChange Log ConfigurationFAR AdministratorAdmin: GeneralCreate DashboardsFAR Safety Author RoleAdmin: GeneralCreate DashboardsFAR Safety Author RoleAdmin: GeneralDiagnose BI Server QueryDenied: Authenticated UserAdmin: GeneralIssue SQL DirectlyFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Agent SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Oevice TypesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Global VariablesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing JobsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing JobsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Session                           |      |
| AdministratorAdministratorAdmin: CatalogChange PermissionsFAR Safety Author RoleAdmin: CatalogToggle Maintenance ModeFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralChange Log ConfigurationFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralCreate DashboardsFAR Safety Author RoleAdmin: GeneralDiagnose BI Server QueryDenied: Authenticated UserAdmin: GeneralIssue SQL DirectlyFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Agent SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Global VariablesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralSer privileged errorsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralSer                    |      |
| Admin: CatalogToggle Maintenance ModeFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralChange Log ConfigurationFAR AdministratorAdmin: GeneralCreate DashboardsFAR Safety Author RoleAdmin: GeneralDiagnose BI Server QueryDenied: Authenticated UserAdmin: GeneralDiagnose BI Server QueryDenied: Authenticated UserAdmin: GeneralIssue SQL DirectlyFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Agent SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Device TypesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Global VariablesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralSee privileged errorsFAR Administrator Role, BI Ser<br>Administrator                                 | vice |
| AdministratorAdministratorAdmin: GeneralChange Log ConfigurationFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralCreate DashboardsFAR Safety Author RoleAdmin: GeneralDiagnose BI Server QueryDenied: Authenticated UserAdmin: GeneralIssue SQL DirectlyFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Agent SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Device TypesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Global VariablesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DobsFAR Safety Author RoleAdmini: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralPerformance MonitorFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralSee privileged errorsFAR Administrator Role, BI Ser<br>Administrator   |      |
| AdministratorAdministratorAdmin: GeneralCreate DashboardsFAR Safety Author RoleAdmin: GeneralDiagnose BI Server QueryDenied: Authenticated UserAdmin: GeneralIssue SQL DirectlyFAR Administrator Role, BI SerAdmin: GeneralManage Agent SessionsFAR Administrator Role, BI SerAdmin: GeneralManage Device TypesFAR Administrator Role, BI SerAdmin: GeneralManage Clobal VariablesFAR Administrator Role, BI SerAdmin: GeneralManage Global VariablesFAR Administrator Role, BI SerAdmin: GeneralManage Map DataFAR Administrator Role, BI SerAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI SerAdmin: GeneralManage SessionsFAR Administrator Role, BI SerAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI SerAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI SerAdmin: GeneralManage SessionsFAR Administrator Role, BI SerAdmin: GeneralManage SessionsFAR Administrator Role, BI SerAdmin: GeneralManage SessionsFAR Administrator Role, BI SerAdmin: GeneralSee privileged errorsFAR Administrator Role, BI SerAdmin: GeneralSee privileged errorsFAR Administrator Role, BI SerAdmin: GeneralSee privileged errorsFAR Administrator Role, BI Ser  | vice |
| Admin: GeneralDiagnose BI Server QueryDenied: Authenticated UserAdmin: GeneralIssue SQL DirectlyFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Agent SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Device TypesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Global VariablesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Global VariablesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing JobsFAR Safety Author RoleAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralPerformance MonitorFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralSee privileged errorsFAR Administrator Role, BI Ser<br>Administrator  | vice |
| Admin: GeneralIssue SQL DirectlyFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Agent SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Device TypesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Global VariablesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing JobsFAR Safety Author RoleAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralPerformance MonitorFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralSee privileged errorsFAR Administrator Role, BI Ser<br>Administrator  |      |
| AdministratorAdministratorAdmini: GeneralManage Agent SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Device TypesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Global VariablesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing JobsFAR Safety Author RoleAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralSee privileged errorsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralSee privileged errorsFAR Administrator Role, BI Ser<br>Administrator  |      |
| AdministratorAdministratorAdmin: GeneralManage Device TypesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Global VariablesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing JobsFAR Safety Author RoleAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralPerformance MonitorFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralSee privileged errorsFAR Administrator Role, BI Ser<br>Administrator   | vice |
| AdministratorAdministratorAdmin: GeneralManage Global VariablesFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing JobsFAR Safety Author RoleAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralPerformance MonitorFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralSee privileged errorsFAR Administrator Role, BI Ser<br>Administrator   | vice |
| AdministratorAdministratorAdmini: GeneralManage Map DataFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing JobsFAR Safety Author RoleAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralPerformance MonitorFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralSee privileged errorsFAR Administrator Role, BI Ser<br>Administrator  | vice |
| AdministratorAdministratorAdmin: GeneralManage Marketing DefaultsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralManage Marketing JobsFAR Safety Author RoleAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralPerformance MonitorFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralSee privileged errorsFAR Administrator Role, BI Ser<br>Administrator   | vice |
| AdministratorAdministratorAdmin: GeneralManage Marketing JobsFAR Safety Author RoleAdmin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralPerformance MonitorFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralSee privileged errorsFAR Administrator Role, BI Ser<br>Administrator   | vice |
| Admin: GeneralManage SessionsFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralPerformance MonitorFAR Administrator Role, BI Ser<br>AdministratorAdmin: GeneralSee privileged errorsFAR Administrator Role, BI Ser<br>Administrator  | vice |
| Administrator       Administrator         Admin: General       Performance Monitor       FAR Administrator Role, BI Ser<br>Administrator         Admin: General       See privileged errors       FAR Administrator Role, BI Ser<br>Administrator   |      |
| AdministratorAdministratorAdmini: GeneralSee privileged errorsFAR Administrator Role, BI See<br>Administrator   | vice |
| Administrator   | vice |
| Adapting Company 1 Concentrations IDs EAR Administration Data DI Con  | vice |
| Admin: General     See sessions IDs     FAR Administrator Role, BI Ser       Administrator     Administrator  | vice |
| Admin: GeneralSee SQL issued in errorsFAR Safety Consumer Role  |      |
| Admin: GeneralView System InformationFAR Administrator Role, BI Ser<br>Administrator  | vice |
| Admin: Security Access to Permissions Dialog FAR Safety Consumer Role   |      |
| Admin: Security Manage Catalog Accounts FAR Administrator Role, BI Ser<br>Administrator   | vice |
| Admin: SecurityManage PrivilegesFAR Administrator Role, BI SecurityAdministratorAdministrator   | vice |
| Admin: Security Set Ownership of Catalog Objects FAR Administrator Role, BI Ser<br>Administrator  | vice |

| Component       | Privilege   | Default Role Granted                                |
|-----------------|---|---|
| Admin: Security | User Population - Can List Application<br>Roles   | FAR Safety Consumer Role, BI System                 |
| Admin: Security | User Population - Can List Catalog Groups         | FAR Safety Consumer Role, BI System                 |
| Admin: Security | User Population - Can List Users                  | FAR Safety Consumer Role, BI System                 |
| Answers         | Access Advanced Tab                               | FAR Safety Author Role                              |
| Answers         | Add EVALUATE_PREDICATE Function                   | FAR Safety Author Role                              |
| Answers         | Create Advanced Filters and Set<br>Operations     | FAR Safety Author Role                              |
| Answers         | Create Analysis From Simple SQL                   | FAR Administrator Role, BI Service<br>Administrator |
| Answers         | Create Prompts                                    | FAR Safety Author Role                              |
| Answers         | Create Views                                      | FAR Safety Author Role                              |
| Answers         | Edit Column Formulas                              | FAR Safety Author Role                              |
| Answers         | Edit Direct Database Analysis                     | FAR Administrator Role, BI Service<br>Administrator |
| Answers         | Enter XML and Logical SQL                         | FAR Safety Author Role                              |
| Answers         | Execute Direct Database Analysis                  | FAR Administrator Role, BI Service<br>Administrator |
| Answers         | Save Column                                       | FAR Safety Author Role                              |
| Answers         | Save Content with HTML Markup                     | FAR Administrator Role, BI Service<br>Administrator |
| Answers         | Save Filters                                      | FAR Safety Author Role                              |
| Answers         | Upload Images                                     | FAR Safety Author Role                              |
| Briefing Book   | Add To or Edit a Briefing Book                    | FAR Safety Author Role                              |
| Briefing Book   | Add to Snapshot Briefing Book                     | FAR Safety Consumer Role                            |
| Briefing Book   | Download Briefing Book                            | FAR Safety Consumer Role                            |
| Catalog         | Archive Catalog                                   | FAR Administrator Role, BI Service<br>Administrator |
| Catalog         | Create Folders                                    | FAR Safety Author Role                              |
| Catalog         | Perform Extended Search                           | FAR Safety Author Role                              |
| Catalog         | Perform Global Search                             | FAR Safety Author Role                              |
| Catalog         | Personal Storage (My Folders and My<br>Dashboard) | FAR Safety Consumer Role                            |
| Catalog         | Reload Metadata                                   | FAR Administrator Role, BI Service<br>Administrator |
| Catalog         | See Hidden Items                                  | FAR Safety Author Role                              |
| Catalog         | Unarchive Catalog                                 | FAR Administrator Role, BI Service<br>Administrator |
| Catalog         | Upload Files                                      | FAR Administrator Role, BI Service<br>Administrator |
| Conditions      | Create Conditions                                 | FAR Safety Author Role                              |
| Dashboards      | Assign Default Customizations                     | FAR Safety Author Role                              |
|                 |   |   |

| Component       | Privilege   | Default Role Granted                                |
|-----------------|---|---|
| Dashboards      | Create Bookmark Links   | FAR Safety Consumer Role                            |
| Dashboards      | Create Prompted Links   | FAR Safety Consumer Role                            |
| Dashboards      | Export Entire Dashboard To Excel                              | FAR Safety Consumer Role                            |
| Dashboards      | Export Single Dashboard Page To Excel                         | FAR Safety Consumer Role                            |
| Dashboards      | Save Customizations   | FAR Safety Consumer Role                            |
| Delivers        | Chain Agents  | FAR Safety Author Role                              |
| Delivers        | Create Agents   | FAR Safety Author Role                              |
| Delivers        | Deliver Agents to Specific or Dynamically<br>Determined Users | FAR Administrator Role, BI Service<br>Administrator |
| Delivers        | Modify Current Subscriptions for Agents                       | FAR Administrator Role, BI Service<br>Administrator |
| Delivers        | Publish Agents for Subscription                               | FAR Safety Author Role                              |
| Formatting      | Save System-Wide Column Formats                               | FAR Administrator Role, BI Service<br>Administrator |
| Home and Header | Access Administration Menu                                    | Denied: Authenticated User                          |
| Home and Header | Access Catalog Search UI                                      | FAR Safety Consumer Role                            |
| Home and Header | Access Catalog UI   | FAR Safety Consumer Role                            |
| Home and Header | Access Data Loader  | Denied: Authenticated User                          |
| Home and Header | Access Home Page  | FAR Safety Consumer Role                            |
| Home and Header | Access Modeler  | Denied: Authenticated User                          |
| Home and Header | Access Rapid Search UI  | FAR Safety Consumer Role                            |
| Home and Header | Access User & Role Admin                                      | Denied: Authenticated User                          |
| Home and Header | Advanced Search Link  | FAR Safety Consumer Role                            |
| Home and Header | Custom Links  | FAR Safety Consumer Role                            |
| Home and Header | Dashboards Menu   | FAR Safety Consumer Role                            |
| Home and Header | Favorites Menu  | FAR Safety Consumer Role                            |
| Home and Header | Help Menu   | FAR Safety Consumer Role                            |
| Home and Header | My Account Link   | FAR Safety Consumer Role                            |
| Home and Header | New Menu  | FAR Safety Consumer Role                            |
| Home and Header | Open Menu   | FAR Safety Consumer Role                            |
| Home and Header | Simple Search Field   | FAR Safety Consumer Role                            |
| List Formats    | Access Options Tab  | FAR Safety Author Role                              |
| List Formats    | Add/Remove List Format Columns                                | FAR Administrator Role, BI Service<br>Administrator |
| List Formats    | Create Headers and Footers                                    | FAR Safety Author Role                              |
| List Formats    | Create List Formats   | FAR Safety Author Role                              |
| Mobile          | Enable Local Content  | FAR Safety Consumer Role                            |
| Mobile          | Enable Search   | FAR Safety Consumer Role                            |
| My Account      | Access to My Account  | FAR Safety Consumer Role                            |

| Component    | Privilege                                       | Default Role Granted                                |
|--------------|---|---|
| My Account   | Change Delivery Options                         | FAR Safety Consumer Role                            |
| My Account   | Change Preferences                              | FAR Safety Consumer Role                            |
| Proxy        | Act As Proxy                                    | Denied: Authenticated User                          |
| RSS Feeds    | Access to RSS Feeds                             | FAR Safety Consumer Role                            |
| Scorecard    | Add Annotations                                 | FAR Safety Consumer Role                            |
| Scorecard    | Add Scorecard Views To Dashboards               | FAR Safety Consumer Role                            |
| Scorecard    | Create Views                                    | FAR Safety Author Role                              |
| Scorecard    | Create/Edit Causes And Effects Linkages         | FAR Safety Author Role                              |
| Scorecard    | Create/Edit Initiatives                         | FAR Safety Author Role                              |
| Scorecard    | Create/Edit KPIs                                | FAR Safety Author Role                              |
| Scorecard    | Create/Edit Objectives                          | FAR Safety Author Role                              |
| Scorecard    | Create/Edit Perspectives                        | FAR Safety Author Role                              |
| Scorecard    | Create/Edit Scorecards                          | FAR Safety Author Role                              |
| Scorecard    | Override Status                                 | FAR Safety Consumer Role                            |
| Scorecard    | View Scorecards                                 | FAR Safety Consumer Role                            |
| Scorecard    | Write Back to Database for KPI                  | FAR Safety Consumer Role                            |
| Segmentation | Access Segment Advanced Options Tab             | FAR Administrator Role, BI Service<br>Administrator |
| Segmentation | Access Segment Tree Advanced Options<br>Tab     | FAR Administrator Role, BI Service<br>Administrator |
| Segmentation | Change Target Levels within Segment<br>Designer | FAR Safety Author Role                              |
| Segmentation | Create Segment Trees                            | FAR Safety Author Role                              |
| Segmentation | Create Segments                                 | FAR Safety Author Role                              |
| Segmentation | Create/Purge Saved Result Sets                  | FAR Administrator Role, BI Service<br>Administrator |
| SOAP         | Access AdministrationSOAPService<br>Service     | FAR Safety Consumer Role, BI System                 |
| SOAP         | Access AnalysisExportViewsService<br>Service    | FAR Safety Consumer Role                            |
| SOAP         | Access CatalogIndexingService Service           | FAR Safety Consumer Role, BI System                 |
| SOAP         | Access CatalogService Service                   | FAR Safety Consumer Role, BI System                 |
| SOAP         | Access ConditionEvaluationService Service       | FAR Safety Consumer Role, BI System                 |
| SOAP         | Access DashboardService Service                 | FAR Safety Consumer Role, BI System                 |
| SOAP         | Access HtmlViewService Service                  | FAR Safety Consumer Role, BI System                 |
| SOAP         | Access IBotService Service                      | FAR Safety Consumer Role, BI System                 |
| SOAP         | Access JobManagementService Service             | FAR Safety Consumer Role, BI System                 |
| SOAP         | Access KPIAssessmentService Service             | FAR Safety Consumer Role, BI System                 |
| SOAP         | Access MetadataService Service                  | FAR Safety Consumer Role, BI System                 |
| SOAP         | Access MsgdbService Service                     | FAR Safety Consumer Role, BI System                 |
|              |   |   |

| Component                   | Privilege                                    | Default Role Granted                |  |  |
|-----------------------------|--|-------------------------------------|--|--|
| SOAP                        | Access ReportEditingService Service          | FAR Safety Consumer Role, BI System |  |  |
| SOAP                        | Access SchedulerService Service              | FAR Safety Consumer Role            |  |  |
| SOAP                        | Access ScorecardAssessmentService<br>Service | FAR Safety Consumer Role, BI System |  |  |
| SOAP                        | Access ScorecardMetadataService Service      | FAR Safety Consumer Role, BI System |  |  |
| SOAP                        | Access SecurityService Service               | FAR Safety Consumer Role, BI System |  |  |
| SOAP                        | Access SOAP                                  | FAR Safety Consumer Role, BI System |  |  |
| SOAP                        | Access Tenant Information                    | BI System                           |  |  |
| SOAP                        | Access UserPersonalizationService Service    | FAR Safety Consumer Role            |  |  |
| SOAP                        | Access XmlGenerationService Service          | FAR Safety Consumer Role, BI System |  |  |
| SOAP                        | Impersonate as system user                   | BI System                           |  |  |
| View Canvas                 | Add/Edit Canvas View                         | FAR Safety Author Role              |  |  |
| View Column<br>Selector     | Add/Edit Column Selector View                | FAR Safety Author Role              |  |  |
| View Compound<br>Layout     | Add/Edit Compound Layout View                | FAR Safety Author Role              |  |  |
| View Contribution<br>Wheel  | Add/Edit Contribution Wheel View             | FAR Safety Author Role              |  |  |
| View Create Segment         | Add/Edit Create Segment View                 | FAR Safety Author Role              |  |  |
| View Create Target<br>List  | Add/Edit Create Target List View             | FAR Safety Author Role              |  |  |
| View Dashboard<br>Prompt    | Add/Edit Dashboard Prompt View               | FAR Safety Author Role              |  |  |
| View Filters                | Add/Edit Filters View                        | FAR Safety Author Role              |  |  |
| View Funnel                 | Add/Edit Funnel View                         | FAR Safety Author Role              |  |  |
| View Gauge                  | Add/Edit Gauge View                          | FAR Safety Author Role              |  |  |
| View Generic Plugin<br>View | Add/Edit Generic Plugin View View            | FAR Safety Author Role              |  |  |
| View Graph                  | Add/Edit Graph View                          | FAR Safety Author Role              |  |  |
| View Heat Matrix            | Add/Edit Heat Matrix View                    | FAR Safety Author Role              |  |  |
| View Javascript view        | Edit Javascript View                         | FAR Safety Author Role              |  |  |
| View Legend                 | Add/Edit Legend View                         | FAR Safety Author Role              |  |  |
| View Logical SQL            | Add/Edit Logical SQL View                    | FAR Safety Author Role              |  |  |
| View Map                    | Add/Edit Map View                            | FAR Safety Author Role              |  |  |
| View Micro Chart            | Add/Edit Micro Chart View                    | FAR Safety Author Role              |  |  |
| View Narrative              | Add/Edit Narrative View                      | FAR Safety Author Role              |  |  |
| View No Results             | Add/Edit No Results View                     | FAR Safety Author Role              |  |  |
| View Performance<br>Tile    | Add/Edit Performance Tile View               | FAR Safety Author Role              |  |  |
| View Pivot Table            | Add/Edit Pivot Table View                    | FAR Safety Author Role              |  |  |
| View Report Prompt          | Add/Edit Report Prompt View                  | FAR Safety Author Role              |  |  |

| Component            | Privilege  | Default Role Granted       |  |
|----------------------|--|----------------------------|--|
| View Selection Steps | Add/Edit Selection Steps View  | FAR Safety Author Role     |  |
| View Static Text     | Add/Edit Static Text View  | FAR Safety Author Role     |  |
| View Table           | Add/Edit Table View  | FAR Safety Author Role     |  |
| View Ticker          | Add/Edit Ticker View   | FAR Safety Author Role     |  |
| View Title           | Add/Edit Title View  | FAR Safety Author Role     |  |
| View Treemap         | Add/Edit Treemap View  | FAR Safety Author Role     |  |
| View Trellis         | Add/Edit Trellis View  | FAR Safety Author Role     |  |
| View View Selector   | Add/Edit View Selector View  | FAR Safety Author Role     |  |
| Write Back           | Manage Write Back FAR Administrator Role, BI Servic<br>Administrator |                            |  |
| Write Back           | Write Back to Database   | Denied: Authenticated User |  |

- 4. To set Catalog Folder-level Permissions:
  - **a.** Login to Analytics.
  - b. Go to Catalog > Shared Folders > Tasks > Permissions. The Permissions dialog box appears.
  - c. Set the Permissions as follows, and click OK.

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

**Note:** Make sure the **Apply permissions** option for the sub-folders and the items is NOT selected.

**d.** Go to Shared folders > Argus Safety > Tasks > Permissions.

The Permissions dialog box appears.

e. Set the Permissions as follows, and click OK.

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

**Note:** Make sure to select the **Apply permissions** option for the sub-folders and the items.

- 5. To add the Data Sources to Roles in BI Publisher:
  - **a.** Login 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.
- Repeat the steps to asbip data source to FARSafetyAuthorRole and FARSafetyConsumerRole as well.

### 13.8 Uploading the Argus Safety.xdrz file to BI Publisher

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 Installation Media>\SUPPORT\BIP

**2.** Log in to BI Publisher using BI Admin User credentials. This displays the BI Publisher Home Page as depicted in the following figure:

| ORACLE BI Publisher                                    | Interprise  | Search All | - <u>-</u>   | O Abreatrator | Hel- Spice C                             |
|--|---|------------|--------------|---------------|--|
| Reter  |   |            | Hume Cetalog | Sterr Date    | <ul> <li>Specific Augilitie =</li> </ul> |
| Create Facur 1 And | Procest           Recent           Others           Others           Stream Recent Research |            |              |               |  |

#### 3. Click Catalog.

| DRACLE BI Publisher        | Enterprise       | South M. | -            | O Abrestatur Heli-   San Dut C       |
|----------------------------|------------------|----------|--------------|--------------------------------------|
| Ruter                      |                  |          | Hume Catalog | 📲 fore = 🔰 Cont =   Specificka place |
| Create                     | Secent           |          |              |                                      |
| Report Jab                 | Record Reports   |          |              |                                      |
| Carta Madel                | Others           |          |              |                                      |
| Browse/Manage              | Univers          |          |              |                                      |
| Report Jobs                | Favorites Manage |          |              |                                      |
| Get Started                | 5.5 million      |          |              |                                      |
| Page Curtante              |                  |          |              |                                      |
| Cracle Technology Tertwork |                  |          |              |                                      |

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

4. Click Shared Folders under Folders.

| DRACLE BI Publisher Enterprise |   | Search 📶 💦 💼 🚺 💽 Administration   Help = _ Sign Out. 📿 |   |  |
|--------------------------------|---|--|---|--|
| Catalog                        |   |  | turne Catalog 😰 hen - 🔝 Queri - Squediti Ar Jah |  |
| 9-19 0 8 K.O.D                 | 1 & Lucion Berelfahre   | Ockepanizaningaz                                       |   |  |
| Folders                        | Companients  Last Modified 8/20/14 2:57 AM   Created By<br>Econd   More-<br>Doord   More- |  |   |  |
|                                |   |  |   |  |
|                                |   |  |   |  |
| 🛛 Tasks                        |   |  |   |  |
| Tasks                          |   |  |   |  |
|                                |   |  |   |  |

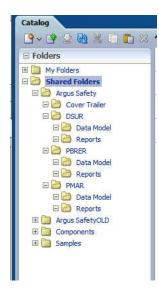
#### 5. Click Upload under Tasks.

| Oracle  |  | Home Catalog 🎦 New | 👻 📮 Open 🐃 Signed In As-orcladmin 🗠 |
|---|--|--------------------|-------------------------------------|
| 9 - 🕑 🙅 📵 🚜 💷 🗅 👂   | K 😵 🗸 Location /Shared Folders   | <b>(</b>           | (                                   |
| Folders   | Argus Intelligence  Last Modified 7/9/12 4:12 A<br>Development<br>Expand   More* |                    |                                     |
| Shared Folders      Argus Inteligence      Components      EVT1 | Components   Last Modified 6/13/12 6:32 AM   C<br>Expand   More*                 | reated By          |                                     |
|   | ENT1   Last Modified 8/21/12 1:27 AM   Created By<br>Expand   More*              | y orcladmin        |                                     |
| ENT2     ENT2     Entrained                                     | ENT2   Last Modified 8/21/12 1:29 AM   Created By<br>Expand   More *             | y orcladmin        |                                     |
|   | Samples   Last Modified 6/13/12 6:32 AM   Create<br>Expand   More*               | td By              |                                     |
|   |  |                    |                                     |
|   |  |                    |                                     |
|   | •  |                    |                                     |
| Tasks   | =  |                    |                                     |
| Argus Intelligence  | -  |                    |                                     |
| 🖄 Expand 🛛 📑 Upload   |  |                    |                                     |
| 🗙 Delete 🛛 💆 Download   |  |                    |                                     |
| Copy 🔏 Cut  |  |                    |                                     |
|   |  |                    |                                     |
| Permissions B Properties  |  |                    |                                     |

This displays the Upload dialog box.

| Upload                  |      |        |        | ×      |
|-------------------------|------|--------|--------|--------|
| Upload                  |      | Browse |        |        |
| Overwrite existing file |      |        |        |        |
|                         |      |        |        |        |
|                         |      |        |        |        |
|                         | <br> | 6      |        | 1      |
|                         |      |        | Upload | Cancel |

- **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. Once done, an Argus Safety folder is created in Shared Folders.
- **8.** Expand the **Argus Safety** folder to verify whether the following data model and reports are present. It should look as shown below:



# 13.9 Integrating Argus Safety with BI Publisher

Perform the following steps for Argus Safety Web server configuration:

- **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.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* 

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.

6. The following URLs need to be excluded from SSO (if SSO is enabled):

*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* 

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

**a.** Add excluded resource (/xmlpserver/services and /xmlpserver/report\_service) on OAM Server for the OBIEE/BIP server application domain.

| icy Configuration System Configuration   |   |   |   |              |  |   |
|--|---|---|---|--------------|--|---|
| u 🕞  | Welcome @ slc0_11                                     | wg Resources                                    |   |              |  | ×   |
| () Search  | slc0_11wg Resources                                   |   |   |              |  | New Resource                              |
| Browse Search  |   |   |   |              |  |   |
| Vev & C C C C C C C C C C C C C C C C C C  | Resource Type HTTP<br>Host Identifier<br>Resource URL |   | Query String<br>Authentication Policy<br>Authorization Policy             | ×            |  | Search Reset                              |
| G Application Domains  | Actions - View -                                      |   | 2 / ×   |              | 🛃 Detach   |   |
| G Al80QAWebgate     G Argus71webgate     G Fusion Apps Integration     G Fusion Apps Surte | 1 HTTP d<br>2 HTTP d                                  | ost Identifier<br>c0_11wg<br>c0_11wg<br>c0_11wg | Resource URL<br>//*<br>/xmlpserver/services<br>/xmlpserver/report_service | Query String | Authentication Policy<br>Protected Resource Policy | Authorization Polic<br>Protected Resource |
| Gisi (nal22) witho     a Gisi (nal22) witho     a Gisio (nal22) witho     b Resources      |   | C0_1100   | /   |              | Protected Resource Policy                          | Protected Resourc                         |

**b.** 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/* 

c. 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>

**d.** Save the file and restart OHS Service.

# 13.10 Argus Console-level Configurations

To enable execution of the BI Publisher reports from Argus Safety UI, configure the following console settings:

- 1. Navigate to **Argus Console** > **Enabled Modules**.
- 2. Enable the **BIP Aggregate Reports** module.
- **3.** Add **iisreset on webserver** to ensure that the changes made to enable the **BIP Aggregate Reports** module are visible.
- 4. Navigate to Argus Console > System Configuration > Common Profile Switches.
- 5. Expand the **Reporting** node on the tree that appears on the left pane.
- 6. Click BIP Aggregate Reporting.

| Code Lists  | Business Configuration    | Access Management         | System Configuration            | Tools |  |
|---|---------------------------|---------------------------|---------------------------------|-------|--|
|   |                           |                           |                                 |       |  |
| COMMON PROP   | FILE - BIP Aggregate Repo | orting                    |                                 |       |  |
| Browser   |                           | Modify Reporting BIP Aggr | egate Reporting                 |       |  |
| Browser<br>Organized by Con<br>Common Prof<br>Advances<br>a Argus bas<br>Case Pror<br>Case Pror<br>Case Pror<br>Case Pror<br>Document<br>Case Pror<br>Document<br>E28<br>Argus Labe<br>Med/Vatch<br>Reporting<br>BIPA<br>Expec<br>Expec<br>Expec<br>Expec<br>Expec<br>Expec | nmon Profile              | 1 March 1997              | rd (• Yes<br>CNo<br>data of BIP |       |  |
| 🚞 Single Sig<br>🚞 User Inter  | 222.22                    |                           |                                 |       |  |
| 🚞 Workflow  |                           |                           |                                 |       |  |

- 7. In the **BIP Common User** and **Password** fields, enter the username and password of a BI Publisher user having administrative permissions. Save the changes. Make sure that the BI Publisher User added here is not same as that of an actual Argus user. It can be a user which is available only for BI Publisher, with complete administrator privileges.
- **8.** Set the Persist data in BIP Aggregate Temp tables to Yes or No. The default value is No.
- **9.** Set the Number of days to persist the BIP Aggregate Temp table data. Defaulted to null.

**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.

### 13.11 Configuring Code Lists

For BI Publisher Reports to be run from Argus Safety, the BI Publisher Report template path in the BI Publisher Server to be configured.

Execute the following steps to configure the report template path in Argus Safety:

- 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 Linux and Unix, 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.

### 13.12 Creating the Database Jobs

A database job must be created for polling the BI Publisher repository tables. It is up to the requirement of the customer to set up the interval based on the need.

The following example explains creating a job that would run every 3 minutes.

/\*Database job that would repeat for every 3 minutes. This job will execute the procedure pkg\_ agg\_rpt\_util.p\_fetchrptoutput, which will pull the BIP Output from the BIP Server into the Argus Database.\*/

DECLARE

n BINARY\_INTEGER;

BEGIN

DBMS\_JOB.SUBMIT (job => n,

what => ' BEGIN

pkg\_agg\_rpt\_util.p\_fetchrptoutput; END ;',

interval => 'TRUNC(SYSDATE + 3/1440,"MI")',

no\_parse => FALSE);

DBMS\_OUTPUT\_PUT\_LINE('Job Number is: ' | | to\_char(n));

COMMIT;

END;

/

Another database job is created to purge the data from the RM tables:

/\*Database job that would repeat for every 3 minutes.This job will execute the procedure pkg\_agg\_rpt\_util.Purge\_RM\_Data, which will purge the data from RM tables \*/

DECLARE

n BINARY\_INTEGER; BEGIN DBMS\_JOB.SUBMIT (job => n, what => ' BEGIN pkg\_agg\_rpt\_util.Purge\_RM\_Data; END ;', interval => 'TRUNC(SYSDATE + 3/1440,''MI'')',

```
no_parse => FALSE);
DBMS_OUTPUT.PUT_LINE('Job Number is: ' | | to_char(n));
COMMIT;
END;
/
```

Both the database jobs should be created and run as BI Publisher Schema User.

### 13.13 Upgrading Flexible Aggregate Reports from 8.0 to 8.1

This section comprises the following:

- Upgrading Argus Safety Database from 8.0 to 8.1 for FAR
- Upgrading BI Publisher Periodic Reports from 8.0 to 8.1 for FAR

### 13.13.1 Upgrading Argus Safety Database from 8.0 to 8.1 for FAR

To upgrade the Flexible Aggregate Report from 8.0 to 8.1 in Argus Safety Database > BIP\_OWNER Schema:

- **1.** Go to C>:\Program Files\Oracle\Argus\DBInstaller\utilities\BIP\_Upgrade.
- 2. Double-click the Argus\_BIP\_Upgrade.bat file.
- 3. Enter TNSNAMES Entry to Connect to the Argus Safety Database.
- Enter DBA user name in &argus\_db. Database.
   For example, enter system.
- 5. Enter password for the DBA user.
- 6. Press Enter to Continue.
- 7. Enter Argus schema owner name.

For example, enter **argus\_app**.

- 8. Enter Argus schema owner password.
- **9.** Enter BIP schema owner name.

For example, enter **bip\_owner**.

- 10. Enter BIP schema owner password.
- 11. Press Enter.
- **12.** If you are unable to connect successfully to the database using **bip\_owner**, review the log file for any errors.

### 13.13.2 Upgrading BI Publisher Periodic Reports from 8.0 to 8.1 for FAR

Refer to the Section 13.8, "Uploading the Argus Safety.xdrz file to BI Publisher."

# **Installing End of Study Unblinding**

This chapter describes the minimum hardware/software requirements and the installation procedures for the End of Study Unblinding (EOSU) utility. It includes the following sections:

- EOSU Hardware/Software Requirements
- How to Install the EOSU Utility

# **EOSU Hardware/Software Requirements**

The following table lists the minimum Hardware and Software required to install End of Study Unblinding:

| Requirement Type    | Description   |
|---------------------|---|
| Hardware            | Refer to the Hardware requirements for Argus Safety 8.1                         |
| Database Server     | (Same requirements as Argus Safety 8.1 Database Server)                         |
|                     | A Tablespace with 500MB free space to create EOSU Schema                        |
|                     | Argus 8.1 schema (This is a prerequisite for the EOSU package to be installed.) |
| Client Machine      | Microsoft Windows 7 (32-bit) (English and Japanese)                             |
|                     | Oracle Client 12.1.0.2  |
|                     | Oracle ODAC 12.1.0.2  |
|                     | Microsoft .NET 3.5 SP1 Framework  |
|                     | Visual C++ 2012 Runtime   |
|                     | Pentium III 1.5 GHz Minimum (Pentium IV 2.0 GHz recommended)                    |
|                     | 512MB RAM Minimum (1GB RAM recommended)   |
|                     | 4GB free hard drive space Minimum (10GB recommended)                            |
|                     | 256 Colors Minimum (64K Recommended)  |
|                     | MS-Office 2010 and 2013   |
|                     | Adobe Acrobat Reader v9.3.4   |
| INIT.ORA parameters | In addition to Argus, make sure to set the following parameter as shown below:  |
|                     | AUDIT_TRAIL=TRUE  |

# How to Install the EOSU Utility

Use the following procedure to install the EOSU utility:

- 1. Copy the installation package files to your local directory and start Launch.exe.
- 2. When the Welcome dialog box opens:
  - Click Argus Safety.
- **3.** When the Argus Safety Setup wizard opens the Argus Safety Setup dialog box:
  - Click Next to continue.
- **4.** When the wizard opens the Customer Information dialog box: Enter the User Name and Company Name. Click **Next**.
- **5.** When the wizard opens the Components Default Directory dialog box: Choose the appropriate folder to install the EOSU Generic software and click Next.
  - Click Browse to locate and select the default directory where EOSU will be installed.
  - Click Next to continue.
- 6. When the wizard opens the Argus Safety Solution Components dialog box:
  - Select **End of Study Unblinding Module** and click **Next** to begin the actual installation.
  - Click Next to continue.
- 7. Argus installs and shows the progress of the installation.
- 8. When the wizard opens the Setup Complete dialog box:
  - Click Finish to exit the Installation program. Argus-EOSU Interface utilities can now be executed.
- **9.** You can now run the Argus EOSU Interface utilities.

Setup has installed an Operations Guide and scripts to create Database schema on your computer. Refer to the Operations Guide to create a new schema to start using EOSU software. The document is in the following directory:

<Installation Folder>\Oracle\End of Study Unblinding\ARGUS\_EOSU.pdf

Alternatively, you can also go select Start > Programs > Oracle > End of Study Unblinding > Documentation > End of Study Unblinding Module to view the documentation.

**Note:** When EOSU is installed alone, the user is asked to select the temporary path and update the Argus.ini 'UploadedLetters' parameter. This parameter uses this same path that is entered as the temporary path by the user.

**Note:** After installing the EOSU utility, refer to the section The Argus Safety 8.1 Application Servers to set up the Argus Cryptography key.

# 15

# **Other Tasks**

This chapter provides information for performing other installation and configuration tasks. It includes discussions of the following:

- Configuring the Argus.xml File
- Configuring the Argus.ini File
- Configuring SSO in Oracle Access Manager 11g
- Installation and Configuration of Oracle Web Tier Suite
- Configuring the WebCenter Security Provider for Identity Assertion
- Installation Maintenance Tasks
- Web Client Tips
- Clearing Oracle Temp Files
- Configuring easyPDF
- Setting Printer Defaults

# Configuring the Argus.xml File

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

<Argus Installation Path>/ArgusWeb/ASP

The Argus.xml file contains two types of xml tags as described in the following table:

| XML Tag                     | Description   |
|-----------------------------|---|
| <argus_db></argus_db>       | This tag 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.</argus_db>         |
|                             | For example, for a database that is recognized as "Testing Database"<br>in Argus Web Login screen and whose alias in the Oracle<br>TNSNAMES.ORA file is "TESTDB", the entry will be |
|                             | <dbname id="TESTDB">Testing Database</dbname> .   |
| <license_key></license_key> | This tag contains the License Key value for the Argus application.<br>Do not update this key unless Oracle Customer Support instructs<br>you to do so.                              |

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

# Configuring the Argus.ini File

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

With some exceptions, the parameters listed in Table 13-2 are used by Argus Web as well as AG Service. However, some are specific to the Web and some are specific to the Transactional (AG) Server

Parameters specific to the Web Server are:

- MessageCachePath
- Upload
- Template
- ArgusInstallPath
- Timeout
- DB Connection
- Pooling parameters.

Parameters specific to the Transactional (AG) Server are:

- PrintRunTime
- PrintService

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

| # | Section     | Parameter         | Sample Value   | Description  |
|---|-------------|-------------------|--|--|
| 1 | Workstation | Cache             | c:\ArgusReports\PDFRe<br>ports\                              | This is the path for PDF Reports<br>(Expedited/Periodic/Screen Prints<br>etc.). In case of multiple web servers,<br>this is a shared path on the network.                              |
| 2 | Workstation | MessageCachePath  | c:\ArgusReports\Messag<br>eCache\                            | This is the shared path to save the<br>system level cache such as data for LM<br>tables, CMN Fields, etc. In case of<br>multiple web servers, this is a shared<br>path on the network. |
|   |             |                   |  | For use with Web Server.   |
| 3 | Workstation | Upload            | c:\ArgusReports\Upload<br>edLetters\                         | This is the shared path for uploaded<br>letters. In case of multiple web servers,<br>this is a shared path on the network.   |
|   |             |                   |  | For use with Web Server.   |
| 4 | Workstation | Template          | C:\Program<br>Files\Oracle\E2BViewer<br>\Templates\          | This location stores the template and report files used to display CIOMS and MedWatch views.   |
|   |             |                   |  | For use with Web Server.   |
| 5 | Workstation | AcrobatReaderPath | C:\Program<br>Files\Adobe\Acrobat<br>7.0\Acrobat\Acrobat.exe | This is the path to the Acrobat Reader exe file.   |

| #  | Section      | Parameter                  | Sample Value                         | Description  |
|----|--------------|----------------------------|--------------------------------------|--|
| 6  | Workstation  | HELP                       | C:\App\Oracle\Docume<br>ntation\     | This is the base folder where all the files related to various modules of Argus are placed.  |
| 7  | Workstation  | PrintRunTime               | 10                                   | This is used by the AG Service Print<br>Utility. It specifies how often the Print<br>Utility shall run to print reports to the<br>printer. The unit is in seconds.   |
|    |              |                            |                                      | For use with Transactional (AG) Server.  |
| 8  | Workstation  | PrintService               | 1 or 0                               | This is also used by AG Service Print<br>Utility. When this is set to 0, the AG<br>Service Process Bulk Transmit Print,<br>generates the report and directly prints<br>the report to the printer. If set to 1, the<br>Bulk Transmit Process creates the PDF<br>in the Cache folder with an associated<br>Batch file. |
|    |              |                            |                                      | The Print Utility then picks up the<br>Batch File, prints the PDF to the printer<br>and deletes the Batch Job File.  |
|    |              |                            |                                      | For use with Transactional (AG) Server.  |
| 9  | Workstation  | ArgusInstallPath           | C:\Program<br>Files\Oracle\ArgusWeb\ | This refers to the path of the location where the ASP files are placed.  |
|    |              |                            | ASP\                                 | For use with Web Server.   |
| 10 | Workstation  | SCANNED_<br>IMAGES         | C:\Temp\Scanned_<br>Images           | This is the location of files that are used<br>by the "New Case from Image"<br>functionality.  |
| 11 | PDFReports   | TempFileDeleteInter<br>val | 1                                    | This key specifies how often the Argus<br>Report Service should run to check for<br>files to delete. By default, this service<br>will delete files from paths specified<br>for "Cache" and "Upload" parameters<br>described above. The unit is in hours.<br>The default value is 1.                                  |
| 12 | PDFReports   | HoursBeforeDelete          | 24                                   | This key is used by Argus Report<br>Service. This key specifies in hours,<br>how old the file must be before it gets<br>deleted. By default, this service will<br>delete files from paths specified for<br>"Cache" and "Upload" parameters<br>described above. The default value is 1.                               |
| 13 | Argus Server | SQLTimes                   | 1                                    | This enables the Argus Web<br>application to start creating log files for<br>all the SQLs that are fired. These log<br>files are created in C:\Temp folder and<br>can be used for debugging.   |
| 14 | Argus Server | Pool_Initial_Size          | 3                                    | This refers to the DB Connection Pool<br>Initial Size.   |
|    |              |                            |                                      | For use with Web Server.   |
| 15 | Argus Server | Pool_Maximum_<br>Size      | 120                                  | This refers to the DB Connection Pool Maximum Size.  |
|    |              |                            |                                      | For use with Web Server.   |
|    |              |                            |                                      |  |

| #  | Section      | Parameter                 | Sample Value | Description   |
|----|--------------|---------------------------|--------------|---|
| 16 | Argus Server | Connection_Time_<br>Out   | 120          | This refers to the time out time in seconds. The connection times out if it is idle for the given time.   |
|    |              |                           |              | For use with Web Server.  |
| 17 | Argus Server | Connection_Wait_<br>Time  | 3            | This refers to the connection wait time<br>in seconds. An exception occurs if the<br>system cannot obtain a DB connection<br>in the given time.                       |
|    |              |                           |              | For use with Web Server.  |
| 18 | Argus Server | PeriodicRptMaxRun<br>Time | 60000        | This refers to the setting in the<br>Argus.ini file that allows you to<br>override the default Argusvr2a EXE<br>timeout setting to approximately 16<br>hours (60000). |

Use the following procedure to configure Argus.ini:

- **1.** Select Start > Run.
- 2. When the Run dialog box opens:
  - Type argus.ini in the **Open** field.
  - Click OK.
- **3.** When the Argus.ini file opens, set the entries in the file to the required values as described in the previous Table.
- **4.** Save the file.
- **5.** Restart the Internet Information Services (IIS) on the server so the changes will take effect.

### Increasing the Internet Explorer Timeout Setting to Run Reports

There can be a problem in running Periodic or System Reports if the Internet Explorer (IE) Setting is set to its default value of 4 (hours) on the Client machine.

Follow the steps listed below to increase the IE Timeout Setting (and thereby run Reports successfully):

- **1.** Start the Registry Editor on the IE client machine.
- 2. Locate the following sub-key: HKEY\_CURRENT\_ USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings.
- **3.** In this sub-key, add the following DWORD entries with 14400000 (4 hours):
  - KeepAliveTimeout
  - ReceiveTimeout
  - ServerInfoTimeout
- **4.** Restart the computer.

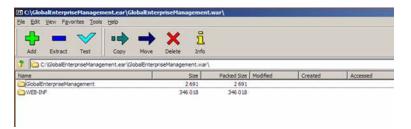
# Deploying a Portlet on Oracle WebLogic Server

To deploy the portlets to the Oracle Portal Server, navigate to the Portlet Installation folder on the Web Server where the module was installed. Perform the following steps for each Portlet being installed.

**1.** Open the .ear file using a Zip utility. The zip program will open with files as seen below.

| 🕂 🗕 🌱                           | •         | ×      | i     |             |                |         |
|---------------------------------|-----------|--------|-------|-------------|----------------|---------|
| Add Extract Test                | Copy Move | Delete | Info  |             |                |         |
| 🌮 📕 C: \GlobalEnterpriseManager | nent.ear\ |        |       |             |                |         |
| Name                            |           |        | Size  | Packed Size | Modified       | Created |
| META-INF                        |           |        | 870   | 870         |                |         |
| GlobalEnterpriseManagement.war  |           | 35     | 2 753 | 352 753     | 2010-10-26 10: | 52      |

**2.** Double click the .war file and you will see the following screen. Double Click the WEB-INF folder.



**3.** Double click the file **portletname.properties** where portletname is the name of the portlet ear file under modification.

| Add Extract Test Copy                 | Move         | X<br>Delete | 1<br>Info  |             |                  |         |          |    |
|---------------------------------------|--------------|-------------|------------|-------------|------------------|---------|----------|----|
| 1 C:\GlobalEnterpriseManagement.ear\  | RobalEnterpr | iseManager  | nent.war\/ | VEB-INF\    |                  |         |          |    |
| Name                                  | 21           |             | Size       | Packed Size | Modified         | Created | Accessed | At |
| dasses                                |              |             | \$ 196     | 5 196       |                  |         |          |    |
| b                                     |              | 1           | 2 256      | 12 256      |                  |         |          |    |
| wsd                                   |              | 22          | 0 181      | 220 181     |                  |         |          |    |
| GlobalEnterpriseManagement.properties |              |             | 164        | 164         | 2010-10-25 15:54 |         |          |    |
| WSRP_v1_Service-java-wsdi-mapping.xml |              | 3           | 0 146      | 30 146      | 2010-10-26 10:52 |         |          |    |
| WSRP_v2_Service-java-wsdl-mapping.xml |              | 4           | 2 200      | 42 200      | 2010-10-26 10:52 |         |          |    |
| 🕆 oracle-portiet.xml                  |              |             | 531        | 531         | 2010-10-18 14:03 |         |          |    |
| oracle-webservices.xml                |              | 1           | 3 999      | 13 999      | 2010-10-26 10:52 |         |          |    |
| portlet.xml                           |              |             | 1881       | 1881        | 2010-10-18 14:03 |         |          |    |
| * standard-webservices.xml            |              | 1.2         | 4 963      | 4 963       | 2010-10-26 10:52 |         |          |    |
| * web.xml                             |              | 1           | 3 454      | 13 454      | 2010-10-18 14:03 |         |          |    |
| weblogic.xml                          |              |             | 516        | 516         | 2010-10-26 10:52 |         |          |    |
| wsrp_mime_cs_mappings.properties      |              |             | 531        | 531         | 2010-10-26 10:52 |         |          |    |

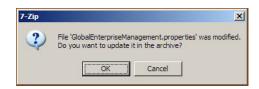
**4.** In the editor find the key named "ArgusURL" and modify the URL value to the value of your Argus Web Server or Argus Web Load Balancer.

ArgusUrl=http://10.178.91.250:8083. For OAM integration, Oracle recommends that using the FQDN of the machine.

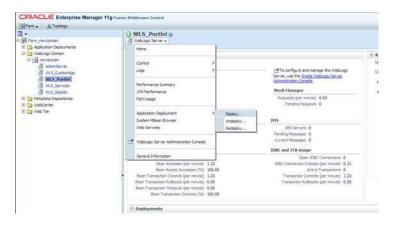
| cation, to be<br><10.0.0.0:77 |     | he dropdown | list on glo | bal application | access portlet |
|-------------------------------|-----|-------------|-------------|-----------------|----------------|
| (10.0.0.0.0.77                | //> |             |             |                 |                |
|                               |     |             |             |                 |                |
|                               |     |             |             |                 |                |

**Note:** Make sure there is no space between the tokens "ArgusUrl", "=" and the actual URL value.

**5.** Save the changes to the properties file and close it. Close the 7-zip manager window and press OK to save the changes in the archive. You are now ready to deploy the ear file.



 Log in to the Oracle Enterprise Manager Admin Console and navigate to WebLogic Domain>Your Domain>WLS\_Portlet. From the top left corner, navigate to Weblogic Server >Application Deployment>Deploy.



**7.** Select **Archive is on the machine where this web browser is running** and click **Browse**. Browse to the modified .ear file on your local machine.

| ORACLE Enterprise Manager 11g Fusion Middlewaya Control   |  |
|---|--|
| Q WLS_Portlet (trade tretcop: terrer) @ : Deploy Java EE Applic   | ation  |
| Select Archive Select Target Appliance Attributes Deployment Settings   |  |
| Select Archive (2)  |  |
| Specify the application or the exploded directory. Optionally you can specify a deployment:   | plan.  |
| Archive or Exploded Directory   |  |
| Java EE ardive, vivib Modules (WAR fles), EIB Modules (EJB JAR fles) and Resource Adaption  | pter Hollules (RAIL files) can be deployed. You can also deploy an exploded archive that is present on the server vitwre Enterpris   |
| If widwe is on the mediane where this web browser is running.   | Ardhive Location   |
| C1GbbalUverManagement ear   | (Grupp.)   |
| C Archive or exploded directory is on the server where Enterprise Manager is running.   |  |
|   | Broom  |
| Deployment Plan   |  |
| The deployment plan is a file that contains the deployment settings for an application. You not have a deployment plan, one will be created automatically during the deployment proce | can use a previouals seved deployment plan for the application Later in the deployment process, you can optionally edit the depl<br>eas when deployment configuration is done. |
| P: Depice a new deployment plan when deployment configuration is done. C Deployment plan is on the machine where this web browser is running.   |  |
|   | (Drawn, )  |
| C Deployment plan is on the server where Enterprise Manager is running.   |  |
|   | franse   |

**8.** The Portlet will now get uploaded to the server.



**9.** Once the Portlet is uploaded, by default **WLS\_Portlet** will be selected. If not then select and click **Next**.

| Argn   | e Select Target Appicator            | Attributes Deployment Settings                   |   |
|--------|--------------------------------------|--|---|
| lert T | arget                                |  |   |
| AL D   | mage                                 |  |   |
|        | Weeks show man has be of sides these | t you mant this application to be deployed       | and for   |
|        |                                      | Type   | Deployed Applications   |
| dian's |                                      |  |   |
| Select |                                      |  |   |
| r      | AdminServer                          | Oracle Webliogic Server                          | DMS Application(11.1.1.1.0), PMW Welcome Page Application(11.1.0.0.0), Non22EManagement(11.1.1), em, wol-wis  |
| Г<br>Г | AdminServer<br>WLS_CListomApp        | Oracle WebLogic Server<br>Oracle WebLogic Server | DMS Application(11.1.1.10), PMW Welcome Page Application(11.1.0.0.0), Non32EDManagement(11.1.1), em, wal-wis<br>DMS Application(11.1.1.10), TestGHP, resl-wis |
| L L Q  | AdminServer                          | Oracle Webliogic Server                          | DMS Application(11.1.1.1.0), PMW Welcome Page Application(11.1.0.0.0), Non22EManagement(11.1.1), em, wol-wis  |
| Г<br>Г | AdminServer<br>WLS_CListomApp        | Oracle WebLogic Server<br>Oracle WebLogic Server | DMS Application(11.1.1.10), PMW Welcome Page Application(11.1.0.0.0), Non32EDManagement(11.1.1), em, wal-wis<br>DMS Application(11.1.1.10), TestGHP, resl-wis |

**10.** Do not change the default selection. Click **Next.** 

|   | anager 11g Fusion Middlewark Control   |  |
|---|--|--|
| WLS_Portlet (Drade Vietz.                   | opctarion) @ : Deploy Java EE Application  |  |
| ect Ardhie Select Target Applica            | Rum Attributes Dephysion Settings  |  |
| pplication Attributes 🕲                     |  |  |
| Arthree Type 3ar                            | a EE Application (EAR file)  |  |
|   | ballaeMaragement.sar   |  |
| Deployment/Ren Gre<br>Deployment Target Vit |  |  |
| Consideration on Adv. and                   | 2 and and a set of the |  |
| * Application Name                          | QuobalCare Management  |  |
|   |  |  |
| Context Root of Web Hodules                 |  |  |
| Web Nockie                                  | Context Root   |  |
| GoballiseManagement.war                     | Gidal.txerNaragement   |  |
| Destribution                                |  |  |
|   | ef Reachure and teat apólication (servicing all requests)<br>C' Datoble and start apólication in administration reade (servicing only administration requests)<br>C' Datoble and   |  |
| Other Options                               |  |  |
| Searce Accessibility                        | 🥙 Use the defaults defined by the deployment's targets. Recommended selection.   |  |

**11.** Click **Deploy** on the last screen to publish the Portlet. Verify that the Portlet was deployed successfully in the Status.

| ORACLE Enterprise Ma  | inager 11g Panish                     | Diddeware Centrel  | ND •                      |
|---|---------------------------------------|--|---------------------------|
| Q WLS_Portlet Cruck man   | pclarery @ 1 Dep                      | loy Java EE Application  | 0                         |
| Denot Andree Select Tarper Application  | Depkyn                                | -61<br>and Settings  |                           |
| Deployment Settings   |                                       |  | Canoni Step + of + Depter |
| Arthine Tapes, Janes<br>Arthine Lacentern, Galo<br>Deployment Nam, Gree<br>Deployment Targert, 1963 | al.herMaragenent.aur<br>de a nen plan | <ul> <li>Application have: Global and Application<br/>Instant: Not analyzed<br/>Control Hall Global and Applications (service) of instantiol<br/>Optimized Trains (Service) and analyzed (service) of instantiol<br/>Optimized Trains (Service) (service) of instantiol<br/>Optimized Trains (Service) (service) of instantiol<br/>Optimized Trains (Service) (s</li></ul> |                           |
| Depleyment Tasks  |                                       |  |                           |
| The table below lats common tasks that  | you may wait to do be                 | Are diskung te kakatan   |                           |
| Name<br>Configure Visió Modules<br>Configure Application Security                                   | So to task                            | Geologian<br>Cardiga t Teunis mikiet in yan Xadiatan.<br>Cardigara Katalan polis myakan, ondertain mgatain and alter security betwee.  |                           |
| (Corpleyment Plan<br>Tau can appointly use the Edit Deploym<br>                                     | ent Pan option to set n               | nne altannad digin-meri aktore uhdo the digilument lasia allove di not cove  |                           |
| fau lan aptonaly seve the diployment<br>Save Diployment Plan  | t plan to your local dale.            | ter an radiality the application later, and your as not depresent plan and not too to add the diploment plan.  |                           |

# Deploying the Global Home Application on a WebLogic Server

### **Configure Global Homepage Properties File**

To update the Global Homepage Properties file:

Specify the SSO Header Key

This Key is used to show User Full Name on the Global Homepage.

Specify the Help URL

Update this property with the Argus Web Server or the Argus Web Load Balancer URL. This URL path launches the online Help for the Global Homepage.

### **Update Global Homepage Properties File**

- **1.** Navigate to the Portlet Installation folder on the Safety Web Server where the module was installed.
- 2. Open the globalhomePage.ear file using a zip utility.
- 3. Open the GlobalHomePage.war file.
- **4.** Drill down through these folders:

```
WEB-INF > classes > Oracle > HSGBU > argussafety > ui > util
```

- 5. Open the argussafetyglobalhomeuibundle.properties in a text editor.
- 6. Update the SSO Header Key and HELP file path:

```
HTTPUserNameHeader=
HelpURL=
```

- 7. Save the changes to the properties file and close it.
- 8. Close the zip utility and save the changes to the archive.

### Deploy Company Logo

- 1. Navigate to the Portlet Installation folder on the Safety Web Server where the module was installed.
- 2. Open the globalhomePage.ear file using a zip utility.
- 3. Double-click the GlobalHomePage.war file.
- 4. Double-click the Images folder.
- **5.** Replace logo\_small.gif with your logo. Note that the File name should be logo\_small.gif.
- 6. Close the zip utility and save the changes to the archive.

### **Pre-Deployment Configuration**

Now, perform the following steps to deploy the global home application on the Weblogic Server.

Log in to the Enterprise Manager Admin console. In the left hand tree navigation, select WebLogic Domain>Your Domain>WLS\_CustomApp in the left hand tree navigation. The WLS\_CustomApp is the name of the server that we have created to deploy Global Home Page. Click the menu just below the name of the server as shown below. Navigate to Application Deployment > Deploy.

| State Atang   |  |   |  |               |                      |  |
|---|--|---|--|---------------|----------------------|--|
| 2-  | WLS_CentonApp-3  |   |  |               |                      | a state of the set                       |
| R California Cartanar   | - manage terver +  |   |  |               | Fair Meteriel 11/2L1 | DECLARATION PROPERTY                     |
| Image: Training and t | Anna Anna Anna Anna Anna Anna Anna Anna  | Afford and ensuite the things<br>and the second second second second second second<br>test and the second | <ul> <li>Impact of an and the second sec</li></ul> |               |                      | an a |
|   | E Producements<br>Application Digitighteente   |   |  |               | agaitheasts is       |  |
|   | and a state of the |   | line   | Activa Sesame | Time (re)            | -101,001                                 |
|   | III California Associatione  |   |  |               | 10.4                 | 4.00                                     |
|   | Primar   |   | 8  |               | 0.00                 | 1.00                                     |
|   |  |   |  |               |                      |  |

2. Log in to the Enterprise Manager Admin console. In the left hand tree navigation, select WebLogic Domain>Your Domain>WLS\_CustomApp in the left hand tree navigation. The WLS\_CustomApp is the name of the server that we have created to deploy Global Home Page. Click the menu just below the name of the server as shown below. Navigate to Application Deployment > Deploy.

|   | TO WLS, Contrandep 3   | Lagent was weldinger the Ministeries   | Stationen or |
|---|--|--|--------------|
| B ran, rectioner  | - 2 manuage (enver a   | Page Material Int B. (2010) 44   | Australia C  |
| 0         Statute Tabulances           0         Statute Tabulances | No forward being in the second | Index of lower for only on the control of the contr |              |
|   | II Productments<br>Application Deployments   |  |              |
|   | tant<br>a Calment Aphatem  | Jama Active Security Proceeding And Active   | n del        |
|   | Chalantinering   | 9 4 6.4  | 4.00         |
|   | (Competence)   | Q # 0.00   | 6.00         |
|   | () Paral Responded<br>Standards and Type   |  |              |

3. The following screen appears. Browse for the application. ear file and click Next.

| WIS Contraction (Contraction Contraction) (Contraction)   | Alben .  | -  |
|---|--|--|
| Select Arrive Select Sager automa internet Reporter Service   |  |  |
| Sedert Arthber 🗊<br>Sport Paugoson of the public literators. Spherik coulor pacify a business par-  |  | (Special Processing)   |
| Andres of Exploded Deservey   |  | (White-sales))   |
| an et ar vira, ter tradeci più fazi, 12 tradeci 23 all'hou antipago i nager ta<br>16 altere es de caster viene ta caste la biana e castego<br>E casterane e casterane e la caste caste antipago e castego<br>E casterane a castera i en ter antipago e bianza la biange e castego<br>E casterane a castera i en ter antipago e bianza la biange e castego | An a fair for an an Annual. You are not a water a value of a fair for a power or to go a value that you brook a come,  | Las the page to topic cleve II<br>aphotoxic Revice 2014<br>Annual Revice 2014 Annual<br>Annual Revice 2014 Annual<br>Annual Revice 2014 Annual<br>Annual Revice Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annual<br>Annu |
| BigBygenetil Plant<br>The payment part a site that some the Approximate settings for an approximation result of<br>the foreign approximate part, one of the particular setting for approximation provide planteer and<br>the Schwart set application and an other instantion of configuration and area.   | e or made and patients dails to the approximation of the approximation of the spin-sector part and are a the other approximation of the approximation of the approximation of the spin-sector of the approximation of the spin-sector of the approximation of the spin-sector of the sp | Hours application in red a 2014<br>chapter or 5 2004 roll as 2014<br>respective or 5 2004 roll as an A<br>respective or 5 2004 roll as a first<br>respective or 5 2004 roll and a first<br>respective of the Dealer franking from<br>the result of the Dealer franking from  |
| C September ( per 4 or the network where the unit income 5 million) C September ( per 4 or the prime must trading to those or contra-   | 2000   | Adventure Crists   |
|   |  |  |
|   |  |  |
|   |  |  |
|   |  |  |
|   |  |  |
|   |  |  |
|   |  |  |
|   |  |  |

4. Wait for the progressing dialog to finish.

| CREATE Enterprise Manager (1) insue instance insue<br>() WDL Contracting y successing time () Briefwy Insue () Applie attack<br>Network Manager () Strategy () Strateg |  |   |
|--|--|---|
| Next in each of the second action is the first of a second of the second action is the second of the     | ng manang ng mang mang mang mang mang ma   | A stream to the second |
| International Info   | Q Presents under Que transmission of Providence of Providence 2 Providence Providenc |   |

**5.** After modal dialogue is completed, you will see a screen for selecting targets. By default **WLS\_CustomApp** will be selected, if not then select and click **Next**.

| can't variant  |  | The second se  |
|--|--|--|
| lant for inside in the case that   | the last for and she is in factors   | da   |
| Abate News<br>F. Montpress<br>R. Mit Distances<br>R. Mit Johnson<br>T. Mit Schware<br>F. Wit Species | Tale<br>David Missingh Serve<br>Oracle Missingh Serve<br>David Missingh Serve<br>David Helitingh Serve<br>Dirac Hastingh Serve | Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Development<br>Develo |

6. Click the "pencil" icon in the Target Metadata Repository section.

| WIN Contractory  | Natagat Highware Workwark Leven<br>erentuge Securit is Deploy Janu EE Application  |  |
|--|--|--|
| mitailes and lage App  | and a state of the     |  |
| Application Attributes 3<br>Anno Trans<br>Anno | NAME & NOT THE OWNER   | (See ) (See ) the 1 of 1 (See ) (See ) |
| + had over here  |  |  |
| Content Start of Web Plantates   |  |  |
| Inter Martine  | Constant<br>Ser  |  |
|  | Cand A the section of the Assessment and the Section of the Merrier Is<br>and the section of the section of the Section of the Merrier Is<br>a three sections of the Section of |  |
| Color Information  | R (broth and drug eachann) serveryd e waardf.<br>C' Borlon an ef yn ywaarsen i'r aderbrenen hen gan gan anwyn an anwyn yw argenen ar yw ar yw ar yw ar yw ar yw<br>C' Borlon an e  |  |
| Stars Accessible   | # Epote abs/dcambio/dcambio/company/company/assesse<br>C (San The assesses on term) keys). Song Advances C in the value of an used of an used of a senger arm in its ship for galacteric a segme.  |  |

**7.** A modal dialog appears that allows you to specify the metadata repository for this application. Choose a metadata repository and click **OK**.

| 1) WIN Contractory  | rise Managar 119 house manager Larger<br>Street server or an Orphony Reen III Application   |  |                             |
|---|---|--|-----------------------------|
| And and and there is  | Applyants Printeres Party of Street   |  |                             |
| Apple stices Attributes   |   |  | Devel, det Tes Level, dame. |
| Advertised<br>Sectored Sectored S | tor Sr-L M Aphanes Dal No<br>No Sharestantan e<br>No Vana and de<br>Statute   |  |                             |
| * Automation (  | the state of the second s  |  |                             |
| Contrast Rand of State Inc.   |   |  |                             |
| Contract Rand of State Plan   |   | Notadata Reportance  |                             |
| Dres.   | - Bertill   | Sect the sectors remain a that the approach of its instruction.  |                             |
| terstadan.  | And<br>the second | Tom the Ball AND<br>Tom Determined<br>Proj Lamon (Roman And Appl<br>Toman and an Appl<br>Determined and Appl<br>Determined a |                             |
| Labor Operator  | ······································  | OK Grue  |                             |
|   | Cost in addition on the page Sequences, by N  | en fan an geen kalemend is yn en engel en wekk om de regislen er tegent.   |                             |

**8.** Specify the **partition** value. You may choose any value but Oracle recommends using the application name itself as the partition value. Click **Next**.

| WES Castronferty main   | Integer Tig Faster Mathemati Central<br>Tables Several (2) Complex Janua EE Application  |                                       |
|---|--|---------------------------------------|
|   | Construction of the second state   |                                       |
| Application Attributes 🐌  |  | (Dente) (Ann.) See 5474 (Bent) (Dente |
| Anton Tana Ja<br>Anton Jacobin Ja<br>Sastaneeri Tan Ja<br>Jaghaneeri Tangir Ja  | which is here update   |                                       |
| * Auduren fanne 1   | Server W   |                                       |
| Contrast Name of Work Providence  |  |                                       |
| tent Harten<br>Self-see   | Generation<br>Set  |                                       |
| 120   | kelA respectivo VII subano ( la la la subana da la subana da<br>Subana da la subana da subana da la subana da |                                       |
| Detrellutare  |  |                                       |
|   | # (person and and a partners person of a magnetic<br>Control on any and a partners of a decourter of the second of the magnetic second of<br>Control on any  |                                       |
| (-Other riphins   |  |                                       |
| The second | # Las no Arbite arbites) is the descendence again increases and exercise.<br>C (gen the second contexture) length through descendence the first of an ideal solution (a) to be reased an end in which the basis and a largest.   |                                       |
|   |  |                                       |

**9.** In the Configure ADF connections section, click **pencil** icon, you will be redirected to the Configure ADF connections screen.

| CRACLE Enterprise Manager Hig Seals Instances Cover<br>2 WLS, Castereday: Seals Security Research () 2 Deploy Java III. Application   |                         |
|---|-------------------------|
| Ben hele start og i kalter tillet bylgeret billeg   |                         |
| Deployment Settings   | Canal And Day of A Date |
| some tals level talsammeng fall for scalarshift of dealershift (2011)     when is call and and any any service of se |                         |
| Registrance Tanks<br>Na tala lata kan kan umum pan hai ya, nai na kalen dadu ng Na agkadan  |                         |
| Net         Of The         Design           Ordyn Life Name         Configer to the market or available or available.         Configer to the market or available or available.           Ordyn Life Name         Configer to the market or available or available.         Configer to the market or available.           Ordyn Life Name         Configer to the market or available or available.         Configer to the market or available.           Ordyn Life Name         Configer to the market or available or available or available.         Configer to the market of the market of the market of the market.  |                         |
| Charlensed Rei  |                         |
| 1 Manual  |                         |
| The initiality species and 42 <sup>th</sup> annucleus and granters are not and its the important pairs of the finance of the finance of the dust's and it the active that a superiord   |                         |
| No. or system to an No 100 Segment for yours is an over all anno lighteen splice with the Aphrone Gala data gives tool.   |                         |
| to provide one of a behavior of period on the test and the test and the extension of the send period of test test the behavior of per-<br>() and decomposition  |                         |
|   |                         |

**10.** In the Configure ADF connections screen, modify the web service connection. Click the **pencil** icon to edit the ADF connection settings.

| unfigure ADF Consections                |                                   |  | Cover, New York Ann |
|---|-----------------------------------|--|---------------------|
| TT Connections                          |                                   |  |                     |
| adapte for ADF president defined in the | reactions, and in this approxime. |  |                     |
| Canverbol Tape                          | hara .                            | Desister   | 64                  |
| Partial Producer: W287 Produce          | Confirmination agricult           | 1000 public product (product)<br>2000 public product (product)   | 1                   |
| THE PERSON NEW YORKS                    | State in a second second          | The second process second seco | 1                   |
| Institutions                            | Costal Astropol estimat           | Inthine was correction   | 2                   |

- **11.** A modal dialog comes where you can change ADF connections. You must modify the URL of the following fields to reflect the settings of your deployed portlets.
  - WSDL URL
  - WSRP\_v2\_PortletManagement\_Service
  - WSRP\_v2\_Markup\_Service
  - WSRP\_v2\_Registration\_Service
  - WSRP\_v2\_ServiceDescription\_Service

| Eveningume Adde Considernations   |   |  |             |                  |
|---|---|--|-------------|------------------|
| Constructions   |   |  |             | (() and () () () |
| All Capacital<br>Departs and another products and products<br>Constrained and an another products<br>Constrained and an another products<br>and an another products and an another products<br>and an | tara a<br>Internation data<br>International | ell for get antergener i esser<br>per contraction de la contractionede la contractionede la contractioned la contractioned | <br>Night I |                  |
|   |   |  | (A) (Ma)    |                  |

**12.** Click **OK** to close the modal dialogue and you will return to the parent screen. Click **Apply** in the top right corner. You will return to the deployment wizard screen 4 of 4. Click **Deploy**. The server will now deploy the ear file and report the success/failure status of the operation.

| WES_Contempore Mana                         | per Thig have dealers have been<br>no seen a Deploy Janua (E Application<br>damp formers around  |                       |                          |
|---|--|-----------------------|--------------------------|
| Configure ADF Connections                   |  |                       | Const., Ine. et 1 (Anth) |
| Configure the ACM connections defined to co | to the local sector and the sector of  |                       |                          |
| Donethel 1 MM                               | Name -   | Description           |                          |
| Barbar Barbara (1998) Barbara               | Transferration of the second sec |                       | 5                        |
| Unite and                                   | land) is post to approve the same  | Tell anne coversa     | 2                        |
|   | Children and Shares and state  | that we use overclose |                          |

# Configuring SSO in Oracle Access Manager 11g

This section describes how to configure SSO in the Oracle Access Manager (OAM) 11g. Following are the pre-requisites to this task:

- The system should have an OAM installation (Identity server, Access server, WebPass, Policy Manager).
- User profiles should exist in the LDAP server as well as in Argus with the same credentials.
- LDAP should be configured in the Argus Console.
- The LDAP flag should be set to ON for the users in Argus.

Perform the following steps to install SSO on the OAM:

 Navigate to the System Configuration tab of OAM and select the New OAM 10g Webgate link.

| Common Configuration   | Welcome OAM Agents ArgusInsight1  | 09  |  |
|--|---|---|--|
| Actions • View • 📑 🗁 % 🍓   | Welcome to Oracle Access Manager 11g  |   |  |
| E Available Services     Common Settings     Server Instances     Session Management | Use this console to     Manage the Access Manager policies already configured     Manage the agent profiles and server profiles of the cont     Register new applications that need single align-on intege     Manage and create trut between pathers for Oracle So | ligured Access Manager servers.<br>abon with Oracle Access Manager.<br>cunty Token Service. |  |
| <ul> <li>Access Manager Settings</li> </ul>  | Manage common settings and configuration for Oracle A   | ccess Manager and Oracle Security Token Service.  |  |
|  |   |   |  |
|  | Click any of the links below to start using the console. Alternat   | ively, you can use the navigation tree on the left as well.                                 |  |
|  | Click any of the links below to start using the console. Alternat   | wely, you can use the navigation free on the left as well.                                  |  |

2. The Create OAM 10g Webgate screen is displayed. Enter the name of the Webgate in the Name field and provide the password for the Webgate in the Access Client Password field. Click Apply.

| icy Configuration System Configuration  |  |                                 |
|---|--|---------------------------------|
|   | O Wekome Create OAM 10G Webgate  | X                               |
| () Search   | Create OAM 10G Webgate   | Apply                           |
| Browse Scarch   | *Name Argustafety11g Auto C  | Virtual host Context Policies 2 |
| Resource Type     Thirp     TokenServiceRP     Wi_suthen  | Access Clerk Password  Hoto Lidentifier  AccuSsfety Lig  User Ceffeed Drawner  |                                 |
| Host Identifiers E<br>AS702Dev<br>AS703CHP  |  |                                 |
| Argustnight7021<br>Argustnight702Dev<br>Argustnight702Dev   | *Seturly © Open<br>○ Smple<br>○ Cert   |                                 |
| Argustnieght002572<br>Argustnieght00257QA<br>Argustnieght0170132<br>Argustnieght0770132<br>Argustafety11g<br>Argustafety11g | Resource List Potentice Resource List Resour |                                 |
| ArgusSafety702MT<br>ArgusSafety702STQA<br>ArgusSafety702STQA<br>ArgusSafety8T70132<br>ArgusSafety8T70132<br>BU_OAM_INT      |  |                                 |

**3.** The following screen is displayed:

| Al 🔹  | and the second se | ArgusSafety1                               | 10 0       | ArgusSafety                      | 11g Resources | ArgusSi   | fety11g : Pro | tected Resource             | ce Policy 🚺 💁 ArgusSafety11g : I                 | Protected Resource Policy   |       |
|---|---|--|------------|----------------------------------|---------------|-----------|---------------|-----------------------------|--|---|-------|
| () Search   | ArgusSafety11g  | 1  |            |                                  |               |           |               |                             |  |   | Apply |
| Browse Search      Vew •      Other Search      Ver •      Parest Components      V      Resource Type                  |   | Access Client P<br>Primary Cookie          | assword •  |                                  |               |           |               |                             | Logout LRL                                       |   |       |
| © HTTP     © TokenSerViceRP     © Housther     V     ● Host Identifiers     >     ■ Austicative V Ide                   |   |  | Security @ | Open<br>Simple<br>Cert<br>Enable |               |           |               |                             | Deny On Not Protected<br>User Defined Parameters | proxySQHeaderVar=IS_SQ<br>URLINUTF8Format=true<br>dent_request_refry_attempts=1<br>mactiveReconfgPenod=10 |       |
| ▷ DAMSuiteAgent V Authentication Schemes  |   | * Max Cache I                              | lements    | Disable                          |               |           |               |                             | * Sleep for<br>Cache Pragma Header               | 60 🔹<br>no-cache  |       |
| AnonymousScheme<br>BasicScheme<br>BasicSessionlessScheme<br>BasicSessionlessScheme                                      |   | Cache<br>Max Con<br>Max Sea                | nections   | 1800 C                           |               |           |               |                             | Cache Control Header<br>Debug<br>3P Valdation    |   |       |
| KerberosSheme<br>LDAPNoPasswordValdationScheme<br>LDAPScheme<br>COAAMAdvanced   |   | * Palover T<br>* AAA Timeout T<br>* Prefer | reshold    | 1 0<br>-1 0                      |               |           |               |                             | Allow Management Operations                      |   |       |
| AAMBasic<br>AM10gScheme<br>AM10gScheme  | Server Lists  |  |            |                                  |               |           |               |                             |  |   |       |
| 01/Scheme   | Primary Server  | List                                       |            | + x                              | Secondary Se  | rver List |               | + x                         |  |   |       |
| > TAPScheme   | Server Name   | Host Name                                  | Host Port  | Max<br>Number of<br>Connecti     | Server Name   | Host Name | Host Port     | Max<br>Number of<br>Connect |  |   |       |
| Application Domains     Application Application     Gravitation Application     Gravitation Application     Gravitation | oan_server •  | sic02htf.us.or.                            | . 5575     | 1                                |               |           |               |                             |  |   |       |
| -   |   |  |            |                                  |               |           |               |                             |  |   |       |
|   |   |  |            |                                  |               |           |               |                             |  |   |       |

**Note:** Refresh the Host Identifier list to view the newly created Webgate within the Policy Configuration tab.

Provide details such as Primary Cookie Domain and Preferred Host, as shown above and click **Apply**:

- Primary Cookie Domain provide FQDN of the machine where you will install webgate, prefixed by a period. For example, .idc.<example.com>. Note the . before the FQDN.
- Preferred Host provide the IP Address of the Argus Web Server where you will install webgate.
- **4.** Expand the list of Application Domains and under this, expand the newly created Webgate.

Double-click on **Resources**. On the **Resources** screen, click the **Create** icon (displayed in the Search Results section, with the + symbol in red).

Create the resource type with the correct host identifier, as displayed in the following screen:

| •<br>③ Search   | Welcome Argus        |               | ArgusSafety11g Resource | s 🛛 🖟 ArgusSafety11g : | Protected Resource Policy | ArgusSafety11g : Prote    | ected Resource Policy | New Resource       |
|---|----------------------|---------------|-------------------------|------------------------|---------------------------|---------------------------|-----------------------|--------------------|
| Browse Search   | Argussurery ry Resor | acces         |                         |                        |                           |                           |                       |                    |
|   | Search               |               |                         |                        |                           |                           |                       |                    |
| Shared Components   |                      |               |                         |                        |                           |                           |                       |                    |
| Resource Type     Artitle   | Resource Type HTTP   | -             | Query String            |                        |                           |                           |                       |                    |
| TokenServiceRP  | Host Identifier      |               | Authentication Policy   |                        |                           |                           |                       |                    |
| @ nl_authen   | Resource URL         |               | Authorization Policy    |                        |                           |                           |                       |                    |
| Host Identifiers  |                      |               |                         |                        |                           |                           |                       | province and prove |
| ArgusSafety11g  |                      |               |                         |                        |                           |                           |                       | Search Res         |
| IANSuteAgent  |                      |               |                         |                        |                           |                           |                       |                    |
| Authentication Schemes  | Search Results       |               |                         |                        |                           |                           |                       |                    |
| AnonymousScheme<br>EasicScheme  | Actions - View -     |               |                         | 3 /                    | × ×                       |                           | Detach                |                    |
| BasicSessoriessSchene   | Resource Type Ho     | st Identifier | Resource URL            | Query String           | Authentication Policy     | Authorization Policy      |                       |                    |
| FAutiSchene   |                      | pusSafety11g  | 1]*                     |                        | Protected Resource Policy | Protected Resource Policy |                       |                    |
| Kerberos5cheme  | 2 HTTP Ar            | pusSafety11g  | 1                       |                        | Protected Resource Policy | Protected Resource Policy |                       |                    |
| Constraints     Constrain |                      |               |                         |                        |                           |                           |                       |                    |

5. Expand the Authentication Policies under the newly created Webgate.

Double-click the **Protected Resource Policy**. The following screen appears:

|  | 😡 Wekome 🔪 ArgusSafety11g 👘 🖉 ArgusSafety11g Resources 🔪 👼 ArgusSafety11g : Protected Resource | e Policy ArgusSafety11g : Protected Resource Policy |       |
|--|--|---|-------|
| () Search                                    | Authentication Policy  |   | Apply |
| Browse Search                                | * Name Protected Resource Policy   | Success LPL   |       |
| ww • 🚷 🕒 😲 😂 🗶                               | Description Policy set during domain creation. Add resources to                                | Palure URL  |       |
| Shared Components                            | this policy to protect them.   | Identity Assertion                                  |       |
| 7 @Resource Type                             |  | Identity Assertion                                  |       |
| Флине  | * Authentication Scheme IDAPScheme •   |   |       |
| TokerServiceRP                               |  |   |       |
| 🚱 wi_authen                                  | Resources Responses  |   |       |
| 7 📑 Host Identifiers                         |  |   |       |
| ArgusSafety11g                               | @ Resources  |   | + x   |
| IAMSuiteAgent     Authentication Schemes     | Nan  |   |       |
| Authentication schemes                       |  |   |       |
| BasicScherne                                 | ArgusSafety11p//*  | •   |       |
| BasicSessionlessScheme                       | ArgusSafety11g:/   | •   |       |
| FAAuthScheme                                 |  |   |       |
| 2 KerberosScheme                             |  |   |       |
| DAPtioPassword/aldator6cheme                 |  |   |       |
| 20 LDAPSchene                                |  |   |       |
| OAAMAdvanced                                 |  |   |       |
| OAAMBasic                                    |  |   |       |
| OAM10g5cheme                                 |  |   |       |
| OAMAdminConsoleScheme                        |  |   |       |
| OF Scheme                                    |  |   |       |
| 00MScheme                                    |  |   |       |
| >   TAPScheme                                |  |   |       |
| 32X509Scheme                                 |  |   |       |
| Application Domains                          |  |   |       |
| ArgusSafety11g                               |  |   |       |
| > @Resources                                 |  |   |       |
| V BAuthentication Policies                   |  |   |       |
| > S Protected Resource Policy                |  |   |       |
| > Authorization Policies                     |  |   |       |
| Generation                                   |  |   |       |
| <ul> <li>Grusion Apps Integration</li> </ul> |  |   |       |

6. Navigate to the **Responses** tab and click the + button to add the **Name**, **Type**, and **Value** for the responses, as shown in the following screen:

|                                       | 😑 Wekeme 🔹 ArguiSalety11g 🔍 Arg  | inSafety11g Resources  | ArgunSalety11g : Protected Re | resource Policy | ArgueSafety11g   Protected Resource Policy |       |
|---------------------------------------|--|------------------------|-------------------------------|-----------------|--|-------|
| @ Search                              | Authentication Policy  | A DATA AND A DATA OF   |                               |                 |  | Apply |
| Browse Search                         | Plane Protected Resource Paley   |                        |                               |                 | cont B                                     |       |
| · · · · · · · · · · · · · · · · · · · |  |                        |                               |                 |  |       |
| Pared Components                      | Description Policy set during domain creat<br>this policy to protect them. | tion. Add resources to |                               |                 | alize UFL                                  |       |
| B Resource Type                       | Are heard, in business date:   |                        |                               | Scherrist,      | r Automation 🖾                             |       |
| (Borne)                               | * Authentication Scheme (DAPScheme   |                        |                               |                 |  |       |
| @ Tokenterstel?                       | - Automation sciente automation  |                        |                               |                 |  |       |
| Onlaster.                             |  |                        |                               |                 |  |       |
| Most Identifiers                      | Resources Responses  |                        |                               |                 |  |       |
| > Argustafety11p                      | G Responses  |                        |                               |                 |  | + x   |
| > TANELiteApent                       |  |                        |                               |                 |  |       |
| Authentication Schemes                | Name   | Type                   | 13                            |                 |  |       |
| Anonymous5cheme                       | PM_URR   | Header                 | - 9                           | aer.uberid      |  |       |
| Basicitiene                           |  |                        |                               |                 |  |       |
| BasicSessoriesScheine                 |  |                        |                               |                 |  |       |
| Adu/Oddene                            | 1  |                        |                               |                 |  |       |
| Rebensideme                           |  |                        |                               |                 |  |       |
| DATePasser/ValdatorGiteme             |  |                        |                               |                 |  | 1     |
| BIDAPScheme 2                         |  |                        |                               |                 |  | 1     |
| CAAMAbarcet                           |  |                        |                               |                 |  |       |
| CAAHEase                              | 1.1  |                        |                               |                 |  |       |
| OAM30pScheme                          |  |                        |                               |                 |  |       |
| OAMAdnerConsoleScheme                 |  |                        |                               |                 |  |       |
| CPS/serve                             |  |                        |                               |                 |  |       |
| > Se Takicheme                        |  |                        |                               |                 |  |       |
| Di 150%dene                           |  |                        |                               |                 |  |       |
| Application Donwine                   |  |                        |                               |                 |  |       |
| GArputSeletv110                       |  |                        |                               |                 |  |       |
| > @Restartes                          |  |                        |                               |                 |  |       |
| 7 Authentication Palicies             |  |                        |                               |                 |  |       |
| > S Protected Resource Policy         |  |                        |                               |                 |  |       |
| > Autheritation Policies              |  |                        |                               |                 |  |       |
| > Token Insuance Policies             |  |                        |                               |                 |  |       |
| - Confusion Ages Unitery ation        |  |                        |                               |                 |  |       |

**7.** Expand the **Authorization Policies** under the newly created Webgate and double-click the **Protected Resource Policy**.

Select the **Constraints** tab and click the **+** button to add the **Name**, **Type**, and **Class** for the constraints, as shown in the following screen:

| Authorization Policy      Authorization   |               | Xee                   |
|---|---------------|-----------------------|
|   |               | ×                     |
| Oriffer     *Name Protected Researce Policy     False URL     Oriffee     Subscription Policy     Description     Table     Constraint     Co   |               |                       |
| ter victority terminality ter   |               |                       |
| Arteristiki Shene<br>Demonstative<br>Entrablem<br>Entrablem<br>Machania<br>Antonia<br>Entrablem<br>Machania<br>Contentaben<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrablem<br>Entrabl | Trpe<br>Alter | + *                   |
| Overlage week blockstochen     Overlage   |               | -                     |
| StatuneCrushNeer<br>Software Content<br>Content Oran<br>Software Software<br>Software Software Software   |               | ana ana ang sa tanà a |
| August Showana Denay Taga Tana Bana Denay Taga Tana Denay Taga Tana Bana Denay Taga Tana Denay Taga Tana Bana  |               |                       |

**Note:** All the names under the Constraints tab with **Type** as **Allow** can access the Argus Safety Server where Webgate has been installed. Select the **Type** as **Deny** if a user should be denied access to the Argus Safety Server where Webgate has been installed.

If no constraint is added, all the users configured on the LDAP Server will have access to the Argus Safety Server where Webgate has been installed.

# Installation and Configuration of Oracle Web Tier Suite

The Oracle Web Tier Suite consists of following products:

- Oracle Process Manager Notification (OPMN)
- Oracle HTTP Server (OHS)
- Oracle Web Cache

### Installing Oracle Web Tier

This section describes the procedure to install Oracle Web Tier (OHS). Prior to this installation, ensure that you have a running instance of WebLogic Server.

- 1. Navigate to folder \ofm\_webtier\_win\_11.1.1.2.0\_32\_disk1\_1of1\Disk1 and double click setup.exe to start the installer. The installer will begin after a check has been made for installer requirements.
- 2. Click Next to continue.

| Oracle Fusion Middleware 11g  | Web Tier Utilities Installation - Step 1 of 13                                       |
|-------------------------------|--|
| Welcome                       | FUSION MIDDLEWARE 118  |
| 🧼 Welcome                     |  |
| Install and Configure         | Welcome to Oracle Fusion Middleware 11gWeb Tier Utilities Installer.                 |
| Prerequisite Checks           | For additional information and installation instructions, please refer to the Oracle |
| Specify Installation Location | Fusion Middleware Installation Guide for Web Tier Utilities.                         |
| Configure Components          | Click Help at any time for context-sensitive help.                                   |
| Specify WebLogic Domain       | Click Next to begin the installation.  |
| Specify Component Details     |  |
| Configure Ports               |  |
| Specify Security Updates      |  |
| Installation Summary          | Copyright (c) 1999, 2009, Oracle and/or its affiliates. All rights reserved.         |
| Installation Progress         |  |
| Configuration Progress        |  |
| I Installation Complete       |  |
|                               |  |
| Help                          | < Back Next > Enish Cancel   |
|                               | Elapsed Time: 1 m 40   |

**3.** Select Install Software - Do Not Configure and click **Next**.

| Oracle Fusion Middleware 11g  | Web Tier Utilities Installation - Step 2 of 13   |
|-------------------------------|--|
| Select Installation           | Type ORACLE 118  |
| Y Welcome                     |  |
| 🗼 Install Only                | Install and Configure  |
| Prerequisite Checks           | Installs binaries in an ORACLE HOME and configures working<br>instance in an INSTANCE HOME.  |
| Specify Installation Location | instance in an instance nowe.  |
| Specify Security Updates      |  |
| Installation Summary          |  |
| ↓<br>♀ Installation Progress  | Install Software - Do Not Configure  |
| i<br>Unstallation Complete    | Before these installed components will work, they must be configured by<br>running the configuration wizard.   |
|                               |  |
|                               | Installs software only. After installation is complete, use config bat from bin<br>directory in ORACLE HOME to configure working instances of these installed<br>components. |
| . Help_                       | < Back Next > Einish Cancel  |
|                               | Elapsed Time: 1m 55s   |

**4.** In the next screen, the installer performs Prerequisite Checks. Click **Next** to continue.

| Oracle Fusion Middleware 11g V<br>Prerequisite Check                     |               | Utilities Installation - Step 3 of 8  |                     | <u>-</u><br>eware <b>11</b> 8  |
|--|---------------|---|---------------------|--|
| Y Welcome  | Selection     | Check   | Progress            | Status   |
| Install Only   | 1             | Checking operating system certification   | 100%                | ~  |
| Prerequisite Checks  | 4             | Checking service pack   | 100%                | <ul> <li>Image: A second s</li></ul> |
| Specify Installation Location  | ¥             | Checking physical memory  | 100%                | ×  |
| Installation Summary   |               |   |                     |  |
| Installation Summary     Installation Progress     Installation Complete |               |   |                     |  |
| Installation Progress  |               | Ē   | joart <u>R</u> etry | Gontinue   |
| Unstallation Progress  | ⊕- <b>√</b> c | Antecking operating system certification<br>hecking service pack<br>hecking physical memory | port <u>Retry</u>   | Çontinue   |

**5.** You can skip security updates so uncheck the option to receive security updates via My Oracle Support. The system will give a warning. Click **Yes** to close the screen and then click **Next**.

| Oracle Fusion Middleware 11g  | Web Tier Utilities Installation - Step 5 of 8   |
|---|---|
| Specify Security U  | pdates  |
| Vieloome<br>Instal Only<br>Prerequisite Checks<br>Specify Installation Location<br>Specify Security Updates | Provide your email address to be informed of security issues, install the product<br>and initiate configuration manager. <u>View details</u> .<br>Email:<br>Easier for you if you use your My Oracle Support<br>email address/username. |
| Installation Summary     Installation Progress     Installation Complete                                    | ✓ I wish to receive security updates via My Oracle Support.<br>My Oracle Support Password:  |
|   | < Back Next > Einith Cancel   |
|   | Elapsed Time: 2m 45s  |

6. On the installation summary screen, click Install. This will install Oracle Web Tier.

| Dracle Fusion Middleware 11g   | ary   |
|--|---|
| Velcome Install Only Prerequisite Checks Secify Installation Location Secify Security Updates Installation Summary Installation Progress Installation Complete | Type: Install Only     Location: C: Voracle/Middleware/Oracle_WT2     Disk Space     Required: 1900 MB     System Components     Oracle Process Manager Notification (OPMN)     Oracle HTTP Server (OHS)     Oracle Web Cache |
| Heip   | Save Response File: Save  |

### **Configuring Oracle Web Tier**

The following section describes the procedure to configure the Oracle Web Tier (OHS).

1. Navigate to the folder Oracle Middleware\_Home\Webtier\_Instance\bin. For example, C:\OracleNew\Middleware\Oracle\_WT1\bin. Here Oracle\_WT1 is the name of the webtier instance created during installation. In the folder, run config.bat to start the configuration wizard.



2. In the next screen, click Next.

| Oracle Fusion Middleware 11g Web Tier Utilities Configuration - Step 2 of 9 |   |  |  |  |
|---|---|--|--|--|
| Configure Components Configure Components                                   |   |  |  |  |
| Vielcome  |   |  |  |  |
| Configure Components  | ✓ Oracle HTTP Server  |  |  |  |
| Specify WebLogic Domain   | ✓ Oracle Web Cache  |  |  |  |
| Specify Component Details   |   |  |  |  |
| Configure Ports   | Oracle Process Manager Notification (OPMN) is always configured |  |  |  |
| Specify Security Updates  |   |  |  |  |
| Installation Summary  |   |  |  |  |
| Configuration Progress  |   |  |  |  |
| i<br>Installation Complete  | Associate Selected Components with WebLogic Domain              |  |  |  |
|   |   |  |  |  |
|   |   |  |  |  |
| Γ   |   |  |  |  |
|   |   |  |  |  |
|   |   |  |  |  |
|   |   |  |  |  |
| Help  | <u> </u>  |  |  |  |
|   | Elapsed Time: 3m 2  |  |  |  |

**3.** Enter details of the weblogic server and click **Next**.

| Specify WebLogic Domain  |  |                               |        |
|--|--|-------------------------------|--------|
| Velcome<br>Configure Components<br>Specify WebLogic Domain<br>Specify Component Details<br>Web Cache Administrator Pas<br>Configure Ports<br>Specify Security Updates<br>Installation Summary<br>Configuration Progress<br>Installation Complete | Domain Host Name:<br>Domain Port No:<br>∐ser Name:<br>Passvvgrd: | localhost<br>7001<br>weblogic |        |
| Help   |  | < Back / Next >               | Einish |

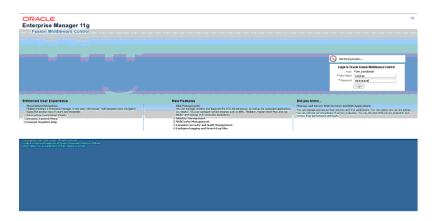
4. In the next screen, click Next.

| Oracle Fusion Middleware 11g  | Web Tier Utilities Configuration ·               | - Step 4 of 10 📃 🗖 🔀                               |
|---|--|--|
| Specify Componen  | t Details  | FUSION MIDDLEWARE 118                              |
| Vielcome     Configure Components     Specify WebLocic Domain     Specify Component Detail:     Web Cache Administrator Pas     Configure Ports | Instance Home Location:<br>Instance Name:        | ble_W/T1%instances%instance2                       |
| Specify Security Undetes     Installation Summary     Configuration Progress     Installation Complete  | QHS Component Name:<br>₩eb Cache Component Name: | ohs1<br>webcache1                                  |
| Leip  |  | < Back Next > Finish Cancel<br>Elaosed Time: 4m 98 |

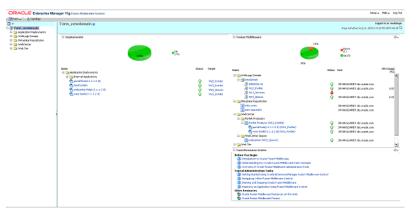
5. Enter a password for Web Cache and click Next.

| Oracle Fusion Middleware 11g | Oracle Fusion Middleware 11g Web Tier Utilities Configuration - Step 5 of 10  |  |  |  |  |
|------------------------------|---|--|--|--|--|
| Web Cache Admin<br>Password  |   |  |  |  |  |
| Y Welcome                    |   |  |  |  |  |
| Configure Components         |   |  |  |  |  |
| Specify WebLogic Domain      |   |  |  |  |  |
| Specify Component Details    |   |  |  |  |  |
| 🔶 Web Cache Administrator    | Web Cache Administrator Password:   |  |  |  |  |
| Configure Ports              | Confirm Password:   |  |  |  |  |
| Specify Security Updates     |   |  |  |  |  |
| Installation Summary         |   |  |  |  |  |
| Configuration Progress       |   |  |  |  |  |
| Installation Complete        |   |  |  |  |  |
|                              | Valid passwords are 5 to 30 characters long, must begin with an alphabetic character, use only alphanumeric, underscore (_), dollar (\$) or pound (#) characters and include at |  |  |  |  |
|                              | least one number.   |  |  |  |  |
| Help 2                       | Sack Next >> Einish Cancel  |  |  |  |  |
|                              | Elapsed Time: 4m 24   |  |  |  |  |

- 6. Select auto configuration port in the Configure Ports screen. Click Next.
- **7.** Skip security updates for now and then click **Next** to continue configuring the Web Tier.
- **8.** After the configuration, navigate to http://localhost:7001/em. This will open the Enterprise Management console for Fusion Middleware as shown below. Log in using the same credentials as that of the WebLogic server.



**9.** Click the Web Tier node on the left.



**10.** Click the name of the OHS instance that you have created during installation. In the following example, the OHS instance is ohs1.

|  | Farm_newdomain_p  |     |         |              |   |             |   | upped as no mode |
|--|---|-----|---------|--------------|---|-------------|---|------------------|
| <ul> <li>Formunevolumede.</li> <li>Formunevolumede.</li> <li>Formunevolumede.</li> </ul>   | energie en e |     |         |              |   |             |   |                  |
| Webl, rogic Documption   | E Deployments   |     |         |              | E fosice.*fiddlowers  |             |   | 0                |
| Maradata Fazzalizaian     Maradata Fazzalizaian     Maradata Fazzalizaian     Maradata     Maradata     Maradata     Maradatat     Maradatat | -   | •#6 |         |              | 🥑   |             | etana<br>05<br>Nacio  |                  |
|  | Notes   |     |         |              | 95  |             |   |                  |
|  | Same  |     | 2 ab.at | farget       | Name  | 31 di se    | Held  | CPUIDLAGE        |
|  | (i) This Internal Applications  |     |         |              | 💷 🔚 Weblange Connain  |             |   |                  |
|  | Contraction(3.1.1.2.2)  |     | Q       | VIS.Porket   | T C Constantin  |             |   |                  |
|  | Statistics .  |     | ÷       | WES JOINT DO | A whether w   | 2           | STORECAPET Microsle con                                     | 8.00             |
|  | Seebowber Mobilitian (200   |     | ÷       | Y53_30aced   | A Millerin  | ¥           | ShrwksOAME1.dc.orade.com                                    | 3.00             |
|  | 06 5 1 - 1 - 2 Monte and a -  |     | - 2     | VES_PORM     | A MULTINE   |             | SIN MICRARY MICRARY AND | 3.0              |
|  |   |     |         |              | Er Cas Meradera Repolitorier  |             |   |                  |
|  |   |     |         |              | S educates  |             | ShreeksCAME1.ab. oradii.com                                 |                  |
|  |   |     |         |              | and the second of   |             | SPARGOMET Mcorada.com                                       |                  |
|  | 8   |     |         |              | III 🛄 WebCentar   |             |   |                  |
|  |   |     |         |              | 🗟 🎦 Portek Producera  | ~           |   |                  |
|  |   |     |         |              | D Portet Protect (MLS_20480)<br>Provide International Control (MLS_20480)   |             | ShviksOANET.dc.oradii.com<br>ShviksOANET.idc.oradii.com     |                  |
|  |   |     |         |              | <ul> <li>An experimentary in a state participant of the partipant of the participant of the participant of the participant</li></ul> |             | WORKSOMET ACCOUNTS  |                  |
|  |   |     |         |              | Ei Ca WeCenter Steper   |             | berreichten die seine ber                                   |                  |
|  |   |     |         |              | S network MLS_Sector)   | 0           | SINNERSDAME? Mr. made.com                                   |                  |
|  |   |     |         |              | 🗉 🥁 Web Tair  | -           |   |                  |
|  |   |     |         |              | E Farm Resource Contre  |             |   |                  |
|  |   |     |         |              | Before You thegin   |             |   |                  |
|  |   |     |         |              | Orbitelation to Oracle Facion Middleware  |             |   |                  |
|  |   |     |         |              | Control of the State          |             |   |                  |
|  |   |     |         |              | Typical Administration Tables   |             |   |                  |
|  |   |     |         |              | 谢 cating stated parg to ade traces or Marage. Natur Plade-  | see control |   |                  |
|  |   |     |         |              | B Neigdong Wither Russon Moldmann Control   |             |   |                  |
|  |   |     |         |              | Starting and Stapping Grade Nation Middleware   |             |   |                  |
|  |   |     |         |              | Depleting on Application/Date (Public Mathematic Control<br>Other Residence on  |             |   |                  |
|  |   |     |         |              | Or sold Funder Photo-unit Recourses and the Web   |             |   |                  |
|  |   |     |         |              | Sa Chanin Facility Phildreney Printers.   |             |   |                  |

**11.** You will see all the details related to Oracle Http server on this console.

|   | nager 11g Fusion Middeware Contor  |         |   |   |   |  | Secip •                   | Neb v LapOut                 |
|---|--|---------|---|---|---|--|---------------------------|------------------------------|
| Spran . 2 texture   |  |         |   |   |   |  | Loged n at weldoors:      |                              |
| <ul> <li>BEfore performing</li> <li>De exploration descenants</li> </ul>    | 요 ohsta<br>@ Onde HTP Serve -  |         |   |   |   |  | spendaded was to 200 3 10 |                              |
| ini 🎦 Saleki, ngin Compile<br>III 🔂 Metudaka Paposhorina<br>Ini 🌆 WebContae | Expose odlood  | .0+     | E CPU and Homes   | y thogo   |   |  |                           | .0+                          |
| C Contractorio  | 0x<br>60   |         | 0.4<br>01   |   |   |  |                           | 0.54                         |
|   | - Fagert Processing Time (mill proving) - Fagert Throughout (management per recent)  | ÷.      | titid t<br>August   | 208 1207 1200<br>112013   | 1500 1210 121                                     |  | 1815 1816 1817 18         | no<br>no<br>Eléntr In<br>(*) |
|   |  | tion of |   |   |   |  |                           | 1ste has 2                   |
|   | Impaired         Repaired Strategy (Second Strategy)                           | φ.<br>  | Trackille thequest<br>tame<br>exected only produ-<br>med plag product<br>mod paths (baths)<br>mod paths (baths)<br>mod paths (baths)<br>mod paths (baths)<br>mod paths. | Teo.gbp.t<br>8.08<br>8.08<br>8.08<br>8.08<br>8.08<br>8.08<br>8.08 | Processed<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0 | Processing Table<br>0.00<br>0.00<br>0.00<br>0.00<br>0.00<br>0.00<br>0.00 |                           |                              |
|   | Constraints     Constrat     Constraints     Constraints     Constraints     Constraints | ат<br>Д | met.garn-t<br>met.gant.kanc.<br>not.janka.<br>met.ganhet<br>met.ganhet<br>not.content   | 8.08<br>8.08<br>8.08<br>8.09                                      | 0 2 8 0 ·   | 0.00<br>0.00<br>0.00<br>0.00   |                           |                              |

### **Oracle Http Server Administration**

This section describes the procedure to perform administrative tasks on the Oracle Http Server.

- 1. Perform steps 8 to 11 from the section Section, "Configuring Oracle Web Tier".
- **2.** Click Oracle Http Server just below instance name at the top of right pane to access a menu.

| ORACLE Enterprise Mana   | ger Hg Fusion Motoware O  | COMING!                                   |   |              |   |                       |                |                       | Setup at 14                          | iby LipOx         |
|--|---|---|---|--------------|---|-----------------------|----------------|-----------------------|--------------------------------------|-------------------|
| Strant. & topology   |   |   |   |              |   |                       |                |                       |                                      |                   |
|  | 😧 ohst 🗴 👘  |   |   |              |   |                       |                |                       | Logged's ac weldogs) Hor             |                   |
| 13 BE Form Jourdanner  | Grack HETP Sonver +   |   |   |              |   |                       |                |                       | Not installed into the 24th Sectored | e Gref Archael Co |
| E b Aspicatur Ospoytema  | tone  |   |   |              |   |                       |                |                       |                                      |                   |
| III 🎦 Weld, ogic Domain<br>III 🔂 Metadata Papositorias   |   |   |   | 0+           | II CPU and Honor  | y thogo               |                |                       |                                      | 0.                |
| in the webcerter   | Mintoing F  |   |   |              | 0.8   |                       |                |                       |                                      |                   |
| U D Wet Ter  | control +   |   |   |              |   |                       |                |                       |                                      |                   |
| Carlos Ca | 100 1   |   |   |              | 0.4   |                       |                |                       |                                      |                   |
| antestel.  |   |   |   | 0.3          | 01  |                       |                |                       |                                      | 0.14              |
|  | Perilbage   |   |   |              |   |                       |                |                       |                                      | 0.33              |
|  |   |   |   | 0.4          |   |                       |                |                       |                                      | 0.21              |
|  | Advantsion 1  | Weathers                                  | 1572 TET 1754 TAT 1757 TET              |              | and and   |                       | ter al el adas | and the second second | 1111 1121 1121 1111                  |                   |
|  | Security +  | Performant Dévolume                       | 1012 1010 1054 1055 1016 1017 1010      | 10.0         | 1505 150<br>August 11   | 8 100P 1580 1<br>2000 | 1576 1516 1611 | 1012 1521 1514        | 1215 11:10 12:11 12:11               | 1219              |
|  | General Managine  | Log Configuration                         |   | . X.         | 140 L   |                       |                |                       |                                      |                   |
|  | Setword Provinces   | Server Ceriliguistics                     | - Faqueri TerrupinA (remera per recard) |              |   |                       | = 0% Unger%)   | -intervery longe (MB) |                                      |                   |
|  |   | PINE Configuration<br>Porto Configuration |   | Table New of |   |                       |                |                       |                                      | Table Terry       |
|  | E INCLUÉRING  | Para Configuration                        |   | 0.           | 🗆 Madula Regard   | Statedace.            |                |                       |                                      | 0.                |
|  | Tane  | nod peri Configuration                    | traughout mercease scan (xt) Part.      |              | Nate  | Troughput             | Precessed      | Phooecomp Tane        |                                      |                   |
|  | anvargeenid Jdc.orade.c   | ned will she canhaintein                  | 0.00 0.00 ++40                          |              | exected on the product of the second | 8.08                  | 0              | 0.00                  |                                      | -                 |
|  | strangound All-cracks   | und feilus continuous                     | 0.40 0.00 9999                          |              | mod_bg_convig_t<br>mod_autho_host.c   | 8.08                  |                | 0.60                  |                                      |                   |
|  |   | Altraneous Cardinavation                  |   |              | mod_witione_r   | 8.08                  | í.             | 0.80                  |                                      |                   |
| 1  |   | And a set of the set.                     | J                                       |              | sudgetter, date   | 8.08                  |                | 0.60                  |                                      |                   |
|  |   |   |   |              | mod_statuses<br>mod_db_z  | 8.08                  |                | 0.00                  |                                      |                   |
|  | The Residence Deadles   |   |   | 0.           | mod_er z  | 1.00                  |                | 0.00                  |                                      |                   |
|  | thefore Yes thegin  |   |   |              | and just hance  | 8.08                  | ě              | 0.80                  |                                      |                   |
|  | Invoduction to Drade i  | HTTE: Server                              |   |              | mod_mine.c  | 8.08                  | :              | 0.00                  |                                      |                   |
|  | B setting started with Mill   | maging to address the barvier with one    | de time price Manager                   |              | mod_porting of  | 8-08                  |                | 0.00                  |                                      | - 19a             |
|  | typical Administration for  |   |   |              |   |                       |                |                       |                                      |                   |
|  | Configuring Grack HET<br>(B) Configuring mode of an<br>(B) Configuring mode of an |   |   |              |   |                       |                |                       |                                      |                   |
|  | Configuring Loca  | •   |   |              |   |                       |                |                       |                                      |                   |
|  | B Configure o resulte   | ×   |   |              |   |                       |                |                       |                                      |                   |
|  | Other Resources   |   |   |              |   |                       |                |                       |                                      |                   |
|  | South Server Re   | sources on the Orada Tardindogr N         | tugh                                    |              |   |                       |                |                       |                                      |                   |
|  | 🤹 Goose al Ferrari  |   |   |              |   |                       |                |                       |                                      |                   |
|  |   |   |   |              |   |                       |                |                       |                                      |                   |
|  |   |   |   |              |   |                       |                |                       |                                      |                   |
|  |   |   |   |              |   |                       |                |                       |                                      |                   |
|  |   |   |   |              |   |                       |                |                       |                                      |                   |
|  |   |   |   |              |   |                       |                |                       |                                      |                   |
|  |   |   |   |              |   |                       |                |                       |                                      |                   |

This menu allows you to perform the following administrative tasks:

- Control > Start Up You can start an OHS instance using this option.
- Control > Shut Down You can stop and OHS instance using this option.
- Control > Restart You can restart an OHS instance using this option.
- Logs > View Log Messages You can view logs of the OHS instance using this option.

### Configuring Oracle Http Server as Reverse Proxy Server for WebLogic

This section describes the procedure to configure the Oracle Http Server to act as a reverse proxy server for the WebLogic Server. Prior to following this procedure, ensure that you have a running instance of WebLogic Server and Oracle Web Tier. Also, you should have Global Home Page URL.

- 1. Perform steps 8 to 11 from the section Section , "Configuring Oracle Web Tier".
- **2.** Navigate to Administration > mod\_wl\_ohs\_configuration from the top menu.

| All the second second   |  |                         |   |  |   |                              |  |                              |               |                                   |
|---|--|-------------------------|---|--|---|------------------------------|--|------------------------------|---------------|-----------------------------------|
| □ •<br>SALforn re-denér   | 😧 ohst o<br>🖓 Cruck HTP Server -   |                         |   |  |   |                              |  |                              |               | Mager) Fort 20,000,00,00          |
| Image: Section Control (Section Control (Sectin Control (Sectin Control (Section Control (S | Scotts Finder Park   | Configuration           | 지 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) | 03<br>03<br>1520 1520<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1<br>1 | OU and Honor      Si      Of      Table   | 30 15±1 1520<br>112010       | 1629 1630 1527<br>==0%039001%0<br>Presented<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0 | 1 152 153 150<br>            | 1825 1534 153 | (v)<br>Table tang<br>⊕+<br>■<br>⇒ |
|   | Conservation Control C | sae vitr sa w which add |   | Ф+<br>А  | molingerse<br>mol sub junct<br>mol sub junct<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molingerse<br>molin | 8-06<br>8-08<br>8-08<br>8-08 |  | 0.00<br>0.00<br>0.00<br>0.00 |               |                                   |

**3.** The following screen appears:

| ORACLE Enterprise Mar  | ager Hig Fusion Middelware Control   |  |   |                       |                           |                       |                          | Seep w Heb w LapOut                                   |
|--|--|--|---|-----------------------|---------------------------|-----------------------|--------------------------|---|
| All same and a specker   |  |  |   |                       |                           |                       |                          |   |
| <ul> <li>S Bit formune-stamps</li> <li>R Da Apale.com their versation</li> </ul> | 😳 ohst o<br>Gruce HTP Server –   |  |   |                       |                           |                       |                          | Negaci non antitette and<br>NEA Alless Present Alless |
|  | Morrealism     Manager index meta page no.     mod. yet, direk carringar atta     mod. yet, direk carringar     Welsuph Carlos     Welsuph Carlos     Welsuph Carlos     Welsuph Net     (Dire         Manager Net         (Dire         (Dire         )         (Dire | en 🍘<br>1 tobe promotion at Gradu HTP 5<br>mendi do protocom | anvarts Grußs wedungs Server                  | Specify parameters co | metrix illufordiscad to t | he nud_sil_phe handle | , wów te Mattipesco wisc | Lants L. Annan  |
|  | (netword(states)   | Wage Gate-   | Welfunde Hent<br>in meganeral vill an ode dan |                       |                           | Log Me                | Entrop                   | :<br>:  |

In the General section enter the following information:

- Weblogic host: FQDN of the machine where weblogic server and other managed servers are running.
- Weblogic port: Port of the WebLogic server.
- **Debug**: Give ERR.
- Log File: You can provide a log file here.

In the Locations Section:

- Click AddRow and add a new row.
- In the WebLogic Host and Port field enter the same values as that in the general section of this page.
- Location field: For entering a value in this field consider an example. If the URL for the Global Home Page deployed on custom server is http://<myhost.idc.example.com:7777>/GlobalHomePage/faces/GlobalHom
   e, then <myhost.idc.example.com> is the FQDN of the machine where WebLogic server is installed and 8001 is the port at which custom server is listening. Now take the path after port /GlobalHomePage/faces/GlobalHome and enter this as the value in the location field.
- Click **Apply** on the top right corner.
- 4. Restart the Oracle http Server using the Restart option of the top level menu.
- 5. After restarting, navigate to http://<myhost.idc.example.com:7777>/ GlobalHomePage/faces/GlobalHome. Here <myhost.idc.example.com> is the

FQDN of the machine where the OHS instance is running and <7777> is the port at which the OHS server is listening.

**Note:** You should see the same page but this time it is being redirected from OHS to the WebLogic Server.

|                             | 119 Fusion Middleware Control                                  |  |  |                          |                 |                          | Setup- Help-        |             |
|-----------------------------|--|--|--|--------------------------|-----------------|--------------------------|---------------------|-------------|
| Fam - & Topology            |  |  |  |                          |                 |                          |                     |             |
| •                           | 😯 ohs1 😡   |  |  |                          |                 | Logged in as w           | veblogic(Host 30.   | 175.84.305  |
| E Farm_nevdonan             | Gade HTTP Server 🖛   |  |  |                          |                 | Page Rainshed Jan 31, 2  | 143 E3 (25:09 PM CM | IT+155:30 🗘 |
| 🗄 🛅 Application Deployments |  |  |  |                          |                 |                          |                     |             |
| 🛙 🛅 WebLogic Domain         | (1) Information  |  |  |                          |                 |                          |                     |             |
| E 🋄 Metadata Republishes    | All changes made in this pe                                    | ge require a server restart to take aff  | ect.                                     |                          |                 |                          |                     |             |
| WebCenter                   | mod_wLohs Configu  | ration (3)   |  |                          |                 |                          | Apply               | Revert.     |
|                             | indo_in_ons comig  |  |  |                          |                 |                          |                     |             |
| webcache 1                  | General  |  |  |                          |                 |                          |                     |             |
|                             | The mod_vi_phs module allows<br>the MatchExpression and Locals | equests to be proxed from an Oracle<br>in sections to specify any overrides.                       | HTTP Server to Cracle WebLogic Server. 5 | peofy peran              | where common fo | all URLs directed to the | mod_vi_ohs hand     | er, and use |
|                             | WebLope Cluster  |  |  |                          |                 |                          |                     |             |
|                             | WebLopc Hist   | rvargsandt els orade.com   |  |                          |                 |                          |                     |             |
|                             | methodic Port  |  |  |                          |                 |                          |                     |             |
|                             |  | Dynamic Server List ON   |  |                          |                 |                          |                     |             |
|                             |  |  |  |                          |                 |                          |                     |             |
|                             | Error Page   |  |  |                          |                 |                          |                     |             |
|                             | Debug  |  |  |                          |                 |                          |                     |             |
|                             | Log File   |  |  |                          |                 |                          |                     |             |
|                             | WebLogic Temp Directory  |  |  |                          |                 |                          |                     |             |
|                             | Exclude Path or Mine Type                                      |  |  |                          |                 |                          |                     |             |
|                             | Platch Expressions   |  |  |                          |                 |                          |                     |             |
|                             | Add Baw 35 Remove  |  |  |                          |                 |                          |                     |             |
|                             | T Had Have by Hermony  |  |  |                          |                 |                          |                     |             |
|                             | Depression   |  |  |                          |                 |                          |                     |             |
|                             | S THP "10" Charles Front Exp                                   | reasion can have the following value<br>while (Melocoport – mod Juebug – c                         | N)rothinaan (+ Azst2                     |                          |                 |                          |                     |             |
|                             | Depression<br>© THP <sup>Exp</sup> reserved RNMCCO<br>         |  |  |                          |                 |                          |                     |             |
|                             | S THP "10" Charles Front Exp                                   | reasion can have the following value<br>initial Methogodius t = Rocal Debug =0<br>WebLogic Cluster | N/of-these of +/test2                    | WebLogic Port            | Path Zim        | Path Prepard             | Log Pile            | De          |
|                             | Depression<br>© THP <sup>Exp</sup> reserved RNMCCO<br>         |  |  | WebLogic<br>Part<br>8001 | Path 2im        | Petr Prepend             | Log Ple             | D           |
|                             | Depression   |  | WebLogic Heet                            | Port                     | Patritics       | Path Prepard             | Log Pie             | D           |

# Configuring the WebCenter Security Provider for Identity Assertion

This section describes how to set the security provider of Web Logic Server to use Oracle Internet Directory which is the OAM identity store.

### Configuring the Oracle Internet Directory Authenticator

This section describes the procedure to configure the Oracle Internet Directory Authenticator.

1. Log in to the WLS Administration Console. From the **Domain Structure** pane, click **Security Realms**. Then click myrealm.

| ORACLE WebLogic Server®  | Administration Console   |   |
|--|--|---|
| Change Center  | 🙆 Home Log Out Preferences 🖾 Record Help   | Welcome, weblogic Connected to: ArgunDomain .   |
| View changes and restarts  | Fore Seminary of Security Realizo  |   |
| Peoding danges exist. They hust be activated<br>to side effect: Virus and shale them non-<br>Otherness, they will be autometically activated<br>when you nest hoodly, add or decite items in<br>this domen.<br><u>Activate Changes</u><br><u>Undo Al Otanges</u>   | security realms in a WebLogic Server domain, but only one can be set as the de                                   | un'n rolen, wounty policies, and mounity providers—that are used to protect life(Lappr-mounces. You can have multiple<br>Multi (form) y man.<br>The life(Lappr Sarver domain. Octo the name of the realm to explore and configure that realm. |
| Domain Structure<br>AreaDanain   | Realms/Filtered - Hore Columns (xist)  |   |
| B-Environment<br>Popkywents  | New Date   | Showing 1 to 1 of 1 Previous   Next   |
| B-Services<br>Security Realms  | 🗖 Name 🔿   | Default Realm   |
| E-Interoperability   | 🗂 myresin  | rue   |
| B-pagnessis  | New. Delete  | Showing Lto Lof 1 Previous (Next  |
| How do L.  |  |   |
| <ul> <li>Configure new security realms</li> </ul>  |  |   |
| Delete security realms     Change the default security realm   |  |   |
| System Status  |  |   |
| Health of Running Servers  |  |   |
| Paled (0) Critical |  | 1   |
| WebLogic Server Ventors, 12.2.2.0<br>Copyright (): 1996-2006, Oracle and/or its affiliates, Al<br>Oracle is a registered trademark of Dracte Corporate   | r<br>Il rights resterend.<br>on and/on its affitates. Other runner may be badamarks of their respective overers. |   |

2. Navigate to Providers > Authentication. Click New to create a new provider.

| ORACLE WebLogic Server®  | Administration Console  |  |  |
|--|---|--|--|
| Change Center  | 🏟 Home Log Out Preferences 🔛 Record Help  | ·  | Welcome, weblogic Connected to: ArgunDomain  |
| View changes and restarts  | Home > Summary of Security Realma > regressive  |  |  |
| Produce photogenetics The provide both the constraint of the second seco | Settings for myrealm Ceediguration Users and Groups Roles and General RORES Security Store User Load Use the page to configure the general behavior |  |  |
| ArgusDomein<br>B-Environment<br>"Doployrebrits<br>B-Services   | Note:<br>Df you are implementing security using 32<br>not evaluate and the security functions (   | ADC (Java Authorization Contract for Containers as defined in 25A 1:<br>for Web applications and E28s in the Administration Console are deal | (3), you must use the DD Dniy security model. Other WebLogic Server models are<br>led.   |
| El Interoperability  | Nemet   | nyrealm  | The name of this security realm. Here Info   |
| B-pagreenes  | Security Model Default:   | DD Only K  | Socialities first default security motion for Web applications on 8.2% that are<br>secured by this security reality. You can override this default during<br>declayment. More Enfa   |
|  | 区 🁸 Combined Role Happing Enabled   |  | Determines how the role inagoings in the Entergine Application, Web<br>assistances and E28 containers interact. This setting is wald only for Web<br>applications and E28 the Autored Security model and that initialize<br>roles from deployment descriptors. None 2nfo |
| How do I   | 🗆 🚓 Use Authorization Providers to Prob   | act JHX Access   | Configures the Webcopic Server Milean servers to use the security realit's<br>Authorization provides to determine whether a Jitt client has demosion to  |
| Manage security for Web applications and<br>EXBs     Set the default security model     Delegate MEans authorization to the realm  | - 'p Advanced<br>   |  | acuts an Yillean attribute or whole an Yillean operation. Here bYGo  |
| System Status  |   |  |  |
| Health of Running Servers  |   |  |  |
| WebLogic Server Venion - 18.3.2.0<br>Copyright & 1996,2000, Oracle and/or to affiliates, Al-<br>Oracle a a mobilized materialized of Oracle Companying   | lights reserved.<br>n and/or its afflictus. Other names may be insidemarks of the   | er moethe overe.   |  |

**3.** Enter **Name** as OID Authenticator and select **type** from the drop-down as OracleInternetDirectoryAuthenticator. Click OK.

| hange Center  | 2 Home Log Out Preferen       | ces 🖾 Record Help  | Welcome, weblogic Connected to: ArgunDomain |
|---|-------------------------------|--|---|
| New changes and restarts  | Home > Summary of Security    | Realma Smyraelm SProvidera >010 Authenticator >Providera |   |
| ending changes exist. They must be activated<br>to take effect. You man activate them nom.<br>Dennise. They and be activated activated<br>inten you rest nedfin, add or detete items in<br>his domain.<br>Activate Changes<br>Undo Al Changes |                               |  |   |
| a secondar  | * Indicates required fields   |  |   |
| lomain Structure<br>rgusDonain  | The name of the authenticat   | ion provider.  |   |
| P-Environment<br>"Deployments<br>P-Services   | * Name:                       | OID Authenticator  |   |
| Security Realins  | This is the type of authentic | ation provider you wish to create.                       |   |
| Diagnestics   | Туре:                         | OracleInternetDirectoryAuthenticator                     |   |
|   | _OK. [.Censel.]               |  |   |
| iow do I 🕮  | 1                             |  |   |
| Manage security providers<br>Configure Authentication and Edentity<br>Asserban providers  |                               |  |   |
| ystem Status 🖂  | 1                             |  |   |
| tealth of Running Servere   |                               |  |   |
| Faled (0)<br>Ortical (0)<br>Overhaded (0)<br>Worney (0)<br>Or (1)   |                               |  |   |

- 4. Go back to the Providers tab and click OID Authenticator, which appears as link.
- 5. In the Common sub tab modify the Control Flag field to Sufficient and click Save.
- **6.** Click the Providers Specific tab and provide values for the fields described in the table below:

| Parameter Name | Description  | Sample Value   |
|----------------|--|--|
| Host           | LDAP Hostname  | i <myhost.vm.example.com></myhost.vm.example.com>    |
| Port           | LDAP Port  | 389  |
| Principal      | LDAP admin principal   | cn=orcladmin   |
| Credential     | Password for admin<br>principal (password of<br>cn=orcladmin)                                  |  |
| User Base DN   | User Search Base - This<br>value can be obtained by<br>checking the Users realm<br>DN from OID | For example,<br>cn=Users,dc=idc,dc=oracle,<br>dc=com |

 Table 15–1
 Values for the Providers Specific tab

| Parameter Name   | Description  | Sample Value  |
|--|--|---|
| All Users Filter   | Set as<br>(&(uid=*)(objectclass=pe<br>rson))   | (&(uid=*)(objectclass=pe<br>rson))                    |
| User Name Attribute  | Set to "uid" from "cn"   | uid   |
| Group Base DN - Group<br>search base - Same as User<br>Base DN | Group Search Base - The DN<br>used to search the Group,<br>can be checked by Groups<br>DN in OID | For example,<br>cn=Groups,dc=idc,dc=oracl<br>e,dc=com |

Table 15–1 (Cont.) Values for the Providers Specific tab

Retain the default values for the remaining attributes. Click Save.

|   | nticatorbook - ArgusDomain - WLS × 🔝 Grade A             |  | strig Grade Internet Directory   |
|---|--|--|--|
| ew changes and restarts   | a >Summary of Security Realms >mynaim >Providers >0      | ID Authenticator >Providers >0404 Identity Assertar >0 | 0 Authenticator  |
| nding changes exist. They must be activated Settin  | gs for OID Authenticator                                 |  |  |
| the effect. You may activate them now.<br>therwise, they will be autometically activated Cond | iguration Performance                                    |  |  |
| hen you next modify, add or delete items in   |  |  |  |
| Com   | non Provider Specific                                    |  |  |
| Activate Changes  |  |  |  |
| Undo Al Dhangez   | 20   |  |  |
|   | this page to define the provider specific configuration. | for this Cracle Internet Deartery & theritopher room   | dar  |
| main Structure.   |  |  |  |
| - Ca  | enection   |  |  |
| Deployments   | lost:  | heovm007.us oracle.com                                 | The host name or an address of the LOAN server. More byfo  |
| Services  |  |  |  |
| Interoperability  | fort:  | 389  | The part number on which the LDAP server is latering. More Info  |
| Degrestics  |  |  |  |
|   | rincipali  | cn-orcladmin   | The Ostangushed Name (DN) of the LOAP user that WebLogic Server should   |
| ~   | -  |  | use to connect to the LDAP serves. More bries  |
| Greet   | lestial  |  | The credential fusually a possiviand) used to connect to the USAP  |
|   |  |  | server, Mare Inform  |
|   | irm Credential   |  |  |
| aw do L. U  | Phi Clevenar   |  |  |
| -   | 55Ltnebled   |  | Specifies whether the SSL protocol should be used when connecting to the   |
| Configure the Oracle Sitemet Directory Authoritication provider                               | D SOLUMEDICO   |  | LDAP pervec Hore prop  |
| Configure Authentication and Identity   | ers  |  |  |
| Assertian providers   | her Base DN:   |  | The base distinguished name (DV) of the tree in the LDAP directory that  |
| Manage security providers   | NOT Dave Linc  | cn=Users,dc=us,dc=ora                                  | contains users. Hore Enfo  |
|   |  |  |  |
| ystem Status 🗉 📲  | Ul Users Filter:   | (S(cn=")(objectclass=pe                                | An LDAP search filter for finding all users beneath the base user<br>distinguished name (DN). Note: D'you change the user name altribute to a  |
| ealth of Running Servers  |  |  | type other than cn, you must duplicate that change in the User Prom Name<br>Plan and User Name Attribute altributes. Your Trin.                |
| Paled (0)   |  |  | Pitter and User Name Attribute attributes. More Info   |
| Critical (0)  | Ser from Name filter:                                    | (S(cn=%u)(objectclass=                                 | An LOAP search Biter for finding a user given the name of the user. The user   |
| Overladed (0)   |  | falen- antioniscientes-                                | name attribute specified in the filter must match the one specified in the All<br>Overs Pilter and User Name Attribute attributes. More Driv   |
| Warning (0)   |  |  | WHEN THE BOARD THE POST OF A DECK. THE POST OF   |
| OK (3)  | Ker Search Scope:  | subtee   | Specifies how deep in the LDAP directory tree the LDAP Authentication  |
|   |  |  | provider should search for users. More brio  |
| A1  | Iser Name Attribute:                                     | 50   | The attribute of an (DAP user object class that specifies the name of the  |
|   |  | 511  | uses The user name attribute specified must most the one specified in the<br>All users Filter and user From Name Filter attributes. More [offs |
|   |  |  | PROVIDE THE BRIDGE CHARGE CARD CONTINUES OF BRIDGE   |
|   | iser Object Class:                                       | person   | The LDAP object data that stores users. More Info  |
| ~   |  |  |  |
| <b>E</b> 4  | Use Retrieved User Name as Principal                     |  | Specifies whether or not the user name retrieved from the LDAP server.   |
|   |  |  | should be used as the Principal in the Subject. More Info  |

# **Configuring the OAM Identity Asserter**

This section describes how to configure the OAM identity asserter in WebLogic server security realm.

1. Log in to the WLS Administration Console. From the **Domain Structure** pane, click **Security Realms**. Then click myrealm.

| ange Center  | 🖨 Home Log Out Preferences 🔛 Record Help            |  | Welcome, weblogic Connected to: ArgunDomail  |
|--|---|--|--|
| ew changes and restarts  | Home +Semmary of Scounty Realmo                     |  |  |
| nding changes exist. They must be activated<br>table effect. You may activate thom non-<br>homese, they will be automatable technologi<br>en you nest modify, add or debits items in<br>a domain.<br>Activate Changes. | security realms in a WebLogic Server domain, but or | ly one can be set as the default (active) realm. | searity providers-that are used to protect WebLogic resources. You can have multiple<br>of the name of the realist to explore and configure that realis. |
| main Structure   | © Customize this table                              |  |  |
| paDanah  | Realms(Filtered - Hore Columns Exist)               |  |  |
| Environment<br>Deployments   | New Double  |  | Showing 1 to 1 of 1 Previous   Next  |
| Services<br>Security Realms  | 🗐 Rame 🔿  | Default Realm                                    |  |
| Interoperability   | myresis   | tue  |  |
| Diagnestos   | New. Delete   |  | Showing Lto 1 of 1 Previous   Next   |
| w do L (i)   |   |  |  |
|  |   |  |  |
| Configure new security realms<br>Delete security realms  |   |  |  |
| Change the default security realm  |   |  |  |
| stem Status 💷  |   |  |  |
| alth of Running Servers  |   |  |  |
| Poled (0)<br>Criscal (0)<br>Overladed (0)<br>Warning (0)<br>OK (1)   |   |  |  |

- **2.** Click the Providers tab to see list of providers.
- **3.** Click **New**. Enter name as OAMIdentity Asserter and select type as OAMIdentityAsserter.

|  | Welcome, weblogic Connected to: newdomail  |
|--|--|
| Home a Summary of Security Realma any realm a Providena  |  |
| Create a New Authentication Provider   |  |
| Create a new Authentication Provider   |  |
| The following properties will be used to identify your new Authentication Provider.<br>* Indicates required fields |  |
| The name of the authentication provider.   |  |
| CAVIED/INVOSIONAL  |  |
| This is the type of authentication provider you wish to create.  |  |
| Type: OAMdenttyAsseter   |  |
| LOK. [LCenost.]  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | Life         Consent.           Conserve Automatications Provider           The following provides           *Jubicator conserve for follow           "Deliverance of the Automatication Provides"           "Brain and The Automatication provides           "Automatication provides you visite to caste.           Type:         Constructions provides |

- **4.** Click **OK** to save the details. Now click the newly added OAMIdentityAsserter, which appears as link to view its details.
- 5. In the Common sub tab select **control flag** as REQUIRED and click **Save**.
- 6. Navigate to the Providers sub tab and provide the details in the table below:

| Parameter Name        | Description   | Sample Value   |  |
|-----------------------|---|--|--|
| Transport Security    | Encryption type for Access<br>Gate communication                        | Open   |  |
| Primary Access Server | Provide OAM server<br>endpoint information in<br>HOST:PORT format       | <myhost.idc.example.com:7<br>777&gt;</myhost.idc.example.com:7<br> |  |
| Access Gate Name      | Copy the Access Gate name from the AG created from Step 3.              | <myhost.example.com>_<br/>AG</myhost.example.com>                  |  |
| Access Gate Password  | Type the Access Gate<br>Password configured in<br>access system console |  |  |

Table 15–2 Values for Provider sub tab

Retain the default values for the remaining attributes.

| Custom Report: My Open Bugs and Enho — *    |  | Book - newdonain - WLS C × 🔁 Toublishessing Grade Internet Directory - 🖓 🕂 | - 1  |
|---|--|--|------|
| nodity, add or delete items in this domain. | Configuration  |  | 2    |
| Domain Structure                            | Common Provider Specific   |  |      |
| revidoman.<br>B-Environment                 | LSeve.   |  |      |
| **Deployments                               | This page allows you to configure additional attributes for this s |  |      |
| B-Services<br>Security Realins              |  |  | - 11 |
| E-Interoperability<br>E-Diagnostics         | Transport Security:  | open 💌   | - 11 |
| an pageoto                                  | C Plaintern Access Server Connections In Pool                      | 5  |      |
|   | Application Domain:  | Idc.oracle.com   |      |
|   | Access Gate Password:  |  |      |
| No help task found                          | 🕰 Please type again To confirm:                                    | ******   |      |
| iystem Status 🖂                             | Key Store Pass Phrase  |  |      |
| realth of Running Servers                   | 🛃 Please type again To confirm:                                    | []   |      |
| Paled (0)<br>Offical (0)<br>Overloaded (0)  | Caress Gate Name   | argus_webgate  |      |
| Warning (0)<br>Ok (6)                       | 😸 Primary Access Serveri   | ARGSAFE0 idc oracle.c  |      |
|   | An Maximum Access Server Connections In Pool                       | 10   |      |
|   | 🖑 Simple Hode Pass Phrase:   |  |      |
|   | 🚓 Please type again To confirm                                     |  |      |
|   | 🚑 Trust Store:   |  |      |
|   | 🚓 SSOHeader Name:  | OAM_REMOTE_USER  |      |
|   | 😸 Secondary Access Server  |  |      |
|   | 🚓 Key Store:   |  |      |
|   | _Seve_   |  |      |
|   |  |  |      |

### Configuring the Default Authenticator and Setting the Order of Providers

This section describes how to configure the deafult authenticator and set the prder of the providers.

- 1. Navigate to the list Click Default Authenticator from the list of **Security Providers** in the console, and set **Control Flag** to SUFFICIENT. Click **Save**.
- **2.** Set the Order for providers as follows:
  - OAMIdentityAsserter REQUIRED
  - OracleInternetDirectoryAuthenticator SUFFICIENT
  - DefaultAuthenticator SUFFICIENT
  - DefaultIdentityAsserter

### Setting EXTRA\_JAVA\_PROPERTIES for WebLogic Domain

1. Log in to the machine where web center has been installed and navigate to user\_projects/domains/wc\_domain/bin. Now edit the file setDomainEnv.cmd.

**Note:** Ensure that you take a backup of the file setDomainEnv.cmd before making changes.

2. Add following code at the end of the file:

```
Let's say EXTRA_JAVA_

PROPERTIES="-Dweblogic.security.SSL.ignoreHostnameVerification=true

-Doracle.mds.bypassCustRestrict=true

-Djps.update.subject.dynamic=true -Doracle.webcenter.spaces.osso=true

-noverify ${EXTRA_JAVA_PROPERTIES}"

Export $EXTRA_JAVA_PROPERTIES
```

3. Restart the Admin servers, managed servers and HTTP Server.

# **Installation Maintenance Tasks**

This section describes maintenance tasks you may need to perform on the installed Argus Safety Solution components. It includes instructions for performing various tasks and tips for using the Web client.

### Installing New Components

The components can be installed using the following procedure:

- **1.** Select Start > Control Panel.
- **2.** When Windows opens the Control Panel, click Add or Remove Programs / Uninstall or change a program.
- 3. When the Add or Remove Programs dialog box opens:
  - Select Argus Safety.
  - Select Change.
- 4. The Argus Safety InstallShield Wizard opens the Preparing Setup dialog box.
- 5. When the wizard opens the Welcome dialog box:.
  - Select Modify.
  - Click **Next** > to continue.
- **6.** When the wizard opens, select Update installed Argus Components and click Next:
  - Select Update installed Argus Components.
  - Click Next > to continue.
- 7. When the wizard opens the Customer Information dialog box:
  - Enter the user name in the **User Name** field.
  - Enter the company name in the **Company Name** field.
  - Select Next > to continue.
- **8.** When the wizard opens the Select Features dialog box it contains a list of currently installed components.
  - Select check box for one or more components to install.
  - Select **Next** > to continue.

**Note:** Ensure the check boxes for components that are already installed contain a checkmark. If the checkmark is cleared from the check box for an existing component, the component will be uninstalled.

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

- **9.** After the installation is complete, the wizard opens the Argus Safety Setup-Maintenance Complete dialog box.
- **10.** Click Finish. A message box appears.

# **Uninstalling Components**

Use the following procedures if it becomes necessary to uninstall a component:

- **1.** Select Start > Control Panel.
- **2.** When Windows opens the Control Panel, click Add or Remove Programs.
- **3.** When the Add or Remove Programs dialog box opens:
  - Select Argus Safety.
  - Select Change/Remove.
- 4. The Argus Safety InstallShield Wizard opens the Preparing Setup dialog box.
- **5.** When the wizard opens the Welcome dialog box:
  - Click **Next** > to continue.
  - Select Modify.
- **6.** When the wizard opens the Customer Information dialog box:
  - Enter the user name in the **User Name** field.
  - Enter the company name in the **Company Name** field.
  - Select Next > to continue.
- **7.** When the wizard opens the Select Features dialog box it contains a list of currently installed.
  - Clear the **check box** for the components to uninstall.
  - Select **Next** > to continue.
- 8. The Argus Safety Components Installer will uninstall the selected components.
- **9.** Follow the on-screen instructions to uninstall the components.

**Note:** If a Locked File Detected dialog opens, select **Don't display this message again**, and click **Reboot**.

# **Removing All Components**

If it becomes necessary to remove all the Argus Safety components, use the following procedure to do so:

- **1.** Select Start > Control Panel.
- 2. When Windows opens the Control Panel, click Add or Remove Programs.
- 3. When the Add or Remove Programs dialog box opens:
  - Select Argus Safety
  - Select Change/Remove to Select Remove/Uninstall
- 4. The Argus Safety InstallShield Wizard opens the Preparing Setup dialog box.
- 5. When the wizard opens the Welcome dialog box:
  - Click **Next** > to continue after **Select Remove**.
  - Select Remove.
- 6. When the Confirm Uninstall dialog box opens, Click OK to proceed.

- 7. The Argus Safety Components Installer uninstalls the required component(s).
- 8. Follow the screen instructions to uninstall the components.

**Note:** If a Locked File Detected dialog appears, select *Don't display this message again,* and click **Reboot**.

If a Shared File Detected dialog appears, select *Don't display this message again*, and click **Yes**.

If a ReadOnly File Detected dialog appears, select *Don't display this message again*, and click **Yes**.

# Web Client Tips

This section describes the recommended Internet Explorer configuration for clients that access Argus Safety Web, Affiliate, Dossier, and Interchange Web.

To configure Internet Explorer:

- **1.** Open Internet Explorer v11.
- 2. Select Tools > Internet Options.
- 3. When the Internet Options dialog box opens:
  - Locate Browsing History
  - Click Settings.
- **4.** When the Settings dialog box opens:
  - Locate Check for newer versions of stored pages.
  - Select Automatically.
  - Click OK.
- 5. Click the Advanced tab of the Internet Options dialog box.,
- 6. When the Advanced tab opens:
  - **a.** Locate the Multimedia section.
  - **b.** Clear the Show image download placeholders check box.
  - **c.** Select the **Show Pictures** check box.
  - d. Clear the Enable Automatic Image Resizing check box.
- 7. Click **OK** to close the Internet Options dialog.

**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 Section , "Enabling SSL Support for Windows 2012" in this Installation Guide.

When logged into Argus Safety System, 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. It is recommended to shut down 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.

# **Clearing Oracle Temp Files**

On the Argus Web, Argus Report and Argus Safety Service Servers, Oracle creates many temp files that begin with OIP and do not have an extension. Oracle does not delete these files and they can cause problems with the maximum number of files in a folder. This prevents Argus from creating new temp files. Therefore, these files must be deleted.

Deleting these files does not harm the system. One way of deleting these files is to use Argus Report Service because it cleans up the files at regular intervals. If you do not use Argus Report Service to clean these files, you will have to clean them manually.

Use the following procedure to configure the Argus Report Service to clean up these files.

**Note:** Oracle will first use the TMP Windows Environment Variable Path for Temp Files. If the TMP Variable is not defined, Oracle will use the path as defined in the registry below.

To configure Argus Report Service to clear Oracle Temp files:

- 1. Start the Windows Registry Editor.
- **2.** Locate the following path: HKEY\_LOCAL\_MACHINE \ SOFTWARE \ ORACLE.
- **3.** Locate and open the folder containing the OO4O sub folder.

**Note:** The folder structure under the Key from Step 2 can vary for each installation, based on the installation client and version used.

**4.** Locate and expand the OO4O folder.

5. Locate the TempFileDirectory folder.

**Note:** Oracle sometimes selects the Temp Folder as the Windows or Windows System Folder. Change this to some other temp folder so the files can be deleted without affecting any other files. For example, you can change the path to C:\Temp\Oracle.

After changing the patch, reboot the machine and continue with the next steps. Once it is set, the Argus Report Service will delete all files within the folder set here. If non-Oracle files exist, they will be deleted.

- 6. Copy the path from the TempFileDirectory key.
- 7. Go to the Argus Installation Folder\Common folder.
- **8.** Open the DeleteUser.bin file in Notepad.
- **9.** Add a new line at the end of the file with the following syntax:
  - <Oracle Temp File Folder>;\*
  - Example C:\Temp;\*

**10.** This line instructs the Argus Report Service to delete all files from this folder.

# Configuring easyPDF

This section describes how to set up easyPDF and Microsoft Office and includes the following sections:

- Setting Up easyPDF
- Setting up Microsoft Office

### Setting Up easyPDF

The easyPDF component is required for printing PDF reports and for use by Interchange features such as transmitting E2B attachments.

The domain account created during the installation of either Argus Web Server, Argus Safety Service or Interchange Service, will be required to continue with the following steps.

Before configuring Windows Service settings, verify the following:

- The domain account created is part of the local Administrator Group on the server being setup.
- Verify that the step in the note below is completed before going to the Configure Windows Service Settings section.

**Note:** You must log on to the server being setup with the domain account at least once to initialize the account, including the printer driver setting, or Argus will not be able to function correctly.

Use the following procedure to configure the Windows service settings:

1. Log on to the computer as the defined domain account.

- 2. Select Start > Control Panel > Administrative Tools > Services.
- 3. When the Services dialog box opens:
  - Locate the BCL easyPDF SDK 7 (or 6) Loader and double-click it.
  - When the BCL easyPDF SDK 7 (or 6) Loader Properties dialog box opens:
  - Click the Log On tab.
  - Enter the defined domain account name in the **This account** field.
  - Enter the defined domain account password in the **Password** field.
  - Enter the defined domain account password in the Confirm password field.
  - Click the General tab.
- 4. When the **General** tab opens:
  - Select Automatic from the Startup type drop-down list.
  - Click OK to close the Properties dialog box.
- **5.** When the system returns to the main Services window, start the BCL easyPDF SDK 7 (or 6) Loader.
- 6. Close the Services window.

### Setting up Microsoft Office

This section provides an example procedure to make Microsoft Office applications, such as MS Word and MS Office, ready for server use. The example shows how Microsoft Word can be set up; you can also set up Microsoft Excel in the same manner.

Make sure that pop-up dialog boxes from Office products do not appear during the PDF conversion.

**Note:** Performance Consideration: If you have any third- party Word macros or add-ins, we recommend removing them. They often add extra overhead to Microsoft Word and slow down the entire PDF conversion process.

Use the following procedure to set up Microsoft Word:

- 1. Log in to the computer as the defined domain account.
- 2. Start Microsoft Word to force the application to register itself.
- **3.** Close all pop-ups that appear during Word initialization.
- 4. Hide the Office Assistant.
- **5.** For Microsoft Word, configure the Customer Feedback Options (and also the other service options, as necessary).
- 6. Exit Microsoft Word.

#### Using Display PDF in Browser

If you are working on a Client machine, you must ensure that you enable/check the **Display PDF in Browser** setting in Adobe Acrobat Reader. If this setting is not enabled, PDF documents will not appear in Argus front-end. This might cause some information status pop-ups to hang on the client machine.

# **Setting Printer Defaults**

When printing Argus reports with Adobe Acrobat, make sure the Page Scaling option in the Print dialog box (File > Print) is set to Shrink to Printable Area.

# **Argus Configuration Files**

By default, Argus Safety logs files in "C:\temp" (default temp directory of Argus Safety). You must ensure that the user under which Safety applications are running has access to this directory.

In the situation where the customer has a different "Temp" directory, the temp directory path needs to be changed 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.

#### **Backing up Configuration Files**

You must ensure to back up the following configuration files before proceeding with this 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. Refer to the following list of commonly modified configuration files:

.\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

# **Argus Integrations**

This chapter provides information about the Argus Integrations and includes discussions of the following:

- Installing Argus Integrations
- Resetting IIS
- Overview: Argus Web Service Interface
- Basic Configuration Overview
- Safety Message Overview
- MedDRA Interface
- Product License Study Interface
- WHO Drug Coding Interface
- Lot Number Interface
- Worklist Intake
- Literature Intake
- Extended E2B Interface

# **Installing Argus Integrations**

Before installing Argus Safety Web, be aware of the following:

- During the installation, the information in this document may be different from what you see on your monitor if additional modules were selected during the Argus Safety Installation.
- A domain account with Local Administrator privileges to the Web server is required after the Argus Safety installation is complete.

Use the following procedure to install Argus Safety Integrations:

- 1. When the system displays the Argus Safety screen:
  - Click **Argus Safety** to start the installation.
- 2. When the system displays the Argus Safety Setup screen:
  - Click Next >.
- **3.** When the system displays the Customer Information screen:
  - Enter the user name in the **User Name** field.

- Enter the company name in the **Company Name** field.
- Click Next >.
- **4.** When the system displays the Default Directory screen, click Browse to select the default installation directory where the Argus Safety Solution Components will be installed.
  - Click Next to display the Argus Safety Components list and select the default installation directory where the Argus Safety Solution Components will be installed.
- 5. When the system displays the component list:
  - Select the modules to install.
  - Click Next >.
- **6.** When the system displays the Argus Safety Solution Components Report Directory screen:
  - Click Browse, select the folder to store the temporary reports in, and click OK.
  - Click **Next** > to continue.

Argus installs and shows the progress of the installation.

- 7. When the system prompts you to enter a port number:
  - Enter the Port for the Argus website (default is 8083, and can be changed to port 80 at any time).
  - Click **Next** > to continue.

The installer installs the website and its related components and shows the progress of the installation.

- 8. When the system displays the Setup Completed screen:
- 9. Click Finish.
- **10.** When the system displays the following message:
- **11.** Click **OK** to reboot the system.

**Note:** After installing Argus Integrations, refer to the section The Argus Safety 8.1 Application Servers to set up the Argus Cryptography key and also to the section Generating Encrypted String from Clear Text on Configured User Cryptography Key to configure Argus Safety Service user passwords.

# **Resetting IIS**

After changes have been made to the areas listed below, IIS needs to be reset to make the latest data / configurations available to the rest of the system:

- **1.** Changes in config files
  - Argus.ini, Argus.xml
- **2.** Changes in following screens through Console:
  - Common Fields
  - System Management

- Enabled Modules
- 3. Loading of MedDRA dictionaries

# **Overview: Argus Web Service Interface**

Argus Web Service Interface supports outbound Interface (MedDRA, WHO Drug and LOT Number) which provides capability to integrate with customer hosted web services and inbound web services (Product-Study-Load Interface) hosted on Argus Safety web server.

All web service based interfaces communicate with the standard SOAP 1.2 Protocol and use WS-Addressing and WS-Security. Argus web service interface leverage Windows Communication Foundation to generate the WS-Addressing and WS-Security header information. It is recommended to test this message before moving too far into business testing. Information on these specifications can be found at the OASIS and W3C websites.

By leveraging WCF, maximum flexibility is provided to the user allowing the selection of which integrations to enable, the transport protocols to use, authentication, etc. by simply updating a standard .config file.

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

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

In a multi-tenant Argus system:

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

### 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 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

(Example: C:\Progam Files\Oracle\ArgusWeb\ASP\Integrations\XSD)

# **Basic Configuration Overview**

### **Outbound Interface**

The web.config file located in the root of the ArgusWeb directory contains all the configuration required for outbound integrations. Two default bindings have been provided, one for basic HTTP traffic and one for SSL communication. For the most basic configuration, simply updating the "address" attribute of the "endpoint" nodes to point to the correct web service address would be sufficient.

To use encryption, the "bindingConfiguration" attribute of the "endpoint" node can be set to "WSHttpBinding\_IRelsysService\_Secure", a binding configuration provided out of the box. As the framework utilizes WCF, additional binding configurations may be created and used as well. Note that the binding configurations between the host and the client must be compatible for successful communication.

Basic user authentication is also supported by the framework. Each endpoint has a counterpart in the ClientCredentials section of the web.config. Simply adding the proper credentials here will instruct WCF to transmit the authentication information.

The framework provides the ability to transform messages using either a custom transformation assembly or an XSLT. Some interfaces, like Lot Number and WHO Drug coding, currently leverage this feature. Activating the transformer is a simple matter of updating the 'TransformerConfiguration' section to map an endpoint to a transformer. If multiple transformers are specified for a particular endpoint, they will be executed in the order in which they appear in the configuration file. The transformers configured by Oracle should not be modified, but additional ones may be added if necessary.

### Inbound Interface

All inbound integrations (file based) are handled by the Argus Safety Windows Service. This service's configuration is located in the RelsysWindowsService.exe.config file located in the .\ArgusWeb\ASP\Argus.NET\Bin directory. This configuration file's primary function is to reference configuration files of configured integrations. The RelsysConfigurationFiles section has several commented "add" nodes. To enable or disable an integration, it is a simple matter of uncommenting or commenting out the node.

This configuration file additionally houses a DatabaseConfiguration section in which the proper database credentials must be specified within the attributes.

# Safety Message Overview

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:

| Interface           | Description  |
|---------------------|--|
| Туре                | An enumeration (currently either "Request" or "Response")<br>to identify the directionality of the message                                   |
| EnterpriseShortName | If Argus Safety is setup as Multi-Tenant system:   |
|                     | EnterpriseShortName will be part of message payload for all outbound interfaces.   |
|                     | EnterpriseShortName is mandatory attribute for Inbound Interface   |
|                     | In single tenant setup, this attribute is not part of<br>outbound message payload and is not required as part of<br>inbound message payload. |
| EXTENSION           | Every Safety Message may also contain an EXTENSION node with CUSTOM sub nodes. These are for future expandability and currently unused.      |

# MedDRA Interface

### **Overview**

MedDRA Encoding web service Interface provides a mechanism to Integrate customer hosted central MedDRA dictionary web service with Argus Safety. Argus Safety expects the data from central MedDRA dictionary web service in defined format as specified by MedDRA dictionary schema.

In a multi-tenant setup, endpoint configuration of central MedDRA 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.

Support for both English and Japanese MedDRA dictionary is supported through this interface. For integrating MedDRA Encoding Web Service Interface with English dictionary refer version 1.0 and for Japanese refer version 1.1 of MedDRA schema

# MedDRA Encoding Safety Message Example

There are two versions of XMLs that are supported by MedDRA Interface (v1.1 and v1.0). The difference between the two is that v1.1 includes support for Japanese Terms. The following example uses "Pain" as the search term for encoding. Examples are mentioned for both MedDRA Xml version 1.0 and 1.1.

### Request (V 1.1)

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">

<s:Header>

<a:Action

s:mustUnderstand="1">http://www.oracle.com/Argus/Contract/v1.0/IRelsysServic e/RelsysServiceRequest</a:Action>

<a:MessageID>urn:uuid:c5b40ac0-a11e-44ea-b3c5-a39636058d63</a:MessageID>

<ActivityId CorrelationId="1872b16d-c293-4abc-8e5c-9ecdab7d3147" xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">

0000000-0000-0000-3100-006000000f0

</ActivityId>

<a:ReplyTo>

<a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>

</a:ReplyTo>

<a:To

s:mustUnderstand="1">http://10.178.87.5/interface/RelsysService.svc</a:To>

```
</s:Header>
```

<s:Body>

<RelsysServiceRequest xmlns="http://www.oracle.com/Argus/Contract/v1.0">

<Msg xmlns:d4p1="http://www.oracle.com/Argus/Types/v1.0"

xmlns:i="http://www.w3.org/2001/XMLSchema-instance">

<d4p1:Version>1.0</d4p1:Version>

```
<d4p1:TransformID />
```

<d4p1:SafetyMessage>

<tnsa:SAFETY\_MESSAGE

xmlns:tns="http://www.oracle.com/Argus/Base/v1.0"

xmlns:tnsa="http://www.oracle.com/Argus/MedDRA\_Request/v1.1"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" tns:Type="Request">

<tnsa:MEDICAL\_DICTIONARY Action="Auto" Source="INDICATION">

<tnsa:TERM>

<tnsa:REPORTED>pain</tnsa:REPORTED>

<tnsa:CODED>pain</tnsa:CODED>

<tnsa:LANG>E</tnsa:LANG>

</tnsa:TERM>

</tnsa:MEDICAL\_DICTIONARY>

</tnsa:SAFETY\_MESSAGE>

</d4p1:SafetyMessage>

</Msg>

</RelsysServiceRequest>

</s:Body>

</s:Envelope>

#### Response (V 1.1)

<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"

xmlns:s="http://www.w3.org/2003/05/soap-envelope">

<s:Header>

<a:Actions:mustUnderstand="1">

http://www.oracle.com/Argus/Contract/v1.0/IRelsysServic

e/RelsysServiceRequestResponse

</a:Action>

<ActivityId CorrelationId="12dda93b-e6fa-4d3a-8d2f-a5cc34588e8a"

xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">

0000000

0-0000-0000-7600-0060000000f3

```
</ActivityId>
```

</s:Header>

<s:Body>

<RelsysServiceRequestResponse

xmlns="http://www.oracle.com/Argus/Contract/v1.0">

```
<RelsysServiceRequestResult
```

```
xmlns:b="http://www.oracle.com/Argus/Types/v1.0"
```

xmlns:i="http://www.w3.org/2001/XMLSchema-instance">

<b:Version>1.0</b:Version>

<br/>cb:TransformID />

<b:SafetyMessage>

<tnsa:SAFETY\_MESSAGE

xsi:noNamespaceSchemaLocation="http://www.oracle.com/Argus/MedDRA\_

Response/v1.1 file:///C:/SS/6 - Argus Interfaces/ASI

6x/RelsysInterfaceLibrary.root/RelsysInterfaceLibrary/RelsysInterfaceComponents/

XSD/v1.1/MedDRA\_Response.xsd" tns:Type="Response"

xmlns:tnsa="http://www.oracle.com/Argus/MedDRA\_Response/v1.1"

xmlns:tns="http://www.oracle.com/Argus/Base/v1.0"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

```
<tnsa:MEDICAL_DICTIONARY>
```

<tnsa:PATHS>

<tnsa:PATH Primary="Y">

<tnsa:LLT>

<tnsa:TEXT>Pain</tnsa:TEXT>

<tnsa:CODE>10033371</tnsa:CODE>

<tnsa:TEXT\_J>??</tnsa:TEXT\_J>

<tnsa:SYNS />

</tnsa:LLT>

<tnsa:PT>

<tnsa:TEXT>Pain</tnsa:TEXT>

<tnsa:CODE>100333712</tnsa:CODE>

<tnsa:TEXT\_J>??</tnsa:TEXT\_J>

</tnsa:PT>

<tnsa:HLT>

<tnsa:TEXT>Pain and discomfort NEC</tnsa:TEXT>

<tnsa:CODE>10033372</tnsa:CODE>

<tnsa:TEXT\_J>?????NEC</tnsa:TEXT\_J>

</tnsa:HLT>

<tnsa:HLGT>

<tnsa:TEXT>General system disorders NEC</tnsa:TEXT>

MedDRA Integration

14-8 Oracle Argus Safety Installation Guide

<tnsa:CODE>10018073</tnsa:CODE>

<tnsa:TEXT\_J>???NEC</tnsa:TEXT\_J>

</tnsa:HLGT>

<tnsa:SOC>

<tnsa:TEXT>General disorders and administration siteconditions</tnsa:TEXT>

<tnsa:CODE>10018065</tnsa:CODE>

<tnsa:TEXT\_J>??????</tnsa:TEXT\_J>

</tnsa:SOC>

</tnsa:PATH>

</tnsa:PATHS>

</tnsa:MEDICAL\_DICTIONARY>

<tns:EXTENSION>

<tns:CUSTOM tns:Name="string" tns:Metadata="string">string</tns:CUSTOM>

</tns:EXTENSION>

</tnsa:SAFETY\_MESSAGE>

</b:SafetyMessage>

</RelsysServiceRequestResult>

</RelsysServiceRequestResponse>

</s:Body>

</s:Envelope>

#### Request (V 1.0)

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing"> <s:Header> <a:Action s:mustUnderstand="1"> http://www.oracle.com/Argus/Contract/v1.0/IRelsysServic e/RelsysServiceRequest </a:Action> <a:MessageID>urn:uuid:c5b40ac0-a11e-44ea-b3c5-a39636058d63</a:MessageID> <ActivityId CorrelationId="1872b16d-c293-4abc-8e5c-9ecdab7d3147" xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics"> 0000000 0-0000-0000-3100-0060000000f0 </ActivityId> <a:ReplyTo> <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address> </a:ReplyTo> <a:To s:mustUnderstand="1">http://10.178.87.5/interface/RelsysService.svc</a:To> </s:Header> <s:Body> <RelsysServiceRequest xmlns="http://www.oracle.com/Argus/Contract/v1.0"> <Msg xmlns:d4p1="http://www.oracle.com/Argus/Types/v1.0" xmlns:i="http://www.w3.org/2001/XMLSchema-instance"> <d4p1:Version>1.0</d4p1:Version> <d4p1:TransformID /> <d4p1:SafetyMessage> <tnsa:SAFETY\_MESSAGE xmlns:tns="http://www.oracle.com/Argus/Base/v1.0" xmlns:tnsa="http://www.oracle.com/Argus/MedDRA\_Request/v1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" tns:Type="Request"> <tnsa:MEDICAL\_DICTIONARY Action="Auto" Source="INDICATION"> <tnsa:TERM> <tnsa:REPORTED>pain</tnsa:REPORTED> <tnsa:CODED>pain</tnsa:CODED>

```
</tnsa:TERM>
```

</tnsa:MEDICAL\_DICTIONARY>

```
</tnsa:SAFETY_MESSAGE>
```

```
</d4p1:SafetyMessage>
```

</Msg>

</RelsysServiceRequest>

</s:Body>

</s:Envelope>

#### Response (V 1.0)

<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"

xmlns:s="http://www.w3.org/2003/05/soap-envelope">

<s:Header>

<a:Action

s:mustUnderstand="1">

http://www.oracle.com/Argus/Contract/v1.0/IRelsysServic

e/RelsysServiceRequestResponse

</a:Action>

<ActivityId CorrelationId="12dda93b-e6fa-4d3a-8d2f-a5cc34588e8a"

xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">

0000000

0-0000-0000-7600-006000000f3

</ActivityId>

</s:Header>

<s:Body>

<RelsysServiceRequestResponse

xmlns="http://www.oracle.com/Argus/Contract/v1.0">

<RelsysServiceRequestResult

xmlns:b="http://www.oracle.com/Argus/Types/v1.0"

xmlns:i="http://www.w3.org/2001/XMLSchema-instance">

<b:Version>1.0</b:Version>

<br/>
<br/>
h:TransformID />

<b:SafetyMessage>

MedDRA Integration

14-10 Oracle Argus Safety Installation Guide

<tnsa:SAFETY\_MESSAGE

xsi:noNamespaceSchemaLocation="http://www.oracle.com/Argus/MedDRA\_

Response/v1.0 file:///C:/SS/6 - Argus Interfaces/ASI

```
6x/RelsysInterfaceLibrary.root/RelsysInterfaceLibrary/RelsysInterfaceComponents/
XSD/v1.0/MedDRA_Response.xsd" tns:Type="Response"
    xmlns:tnsa="http://www.oracle.com/Argus/MedDRA_Response/v1.0"
    xmlns:tns="http://www.oracle.com/Argus/Base/v1.0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <tnsa:MEDICAL_DICTIONARY>
      <tnsa:PATHS>
       <tnsa:PATH Primary="Y">
        <tnsa:LLT>
         <tnsa:TEXT>Pain</tnsa:TEXT>
         <tnsa:CODE>10033371</tnsa:CODE>
         <tnsa:SYNS />
        </tnsa:LLT>
        <tnsa:PT>
         <tnsa:TEXT>Pain</tnsa:TEXT>
         <tnsa:CODE>100333712</tnsa:CODE>
        </tnsa:PT>
        <tnsa:HLT>
         <tnsa:TEXT>Pain and discomfort NEC</tnsa:TEXT>
         <tnsa:CODE>10033372</tnsa:CODE>
        </tnsa:HLT>
        <tnsa:HLGT>
         <tnsa:TEXT>General system disorders NEC</tnsa:TEXT>
         <tnsa:CODE>10018073</tnsa:CODE>
        </tnsa:HLGT>
        <tnsa:SOC>
         <tnsa:TEXT>General disorders and administration site
conditions</tnsa:TEXT>
         <tnsa:CODE>10018065</tnsa:CODE>
        </tnsa:SOC>
       </tnsa:PATH>
      </tnsa:PATHS>
      </tnsa:MEDICAL_DICTIONARY>
      <tns:EXTENSION>
      <tns:CUSTOM tns:Name="string"
tns:Metadata="string">string</tns:CUSTOM>
      </tns:EXTENSION>
```

```
</tnsa:SAFETY_MESSAGE>
```

Product License Study Interface

Argus Integrations 14-11

</b:SafetyMessage>

</RelsysServiceRequestResult>

</RelsysServiceRequestResponse>

</s:Body>

</s:Envelope>

### MedDRA Dictionary: XML Schema

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

Validate MedDRA Interface request and response against the following schema files.

#### **Request: MEDDRA\_Request**

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

#### Schema File

Version 1.0

Top level file: v1.0 MedDRA\_Request.xsd

Sub level file: \v1.0\Base.xsd

#### Version 1.1

Top level file: \v1.1\MedDRA\_Request.xsd Sub level file: \v1.0\Base.xsd

#### Namespace

http://www.oracle.com/Argus/MedDRA\_Request/v1.0 http://www.oracle.com/Argus/MedDRA\_Request/v1.1

where v 1.0, 1.1 is the version of the schema

| Node/Attribute<br>Name | Description  |
|------------------------|--|
| MEDICAL_<br>DICTIONARY | The MEDICAL_DICTIONARY node is the first child node identifying MedDRA integration |

| Node/Attribute<br>Name | Description  |
|------------------------|--|
| Action                 | An enumeration supporting the following values (currently only one):   |
|                        | Auto   |
|                        | This attribute will be present in the request when a full<br>hierarchy is required to be passed back to auto encode the<br>term without using the MedDRA Browser. With an "Auto"<br>message, the system requires that an LLT Term be passed<br>in the request. If the full Hierarchy is not found /<br>returned, the system will open the MedDRA Browsers and<br>display the LLTs returned for manual encoding by the user<br>using the local MedDRA instance. If multiple paths are<br>returned, the Primary SOC path will be used. |
| Source                 | An enumerated value that specifies additional information<br>that may be required for coding based on origination as<br>follows:   |
|                        | <ul> <li>Reaction</li> <li>Case Form   Patient Tab   Patient Tab   Other</li> <li>Relevant History   Reaction</li> <li>Case Form   Patient Tab   Parent Tab   Other</li> <li>Relevant History   Reaction</li> </ul>  |
|                        | <ul> <li>Indication</li> <li>Case Form   Patient Tab   Patient Tab   Other</li> <li>Relevant History   Indication</li> <li>Case Form   Patient Tab   Parent Tab   Other</li> <li>Relevant History   Indication</li> </ul>  |
|                        | <ul> <li>Condition should be verbatim</li> <li>Case Form   Patient Tab   Patient Tab   Other</li> <li>Relevant History   Verbatim</li> <li>Case Form   Patient Tab   Parent Tab   Other</li> <li>Relevant History   Verbatim</li> </ul>  |
|                        | <ul> <li>Lab</li> <li>Console   Code Lists   Lab Test Type</li> </ul>  |
| Description            | Case Form   Events Tab   Event Tab   Description to be<br>Coded  |
|                        | Case Form   Events Tab   Death Information   Cause of<br>Death and Autopsy Results   Description as Reported   |
| Diagnosis              | Argus Case Form   Analysis Tab   Analysis Tab  <br>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 the following nodes.  |
|                        | Reported   |
|                        | Coded  |
| Term(v 1.1)            | The TERM node specifies the information about a specific term that is either being looked up or populated with data and supports the following nodes.  |
|                        | Reported   |
|                        | Coded  |
|                        | Lang   |

# Request: MEDDRA\_Response

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

#### Schema File

Version 1.0

Top level file: \v1.1\MedDRA\_Response.xsd Sub level file: \v1.0\Base.xsd

Version 1.1

Top level file: \v1.1\MedDRA\_Response.xsd

#### Namespace

http://www.oracle.com/Argus/MedDRA\_Response/v1.0

http://www.oracle.com/Argus/MedDRA\_Response/v1.1

where v1.0, 1.1 is the version of the schema

| Node/Attribute |   |
|----------------|---|
| Name           | Description   |
| Primary        | The primary attribute will contain "Y" if the term is the<br>Primary SOC path for the selected term. In the event that<br>multiple terms are returned for a MedDRA level, this<br>attribute is only available on the Primary Term |
| PATHS/PATH     | MedDRA Hierarchy with English Terms only  |
| (version 1.0)  |   |
| PATHS/PATH     | MedDRA Hierarchy with English and Japanese Terms  |
| (Version 1.1)  |   |

### Flow of MedDRA Auto Encoding

When Argus Safety makes a call to the web service, it will populate the REPORTED and CODED nodes with data entered by the user. The REPORTED term is essentially a verbatim while the coded term is the term that is expected to be coded by the remote system. The returned message should contain a PATHS node with PATH subnodes that have been encoded by the remote system. Argus displays the returned LLTs in the MedDRA browser from which the user can select the correct LLT (MedDRA Browser does not open on the Case Bookin Screen). The encoded term is placed on the case form if auto-encoding is enabled an exact match is found of the searched term in the XML. If multiple matches are returned for an exact match, the primary path is used. If the web service does not return any results or is unavailable, Argus presents the user with the MedDRA browser with local dictionary information, if the system is configured to allow this.

### Configuration

Argus Console

MedDRA integration must be enabled using Argus Console. This can be done by opening Console from Argus Safety Web and selecting "System Configuration > System Management" from the menu. Expand the "Case Processing" tree branch and select "Dictionary Browser".

Argus Safety MedDRA Coding Method

Select the radio button to use web services.

- Use Local MedDRA if Term not found by Web Services

An optional check box available to determine whether Argus has to use the local MedDRA instance if the web service hosting MedDRA is not available, fails, or does not return a valid match.

- Use Local MedDRA for Japanese terms
- Web.config

web.config file on each web server under 'ArgusWeb/ASP/' must have the endpoint with the "name" attribute of "MedDRA" 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://remotewebservice/MedDRAAutoEncode.svc" binding="wsHttpBinding" bindingConfiguration="WSHttpBinding\_IRelsysService\_ Unsecure" contract="IRelsysService" name="MedDRA">

Also, the Argus .Net/web.config file on each web server should have the correct Value for the Key MedDRAXMLVersion depending on which version of MedDRA XML is used.

For example:

<add key="MedDRAXMLVersion" value="1.1"/>

OR

<add key="MedDRAXMLVersion" value="1.0"/>

Additionally, the ArgusNet/web.config mentions the paths for both the Request and Response XSDs depending on the version used.

<add InputXSD="...\...\Integrations\XSD\v1.1\MedDRA\_Response.xsd" />

<add InputXSD="..\..\Integrations\XSD\v1.1\MedDRA\_Request.xsd" />

# Product License Study Interface

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

 In the Integrations folder in the following path <Installation Path>\Oracle\ArgusWeb\ASP\Integrations, open the file Service.config. Search for the section called DatabaseConfiguration:

<DatabaseConfiguration DBName="" DBUser="" DBPassword="" />

The DBName, DBUser and DBPassword need to be populated manually.

DBName: This is the TNS of the Argus database

DBUser: This is the user name of a AG Service user. The PSL web service uses this User Context to perform updates in the Argus Safety Database.

DBPassword: Generate new encrypted string, as mentioned in the Generating Encrypted String from Clear Text on Configured User Cryptography Key section.

A sample configuration would be:

<DatabaseConfiguration DBName="ARGOLDDEMO" DBUser="agservice1" DBPassword="BC90A10363A26C147DEF172D61AAEC110296FA9E181E7FFA687D 58CE08610C08" />

Security Configuration

If the PSL web service is desired to be run under security, appropriate binding configurations need to be configured in web.config under the Integrations folder. This can be done either manually or through the Service Config Utility.

Logging

PSL Web service performs two kinds of logging. One is file logging using the Relsys Logger. This involves logging information about the errors, warnings, and processing of the PSL web service code. The configuration for this type of logging is present in web.config, under the section <logConfig>. There are four types of logging - Error, Warning, Information, and Verbose. By default, the logger is configured to be of Error level. The logger internally uses log4net component to perform the logging. The RollingLogFileAppender which is by default present in web.config needs to be configured to log information to a specific file on a local folder. Ensure that read/write permissions are available to the web service for this folder.

Another type of logging is the SOAP message logger, called the RequestLogger. This logger 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 in this release. This logging can be turned off by setting the Enabled attribute to false in Service.config as shown below:

<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>

**Note:** 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/Customer Support teams.

# WHO Drug Coding Interface

### Overview

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.

### WHO Drug Coding Safety Message Example

#### Request

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing">
 <s:Header>
 <a:Actions:mustUnderstand="1">
http://www.oracle.com/Argus/Contract/v1.0/IRelsysService/RelsysServiceRequest
 </a:Action>
 <a:MessageID>urn:uuid:7a0f0c6e-f7f9-41f3-85bf-750a00cb16e7</a:MessageID>
 <ActivityId CorrelationId="09440b01-70e2-4d24-b12c-202119e3adea"
 xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">
  0000000
  0-0000-0000-8f0f-0060010000f1
 </ActivityId>
 <a:ReplyTo>
   <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
 </a:ReplyTo>
 <a:To
s:mustUnderstand="1">http://10.178.87.5/interface/RelsysService.svc</a:To>
 </s:Header>
 <s:Body>
 <RelsysServiceRequest xmlns="http://www.oracle.com/Argus/Contract/v1.0">
   <Msg xmlns:b="http://www.oracle.com/Argus/Types/v1.0"
   xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
    <b:Version>1.0</b:Version>
    <br/>cb:TransformID>WHO_DRUG</b:TransformID>
    <b:SafetyMessage>
     <tnsa:SAFETY_MESSAGE tns:Type="Request"
    xmlns:tnsa="http://www.oracle.com/Argus/WHODrug_Request/v1.0"
    xmlns:tns="http://www.oracle.com/Argus/Base/v1.0">
      <tnsa:DRUG_DICTIONARY>
       <tnsa:DRUG>
```

<tnsa:DRUG\_NAME>n22</tnsa:DRUG\_NAME>

```
</tnsa:DRUG>
```

</tnsa:DRUG\_DICTIONARY>

```
</tnsa:SAFETY_MESSAGE>
```

```
</b:SafetyMessage>
```

</Msg>

</RelsysServiceRequest>

</s:Body>

</s:Envelope>

#### Response

<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"

xmlns:s="http://www.w3.org/2003/05/soap-envelope">

<s:Header>

<a:Action

s:mustUnderstand="1">

http://www.oracle.com/Argus/Contract/v1.0/IRelsysServic

e/RelsysServiceRequestResponse

</a:Action>

<ActivityId CorrelationId="ffb00b07-d1f8-4fa9-ae9f-488d79dda872"

xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics"> 0000000

000000

0-0000-0000-8f0f-0060010000f1

</ActivityId>

</s:Header>

<s:Body>

<RelsysServiceRequestResponse

xmlns="http://www.oracle.com/Argus/Contract/v1.0">

<RelsysServiceRequestResult

xmlns:d4p1="http://www.oracle.com/Argus/Types/v1.0"

xmlns:i="http://www.w3.org/2001/XMLSchema-instance">

<d4p1:Version>1.0</d4p1:Version>

<d4p1:TransformID />

<d4p1:SafetyMessage>

<tnsa:SAFETY\_MESSAGE

xmlns:tns="http://www.oracle.com/Argus/Base/v1.0"

xmlns:tnsa="http://www.oracle.com/Argus/WHODrug\_Response/v1.0"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://www.oracle.com/Argus/WHODrug\_ Response/v1.0 file:///E:/6%20-%20Argus%20Interfaces/ASI%2042%20SP3/RelsysInterfaceLibrary.r oot/RelsysInterfaceLibrary/RelsysInterfaceComponents/XSD/v1.0/WHODrug\_ Response.xsd" tns:Type="Response"> <tnsa:DRUG\_DICTIONARY> <tnsa:DRUGS> <tnsa:DRUG> <tnsa:DRUG\_CODE>000200.01.005</tnsa:DRUG\_CODE> <tnsa:DRUG\_NAME>TYLENOL</tnsa:DRUG\_NAME> <tnsa:GENERIC\_NAME>PARACETAMOL</tnsa:GENERIC\_NAME> <tnsa:ATCS> <tnsa:ATC> <tnsa:CODE>65GGH</tnsa:CODE> <tnsa:DESCRIPTION>ATC Desc 1a</tnsa:DESCRIPTION> </tnsa:ATC> <tnsa:ATC> <tnsa:CODE>94534</tnsa:CODE> <tnsa:DESCRIPTION>ATC Desc 2a</tnsa:DESCRIPTION> </tnsa:ATC> </tnsa:ATCS> <tnsa:INGREDIENTS> <tnsa:INGREDIENT>PARACETAMOL</tnsa:INGREDIENT> </tnsa:INGREDIENTS> <tnsa:MEDICINAL\_PRODUCT\_ID /> <tnsa:DRUG\_MANUFACTURER> MCNEIL LABORATORIES, **INCORPORATED** </tnsa:DRUG MANUFACTURER> </tnsa:DRUG> <tnsa:DRUG> <tnsa:DRUG\_CODE> 004468.01 begin\_of\_the\_skype\_highlighting 004468.01 end\_of\_the\_skype\_highlighting.003 </tnsa:DRUG\_CODE> <tnsa:DRUG\_NAME>TYLENOL ALLERGY SINUS</tnsa:DRUG\_NAME> <tnsa:GENERIC\_NAME />

<tnsa:ATCS>

<tnsa:ATC>

<tnsa:CODE>4UUT1</tnsa:CODE>

<tnsa:DESCRIPTION>ATC Desc 1b</tnsa:DESCRIPTION>

</tnsa:ATC>

<tnsa:ATC>

<tnsa:CODE>13LLP</tnsa:CODE>

<tnsa:DESCRIPTION>ATC Desc 2b</tnsa:DESCRIPTION>

</tnsa:ATC>

</tnsa:ATCS>

<tnsa:INGREDIENTS>

<tnsa:INGREDIENT>PARACETAMOL</tnsa:INGREDIENT>

<tnsa:INGREDIENT>CHLORPHENAMINE

MALEATE</tnsa:INGREDIENT>

<tnsa:INGREDIENT>

PSEUDOEPHEDRINE

HYDROCHLORIDE

</tnsa:INGREDIENT>

</tnsa:INGREDIENTS>

<tnsa:MEDICINAL\_PRODUCT\_ID />

<tnsa:DRUG\_MANUFACTURER>JOHNSON</tnsa:DRUG\_ MANUFACTURER>

</tnsa:DRUG>

</tnsa:DRUGS>

</tnsa:DRUG\_DICTIONARY>

<tns:EXTENSION>

<tns:CUSTOM tns:Name="" tns:Metadata="" />

</tns:EXTENSION>

</tnsa:SAFETY\_MESSAGE>

</d4p1:SafetyMessage>

</RelsysServiceRequestResult>

</RelsysServiceRequestResponse>

</s:Body>

</s:Envelope>

### 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.

#### 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

Sub level 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_<br>DICTIONARY | First Child node under SAFETY_MESSAGE which represents the WHO Drug Dictionary integration |
| DRUG/DRUG_<br>NAME  | WHO Drug Name that needs to be searched in central WHO Drug Coding system.                 |

#### 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

Sub level 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_<br>DICTIONARY | First Child node under SAFETY_MESSAGE which represents the Drug Dictionary integration. |
| DRUGS/DRUG          | WHO DRUG details  |

### Flow of Drug Dictionary Coding

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.

### 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 check box 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://remotewebservice/WHODrugLookup.svc" binding="wsHttpBinding" bindingConfiguration="WSHttpBinding\_ IRelsysService\_Unsecure" contract="IRelsysService" name="WHODrug"></endpoint>

# Lot Number Interface

### Overview

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.

### Lot Number Safety Message Example

#### Request

```
<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"
xmlns:s="http://www.w3.org/2003/05/soap-envelope">
 <s:Header>
  <a:Action
 s:mustUnderstand="1">
  http://www.oracle.com/Argus/Contract/v1.0/IRelsysServic
  e/RelsysServiceRequest
 </a:Action>
 <a:MessageID>urn:uuid:4ea4a68c-9930-4681-a3dd-839b04821320</a:MessageID>
 <ActivityId CorrelationId="b7b67964-6e82-46d7-97ed-ff0e9f36dc66"</p>
 xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">
  0000000
  0-0000-0000-0000-000000000000
 </ActivityId>
 <a:ReplyTo>
   <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
 </a:ReplyTo>
 </s:Header>
 <s:Body>
 <RelsysServiceRequest xmlns="http://www.oracle.com/Argus/Contract/v1.0">
   <Msg xmlns:d4p1="http://www.oracle.com/Argus/Types/v1.0"
  xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
    <d4p1:Version>1.0</d4p1:Version>
    <d4p1:TransformID>LOT_NUMBER</d4p1:TransformID>
    <d4p1:SafetyMessage>
     sb:SAFETY MESSAGE
xmlns:tns="http://www.oracle.com/Argus/Base/v1.0"
xmlns:tnsa="http://www.oracle.com/Argus/ProductFamilyEntity/v1.0"xmlns:tnsb="
http://www.oracle.com/Argus/Lot_Request/v1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" tns:Type="Request">
      <tnsb:LOT_LOOKUP>
       <tnsb:LOT>
        <tnsa:LOT_NUMBER>666</tnsa:LOT_NUMBER>
       </tnsb:LOT>
```

```
</tnsb:LOT_LOOKUP>
```

```
</tnsb:SAFETY_MESSAGE>
```

```
</d4p1:SafetyMessage>
```

```
</Msg>
```

</RelsysServiceRequest>

```
</s:Body>
```

</s:Envelope>

#### Response

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing">
 <s:Header>
  <a:Action s:mustUnderstand="1">
  http://www.oracle.com/Argus/Contract/v1.0/IRelsysServic
  e/RelsysServiceRequestResponse
 </a:Action>
 <a:RelatesTo>urn:uuid:4ea4a68c-9930-4681-a3dd-839b04821320</a:RelatesTo>
 </s:Header>
 <s:Body>
 <RelsysServiceRequestResponse
 xmlns="http://www.oracle.com/Argus/Contract/v1.0">
   <RelsysServiceRequestResult
xmlns:b="http://www.oracle.com/Argus/Types/v1.0"
  xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
    <b:Version>1.0</b:Version>
    <br/>b:TransformID />
    <b:SafetyMessage>
    <tnsb:SAFETY_MESSAGE
    tns:Type="Response"
    xmlns:tnsb="http://www.oracle.com/Argus/Lot_Response/v1.0"
    xmlns:tns="http://www.oracle.com/Argus/Base/v1.0"
    xmlns:tnsa="http://www.oracle.com/Argus/ProductFamilyEntity/v1.0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <tnsb:LOT_LOOKUP>
       <tnsb:LOT>
        <tnsa:LOT_NUMBER>5043AX1</tnsa:LOT_NUMBER>
        <tnsa:EXPIRATION_DATE>2010-06-07</tnsa:EXPIRATION_DATE>
```

<trs:CUSTOM tns:Name="Thermisol" tns:Metadata="Thermisol Indicator">15</tns:CUSTOM>

<trs:CUSTOM tns:Name="Albumin" tns:Metadata="Albumin Status">11.4mg/gC</tns:CUSTOM>

</tnsb:LOT>

<tnsb:LOT>

<tnsa:LOT\_NUMBER>javascript</tnsa:LOT\_NUMBER>

<tnsa:EXPIRATION\_DATE>2014-12-15</tnsa:EXPIRATION\_DATE>

<tns:CUSTOM tns:Name="Thermisol" tns:Metadata="ThermisolIndicator">22</tns:CUSTOM>

<tns:CUSTOM tns:Name="Albumin" tns:Metadata="Albumin</th>Status">19.5mg/gC</tns:CUSTOM>

</tnsb:LOT>

</tnsb:LOT\_LOOKUP>

<tns:EXTENSION>

<tns:CUSTOM tns:Name="string" tns:Metadata="string">string</tns:CUSTOM>

<tns:CUSTOM tns:Name="string" tns:Metadata="string">string</tns:CUSTOM>

</tns:EXTENSION>

</tnsb:SAFETY\_MESSAGE>

</b:SafetyMessage>

</RelsysServiceRequestResult>

</RelsysServiceRequestResponse>

</s:Body>

</s:Envelope>

### 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.

#### **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

Sub level 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: |
|                | ■ LOT_NUMBER   |
|                | <ul> <li>EXPIRATION_DATE</li> </ul>  |

### **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

Sub level 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<br>name | Description  |  |  |
|------------------------|--|--|--|
| LOT_LOOKUP             | First Child node under SAFETY_MESSAGE which represents the Lot Number integration.                                   |  |  |
| LOT                    | LOT Number   |  |  |
|                        | <ul> <li>Expiration Date</li> </ul>  |  |  |
|                        | Custom   |  |  |
|                        | Provides a mechanism   |  |  |
|                        | <b>Name</b> : Attribute value is used to identify Case Form field that is to be populated with data in the node      |  |  |
|                        | <b>Metadata</b> : Attribute value is used as labels in the LOT Number selection selection dialog displaying the data |  |  |

### Flow of Lot Validation

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.

### 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://remotewebservice/LotValidate.svc" binding="wsHttpBinding" bindingConfiguration="WSHttpBinding\_IRelsysService\_Unsecure" contract="IRelsysService" name=" LotQuery"></endpoint>

<add Transformer="LotQuery2" Assembly="RelsysInterfaceComponents" Type="Relsys.InterfaceComponents.XSLTTFactory" 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.

### 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: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.

# 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.

## Flow of Worklist Intake

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.

### Worklist Intake Safety Message Example

```
Request - Worklist Intake Safety Message (Multi-Tenant System)
<?xml version="1.0" encoding="utf-8"?>
<tnsc:SAFETY_MESSAGE
xmlns:tnszz="http://www.oracle.com/Argus/Base/v1.0"
xmlns:tnsc="http://www.oracle.com/Argus/Case_Intake/v1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
tnszz:Type="Request" tnszz:EnterpriseShortName ="ENT01">
<tnsc:CASE_INTAKE>
<tnsc:CASES>
<tnsc:CASE>
<tnsc:CASE_TYPE>Spontaneous</tnsc:CASE_TYPE>
<tnsc:COUNTRY_OF_INCIDENCE>UNITED STATES</tnsc:COUNTRY_OF_
INCIDENCE>
<tnsc:EVENT_PT>Pain</tnsc:EVENT_PT>
<tnsc:EVENT_VERBATIM>Pain</tnsc:EVENT_VERBATIM>
<tnsc:FLTH>LT</tnsc:FLTH>
<tnsc:GENERIC_NAME>D-RIBOSE</tnsc:GENERIC_NAME>
<tnsc:INITIAL_DATE>2012-01-31</tnsc:INITIAL_DATE>
<tnsc:PRIORITY>1</tnsc:PRIORITY>
<tnsc:PRODUCT_NAME>Cure All</tnsc:PRODUCT_NAME>
<tnsc:REPORTER_TYPE>Health Care Professional</tnsc:REPORTER_TYPE>
<tnsc:SITE>US</tnsc:SITE>
<tnsc:STUDY_ID>STUDY 001</tnsc:STUDY_ID>
<tnsc:SUR>No</tnsc:SUR>
<tnsc:ATTACHMENTS xmlns:tnsc="http://www.oracle.com/Argus/Case_
Intake/v1.0">
<tnsc:ATTACHMENT>
<tnsc:FILENAME>Case12345.pdf</tnsc:FILENAME>
<tnsc:DOCID>001219988776655</tnsc:DOCID>
```

<tnsc:CLASSIFICATION>CIRM Case</tnsc:CLASSIFICATION>

<tnsc:ATTACHMENT\_DESC>Contains case data for 12345</tnsc:ATTACHMENT\_DESC>

</tnsc:ATTACHMENT>

</tnsc:ATTACHMENTS >

</tnsc:CASE>

</tnsc:CASES>

</tnsc:CASE\_INTAKE>

<tnszz:EXTENSION>

<tnszz:CUSTOM tnszz:Name="My Name" tnszz:Metadata="My Metadata">My Value</tnszz:CUSTOM>

</tnszz:EXTENSION>

</tnsc:SAFETY\_MESSAGE>

#### Response - Worklist Intake Safety Message (Multi-Tenant system)

<?xml version="1.0" encoding="utf-8"?>

<tnse:SAFETY\_MESSAGE xmlns:tns="http://www.oracle.com/Argus/Base/v1.0" xmlns:tnse="http://www.oracle.com/Argus/Case\_Intake\_Ack/v1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns:a="http://tempuri.org/CaseIntakeResponse.xsd"

tns:Type="Response"> tns:EnterpriseShortName="ENT01">

<tnse:CASE\_INTAKE>

<tnse:CASES>

<tnse:CASE>

<tnse:INTAKE\_DATE>03-NOV-2014 10:08:49</tnse:INTAKE\_DATE>

<tnse:CASE\_NUMBER>12US00000001</tnse:CASE\_NUMBER>

<tnse:CASE\_ID>10285117</tnse:CASE\_ID>

<tnse:CASE\_PRODUCT>Cure All</tnse:CASE\_PRODUCT>

<tnse:DATE\_TIME>03-NOV-2014 15:40:07</tnse:DATE\_TIME>

<tnsc:ATTACHMENTS xmlns:tnsc="http://www.oracle.com/Argus/Case\_ Intake/v1.0">

<tnsc:ATTACHMENT>

<tnsc:FILENAME>Case12345.pdf</tnsc:FILENAME>

<tnsc:DOCID>001219988776655</tnsc:DOCID>

<tnsc:CLASSIFICATION></tnsc:CLASSIFICATION>

<tnsc:ATTACHMENT\_DESC>Contains case data for 12345</tnsc:ATTACHMENT\_DESC>

</tnsc:ATTACHMENT>

</tnsc:ATTACHMENTS>

</tnse:CASE>

</tnse:CASES>

</tnse:CASE\_INTAKE>

<tnszz:EXTENSION xmlns:tnszz="http://www.oracle.com/Argus/Base/v1.0">

<tnszz:CUSTOM tnszz:Name="My Name" tnszz:Metadata="My Metadata">My Value</tnszz:CUSTOM>

</tnszz:EXTENSION>

</tnse:SAFETY\_MESSAGE>

#### Request - Worklist Intake Safety Message (Single-Tenant System)

<?xml version="1.0" encoding="utf-8"?>

<tnsc:SAFETY\_MESSAGE

xmlns:tnszz="http://www.oracle.com/Argus/Base/v1.0"

xmlns:tnsc="http://www.oracle.com/Argus/Case\_Intake/v1.0"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

tnszz:Type="Request"

<tnsc:CASE\_INTAKE>

<tnsc:CASES>

<tnsc:CASE>

<tnsc:CASE\_TYPE>Spontaneous</tnsc:CASE\_TYPE>

<tnsc:COUNTRY\_OF\_INCIDENCE>UNITED STATES</tnsc:COUNTRY\_OF\_ INCIDENCE>

<tnsc:EVENT\_PT>Pain</tnsc:EVENT\_PT>

<tnsc:EVENT\_VERBATIM>Pain</tnsc:EVENT\_VERBATIM>

<tnsc:FLTH>LT</tnsc:FLTH>

<tnsc:GENERIC\_NAME>D-RIBOSE</tnsc:GENERIC\_NAME>

<tnsc:INITIAL\_DATE>2012-01-31</tnsc:INITIAL\_DATE>

<tnsc:PRIORITY>1</tnsc:PRIORITY>

<tnsc:PRODUCT\_NAME>Cure All</tnsc:PRODUCT\_NAME>

<tnsc:REPORTER\_TYPE>Health Care Professional</tnsc:REPORTER\_TYPE>

<tnsc:SITE>US</tnsc:SITE>

<tnsc:STUDY\_ID>STUDY 001</tnsc:STUDY\_ID>

<tnsc:SUR>No</tnsc:SUR>

<tnsc:ATTACHMENTS xmlns:tnsc="http://www.oracle.com/Argus/Case\_ Intake/v1.0">

<tnsc:ATTACHMENT>

<tnsc:FILENAME>Case12345.pdf</tnsc:FILENAME>

<tnsc:DOCID>001219988776655</tnsc:DOCID>

<tnsc:CLASSIFICATION>CIRM Case</tnsc:CLASSIFICATION>

<tnsc:ATTACHMENT\_DESC>Contains case data for 12345</tnsc:ATTACHMENT\_DESC>

</tnsc:ATTACHMENT>

</tnsc:ATTACHMENTS >

</tnsc:CASE>

</tnsc:CASES>

</tnsc:CASE\_INTAKE>

<tnszz:EXTENSION>

<tnszz:CUSTOM tnszz:Name="My Name" tnszz:Metadata="My Metadata">My Value</tnszz:CUSTOM>

</tnszz:EXTENSION>

</tnsc:SAFETY\_MESSAGE>

#### Response - Worklist Intake Safety Message (Single-Tenant system)

<?xml version="1.0" encoding="utf-8"?>

<tnse:SAFETY\_MESSAGE xmlns:tns="http://www.oracle.com/Argus/Base/v1.0" xmlns:tnse="http://www.oracle.com/Argus/Case\_Intake\_Ack/v1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns:a="http://tempuri.org/CaseIntakeResponse.xsd"

tns:Type="Response">

<tnse:CASE\_INTAKE>

<tnse:CASES>

<tnse:CASE>

<tnse:INTAKE\_DATE>03-NOV-2014 10:08:49</tnse:INTAKE\_DATE>

<tnse:CASE\_NUMBER>12US00000001</tnse:CASE\_NUMBER>

<tnse:CASE\_ID>10285117</tnse:CASE\_ID>

<tnse:CASE\_PRODUCT>Cure All</tnse:CASE\_PRODUCT>

<tnse:DATE\_TIME>03-NOV-2014 15:40:07</tnse:DATE\_TIME>

<tnsc:ATTACHMENTS xmlns:tnsc="http://www.oracle.com/Argus/Case\_ Intake/v1.0">

<tnsc:ATTACHMENT>

<tnsc:FILENAME>Case12345.pdf</tnsc:FILENAME>

<tnsc:DOCID>001219988776655</tnsc:DOCID>

<tnsc:CLASSIFICATION></tnsc:CLASSIFICATION>

<tnsc:ATTACHMENT\_DESC>Contains case data for 12345</tnsc:ATTACHMENT\_DESC>

</tnsc:ATTACHMENT>

</tnsc:ATTACHMENTS>

</tnse:CASE>

</tnse:CASES>

</tnse:CASE\_INTAKE>

```
<tnszz:EXTENSION xmlns:tnszz="http://www.oracle.com/Argus/Base/v1.0">
```

<tnszz:CUSTOM tnszz:Name="My Name" tnszz:Metadata="My Metadata">My Value</tnszz:CUSTOM>

</tnszz:EXTENSION>

</tnse:SAFETY\_MESSAGE>

### 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.

# 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)

### Flow of Literature Intake

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 Intake.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.

- 1. Accept
- 2. Reject
- 3. Assign User
- 4. Assign Literature Type
- 5. Modify Product Family

### 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).

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.

#### Metadata Configuration

- 1. Go to the Argus Web server machine.
- 2. Open the service.config file located at

C:\Program Files\Oracle\Argus\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>

# **Extended E2B Interface**

This section provides information about the Extended E2B Interface.

# **E2B Mapping Updates**

The following steps in this section will create Extension Profile using E2B Mapping.

- 1. Log on to ESM Mapping Utility.
- 2. Select a **Profile** from the drop-down list.

For example, ICH-ICSR V2.1 MESSAGE TEMPLATE - EMA.

- **3.** Click the Administrator menu and select the **Copy Profile** option. Enter the Extension Profile name, Click on Save button and then OK button.
- 4. Select the newly created profile from the drop-down list.
- **5.** Click the Receive tab. Select any DTD element. For example, SAFETYREPORTVERSION.
- **6.** Select the Extended E2B check box and click Save. This profile is now enabled as an extended profile.
- 7. Exit from the ESM Mapping Utility.

## Adding Extension Elements to DTD

The following steps in this section will add the Extension element in the DTD file.

- Take the DTD file corresponding to the base profile chosen in the above section from the '<ESM Installation Directory>\Argus\InterchangeService\DTDFiles' folder and make a copy of that profile. In this example, we will make a copy of 'EMA-ICSR-V2.1.dtd' and name it as 'EMA-ICSR-V2.1-Extension.dtd'.
- **2.** Open the file 'EMA-ICSR-V2.1-Extension.dtd' and include the extension DTD Element "patientethnicity\_extension?". To do so, add the element details in the header row, as highlighted in the following image:

**3.** Add the element details as an individual entity, as highlighted in the following image:

```
EMEAEXT-ICSR-V2.1.dtd
<!-- B.3.2 Results of tests and procedures relevant to the investigation of the patient -->
Field ref:
Field title:
                   B.3.2
                   Results of tests and procedures relevant to the investigation of the patient
Field name:
Field length:
Field values:
                  resultstestsprocedures
2000AN
<! ELEMENT resultstestsprocedures (#PCDATA)>
<! ATTLIST
           resultstestsprocedures
         %lang.att;
<!-- B.3.2a Ethnicity of the patient -->
Field ref:
Field title:
                  B.3.2a
Ethnicity of the patient
patientethnicity_extension
200AN
Field name
Field length:
Field values:
<!-- B.4.k.1 Characterization of drug -->
Field ref:
Field title:
                  B.4.k.1
Characterization of drug
Field name: dru
Field length: 1N
Field values:
                   drugcharacterization
1=Suspect
2=Concomitant
3=Interacting
< ! ELEMENT drugcharacterization (#PCDATA)>
<!ATTLIST drugcharacterization
         %lang.att;
```

**4.** Save the updated DTD file in the same folder where all other DTD files exist on the ESM Server.

### Prepare Factory Data for Extension Elements

The following steps in this section will create a factory data for extension elements. Factory data is required to import extension XML.

- 1. CFG\_E2B: This table keeps the details of all the E2B elements present in all the E2B profiles. The following is a description of all the fields in this table:
  - Profile (PROFILE): This is an alphanumeric field. It is the name of the profile to which the extension elements will be added.
  - DTD Element (DTD\_ELEMENT): This is an alphanumeric field. It is the name of the extension element. This should always end with text '\_EXTENSION'. The name may contain [a-z], [A-Z], [0-9], or an underscore character. This shall be the same as the name of the extension element specified in the DTD file.
  - Hierarchy Level (HIE\_LEVEL): This is a numeric field. This number shall be the same as that of the other DTD elements under the same parent element.
  - DTD Length (DTD\_LENGTH): This is a numeric field. This is the maximum allowed length for the extension element value.
  - Mandatory (MANDATORY): This is an alphanumeric field. If the extension element is mandatory, then the value of this field shall be 'M'. If the extension is mandatory optional, it shall be 'MO'. If it is none of the above, leave it blank.
  - Order of Execution (ORDER\_OF\_EXECUTION): This is a numeric field. It identifies the order of an E2B element while building the E2B report. This number shall be between the ORDER\_OF\_EXECUTION values of the E2B elements between which the extension element is to be placed.

For example, if the new extension element PATIENTETHNICITY\_ EXTENSION is to be placed between PATIENTHEIGHT and PATIENTSEX which have ORDER\_OF\_EXECUTION as 116 and 117, then the value of ORDER\_OF\_EXECUTION for the new extension field can be anything like 116.1, 116.2, etc.

- Association Element (AE\_SELECT\_STMT\_ELEMENT\_ASSOC): This is an alphanumeric field. It is the name of that element which contains the transmission mapping SQL of this element. Generally, it shall be the same as the parent element.
- Column Position (AE\_SELECT\_STMT\_COL\_POSITION): This is a numeric field. This is the position of the element in the transmission mapping SQL query, which is specified with the Association element.

For example, if the SQL with the association element has 10 fields/columns in the SELECT statement, and the current E2B element maps to the fourth field/column, then the value of this field shall be set to 4.

- Parent element (PARENT\_ELEMENT): This is an alphanumeric field. It identifies the name of the parent E2B element in the E2B XML hierarchy structure. It shall be the same as the value specified for the other peer E2B elements.
- Data Element (DATA\_ELEMENT): This is an alphanumeric field. This is the reference number of the element specified by ICH like A.1.2 for OCCURCOUNTRY, B.1.1 for PATIENTINITIAL, etc. This field can be empty for extension elements. However, if preferred, the end-user can specify any value for this field.
- AE Case Form GUI (AE\_CASE\_FORM\_GUI): This is an alphanumeric field. This field shall specify the Case Form GUI location of the field to which the E2B element is mapped in the format? <Tab Name> - <Section Name> - <Field Name>".

For example, "Patient Tab - Patient Details - Ethnicity".

- Title (DTD\_ELEMENT\_TITLE): This is an alphanumeric field. This field specifies the display title for the extension element e.g. "Ethnicity". This title is displayed in the Decoded View screen in E2B viewer.
- Element Type (DTD\_ELEMENT\_TYPE): This is a numeric field. It contains the type of the E2B element, as described in the CFG\_DTD\_ELEMENT\_TYPE table.
  - Other
  - E2B Code
  - Country
  - Time Period Unit
  - Yes/No
  - Date Format
  - Date
  - MedDRA Version
  - MedDRA Term/Code
- **2.** Factory Data for CFG\_E2B table: Create a .ctl file and use sqlloader utility to load the factory data in CFG\_E2B table. This table holds the extension elements definition, import business logic, mandatory, order of execution, etc.

- **3.** LM\_ESM\_ARGUS\_MAPPING: This table is used to map the E2B elements with the Case Form field during E2B Import. This table is not used during the E2B transmission process.
  - DTD Element (DTD\_ELEMENT): This is an alphanumeric field. It is the name
    of the extension element, as specified in CFG\_E2B table. This should always
    end with text '\_EXTENSION'. The name may contain [a-z], [A-Z], [0-9] or an
    underscore character. This shall be the same as the name of the extension
    element specified in the DTD file.
  - Field ID (FIELD\_ID): This is a numeric field. It shall contain the CMN\_ FIELDS.FIELD\_ID value of the Case Form field, which shall be populated or updated for the extension element during E2B Import.
- **4.** Factory data for LM\_ESM\_ARGUS\_MAPPING table: Create a .ctl file and use the sqlloader utility to load factory data in the LM\_ESM\_ARGUS\_MAPPING table. This table holds the mapping from DTD elements to the Argus Case Form fields.

### **Create Business Logic for Extension Elements**

The following steps in this section will create an import business logic as a PL/SQL block for each extension elements using E2B Mapping.

- 1. Log on to the ESM Mapping Utility.
- 2. Select the extension profile from the drop down list.
- **3.** Click on the Receive Tab and select the extension element and write the import business logic as a PL/SQL block and click on the save button to save the PLSQL block.
- 4. Exit from the ESM Mapping Utility after completing the business logic.

### Configure Reporting Destination for Extension Profile

The following steps in this section will configure the extension profile in Reporting Destination using Argus Console.

- **1.** Log on to Argus Safety.
- 2. Open the Console and click on the Code List | Reporting Destination.
- **3.** Select the agency name to modify and click on the EDI tab.
- **4.** Select the extension profile from the message profile drop down Example: "EXTENDED E2B PROFILE"
- Enter the extension DTD file with full path into URL of Message DTD field Example: "C:\Program Files\Oracle\ESMService\DTD\EMA-ICSR-V2.1-Extension.dtd"

**Note:** This field is used only for transmission of E2B extension for import this field is not used, since the DTD path is already embedded in the E2B file.

**6.** Click on the Save button to save the changes. Argus is configured for E2B extension for selected agency.

### Extension Elements Sample XML

<patient>

<patientinitial>TMS</patientinitial>

<patientonsetage>66</patientonsetage>

<patientonsetageunit>801</patientonsetageunit>

<patientsex>1</patientsex>

<patientethnicity\_extension>Asian</patientethnicity\_extension>

<reaction>

<primarysourcereaction>fever</primarysourcereaction>

<reactionmeddraversionllt>10.1</reactionmeddraversionllt>

<reactionmeddrallt>10016558</reactionmeddrallt>

<reactionmeddraversionpt>10.1</reactionmeddraversionpt>

<reactionmeddrapt>Pyrexia</reactionmeddrapt>

<reactionintensity\_extension>Mild</reactionintensity\_extension>

<reactionhospstartdateformat\_extension>102</reactionhospstartdateformat\_extension>

<reactionhospstartdate\_extension>20090117</reactionhospstartdate\_extension>

<reactionhospstopdateformat\_extension>102</reactionhospstopdateformat\_extension>

<reactionhospstopdate\_extension>20090123</reactionhospstopdate\_extension>

</reaction>

</patient>

### Extension Elements Sample Import PL/SQL Block

DECLARE

v\_xml varchar2(32767);

l\_ethnicity\_id number;

l\_return number := 0;

BEGIN

v\_xml := ESM\_IMP.F\_READ\_EXTENSION(:REPORT\_ID,:DTD\_ELEMENT);

if v\_xml is not null then

l\_ethnicity\_id := ESM\_IMP\_UTL.f\_get\_id\_from\_value('LM\_ ETHNICITY','ETHNICITY',v\_xml,'ETHNICITY\_ID');

if l\_ethnicity\_id > 0 then

l\_return := ESM\_IMP.F\_WRITE(:REPORT\_ID,:PARENT\_ELEMENT,:DTD\_ ELEMENT,:PROFILE,'CASE\_PAT\_INFO','ETHNICITY\_ID',l\_ethnicity\_id);

end if;

end if;

END;

<u>17</u>

# Argus Password Management -Cryptography Tool

This chapter provides instructions for using the Cryptography tool in Argus Safety.

# **Cryptography Tool Overview**

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.

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

Once the key file has been created, it should be copied 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.

**Note:** Once the ArgusSecureKey.ini file has been generated, there is no need to run this tool again while launching Argus Safety Schema Creation Tool. The tool should only be run again if you are resetting passwords, keys or have lost the ArgusSecureKey.ini file.

# Installing or Upgrading to Argus Safety 8.1

Whether you are upgrading to Argus Safety 8.1 or installing a fresh instance of it, it will be necessary to generate new keys using the Cryptography Key Editor. The first step is to create or upgrade the database. After creating or upgrading the database, all

application servers will need to be updated by copying the ArgusSecureKey.ini to their respective .\Windows folder.

### The Argus Safety 8.1 Database

Prior to creating a 8.0 database or upgrading to a 8.1 database, a new Cryptography Key needs to be generated using the Cryptography Key Editor. Running the Schema Creation tool prior to creating the key will inform the user that the cryptography key is required.

To generate a new Cryptography key, refer to the Generating a New Cryptography Key section.

You must also run the Argus Safety Schema Creation Tool to create or upgrade the database.

### The Argus Safety 8.1 Application Servers

After the application servers have been installed with 8.1, copy the ArgusSecureKey.ini file from the .\Windows folder of the system which was used to create or upgrade the database to the .\Windows folder of each installed application server.

### Generating a New Cryptography Key

Prior to running the Schema Creation tool the first time, it is necessary to generate a key file (ArgusSecureKey.ini) using the Cryptography Key Editor.

To create a new Cryptography Key, follow these steps:

1. Launch the Cryptography Key Editor.

The Key Editor Utility screen appears.

|                 | k          | Key Edit     | or Utility                                | Ŀ        | . 🗆      | × |
|-----------------|------------|--------------|---|----------|----------|---|
| elect Installat | tion type: |              |   |          |          |   |
|                 | if you war | -            | ate new Arg                               | usSecur  | eKey.ini |   |
| 1               | lew        |              |   |          |          |   |
| you want to     | perform op | perations li | ve ArgusSec<br>ke edit key,<br>AES encryp | re-encry |          |   |
| Ex              | istina     |              |   |          |          |   |

2. Click New.

The following screen appears.

| Generation | ate Key fo  | or Ne  | 💶          | □ X |
|------------|-------------|--------|------------|-----|
| Note to be | added as co | omment |            |     |
| I          |             |        |            | ^   |
|            |             |        |            |     |
| -          |             |        |            | ~   |
| Enter ARG  | USUSER pa   | ssword | i.         |     |
|            |             |        | 3-16-1<br> |     |
| Confirm pa | ssword      |        |            |     |
|            |             |        |            |     |
| Г          | OK          |        | Cancel     | 1   |
|            | UN          |        | Canoci     |     |

- **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 why this key was generated or for what environments it is used.
- **4.** In the **Enter ARGUSUSER password** field, enter the password for the database user called ARGUSUSER.
- 5. Confirm the password in the **Confirm password** field.
- 6. Click OK.

The ArgusSecureKey.ini file gets created in the <Installation folder> \ CryptoKeyEditor\output\<DateTimeStamp>\.

The Argus Secure Key Path dialog box appears.

| 0                                   | Argus Secure Key Path                          |  |  |  |  |  |
|-------------------------------------|--|--|--|--|--|--|
| Click on the link below to open the | folder   |  |  |  |  |  |
| C:\Program Files (x86)\Oracle\Argu  | Is\CryptoKeyEditor\output\13-Sep-2014-04-23-46 |  |  |  |  |  |
| Copy to windows folder              | Close, I will copy it manually                 |  |  |  |  |  |

- **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** to close the dialog box and copy the file manually from the window that gets opened by clicking on the link mentioned above (in step 9).
- **9.** Click **Copy to windows folder** to move the generated ArgusSecureKey.ini file to the .\Windows folder.

# **Resetting Password / Changing the Cryptography Key**

This section lists the steps to perform the following tasks:

- Resetting the ARGUSUSER Password
- Editing Keys
- Re-encrypting Common User Passwords

- Generating Encrypted String from Clear Text on Configured User Cryptography Key
- Resetting the Environment if ArgusSecureKey.ini is Lost

# **Resetting 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.

Execute the following steps to reset the ARGUSUSER password:

1. Launch the Cryptography Key Editor.

The Key Editor Utility screen appears.

| 0                  | Key Editor Utili   | ty     |              | x  |  |  |  |
|--------------------|--|--------|--------------|----|--|--|--|
| Select Installatio | Select Installation type:  |        |              |    |  |  |  |
| Select New if      | you want to generate new A   | ArgusS | ecureKey.ini | i. |  |  |  |
| Ne                 | N  |        |              |    |  |  |  |
| you want to p      | Select Existing if you already have ArgusSecureKey.ini and<br>you want to perform operations like edit key, re-encrypt<br>database passwords or generate AES encrypted |        |              |    |  |  |  |
| Exist              | ng   |        |              |    |  |  |  |
|                    |  |        |              |    |  |  |  |

2. Click Existing.

The Key Editor Login or Re-encrypt ARGUSUSER screen appears.

| Key Editor Login or Re       | x |
|------------------------------|---|
| Enter the ARGUSUSER password |   |
|                              |   |
| Database name                |   |
|                              |   |
| Login Re-encrypt Close       |   |

- **3.** In the **Enter the ARGUSUSER password** field, enter the password for the database user called ARGUSUSER.
- 4. Enter the name of the database in the **Database name** field.
- 5. Click Re-encrypt.

The following dialog appears.



- 6. Click Yes.
- **7.** Copy the updated ArgusSecureKey.ini File from the .\Windows folder to all the .\Windows folder of all the application servers.
- 8. Verify that you can login to the Argus Safety application.

# **Editing Keys**

An administrator might want to change a key due to various reasons like a policy to change key every few days, network compromise, etc.

Execute the following steps to edit the cryptography keys:

1. Launch the Cryptography Key Editor.

The Key Editor Utility screen appears.

|                        | Key Editor Utility  | >              |
|------------------------|---|----------------|
| ect Installation type: |   |                |
| Select New if you wa   | ant to generate new Argus   | sSecureKey.ini |
| New                    |   |                |
| you want to perform    | already have ArgusSecu<br>operations like edit key, re<br>or generate AES encrypt | e-encrypt      |
| Existing               |   |                |
| Existing               |   |                |

2. Click Existing.

The Key Editor Login or Re-encrypt ARGUSUSER screen appears.

| 🖻 Key Editor Login or Re 🗕 🗖 🗙 |  |  |  |  |  |
|--------------------------------|--|--|--|--|--|
| Enter the ARGUSUSER password   |  |  |  |  |  |
|                                |  |  |  |  |  |
| Database name                  |  |  |  |  |  |
|                                |  |  |  |  |  |
| Login Re-encrypt Close         |  |  |  |  |  |

- **3.** In the **Enter the ARGUSUSER password** field, enter the password for the database user called ARGUSUSER.
- 4. Enter the name of the database in the **Database name** field.
- 5. Click Login.

The Key Editor Options for Existing Installation screen appears.

| 2  | Key E       | ditor Options for Existing Installation | _ 🗆 X        |
|--|-------------|---|--------------|
| DataBase: docu80db<br>Enter DBA User Name:<br>Edit Key | ARGUS_APP   | Enter DBA User Password:                | Validate     |
| User Key:  | 256 ¥       |   | Re-Generate  |
| Re-encrypt   |             |   |              |
| DB User Name<br>ARGUS_LOGIN                            | DB User Pas | ssword                                  |              |
| ARGUS_LOGIN_I  |             |   |              |
| ARGUS_LOGIN_I  | PS          |   |              |
| DLP is disabled  |             |   |              |
| Generate Encrypted                                     | j l         |   |              |
| Clear text: Pa<br>Encrypted String:                    | assword1@3  |   |              |
| Status   |             |   |              |
|  |             |   | ^<br>~       |
| Execute C  | lose        |   | Clear Status |

- 6. Enter the DBA User Name and User Password.
- 7. Click Validate.
- 8. Check the Edit Key check box.

This enables the child check boxes of User Key and Cookie Key.

| •  |       | Key Edit      | tor Options for Existing                           | g Installation | _ 🗆 🗙        |
|--|-------|---------------|--|----------------|--------------|
| DataBase: docu80db<br>Enter DBA User Name:<br>✔ Edit Key | ARGUS | _APP          | Enter DBA User Password:                           |                | Validate     |
| <ul> <li>✓ User Key:</li> <li>✓ Cookie Key:</li> </ul>   |       |               | BE0F7E283BFE7508BE1897D<br>CBEFB5F23E36CEBF8F1F82I |                |              |
| Key Size   | 256   | ~             |  |                | Re-Generate  |
| Re-encrypt   |       |               |  |                |              |
| DB User Name   | E     | DB User Passw | rord   |                |              |
| ARGUS_LOGIN  |       |               |  |                |              |
| ARGUS_LOGIN_I  |       |               |  |                |              |
| ARGUS_LOGIN_IF   | S     |               |  |                |              |
| DLP is disabled  |       |               |  |                |              |
| Generate Encrypted                                       | 1     |               |  |                |              |
| Clear text:  |       |               |  |                |              |
| Status   |       |               |  |                |              |
|  |       |               |  |                | ×<br>×       |
| Execute  | ose   |               |  |                | Clear Status |

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.

- **9.** Select the check boxes in front of the key that you want to change.
- **10.** Change the Key Size drop-down list value, if you wish to change the key size. Key Size is measured in bits of the key used in a cryptographic algorithm.
- **11.** Click **Re-Generate**.

This will change the value of the checked items and the new value will be visible in the textbox.

12. Click Execute.

The Reason for this Action dialog box appears, prompting the user to add a reason for his action.

| 0               | Reason for this Action                   | <b>– –</b> X        |
|-----------------|--|---------------------|
| Please enter r  | eason for this action:*                  |                     |
| I               |  | ^                   |
|                 |  |                     |
|                 |  |                     |
|                 |  |                     |
|                 |  | ~                   |
|                 | any sensitive information like (password | , etc) as this text |
| will be present | t as clear text in audit log.            |                     |
| OK              | Cancel                                   |                     |
|                 |  |                     |

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.
- **15.** 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.
- **16.** 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:
- **17.** Items to be changed from the User Interface:
- **18.** Argus Services: Open Argus Safety Service Configuration: Open all the processes and enter password again.
- **19.** Cyclone: Open ESM Mapping utility and reenter Cyclone password.
- **20.** ESM Common User: Open ESM Mapping utility and reenter ESM Common user password.
- **21.** Re-enter the DBPassword in the configuration files, as explained in the following sections:
- **22.** Point 2 of the RelsysWindowsService.exe.config sub-section.
- **23.** Point 5 of the Configuring the Dossier Application section.
- 24. The Product License Study Interface section.

### **Re-encrypting 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.

Execute the following steps to re-encrypt the common user passwords:

1. Launch the Cryptography Key Editor.

The Key Editor Utility screen appears.

| Ke         | ey Edito                      | or Utility  | L  | -                                      |  | 3   |
|------------|-------------------------------|---|--|--|--|---|
| n type:    |                               |   |  |  |  |   |
| you want   | to genera                     | ite new Arg   | usSec  | cureKey                                | y.ini  |   |
| W          |                               |   |  |  |  |   |
| erform ope | erations lik                  | ce edit key,  | re-en  |  | hd   |   |
|            |                               |   |  |  |  |   |
|            | you want<br>w<br>g if you alr | n type:<br>you want to genera<br>w<br>g if you already hav<br>erform operations lik | n type:<br>you want to generate new Arg<br>w<br>g if you already have ArgusSec<br>erform operations like edit key, | you want to generate new ArgusSec<br>w | n type:<br>you want to generate new ArgusSecureKe<br>w<br>g if you already have ArgusSecureKey.ini ar<br>erform operations like edit key, re-encrypt | n type:<br>you want to generate new ArgusSecureKey.ini<br>w<br>g if you already have ArgusSecureKey.ini and<br>terform operations like edit key, re-encrypt |

2. Click Existing.

The Key Editor Login or Re-encrypt ARGUSUSER screen appears.

| 🖸 Key Editor Login or Re 🗕 🗖 🗙 |
|--------------------------------|
| Enter the ARGUSUSER password   |
|                                |
| Database name                  |
|                                |
| Login Re-encrypt Close         |

- **3.** In the **Enter the ARGUSUSER password** field, enter the password for the database user called ARGUSUSER.
- **4.** Enter the name of the database in the **Database name** field.
- 5. Click Login.

The Key Editor Options for Existing Installation screen appears.

| 2  | Key E      | ditor Options for Existing Installation | _ 🗆 X        |
|--|------------|---|--------------|
| DataBase: docu80db<br>Enter DBA User Name: | ARGUS_APP  | Enter DBA User Password: ••••••         | Validate     |
| User Key:                                  |            |   |              |
| Key Size                                   | 256 🗸      |   | Re-Generate  |
| Re-encrypt DB User Name                    | DB User Pa | ssword                                  |              |
| Generate Encrypted                         |            |   |              |
| Status                                     | ose        |   | Clear Status |

- **6.** Enter the DBA User Name and User Password.
- 7. Click Validate.
- **8.** Check the **Re-encrypt** check box.
- **9.** Enter the passwords for the common users.

| •  | Key E       | ditor Options for Existing | g Installation | _ 🗆 X        |
|--|-------------|----------------------------|----------------|--------------|
| DataBase: DOCU80DB<br>Enter DBA User Name:<br>Edit Key | ARGUS_APP   | Enter DBA User Password:   | •••••          | Validate     |
| User Key: [  |             |                            |                |              |
| Key Size   | 256 🗸       |                            |                | Re-Generate  |
| Re-encrypt   |             |                            |                |              |
| DB User Name   | DB User Pa: | ssword                     |                |              |
| ARGUS_LOGIN  | •••••       |                            |                |              |
| ARGUS_LOGIN_I  | •••••       |                            |                |              |
| ARGUS_LOGIN_IPS  |             |                            |                |              |
| DLP is disabled  |             |                            |                |              |
| Generate Encrypted                                     |             |                            |                |              |
| Clear text:  |             |                            |                |              |
| Status   |             |                            |                |              |
|  |             |                            |                | ×            |
| Execute Clos   | se .        |                            |                | Clear Status |

#### 10. Click Execute.

The Reason for this Action dialog box appears, prompting the user to add a reason for his action.

|                   | Reason for this Action  | <b>– – ×</b>         |
|-------------------|---|----------------------|
| Please enter reas | son for this action:*   |                      |
| 1                 |   | <u>^</u>             |
|                   |   |                      |
|                   |   |                      |
|                   |   |                      |
|                   |   | ~                    |
|                   |   |                      |
|                   | y sensitive information like (password)<br>clear text in audit log. | 1, etc) as this text |
| ОК                | Cancel  |                      |
|                   |   |                      |

- **11.** The text entered here is visible in the Audit Log in the Argus Safety application.
- **12.** Click **OK**.
- **13.** Check the status box to verify if the operation has been successful.

# Generating Encrypted String from Clear Text on Configured User Cryptography Key

Generate the encrypted string from clear text, using the configured UserCryptoKey in ArgusSecureKey.ini.

Execute the following steps to re-encrypt the common user passwords:

1. Launch the Cryptography Key Editor.

The Key Editor Utility screen appears.

|                    | Key Editor Utility  | - 🗆 X          |
|--------------------|---|----------------|
| elect Installation | type:   |                |
| Select New if y    | you want to generate new Argu   | sSecureKey.ini |
| Nev                | v   |                |
| you want to pe     | if you already have ArgusSecu<br>Inform operations like edit key, re<br>words or generate AES encrypt | e-encrypt      |
| Existi             | ng  |                |
| l                  |   |                |

2. Click Existing.

The Key Edit Login screen appears.

| 🖻 Key Editor Login or Re 🗕 🗖 🗙 |
|--------------------------------|
| Enter the ARGUSUSER password   |
|                                |
| Database name                  |
|                                |
| Login Re-encrypt Close         |

- **3.** In the **Enter the ARGUSUSER password** field, enter the password for the database user called ARGUSUSER.
- **4.** Enter the name of the database in the **Database name** field.
- 5. Click Login.

The Key Editor Options for Existing Installation screen appears.

| ataBase: docu80db    |            |                          |             |
|----------------------|------------|--------------------------|-------------|
| inter DBA User Name: | ARGUS_APP  | Enter DBA User Password: | Validate    |
| ] Edit Key           |            |                          |             |
| User Key:            |            |                          |             |
| Cookie Key:          |            |                          |             |
| Key Size             | 256 🗸      |                          | Re-Generate |
| ] Re-encrypt         |            |                          |             |
| DB User Name         | DB User Pa | issword                  |             |
|                      |            |                          |             |
|                      |            |                          |             |
|                      |            |                          |             |
|                      |            |                          |             |
| Generate Encrypted   |            |                          |             |
| Cleartext:           |            |                          |             |
| Encrypted String:    |            |                          |             |
| Eliciypted Staling.  |            |                          |             |
| tatus                |            |                          |             |
|                      |            |                          | -           |
|                      |            |                          |             |
|                      |            |                          |             |

- **6.** Enter the DBA User Name and User Password.
- 7. Click Validate.
- **8.** Check the **Generate Encrypted** check box.
- **9.** Enter the password in the **Clear text** field.

| 9   | Key E        | ditor Options for Existing Installat | ion 🗕 🗆 🗙    |
|---|--------------|--------------------------------------|--------------|
| DataBase: docu80db<br>Enter DBA User Name | e: ARGUS_APP | Enter DBA User Password: ••••••      | Validate     |
| Edit Key                                  |              |                                      |              |
| User Key: Cookie Key:                     |              |                                      |              |
| Key Size                                  | e 256 V      |                                      | Re-Generate  |
| Re-encrypt                                |              |                                      |              |
| DB User Name                              | DB User Pa   | issword                              |              |
| ARGUS_LOGIN                               |              |                                      |              |
| ARGUS_LOGIN_                              | ]            |                                      |              |
| ARGUS_LOGIN_                              | IPS          |                                      |              |
| DLP is disabled                           |              |                                      |              |
| Generate Encrypte                         | ed           |                                      |              |
| Clear text: F                             | assword1@3   |                                      |              |
| Encrypted String:                         |              |                                      |              |
| Status                                    |              |                                      |              |
|   |              |                                      | ~            |
|   |              |                                      | ~            |
| Execute                                   | Close        |                                      | Clear Status |

### 10. Click Execute.

The Reason for this Action dialog box appears, prompting the user to add a reason for his action.

| 3              | Reason for this Action   |         | x  |
|----------------|--|---------|----|
| Please enter r | reason for this action:*   |         |    |
| 1              |  |         | ~  |
|                |  |         |    |
|                |  |         |    |
|                |  |         |    |
|                |  |         | ~  |
|                | r any sensitive information like (password, etc) as<br>t as clear text in audit log. | this te | xt |
| ОК             | Cancel   |         |    |
|                |  |         |    |

- **11.** The text entered here is visible in the Audit Log in the Argus Safety application.
- **12.** Click **OK**.
- **13.** 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.

# Resetting the Environment if ArgusSecureKey.ini is Lost

This section lists the steps to be followed in resetting the environment if the ArgusSecureKey.ini is lost. In such a scenario, execute the following steps:

- 1. Follow the steps listed in the Resetting the ARGUSUSER Password section to generate a new key and copy it to the Windows folder.
- **2.** Follow the steps listed in the Re-encrypting Common User Passwords section to re-encrypt common user passwords.
- 3. Re-encrypt strings in the following locations:
- 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

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

Re-enter the DBPassword in the configuration files, as explained in the following sections:

- 5. Point 2 of the RelsysWindowsService.exe.config sub-section
- 6. Point 5 of the Configuring the Dossier Application section
- 7. The Product License Study Interface section

# **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.

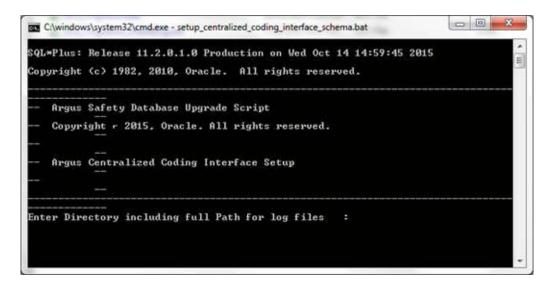
- setup\_centralized\_coding\_interface\_schema.bat
- setup\_dsnav\_centralized\_coding.bat
- dms\_migration.bat

# 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 codeable items as 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



1. Execute the batch file **setup\_centralized\_coding\_interface\_schema.bat**.

- **a.** Provide a log folder name such as C:\DSnavLog.
- **b.** Provide a database name.
- c. Provide DBA user credentials such as system and password.
- d. Provide an RLS schema owner name and password.

You can 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. Provide an Argus schema owner name such as ARGUS\_APP and password.
- f. Provide an Argus Safety role name.
- 2. The script creates two users, ARGUS\_DMS and DMS\_LOGIN, and their tablespaces. The Interface schema object is present in the ARGUS\_DMS schema.
  - **a.** Provide the password for user ARGUS\_DMS.
  - **b.** Provide the password for user DMS\_LOGIN.
  - **c.** Provide a temporary tablespace name; if no input is provided, TEMP tablespace is taken by default.
  - **d.** The script creates two tablespaces: DMS\_DATA\_01.DBF, and DMS\_INDEX\_01.DBF. Provide the path and data file name such as:

C:\APP\ORADATA\DBNAMD\DMS\_DATA\_01.DBF

C:\APP\ORADATA\DBNAMD\DMS\_INDEX\_01.DBF

- **e.** Enter a log file name.
- f. Press Enter when the Users and Roles are located.
- g. Verify the log file to validate the successful completion of the script.
- **3.** Log in to the application and enable the Centralized Coding module. Configure Centralized Coding from the dictionary selection page in the Console.

# setup\_dsnav\_centralized\_coding.bat

Execute this script to encode existing events present in the Argus Centralized Coding Interface schema against the DSX Centralized Coding dictionary present in a separate database/schema.

This script executes only when the Interface schema is present. (Refer setup\_ centralized\_coding\_interface\_schema.bat created earlier.)

1. Execute the batch file Setup\_dsnav\_centralized\_coding.bat.

| 🖾 C:\Windows\system32\cmd.exe   | _ 🗆 × |
|---|-------|
| SQL*Plus: Release 11.2.0.4.0 Production on Thu Oct 15 15:55:59 2015   | *     |
| Copyright (c) 1982, 2013, Oracle. All rights reserved.  |       |
| ABBAABAABAABAABAABAABAABAABAABAABAABAAB   |       |
| Enter Directory including full Path for log files :<br>Enter log file name :  |       |
| NARAARANARAARAARAARAARAARAARAARAARAARAAR  |       |
| Enter INSNAMES entry to connect to safety database :<br>Enter Database Administrator User Name :<br>Enter Password for User ARGUS_DMS : | -1    |

**a.** Provide a log folder name such as C:\DSnavLog.

- **b.** Provide a log file name.
- **c.** Provide the Argus Safety DB name.
- **d.** Provide database administrator name such as *system* and password.
- e. Provide the password for ARGUS\_DMS schema.
- **2.** Before proceeding, add the DXS Argus Centralized Coding database TNSNAMES entry on the Argus database server where the Interface schema was created.

| 👼 C:\Windows\system32\cmd.exe 📃 🗆 🗙   |
|---|
| Connected.  |
| If User failed to connect to Database, then stop here restart the tool.<br>To stop processing click top right corner X icon or Press Ctrl-C and type exit t<br>o close session<br>Press Enter if the Script successfully connected as system@ar12cdb3 |
| ######################################  |
| Enter the tnsname entry to connect from the ARGUS database to the DSNAU database<br>:   |
| Enter the name of the database link which will be created to connect from the<br>interface schema to the DXS schema on the dsNavigator database :   |
| Enter the name for the DXS Schema name :<br>Enter the password for the DXS schema password :  |

a. Provide the TNSNAME of the DXS Argus Centralized Coding database.

b. Provide the database link name that is created to connect from the Argus Interface schema to the DXS Argus Centralized Coding schema.

c. Provide DSX schema name and password.

**3.** If the credentials are successfully verified, a DBlink is created from the Argus Interface schema to the DXS Argus Centralized Coding schema.

**Note:** After successful completion of the script, verify that the DBlink from the DXS Centralized Coding schema to the Argus Safety Interface schema is present and validated.

**4.** This script also creates some triggers on the Argus Interface schema that are invoked whenever cases are added to the Argus Centralized Coding Interface schema table. The trigger invokes remote procedures on the DXS Centralized Coding database that start DXS activity.

# 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

# Single Enterprise Migration in One Execution

To migrate encoded terms for case data for a particular enterprise, provide an enterprise\_id such as 1.

# 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, provide only one enterprise\_id such as 1 when prompted.
- To migrate encoded terms of case data for all enterprises in one go, provide 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.

| mC:\Windows\system32\cmd.exe   |     |
|--|-----|
| Enter Directory including full Path for log files :<br>Enter log file name :                                 | -   |
| Enter INSNAMES entry to connect to database :<br>Enter Argus Schema User Name :<br>Enter Password for User : |     |
| ANNALABARARARARARARARARARARARARARARARARARAR  |     |
| Enter the ENIERPRISE_ID :  |     |
| NUMBERS AND  | *** |
| Enter Argus Application User Name [admin] :  |     |

- **1.** Provide a log folder name such as C:\DSnavLog.
- **2.** Provide a log file name.
- **3.** Enter the TNSNAMES of the Argus Safety database when the Interface schema was created.
- 4. Provide the Argus Safety schema owner name and password.
- **5.** Depending 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.** Provide the application user name; if no input is provided, *admin* is taken as user input.
- 7. Verify the log file to validate successful completion of the script.