Oracle® Argus Safety

Installation Guide

Release 8.0

E54665-04

October 2015

Oracle Argus Safety Installation Guide, Release 8.0

E54665-04

Contents

4 Installing Argus Safety Web

5 Setting up Client Browser

6 Installing Argus Safety Service

7 Installing and Configuring EDI Gateway

8 Configuring Oracle B2B

11 Enabling IIS HTTP Compression

12 Configuring E-mail

13 Enabling and Configuring BIP Periodic Reports

14 Installing End of Study Unblinding

15 Other Tasks

16 Argus Integrations

17 Argus Password Management - Cryptography Tool

A Third Party Attributions

Preface

This guide describes installing or upgrading to Oracle Argus Safety 8.0. 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 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 2008 Server.

Chapter 12, "Configuring E-mail"

This chapter provides information about configuring E-mail.

Chapter 13, "Enabling and Configuring BIP Periodic Reports"

This chapter provides information about configuring BIP.

Chapter 8, "Configuring Oracle B2B"

This chapter provides information about configuring B2B.

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.

Appendix A, "Third Party Attributions"

This Appendix provides information about third party software.

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:

- *Oracle Argus Safety User's Guide*
- *Oracle Argus Safety Administrator's Guide*
- *Oracle Argus Safety Database Administrator's Guide*
- *Oracle Argus Dossier User's Guide*
- *Oracle Argus Affiliate User's Guide*
- *Oracle Argus Unblinding User's Guide*
- *Oracle Argus Interchange User's Guide*
- *Oracle Argus Safety Interchange Administrator's Guide*
- *Oracle Argus Interchange UICH DTD 2.1 Mapping Reference Guide*
- *Oracle Argus Safety BIP Extensibility Guide*

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.

1 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**
- **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 offload Interchange Service from the Argus Transaction Server. Alternatively, Interchange Service can be installed on the Transaction Server itself.

- **Argus Safety Web Client**

  On the web client system, a new window may open (instead of opening in the same application window) when you try to view a Microsoft Office 2007 program document from the Argus Application in Microsoft Internet Explorer 9.

  Refer to the following Microsoft article for more information and workaround:

  `http://support.microsoft.com/kb/927009`

- **Argus End of Study Unblinding Tool**
- **Argus Safety OBIEE/BIP Server**

  This server installation is optional and is required only if Argus Safety BIP Periodic Reporting is selected.

  Argus 8.0 supports OBIEE/BIP 11.1.1.7.1.

  Refer to the OBIEE 11g 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 11.2.0.4 / 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 Safety Database Server	Argus Safety Web Server	Argus Transaction Server	Argus Interchange Server	Argus Safety Web Client	Argus End of Study Unblinding Tool (EOSU) + Schema Creation Tool ** + Interchange Mapping Tool
OPERATING SYSTEM						
Microsoft Windows 2008 R2 SP1						
Microsoft Windows 2008	Yes	Yes	Yes	Yes		Yes
IIS Version 7.5 ***		Yes				
Microsoft Windows 2012						
Microsoft Windows 2012	Yes	Yes	Yes	Yes		Yes
IIS Version 8.0 ***		Yes				
Microsoft Windows 2012 R2						
Microsoft Windows 2012 R2	Yes	Yes	Yes	Yes		Yes
IIS Version 8.5 ***		Yes				

Software Requirements	Argus Safety Database Server	Argus Safety Web Server	Argus Transaction Server	Argus Interchange Server	Argus Safety Web Client	Argus End of Study Unblinding Tool (EOSU) + Schema Creation Tool ** + Interchange Mapping Tool
Windows Client Machines and Internet Explorer						
Microsoft Windows 7 (32/64-bit)					Yes	Yes
Microsoft Windows 8 (32/64-bit)					Yes	Yes
Microsoft Internet Explorer, Version 9.0 (32-bit)					Yes	
Microsoft Internet Explorer, Version 10.0 (32-bit)					Yes	
Microsoft Internet Explorer, Version 11.0 (32-bit)					Yes	
ORACLE DATABASE SERVER (STANDARD/ENTERPRISE) - VERSION 12C (12.1.0.2) or VERSION 11.2.0.4 *						
Microsoft Windows 2008/2012	Yes					
Oracle Enterprise Linux X86/86-64 (Version 5.5.0.0.0/5.7.0.0/6.2/6.4 UEK)	Yes					
Sun Solaris 10/11	Yes					
Other Oracle Database Components						
Oracle Advanced Security Transparent Data Encryption (TDE)****	Optional					
Oracle Advanced Security Network Encryption	Optional					
ORACLE CLIENT						
Oracle 11g Client 11.2.0.4 (32-bit only), OLE Objects, ODAC, MTS, ODP.NET		Yes	Yes	Yes		Yes
Oracle 12c Client 12.1.0.2 (32-bit only), Oracle Call Interface, ODAC, MTS, ODP.NET		Yes	Yes	Yes		Yes
OTHER MANDATORY SOFTWARE'S						
Microsoft Visual C++ 2012 Runtime		Yes	Yes	Yes		Yes
Microsoft Visual Basic Power Packs 10.0						Required for Interchange Mapping Tool
Microsoft .NET 3.5 SP1 Framework		Yes	Yes	Yes		Yes
Microsoft Word + Excel 2007/2010/2013 (32-bit)		Required for Dossier only	Yes	Yes	Yes	Required for Schema Creation MedDRA Recode and End of Study only

Software Requirements	Argus Safety Database Server	Argus Safety Web Server	Argus Transaction Server	Argus Interchange Server	Argus Safety Web Client	Argus End of Study Unblinding Tool (EOSU) + Schema Creation Tool ** + Interchange Mapping Tool
Adobe Acrobat Reader with East Asian Fonts					Yes	
OPTIONAL SOFTWARE						
Documentum DFC Client, Version 6.5 SP2/SP3 Or 6.7 SP2 (64-bit)		Yes	Yes	Yes		
RightFax 9.4/10.5 -Required files only			Yes			
OPTIONAL SUPPORTED FEATURES						
Oracle Components						
Oracle Access Manager 11g - WebGate 10.1.4.3 (32-bit only)	Required only for Sign-On integration with Oracle Access Manager.					
Oracle WebCenter - 11.1.1.7 (on WebLogic 10.3.6)	Required only for multi-tenant installations (Optional - Required only to deploy the Global Application module. Ideally, the WebCenter Portal Server should be deployed on a separate Web Server. Alternatively, the Global Application module can also be deployed on Argus Safety Web Server directly).					
Oracle Business Intelligence Enterprise Edition (OBIEE) / BIP - 11.1.1.7.1						
Third Party Integrations						
LDAP/LDAPS Protocol Version 3.0	LDAP authentication support					
SMTP Protocol	E-mail support					
Documentum DFC, Version 6.5 SP2/SP3 Or 6.7 SP2 (64-bit)	Required only when Documentum is used for Storage.					
RightFax 9.4/10.5	Required only for faxing Expedited Reports.					
Gateway for E2B Reporting						
Oracle B2B - 11.1.1.7.0	Certified with both AS1 and AS2 protocols for E2B exchanges between regulatory authorities and pharmaceutical companies.					
Axway Synchrony, Version 5.10.1 (64-bit)	Required for E2B Report 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 mandatory IIS components.

**** Refer to **Note 3** for Oracle Database TDE feature.

**** 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:** To install IIS, the following components are required:

- Web Server > Management Tools
  - IIS Management Console
  - IIS 6 Management Compatibility
  - IIS Management Scripts and Tools
- Web Server > Application Development
  - ASP
  - ASP.NET 3.5
  - Server Side Includes
- Web Server > Performance
  - Dynamic Content Compression
  - Static Content Compression

****** Note 3:** Oracle Database TDE feature is part of the Oracle Advanced Security option available for Oracle Database Enterprise Edition 11g (http://www.oracle.com/technetwork/database/options/advanced-security/index.html).

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

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

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.

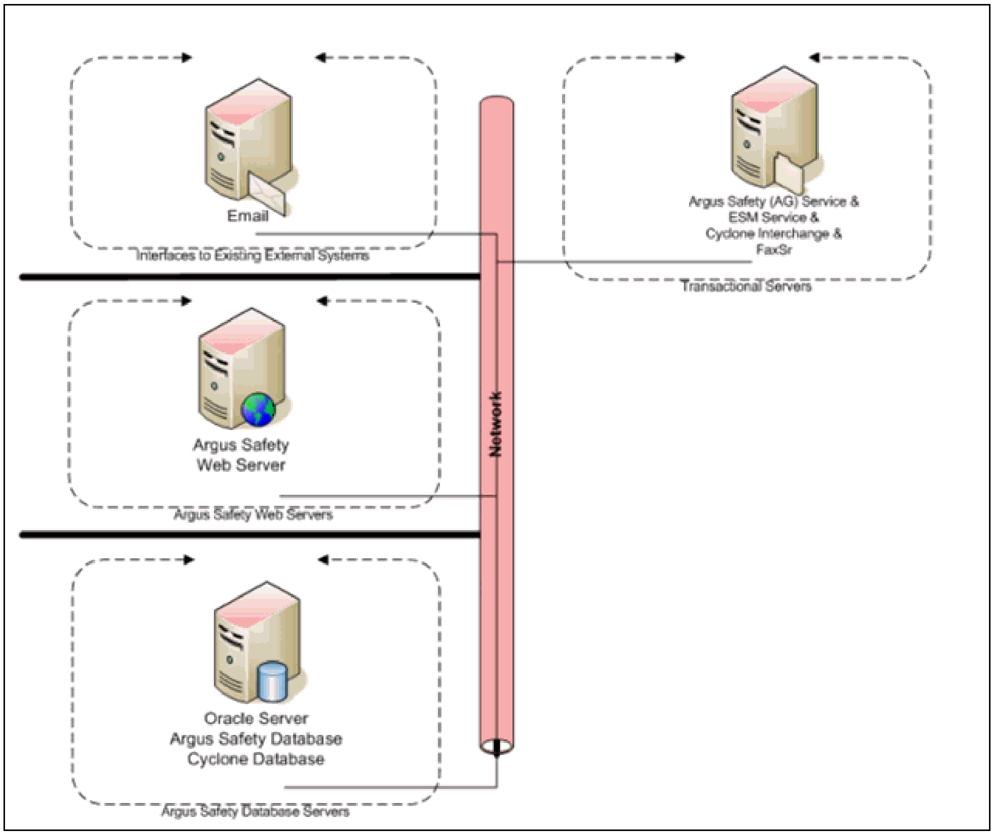
Small Company: A small company is a company that has from 1 to 50 concurrent users and fewer than 200 new cases reported each month.

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.

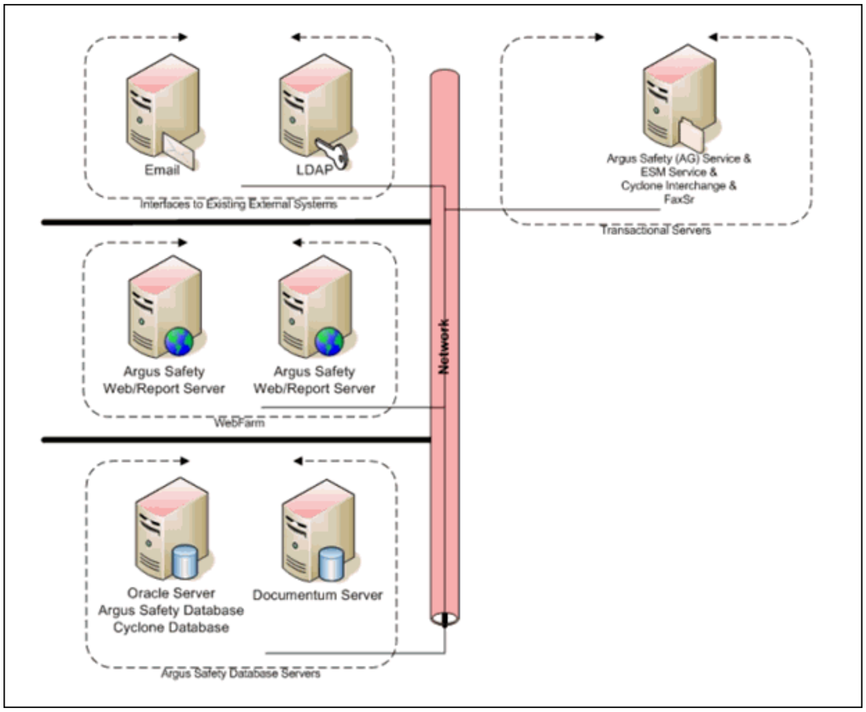
Recommended Hardware Topology for a Small Company

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



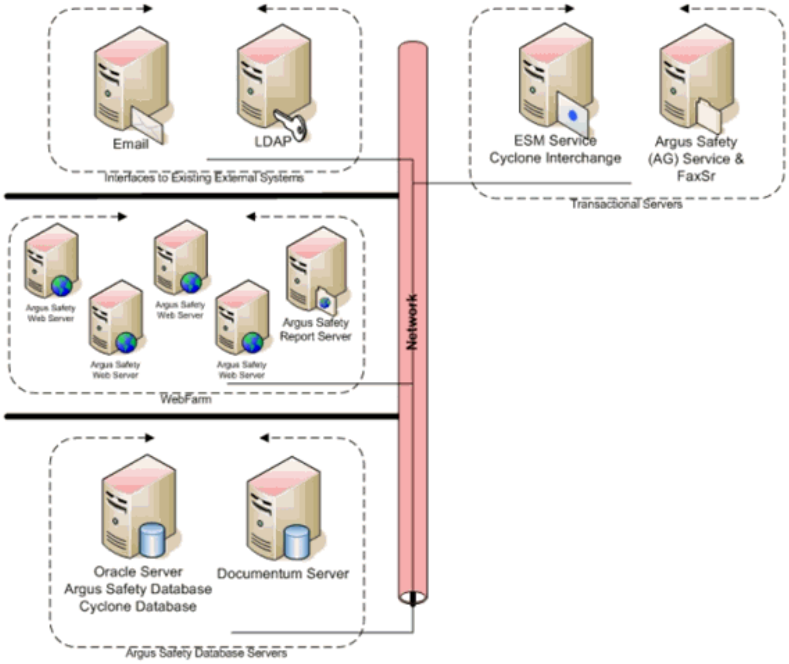
Recommended Hardware Topology for a Mid-sized Company

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


Email
LDAP
Interfaces to Existing External Systems
Argus Safety (AG) Service &
ESM Service &
Cyclone Interchange &
FaxSr
Transactional Servers
Network
Argus Safety Web/Report Server
Argus Safety Web/Report Server
WebFarm
Oracle Server
Argus Safety Database
Cyclone Database
Documentum Server
Argus Safety Database Servers

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:

Hardware Requirements	Argus Safety Database Server				Argus Safety Web Server			Argus Transaction Server			Argus Interchange Server			Argus Safety Web Client	Argus End of Study Unblinding Tool (EOSU)
	Small	Mid-Size	Large	Very Large	Small	Mid-Sized	Large	Small	Mid-Sized	Large	Small	Mid-Sized	Large		
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 CPU X 3 GHz					Yes			Yes			Yes				Yes
2 Dual Core CPUs X 3 GHz						Yes	Yes		Yes	Yes		Yes	Yes		
Equivalent to 2 - 4 Dual Core X 3GHz	Yes														
Equivalent to 4 - 8 Dual Core X 3GHz		Yes													
Equivalent to 16 Dual Core X 3GHz			Yes	Yes											
Pentium IV X 3 GHz														Yes	
Virtualization															
Physical Server					Yes			Yes			Yes				
Oracle Virtual Machine (OVM 2.2.1/2.2.2)	Optional				Yes			Yes			Yes				
Others															
Exadata 11g R2	Optional														
RAC 11g R2	Optional														
Minimum Resolution					1280X1024			1280X1024			1280X1024			1280X1024	1280X1024

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**

2

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.

3

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

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.

- BIP Schema:

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

- DLP Schema:

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

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 Parameters	Small	Mid-Sized	Large	Very Large
1	MEMORY_ TARGET	2 GB	3 GB	10 GB	>10 GB
2	PROCESSES	Expected concurrent users + 100	Expected concurrent users + 100	Expected concurrent users + 100	Expected concurrent users + 100
3	MEMORY_ MAX_TARGET	>= value set for MEMORY_ TARGET	>= value set for MEMORY_ TARGET	>= value set for MEMORY_ TARGET	>= value set for MEMORY_TARGET
4	OPTIMIZER_ SECURE_VIEW_ MERGING	FALSE	FALSE	FALSE	FALSE
5	CURSOR_ SHARING	EXACT	EXACT	EXACT	EXACT
6	WORKAREA_ SIZE_POLICY	AUTO	AUTO	AUTO	AUTO
7	JOB_QUEUE_ PROCESSES	25	25	25	25
8	SHARED_ POOL_SIZE	500 MB	500 MB	1 GB	2 GB
9	DB_CACHE_ SIZE	500 MB	500 MB	1 GB	2 GB
10	DB_BLOCK_ SIZE (bytes)	8192	8192	8192	8192
11	PGA_ AGGREGATE_ 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 Log Files	5 Groups * 100 MB	5 Groups * 100 MB	5 Groups * 100 MB	5 Groups * 100 MB
2	TEMP Tablespace Size	8 GB	16 GB	32 GB	64 GB
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 8.0 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:

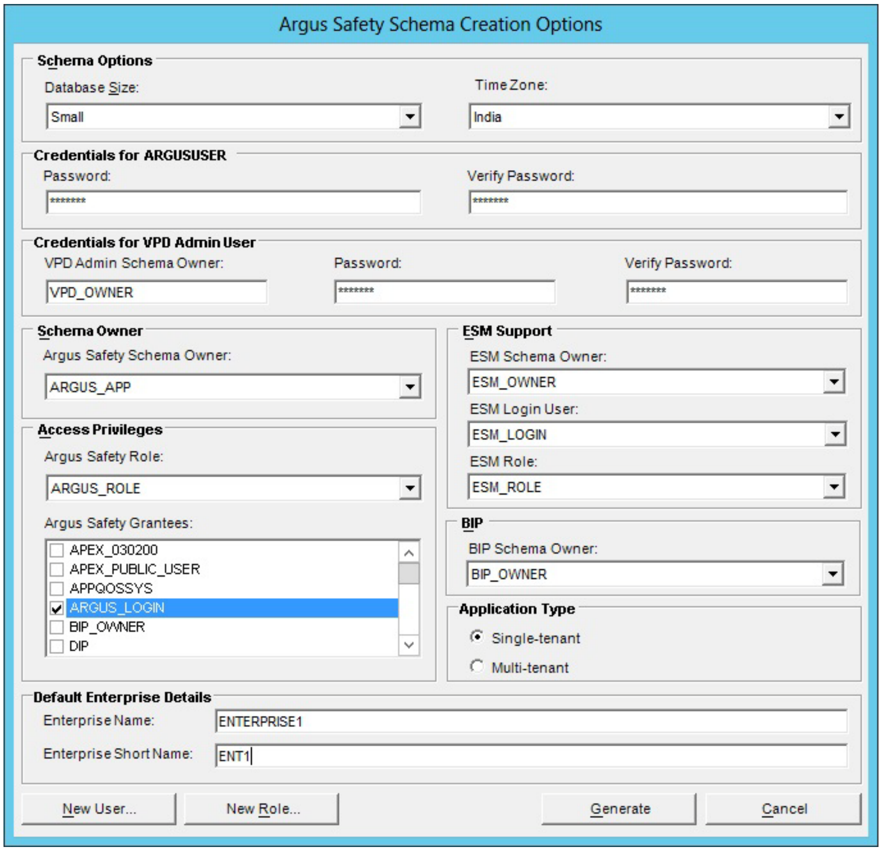
- A blank Oracle database instance is available
- A SYSTEM user account is available
- The Oracle database is available from the machine where the schema creation tool is installed

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:



Argus Safety Schema Creation Options

Schema Options
Database Size: Small
Time Zone: India

Credentials for ARGUSUSER
Password: *******
Verify Password: *******

Credentials for VPD Admin User
VPD Admin Schema Owner: VPD_OWNER
Password: *******
Verify Password: *******

Schema Owner
Argus Safety Schema Owner: ARGUS_APP

ESM Support
ESM Schema Owner: ESM_OWNER
ESM Login User: ESM_LOGIN
ESM Role: ESM_ROLE

Access Privileges
Argus Safety Role: ARGUS_ROLE
Argus Safety Grantees:
☐ APEX_030200
☐ APEX_PUBLIC_USER
☐ APPQOSSYS
☑ ARGUS_LOGIN
☐ BIP_OWNER
☐ DIP

BIP
BIP Schema Owner: BIP_OWNER

Application Type
● Single-tenant
○ Multi-tenant

Default Enterprise Details
Enterprise Name: ENTERPRISE1
Enterprise Short Name: ENT1

   - 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 **Reenter Password** field.

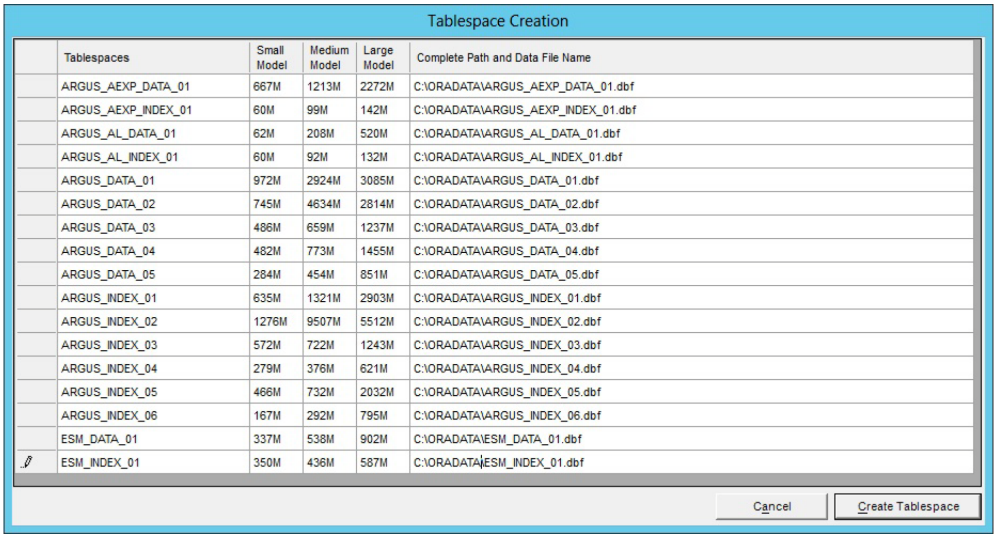
4. When the system displays the New User dialog box:
   - Enter the user name in the **New User Name** field.
   - Enter the user's password in the **New User Password** field.
   - Reenter the user's password in the **Reenter Password** field.
   - Verify that the **Default Tablespace** and **Temporary 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.
   - Enter password for the ARGUSUSER user.
   - Under BIP, create a new BIP Schema by clicking **New User**, and select the created schema from the BIP 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 Model	Medium Model	Large Model	Complete Path and Data File Name
ARGUS_AEXP_DATA_01	667M	1213M	2272M	C:\ORADATA\ARGUS_AEXP_DATA_01.dbf
ARGUS_AEXP_INDEX_01	60M	99M	142M	C:\ORADATA\ARGUS_AEXP_INDEX_01.dbf
ARGUS_AL_DATA_01	62M	208M	520M	C:\ORADATA\ARGUS_AL_DATA_01.dbf
ARGUS_AL_INDEX_01	60M	92M	132M	C:\ORADATA\ARGUS_AL_INDEX_01.dbf
ARGUS_DATA_01	972M	2924M	3085M	C:\ORADATA\ARGUS_DATA_01.dbf
ARGUS_DATA_02	745M	4634M	2814M	C:\ORADATA\ARGUS_DATA_02.dbf
ARGUS_DATA_03	486M	659M	1237M	C:\ORADATA\ARGUS_DATA_03.dbf
ARGUS_DATA_04	482M	773M	1455M	C:\ORADATA\ARGUS_DATA_04.dbf
ARGUS_DATA_05	284M	454M	851M	C:\ORADATA\ARGUS_DATA_05.dbf
ARGUS_INDEX_01	635M	1321M	2903M	C:\ORADATA\ARGUS_INDEX_01.dbf
ARGUS_INDEX_02	1276M	9507M	5512M	C:\ORADATA\ARGUS_INDEX_02.dbf
ARGUS_INDEX_03	572M	722M	1243M	C:\ORADATA\ARGUS_INDEX_03.dbf
ARGUS_INDEX_04	279M	376M	621M	C:\ORADATA\ARGUS_INDEX_04.dbf
ARGUS_INDEX_05	466M	732M	2032M	C:\ORADATA\ARGUS_INDEX_05.dbf
ARGUS_INDEX_06	167M	292M	795M	C:\ORADATA\ARGUS_INDEX_06.dbf
ESM_DATA_01	337M	538M	902M	C:\ORADATA\ESM_DATA_01.dbf
ESM_INDEX_01	350M	436M	587M	C:\ORADATA\ESM_INDEX_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**.
2. 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:

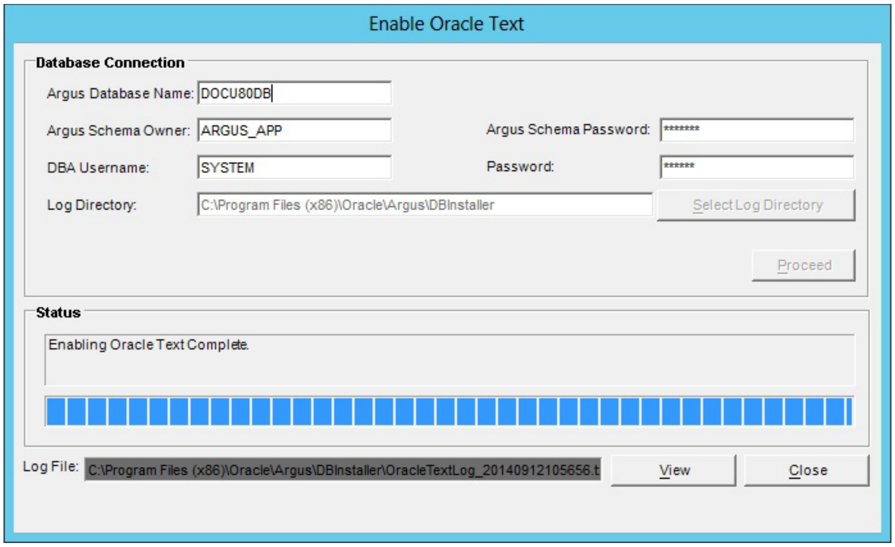
- DB Installer checks whether Oracle Text is installed. If not, it displays an error message that *Oracle Text not installed. Please install Oracle Text before adding this feature*.
- Estimates the Tablespace Size Requirements and adjusts as required.
- Populates existing cases in the Oracle Text duplicate 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**.



Enable Oracle Text

Database Connection

Argus Database Name: DOCU80DB

Argus Schema Owner: ARGUS_APP

Argus Schema Password: *******

DBA Username: SYSTEM

Password: ******

Log Directory: C:\Program Files (x86)\Oracle\Argus\DBInstaller

Status

Enabling Oracle Text Complete.

Log File: C:\Program Files (x86)\Oracle\Argus\DBInstaller\OracleTextLog_20140912105656.t

   - 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

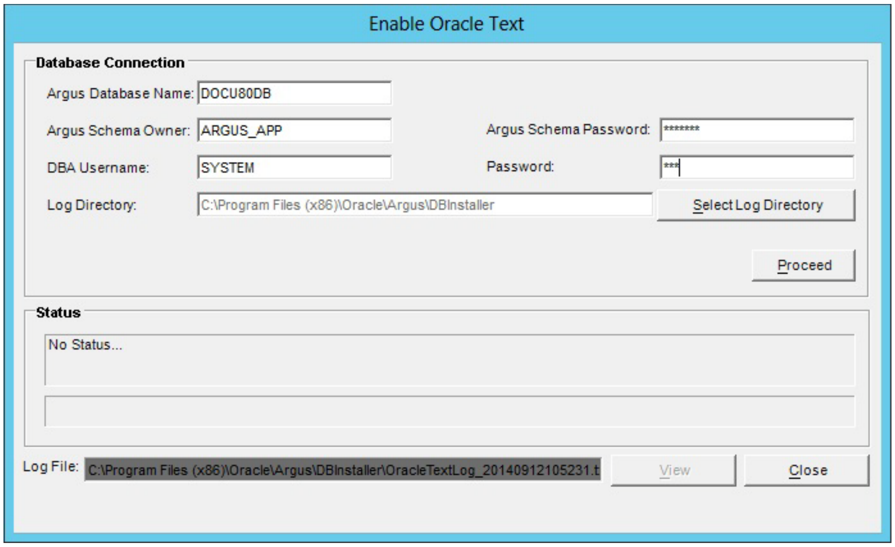
After Oracle Text is disabled, the system performs the following functions:

- 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:



Enable Oracle Text

Database Connection

Argus Database Name: DOCU80DB

Argus Schema Owner: ARGUS_APP

Argus Schema Password: *******

DBA Username: SYSTEM

Password: ***

Log Directory: C:\Program Files (x86)\Oracle\Argus\DBInstaller

Status

No Status...

Log File: C:\Program Files (x86)\Oracle\Argus\DBInstaller\OracleTextLog_20140912105231.t

- 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

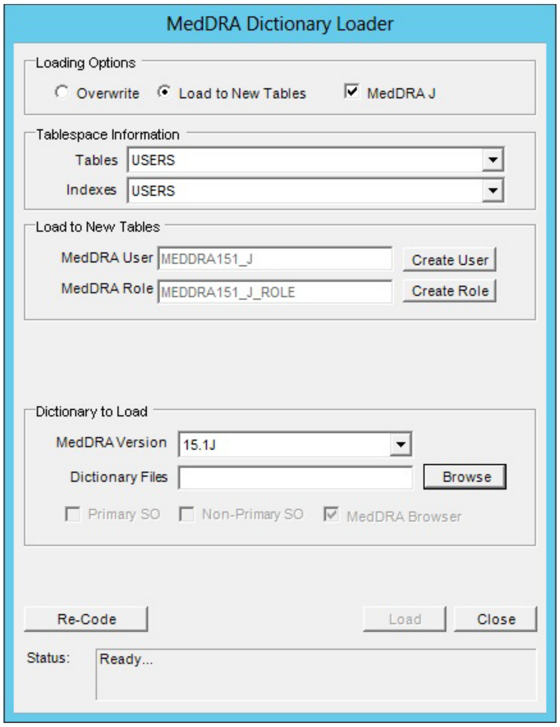
Note: If loading MedDRA V8 or V8.1, the smq_list.asc and smq_content.asc files containing SMQ data must be placed in the same folder as the other dictionary files.

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 an do the following:



MedDRA Dictionary Loader

Loading Options

○ Overwrite ● Load to New Tables ☑ MedDRA J

Tablespace Information

Tables: USERS

Indexes: USERS

Load to New Tables

MedDRA User: MEDDRA151_J

MedDRA Role: MEDDRA151_J_ROLE

Dictionary to Load

MedDRA Version: 15.1J

Dictionary Files:

□ Primary SO □ Non-Primary SO ☑ MedDRA Browser

Status: Ready...

   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.

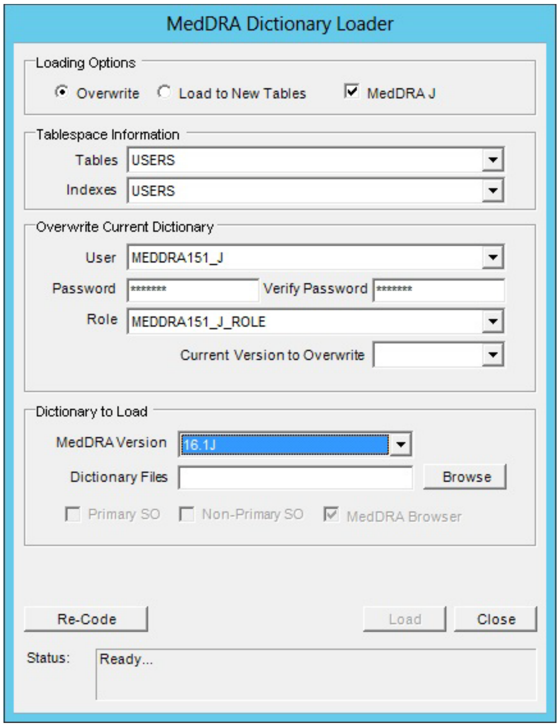
   - Click **MedDRA Loader**.

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:



MedDRA Dictionary Loader

Loading Options

● Overwrite ○ Load to New Tables ☑ MedDRA J

Tablespace Information

Tables: USERS

Indexes: USERS

Overwrite Current Dictionary

User: MEDDRA151_J

Password: ******* Verify Password: *******

Role: MEDDRA151_J_ROLE

Current Version to Overwrite:

Dictionary to Load

MedDRA Version: 16.1J

Dictionary Files:

□ Primary SO □ Non-Primary SO ☑ MedDRA Browser

Status: Ready...

- 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

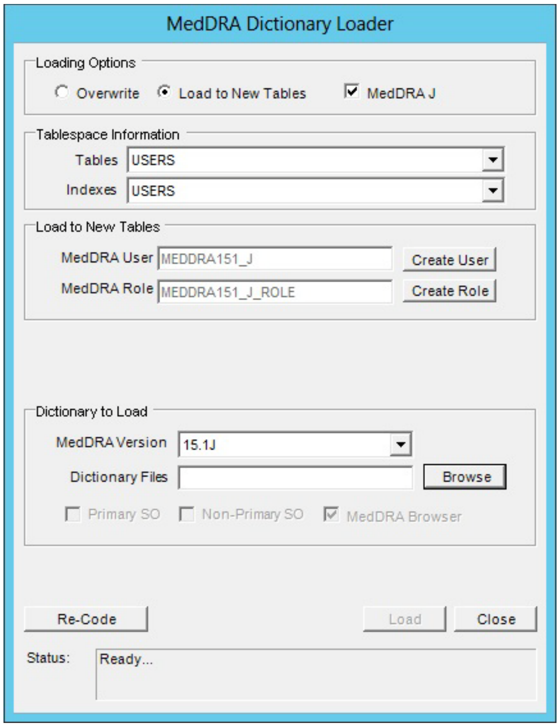
The following table lists and describes the options in the dialog box.

Event Recoding Dialog Box Options

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 determined at LLT Level Only]	Check one or both of the following options: 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 **will not** 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.

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 Dictionary Loader

Loading Options

○ Overwrite ● Load to New Tables ☑ MedDRA J

Tablespace Information

Tables: USERS

Indexes: USERS

Load to New Tables

MedDRA User: MEDDRA151_J

MedDRA Role: MEDDRA151_J_ROLE

Dictionary to Load

MedDRA Version: 15.1J

Dictionary Files:

□ Primary SO □ Non-Primary SO ☑ MedDRA Browser

Status: Ready...

- 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

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 an do 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 the following message.
   - Click **OK**.

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

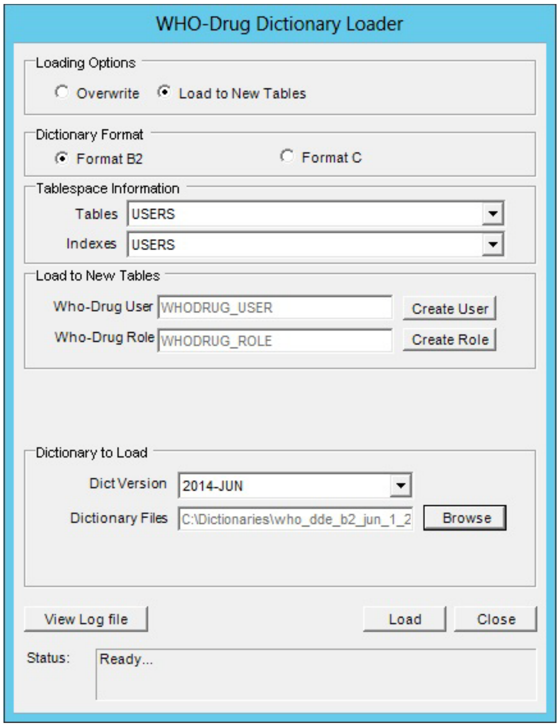
Use the following procedure to load WHO-Drug dictionary to new tables:

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.



WHO-Drug Dictionary Loader

Loading Options
○ Overwrite ● Load to New Tables

Dictionary Format
● Format B2 ○ Format C

Tablespace Information
Tables: USERS
Indexes: USERS

Load to New Tables
Who-Drug User: WHODRUG_USER
Who-Drug Role: WHODRUG_ROLE

Dictionary to Load
Dict Version: 2014-JUN
Dictionary Files: C:\Dictionaries\who_dde_b2_jun_1_2

Status: Ready...

- 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**.

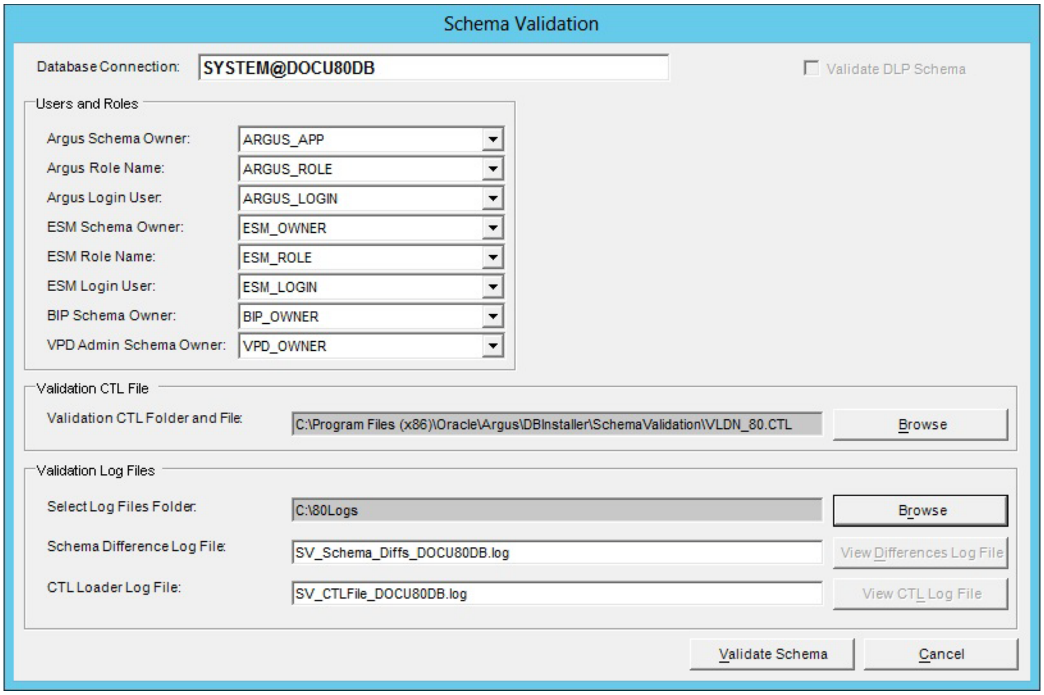
Validating the Argus Safety Database

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.



Database Connection: SYSTEM@DOCU80DB

□ Validate DLP Schema

Argus Schema Owner: ARGUS_APP

Argus Role Name: ARGUS_ROLE

Argus Login User: ARGUS_LOGIN

ESM Schema Owner: ESM_OWNER

ESM Role Name: ESM_ROLE

ESM Login User: ESM_LOGIN

BIP Schema Owner: BIP_OWNER

VPD Admin Schema Owner: VPD_OWNER

Validation CTL Folder and File: C:\Program Files (x86)\Oracle\Argus\DBInstaller\SchemaValidation\VLDN_80.CTL

Select Log Files Folder: C:\80Logs

Schema Difference Log File: SV_Schema_Diffs_DOCU80DB.log

CTL Loader Log File: SV_CTLFile_DOCU80DB.log

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

This section provides information about how to enable and disable Data Lock Point (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.

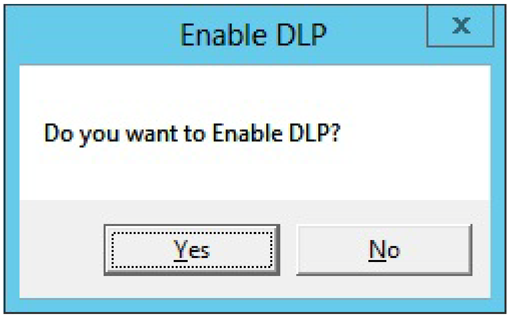
Enabling DLP

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.

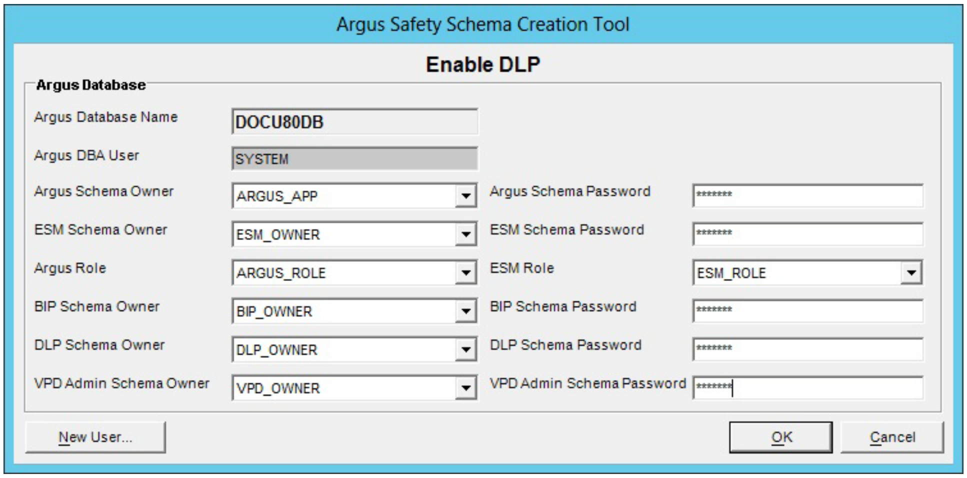
Use the following procedure to enable DLP:

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


Enable DLP

Do you want to Enable DLP?

3. When the system displays the expanded Enable DLP window:


Argus Safety Schema Creation Tool

Enable DLP

Argus Database

Argus Database Name: DOCU80DB

Argus DBA User: SYSTEM

Argus Schema Owner: ARGUS_APP | Argus Schema Password: *******

ESM Schema Owner: ESM_OWNER | ESM Schema Password: *******

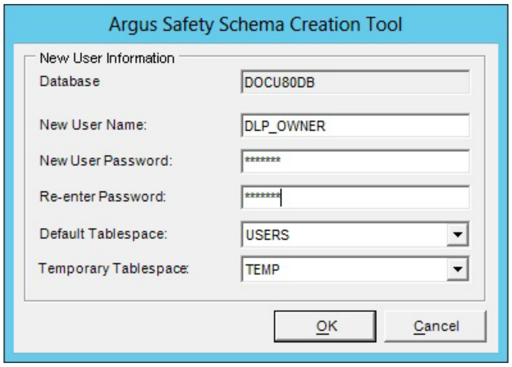
Argus Role: ARGUS_ROLE | ESM Role: ESM_ROLE

BIP Schema Owner: BIP_OWNER | BIP Schema Password: *******

DLP Schema Owner: DLP_OWNER | DLP Schema Password: *******

VPD Admin Schema Owner: VPD_OWNER | VPD Admin Schema Password: *******

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


Argus Safety Schema Creation Tool

New User Information

Database: DOCU80DB

New User Name: DLP_OWNER

New User Password: *******

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

Default Tablespace: USERS

Temporary Tablespace: TEMP

- Enter the required details for the new DLP Schema 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.

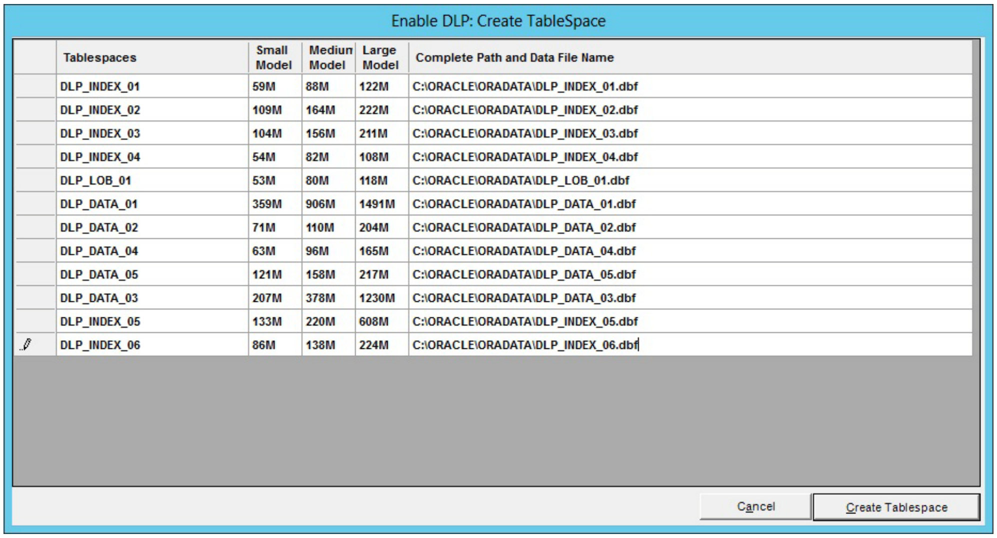
5. Enter the required user information.

   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:



Enable DLP: Create TableSpace

Tablespaces	Small Model	Medium Model	Large Model	Complete Path and Data File Name
DLP_INDEX_01	59M	88M	122M	C:\ORACLE\ORADATA\DLP_INDEX_01.dbf
DLP_INDEX_02	109M	164M	222M	C:\ORACLE\ORADATA\DLP_INDEX_02.dbf
DLP_INDEX_03	104M	156M	211M	C:\ORACLE\ORADATA\DLP_INDEX_03.dbf
DLP_INDEX_04	54M	82M	108M	C:\ORACLE\ORADATA\DLP_INDEX_04.dbf
DLP_LOB_01	53M	80M	118M	C:\ORACLE\ORADATA\DLP_LOB_01.dbf
DLP_DATA_01	359M	906M	1491M	C:\ORACLE\ORADATA\DLP_DATA_01.dbf
DLP_DATA_02	71M	110M	204M	C:\ORACLE\ORADATA\DLP_DATA_02.dbf
DLP_DATA_04	63M	96M	165M	C:\ORACLE\ORADATA\DLP_DATA_04.dbf
DLP_DATA_05	121M	158M	217M	C:\ORACLE\ORADATA\DLP_DATA_05.dbf
DLP_DATA_03	207M	378M	1230M	C:\ORACLE\ORADATA\DLP_DATA_03.dbf
DLP_INDEX_05	133M	220M	608M	C:\ORACLE\ORADATA\DLP_INDEX_05.dbf
DLP_INDEX_06	86M	138M	224M	C:\ORACLE\ORADATA\DLP_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.

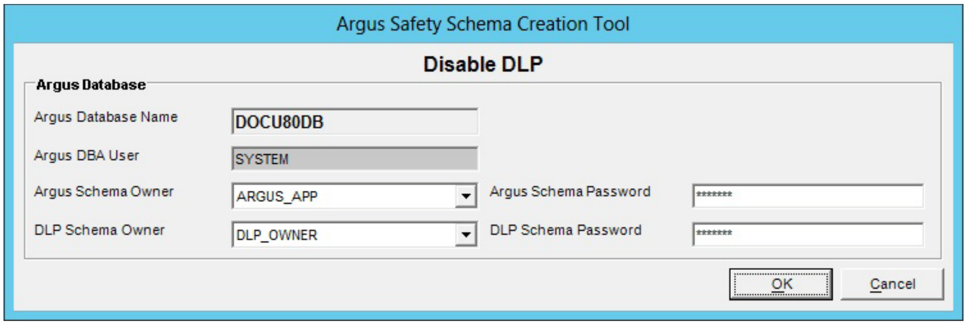
Disabling DLP

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.



Argus Safety Schema Creation Tool

Disable DLP

Argus Database

Argus Database Name: DOCU80DB

Argus DBA User: SYSTEM

Argus Schema Owner: ARGUS_APP

Argus Schema Password: *******

DLP Schema Owner: DLP_OWNER

DLP Schema 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:

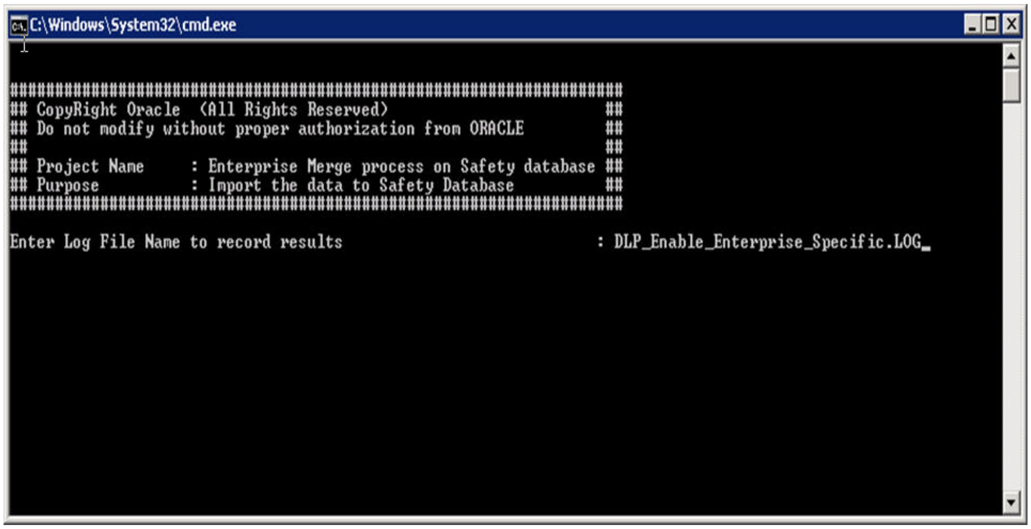
1. Extract the custom DLP Enable Enterprise Specific from C:\Program Files\Oracle\Argus\DBInstaller\Utilities\DLP_Enable_Enterprise_Specific into a machine's local folder where Argus Safety 8.0 is installed.

Execute the following steps to set up the base database:

1. Set up an Argus Safety 8.0 multi-tenant or single-tenant database. Enable DLP on the Argus Safety 8.0 database, using standard Argus DLP option available in the Schema Creation Tool.
2. Validate the schema using the Schema Validation in Argus Safety 8.0 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.

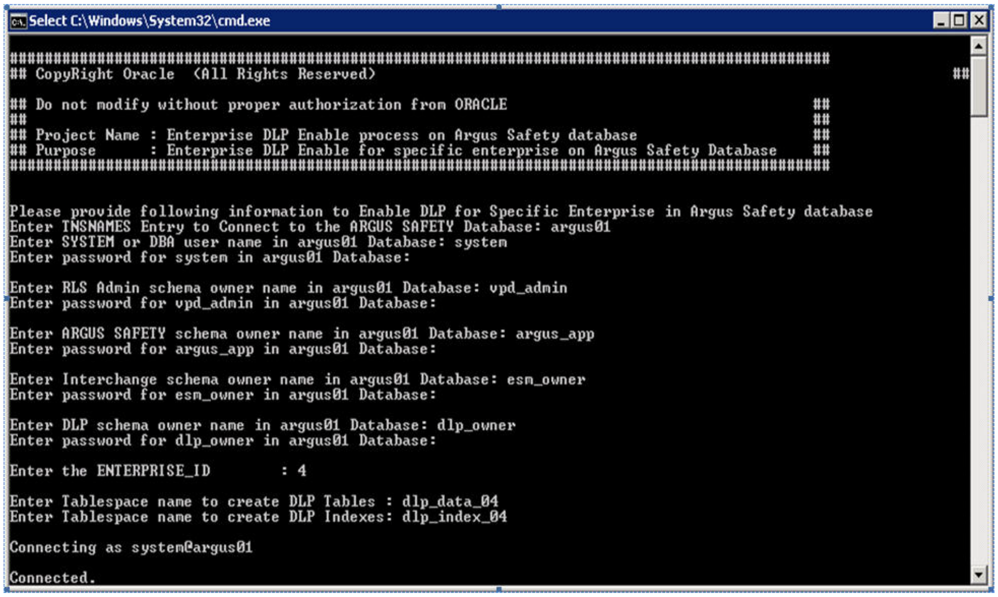
Execute the following steps to enable DLP on a Specific Enterprise or Delta Cases in a Specific Enterprise:

1. 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



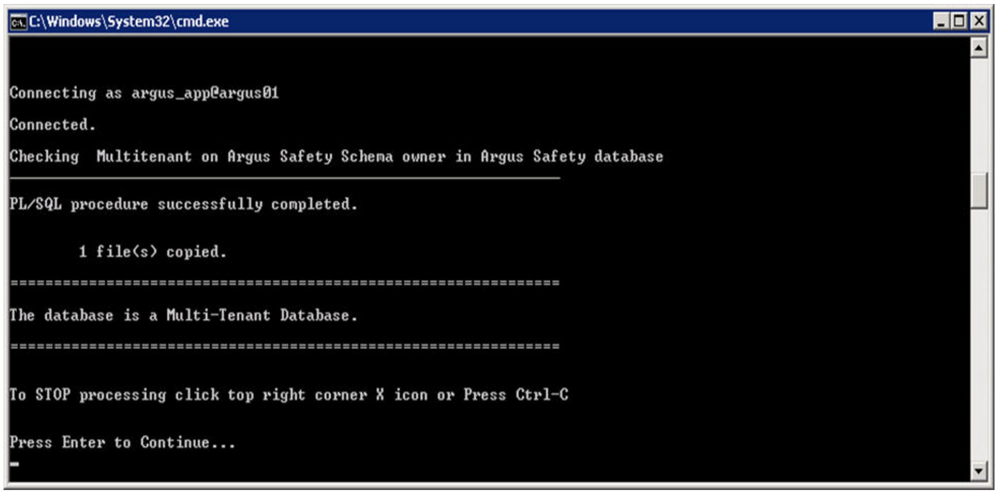
```
####################################################################
## CopyRight Oracle  (All Rights Reserved)                        ##
## Do not modify without proper authorization from ORACLE         ##
##                                                                ##
## Project Name     : Enterprise Merge process on Safety database ##
## Purpose          : Import the data to Safety Database          ##
####################################################################

Enter Log File Name to record results                            : DLP_Enable_Enterprise_Specific.LOG_
```

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



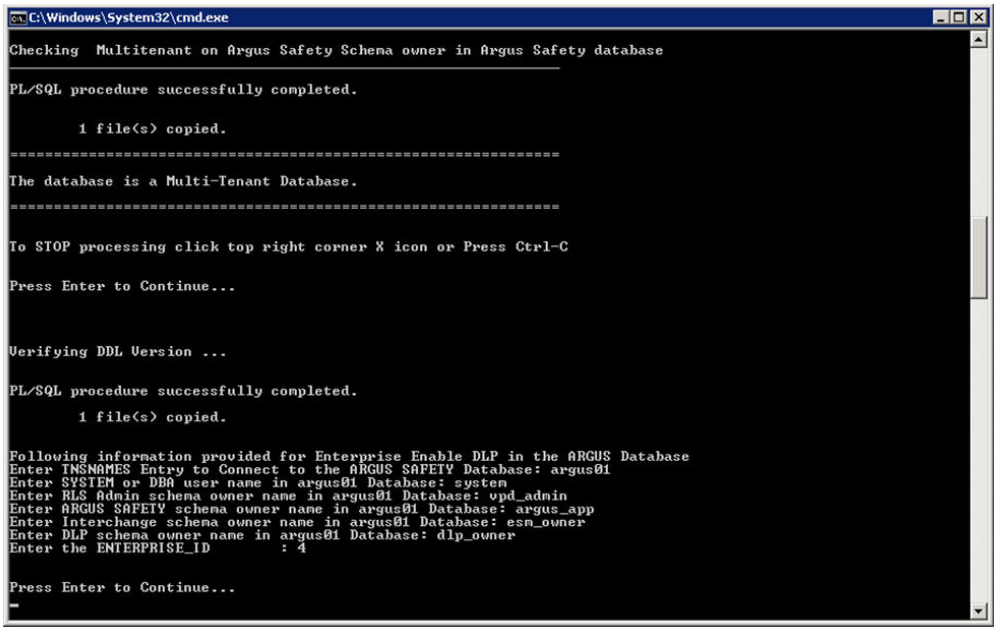
```
##############################################################################################
## CopyRight Oracle  (All Rights Reserved)                                                        ##

## Do not modify without proper authorization from ORACLE                                   ##
##                                                                                          ##
## Project Name : Enterprise DLP Enable process on Argus Safety database                    ##
## Purpose      : Enterprise DLP Enable for specific enterprise on Argus Safety Database    ##
##############################################################################################


Please provide following information to Enable DLP for Specific Enterprise in Argus Safety database
Enter TNSNAMES Entry to Connect to the ARGUS SAFETY Database: argus01
Enter SYSTEM or DBA user name in argus01 Database: system
Enter password for system in argus01 Database:

Enter RLS Admin schema owner name in argus01 Database: vpd_admin
Enter password for vpd_admin in argus01 Database:

Enter ARGUS SAFETY schema owner name in argus01 Database: argus_app
Enter password for argus_app in argus01 Database:

Enter Interchange schema owner name in argus01 Database: esm_owner
Enter password for esm_owner in argus01 Database:

Enter DLP schema owner name in argus01 Database: dlp_owner
Enter password for dlp_owner in argus01 Database:

Enter the ENTERPRISE_ID        : 4

Enter Tablespace name to create DLP Tables : dlp_data_04
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.



```


Connecting as argus_app@argus01

Connected.

Checking  Multitenant on Argus Safety Schema 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...
_
```

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



```
Checking  Multitenant on Argus Safety Schema 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...


Verifying DDL Version ...

PL/SQL procedure successfully completed.

        1 file(s) copied.

Following information provided for Enterprise Enable DLP in the ARGUS Database
Enter TNSNAMES Entry to Connect to the ARGUS SAFETY Database: argus01
Enter SYSTEM or DBA user name in argus01 Database: system
Enter RLS Admin schema owner name in argus01 Database: vpd_admin
Enter ARGUS SAFETY schema owner name in argus01 Database: argus_app
Enter Interchange schema owner name in argus01 Database: esm_owner
Enter DLP schema owner name in argus01 Database: dlp_owner
Enter the ENTERPRISE_ID        : 4

Press Enter to Continue...
_
```

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 8.0, 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 8.0 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 8.0 DLP Enabled system with DLP_Enable_Enterprise_Specific scripts applied on top of it:

Owner	Type	Name	Reason for extra object
DLP	TABLE	DLP_ENABLE_CASE_HISTORY	Objects are part of Enable DLP Enterprise Specific implementation.
DLP	INDEX	PK_DLP_ENABLE_CASE_HISTORY	Objects are part of Enable DLP Enterprise Specific 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.
>
> The following grants need not be provided if the DBA user has been created through the Argus 8.0 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 8.0.

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.

Note: Customers can use the Argus Safety (AS) 8.0 software to upgrade the Argus Safety database from AS 7.0.2 or AS 7.0.3, using the Database zip file.

AS 7.0.2 to AS 7.0.3, using the database zip file in the AS 8.0 software:

Extract 'Database_released_code_703.zip' from the 'Previous Database Upgrades' folder of AS 8.0 software into the 'Database_released_code_703_from_702' folder code.

This will upgrade the database from AS 7.0.2 to AS 7.0.3. For further details, refer to the Oracle Argus Safety 7.0.3 Installation Guide.

AS 7.0.3 to AS 7.0.3.1, using the database zip file in the AS 8.0 software:

Extract 'Database_released_code_7031.zip' from the 'Previous Database Upgrades' folder of AS 8.0 software into the 'Database_released_code_7031_from_703' folder code.

This will upgrade the database from AS 7.0.3 to AS 7.0.3.1.

For further details, refer to the Oracle Argus Safety 7.0.3.1 Release Notes (Database Upgrade section).

Clean-up Scripts to be Run Before Upgrading the Database

Note: There may be scenarios where DDL/DML scripts can differ due to single-tenancy and multi-tenancy.

Execute the single-tenant script in a single-tenant database and the multi-tenant script in a multi-tenant database.

Before executing the SQLs given below, make sure that you remove the empty lines within the SQL statements listed throughout this section.

Data Clean-up on Duplicate Event Details Information on a Single-tenant Database

Execute the following query to verify duplicate records:

```
select case_id, prod_seq_num, event_seq_num, count(*)
```

```
from case_event_detail

group by case_id, prod_seq_num, event_seq_num

having count(1) > 1;
```

If the above-listed SQLs result in 0 rows (that is, no duplicate data is found), then we do not need to execute the cleanup scripts.

If duplicate records are found, execute sub-section scripts to clean-up duplicate records from Argus Safety and Argus DLP-related tables.

Argus Safety Data Clean-up on Duplicate Event Details Execute the following steps sequentially on the Argus Safety database as an Argus Safety Schema Owner (such as ARGUS_APP), to remove duplicate rows from Event Detail (CASE_EVENT_DETAIL table):

1. Drop the Foreign key constraint between CASE_EVENT_CONSEQUENCE and CASE_EVENT_DETAIL by entering the following SQL:

   ```
   alter table case_event_consequence drop constraint fk_case_event_
   detail_seq_num;
   ```

2. Create Foreign key constraint between CASE_EVENT_CONSEQUENCE and CASE_EVENT_DETAIL using ON DELETE CASCADE by entering the following SQL:

   ```
   alter table case_event_consequence add (

   constraint fk_case_event_detail_seq_num

   foreign key (case_id, ed_seq_num)

   references case_event_detail (case_id,seq_num) on delete cascade);
   ```

3. Delete event detail rows where it was already marked for logical deletion and is duplicated by entering the following SQL:

   ```
   delete from case_event_detail

   where deleted is not null

   and exists (select 'x' from case_event_detail a

   where a.case_id = case_event_detail.case_id

   and a.prod_seq_num = case_event_detail.prod_seq_num

   and a.event_seq_num = case_event_detail.event_seq_num

   and a.deleted is null);

   commit;
   ```

4. Delete event detail rows where they are duplicated, by entering the following SQL:

   ```
   delete from case_event_detail a

   where a.seq_num <
   ```

```
any (select b.seq_num

from case_event_detail b

where a.case_id = b.case_id

and a.prod_seq_num = b.prod_seq_num

and a.event_seq_num = b.event_seq_num);

commit;
```

5. Verify that no duplicate rows exist in CASE_EVENT_DETAIL, by entering the following SQL:

   ```
   select case_id, prod_seq_num, event_seq_num, count(*)

   from case_event_detail

   group by case_id, prod_seq_num, event_seq_num

   having count(1) > 1;
   ```

6. Drop the Foreign key constraint between CASE_EVENT_CONSEQUENCE and CASE_EVENT_DETAIL by entering the following SQL:

   ```
   alter table case_event_consequence drop constraint fk_case_event_
   detail_seq_num;
   ```

7. Create a foreign key constraint between CASE_EVENT_CONSEQUENCE and CASE_EVENT_DETAIL without ON DELETE CASCADE, by entering the following SQLs:

   ```
   alter table case_event_consequence add (

   constraint fk_case_event_detail_seq_num

   foreign key (case_id, ed_seq_num)

   references case_event_detail (case_id,seq_num));
   ```

DLP Data Clean-up on Duplicate Event Details If DLP is enabled on the Argus Safety database, you need to execute the following steps (in addition to the steps listed above), sequentially:

Note: Execute DLP Data Clean-up ONLY AFTER executing the Argus Safety clean-up scripts.

1. Log on to DLP database as DLP schema owner (such as DLP_OWNER) to remove duplicate rows from Event Detail (DLP_CASE_EVENT_DETAIL and DLP_CASE_EVENT_CONSEQUENCE tables).
2. Delete invalid records from the DLP_CASE_EVENT_DETAIL table, by entering the following SQL:

   ```
   delete from dlp_case_event_detail a

   where (case_id, seq_num) in
   ```

```
(
select case_id, seq_num from dlp_case_event_detail
minus
select case_id, seq_num from &user..case_event_detail
);
Commit;
```

Note: Replace "&user." with the name of the Argus Safety Schema Owner.

3. Delete invalid records from the DLP_CASE_EVENT_CONSEQUENCE table, by entering the following SQL:

```
delete from dlp_case_event_consequence a
where (case_id, seq_num) in
(
select case_id, seq_num from dlp_case_event_consequence
minus
select case_id, seq_num from &user..case_event_consequence
);
Commit;
```

Note: Replace "&user." with the name of the Argus Safety Schema Owner.

Data Clean-up on Duplicate Event Details Information on a Multi-tenant Database

This section lists the SQL to verify if any duplicate record exists in the Argus Safety database.

Execute the statement given below to set the context:

```
BEGIN
pkg_rls.set_context ('system', 0, 'ARGUS_SAFETY');
END;
/
```

Execute the following query to verify duplicate records:

```
select enterprise_id, case_id, prod_seq_num, event_seq_num, count(*)
from case_event_detail
group by enterprise_id, case_id, prod_seq_num, event_seq_num
having count(1) > 1;
```

If the above-listed SQLs result in 0 rows (that is, no duplicate data is found), then we do not need to execute the clean-up scripts.

If duplicate records are found, execute sub-section scripts to clean-up duplicate records from Argus Safety and Argus DLP-related tables.

Argus Safety Data Clean-up on Duplicate Event Details Execute the following steps sequentially on the Argus Safety database as an Argus Safety Schema Owner (such as ARGUS_APP), to remove duplicate rows from Event Detail (CASE_EVENT_DETAIL table):

1. Drop the Foreign key constraint between CASE_EVENT_CONSEQUENCE and CASE_EVENT_DETAIL by entering the following SQL:

   ```
   alter table case_event_consequence drop constraint fk_case_event_
   detail_seq_num;
   ```

2. Create Foreign key constraint between CASE_EVENT_CONSEQUENCE and CASE_EVENT_DETAIL using ON DELETE CASCADE by entering the following SQL:

   ```
   alter table case_event_consequence add (

   constraint fk_case_event_detail_seq_num

   foreign key (enterprise_id, case_id, ed_seq_num)

   references case_event_detail (enterprise_id, case_id,seq_num) on delete
   cascade);
   ```

3. Delete event detail rows where it was already marked for logical deletion and is duplicated by entering the following SQL:

   ```
   delete from case_event_detail

   where deleted is not null

   and exists (select 'x' from case_event_detail a

   where a.enterprise_id = case_event_detail.enterprise_id

   and a.case_id = case_event_detail.case_id

   and a.prod_seq_num = case_event_detail.prod_seq_num

   and a.event_seq_num = case_event_detail.event_seq_num

   and a.deleted is null);

   commit;
   ```

4. Delete event detail rows where they are duplicated, by entering the following SQL:

   ```
   delete from case_event_detail a

   where a.seq_num <

   any (select b.seq_num

   from case_event_detail b

   where a.enterprise_id = b. enterprise_id
   ```

```
and a.case_id = b.case_id

and a.prod_seq_num = b.prod_seq_num

and a.event_seq_num = b.event_seq_num);

commit;
```

5. Verify that no duplicate rows exist in CASE_EVENT_DETAIL, by entering the following SQL:

```
select enterprise_id, case_id, prod_seq_num, event_seq_num, count(*)

from case_event_detail

group by enterprise_id, case_id, prod_seq_num, event_seq_num

having count(1) > 1;
```

6. Drop the Foreign key constraint between CASE_EVENT_CONSEQUENCE and CASE_EVENT_DETAIL by entering the following SQL:

```
alter table case_event_consequence drop constraint fk_case_event_
detail_seq_num;
```

7. Create a foreign key constraint between CASE_EVENT_CONSEQUENCE and CASE_EVENT_DETAIL without ON DELETE CASCADE, by entering the following SQL:

```
alter table case_event_consequence add (

constraint fk_case_event_detail_seq_num

foreign key (enterprise_id, case_id, ed_seq_num)

references case_event_detail (enterprise_id, case_id,seq_num));
```

DLP Data Clean-up on Duplicate Event Details If DLP is enabled on the Argus Safety database, you need to execute the following steps (in addition to the steps listed above) sequentially:

Note: Execute DLP Data Clean-up ONLY AFTER executing the Argus Safety clean-up scripts.

1. Log on to DLP database as DLP schema owner (such as DLP_OWNER) to remove duplicate rows from Event Detail (DLP_CASE_EVENT_DETAIL and DLP_CASE_EVENT_CONSEQUENCE tables)

   Execute the statement given below to set the context:

```
BEGIN

pkg_rls.set_context ('system', 0, 'ARGUS_SAFETY');

END;

/
```

2. Delete invalid records from the DLP_CASE_EVENT_DETAIL table, by entering the following SQL:

```
delete from dlp_case_event_detail a

where (enterprise_id, case_id, seq_num) in

(

select enterprise_id, case_id, seq_num from dlp_case_event_detail

minus

select enterprise_id, case_id, seq_num from &user..case_event_detail

);

Commit;
```

Note: Replace "&user." with the name of the Argus Safety Schema Owner.

3. Delete invalid records from the DLP_CASE_EVENT_CONSEQUENCE table, by entering the following SQL:

```
delete from dlp_case_event_consequence a

where (enterprise_id, case_id, seq_num) in

(

select enterprise_id, case_id, seq_num from dlp_case_event_consequence

minus

select enterprise_id, case_id, seq_num from &user..case_event_
consequence

);

Commit;
```

Note: Replace "&user." with the name of the Argus Safety Schema Owner.

Database Upgrade Procedure (with or without DLP) from AS 7.0.3.1 to AS 8.0

Note: The Oracle Database Server version should be upgraded to 11.2.0.4 or 12c (12.1.0.1.0, 12.1.0.2.0) prior to upgrading the database from AS 7.0.3.1 to AS 8.0.

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**.

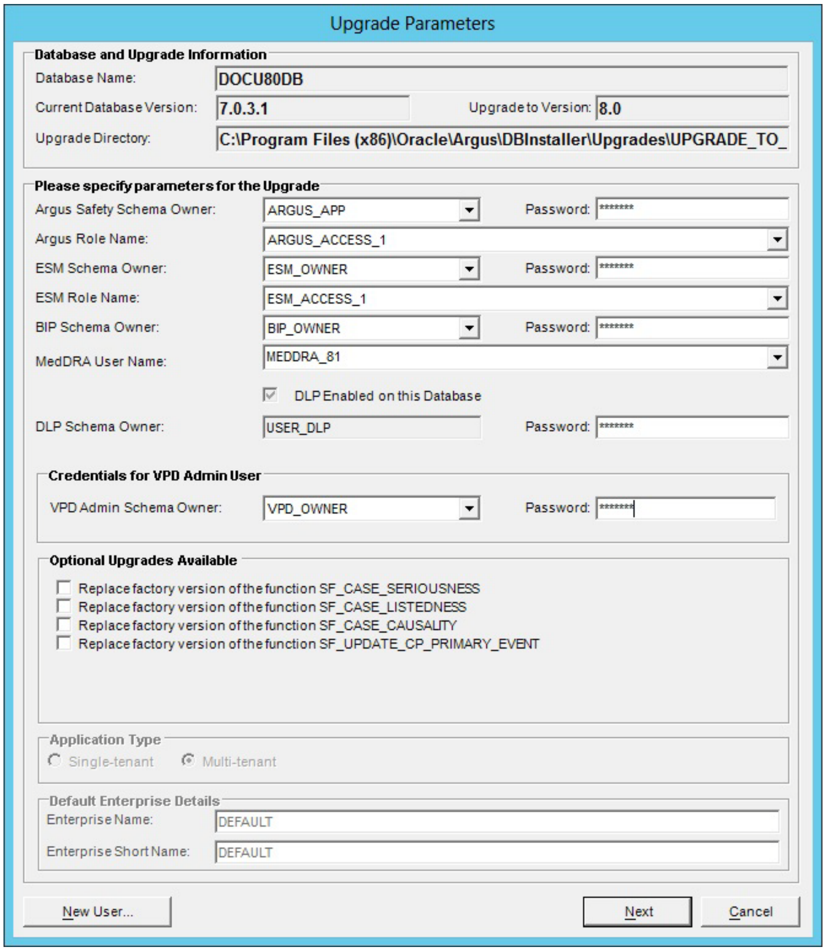
3. When the system opens the Connect to Database dialog box:

   - 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:



Upgrade Parameters

Database and Upgrade Information

Database Name: DOCU80DB

Current Database Version: 7.0.3.1   Upgrade to Version: 8.0

Upgrade Directory: C:\Program Files (x86)\Oracle\Argus\DBInstaller\Upgrades\UPGRADE_TO_

Please specify parameters for the Upgrade

Argus Safety Schema Owner: ARGUS_APP   Password: *******

Argus Role Name: ARGUS_ACCESS_1

ESM Schema Owner: ESM_OWNER   Password: *******

ESM Role Name: ESM_ACCESS_1

BIP Schema Owner: BIP_OWNER   Password: *******

MedDRA User Name: MEDDRA_81

☑ DLP Enabled on this Database

DLP Schema Owner: USER_DLP   Password: *******

Credentials for VPD Admin User

VPD Admin Schema Owner: VPD_OWNER   Password: *******

Optional Upgrades Available

□ Replace factory version of the function SF_CASE_SERIOUSNESS
□ Replace factory version of the function SF_CASE_LISTEDNESS
□ Replace factory version of the function SF_CASE_CAUSALITY
□ Replace factory version of the function SF_UPDATE_CP_PRIMARY_EVENT

Application Type

○ Single-tenant   ● Multi-tenant

Default Enterprise Details

Enterprise Name: DEFAULT

Enterprise Short Name: DEFAULT

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

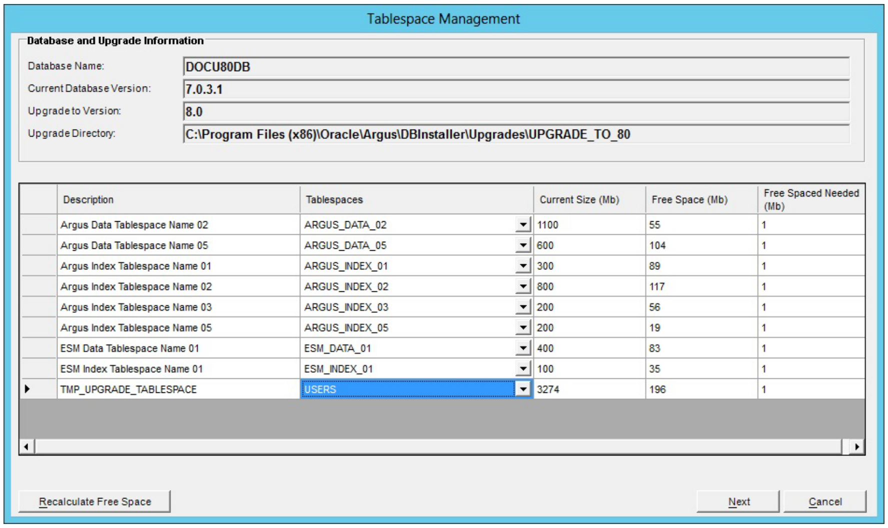
- Credentials for VPD Admin User - This includes the VPD Admin Schema Owner, Password, and Verify Password.
- Application Type - This includes the following two options:
  - Single Tenant – Select this option if you are upgrading this database and leaving it as a single tenant model.
  - Multi Tenant – Select this option if you are upgrading this database and changing to 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 BIP Schema and select it from the BIP Schema Owner drop-down list.
- Enter the BIP 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 database:



Tablespace Management

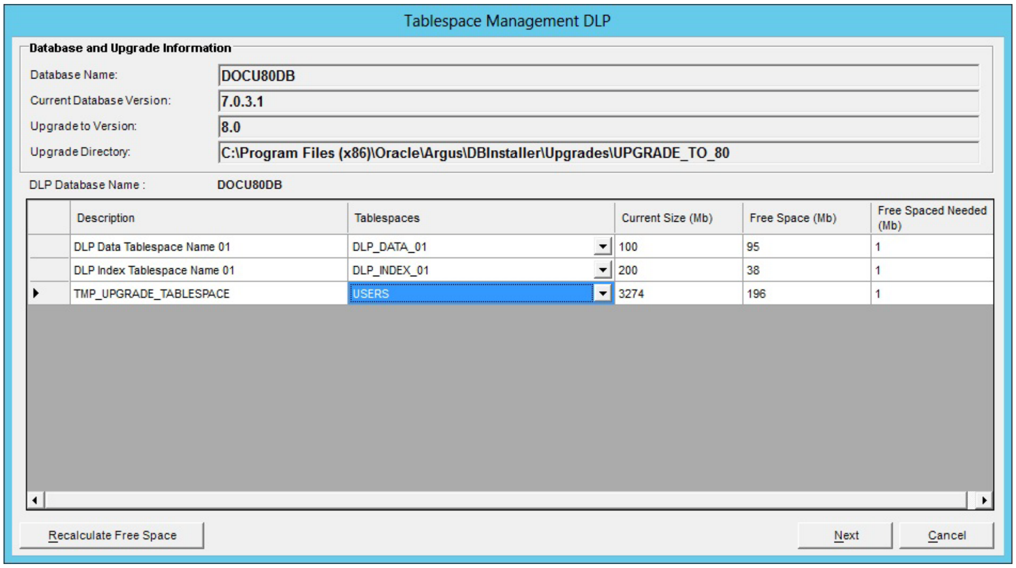
Database and Upgrade Information

Database Name: DOCU80DB
Current Database Version: 7.0.3.1
Upgrade to Version: 8.0
Upgrade Directory: C:\Program Files (x86)\Oracle\Argus\DBInstaller\Upgrades\UPGRADE_TO_80

	Description	Tablespaces	Current Size (Mb)	Free Space (Mb)	Free Spaced Needed (Mb)
	Argus Data Tablespace Name 02	ARGUS_DATA_02	1100	55	1
	Argus Data Tablespace Name 05	ARGUS_DATA_05	600	104	1
	Argus Index Tablespace Name 01	ARGUS_INDEX_01	300	89	1
	Argus Index Tablespace Name 02	ARGUS_INDEX_02	800	117	1
	Argus Index Tablespace Name 03	ARGUS_INDEX_03	200	56	1
	Argus Index Tablespace Name 05	ARGUS_INDEX_05	200	19	1
	ESM Data Tablespace Name 01	ESM_DATA_01	400	83	1
	ESM Index Tablespace Name 01	ESM_INDEX_01	100	35	1
▶	TMP_UPGRADE_TABLESPACE	USERS	3274	196	1

- 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.



Database and Upgrade Information

Database Name: DOCU80DB

Current Database Version: 7.0.3.1

Upgrade to Version: 8.0

Upgrade Directory: C:\Program Files (x86)\Oracle\Argus\DBInstaller\Upgrades\UPGRADE_TO_80

DLP Database Name : DOCU80DB

	Description	Tablespaces	Current Size (Mb)	Free Space (Mb)	Free Spaced Needed (Mb)
	DLP Data Tablespace Name 01	DLP_DATA_01	100	95	1
	DLP Index Tablespace Name 01	DLP_INDEX_01	200	38	1
▸	TMP_UPGRADE_TABLESPACE	USERS	3274	196	1

- 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.
    - 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 8.0 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 8.0 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 8.0 on a computer where Oracle 11.2.0.4 or 12c (12.1.0.1.0, 12.1.0.2.0) is installed.
- The source databases should be schema validated at Argus Safety 8.0.
- 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 8.0 application. Make sure that Oracle Client version is 11.2.0.4 or 12c (12.1.0.1.0, 12.1.0.2.0).
- The Target databases should be Schema Validated at Argus 8.0.
- 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:

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 Import 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.

l. 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:** If no dictionary credential is provided while exporting the source database, you must make sure that before you import, you create a dummy DICTIONARY.DMP file.
>
> To create the dummy dump file, right-click export dump files directory and click on Create a Text Document and rename it from *.txt to DICTIONARY.DMP.

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_70 folder.

3. Export the Source database by running C:\CONFIG_EXP_IMP_70\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. Create a new database using Argus Safety 8.0 Schema Creation tool.
6. Import into Target database by running C:\CONFIG_EXP_IMP_70\ Data_ ImportConfigOnly_11g.bat and follow the prompts. Ignore any "ORA-28101: policy already exists" error.
7. Validate Schema on the target database using Schema Validation Tool.
8. Copy ArgusSecureKey.ini from the source database folder and paste it in the .\Windows folder of application server(s) which are intended to be used with the target database.
9. In case you do not have ArgusSecureKey.ini, follow the steps listed in the Resetting the Environment if ArgusSecureKey.ini is Lost section.

4

Installing Argus Safety Web

This chapter includes the following sections:

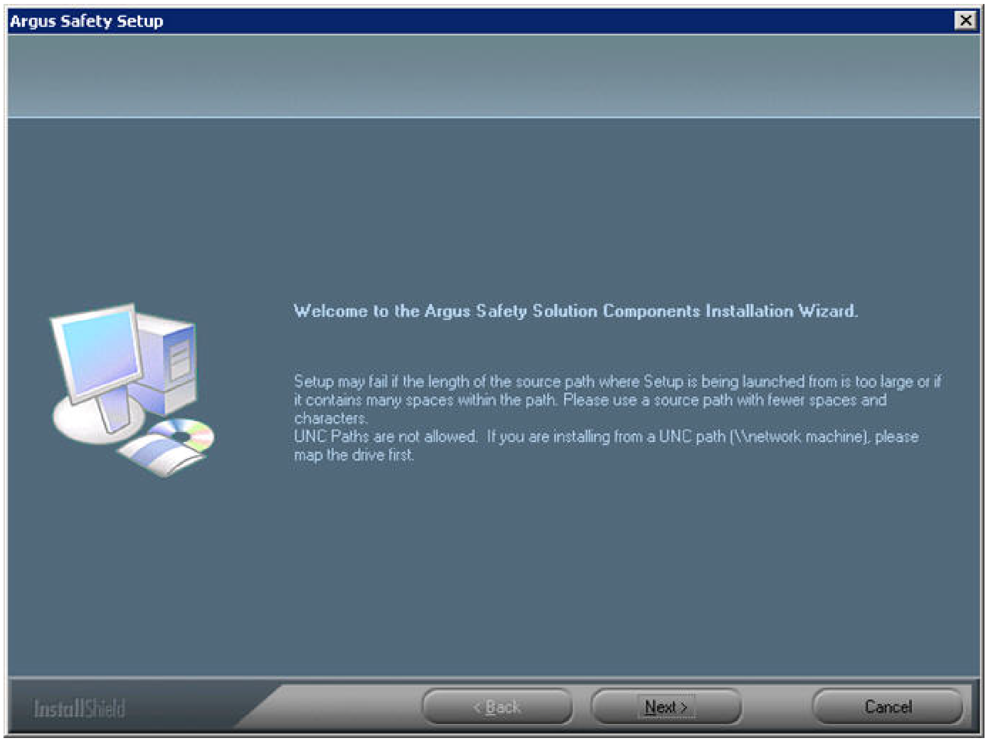
Installing Argus Safety Web

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:

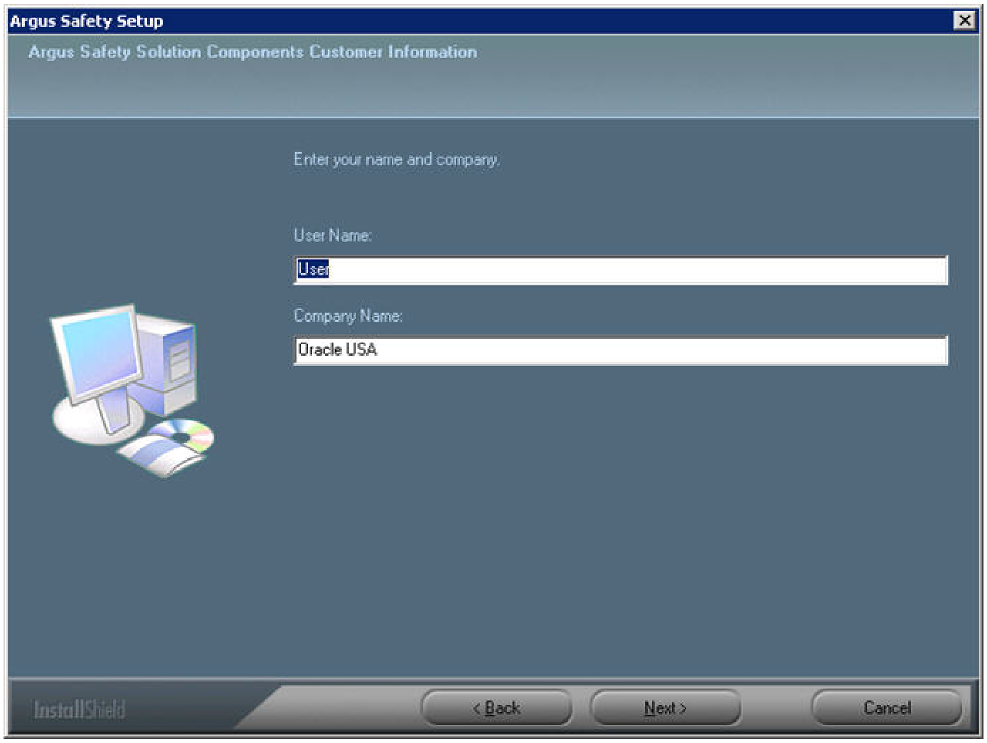
1. Open the Argus Safety folder and click **setup.exe**.
2. When the system displays the Argus Safety Setup screen, click **Next >**.


Argus Safety Setup

Welcome to the Argus Safety Solution Components Installation Wizard.

Setup may fail if the length of the source path where Setup is being launched from is too large or if it contains many spaces within the path. Please use a source path with fewer spaces and characters.
UNC Paths are not allowed. If you are installing from a UNC path (\\network machine), please map the drive first.

3. When the system displays the Customer Information screen:


Argus Safety Setup

Argus Safety Solution Components Customer Information

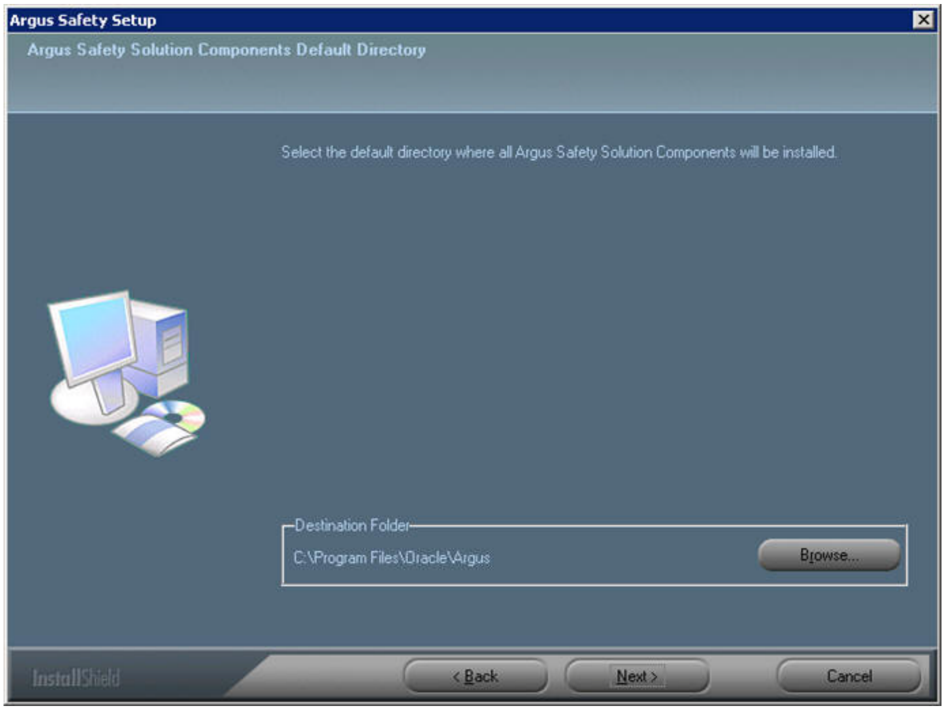
Enter your name and company.

User Name:
User

Company Name:
Oracle USA

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.



Argus Safety Setup

Argus Safety Solution Components Default Directory

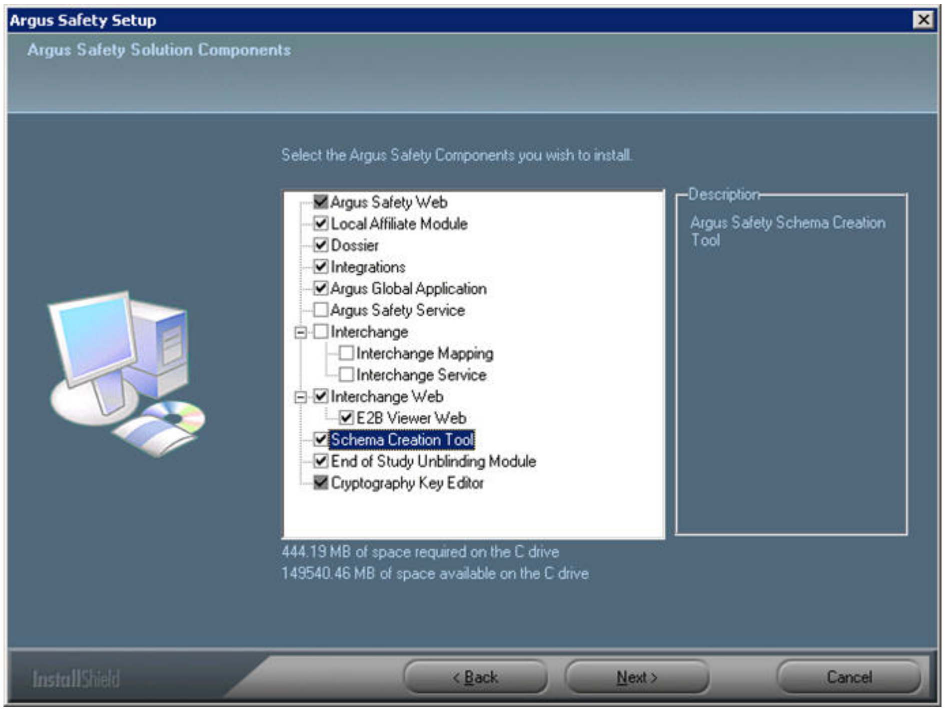
Select the default directory where all Argus Safety Solution Components will be installed.

Destination Folder

C:\Program Files\Oracle\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**.



Argus Safety Setup

Argus Safety Solution Components

Select the Argus Safety Components you wish to install.

- ☑ Argus Safety Web
- ☑ Local Affiliate Module
- ☑ Dossier
- ☑ Integrations
- ☑ Argus Global Application
- □ Argus Safety Service
- □ Interchange
  - □ Interchange Mapping
  - □ Interchange Service
- ☑ Interchange Web
  - ☑ E2B Viewer Web
- ☑ Schema Creation Tool
- ☑ End of Study Unblinding Module
- ☑ Cryptography Key Editor

Description

Argus Safety Schema Creation Tool

444.19 MB of space required on the C drive
149540.46 MB of space available on the C drive

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

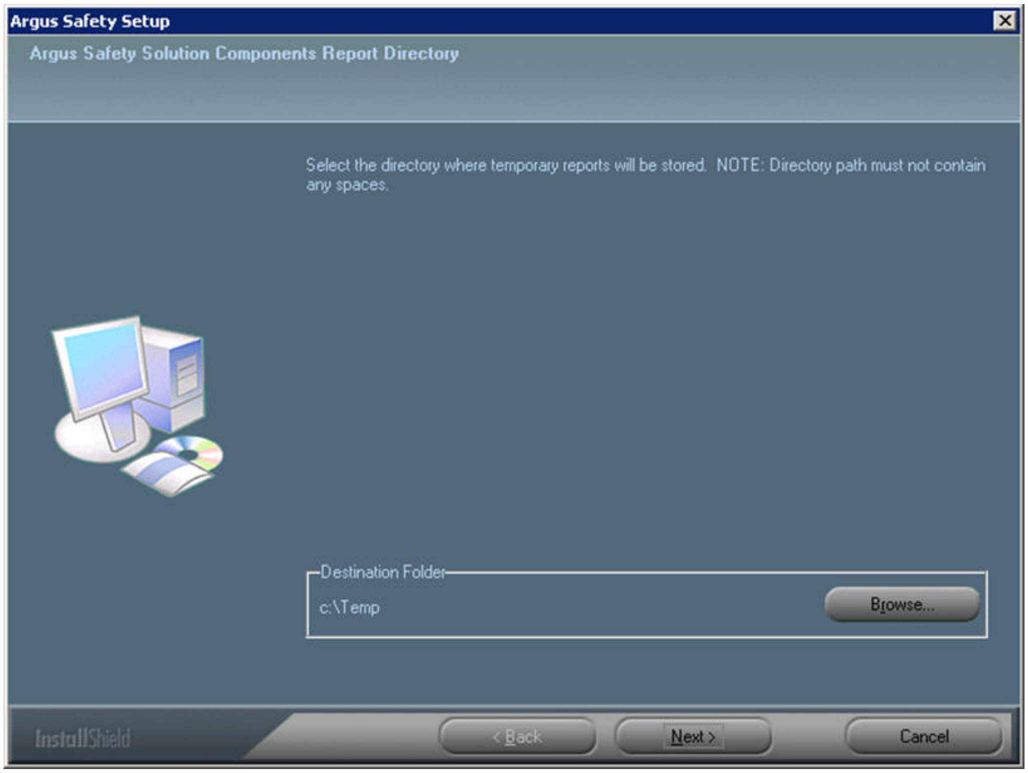
On selecting this option, global modules get installed on the same web server as Argus Safety Web and are accessible as a separate URL from the same web server. Global modules are components of Global Application having the same functionality as Portlets in the Global Homepage for Web Center.

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.

10. 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).



Argus Safety Setup

Argus Safety Solution Components Report Directory

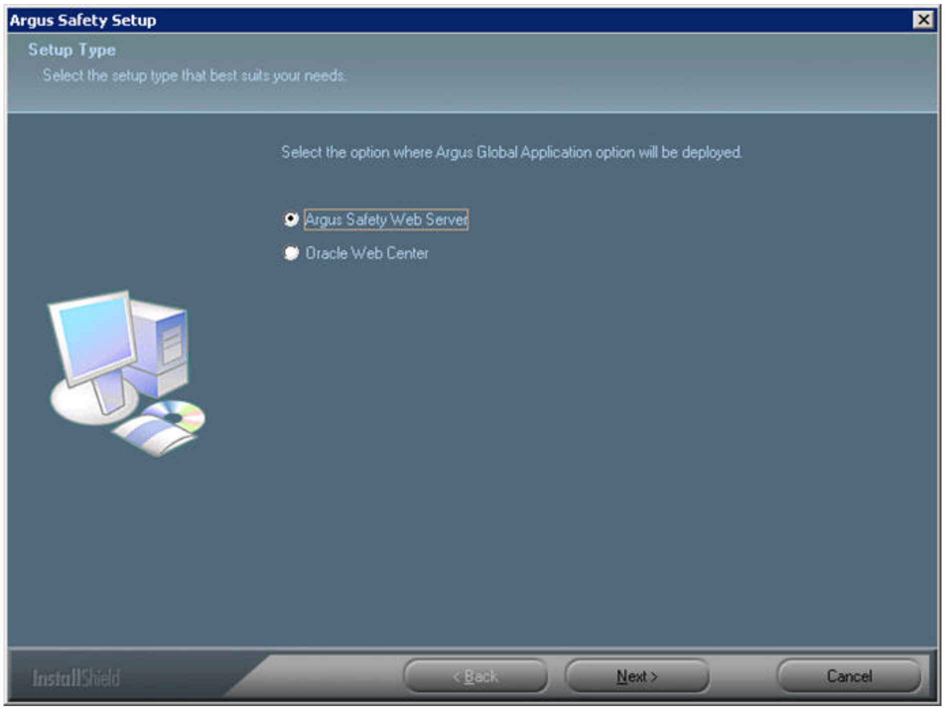
Select the directory where temporary reports will be stored. NOTE: Directory path must not contain any spaces.

Destination Folder

c:\Temp

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

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



Argus Safety Setup

Setup Type

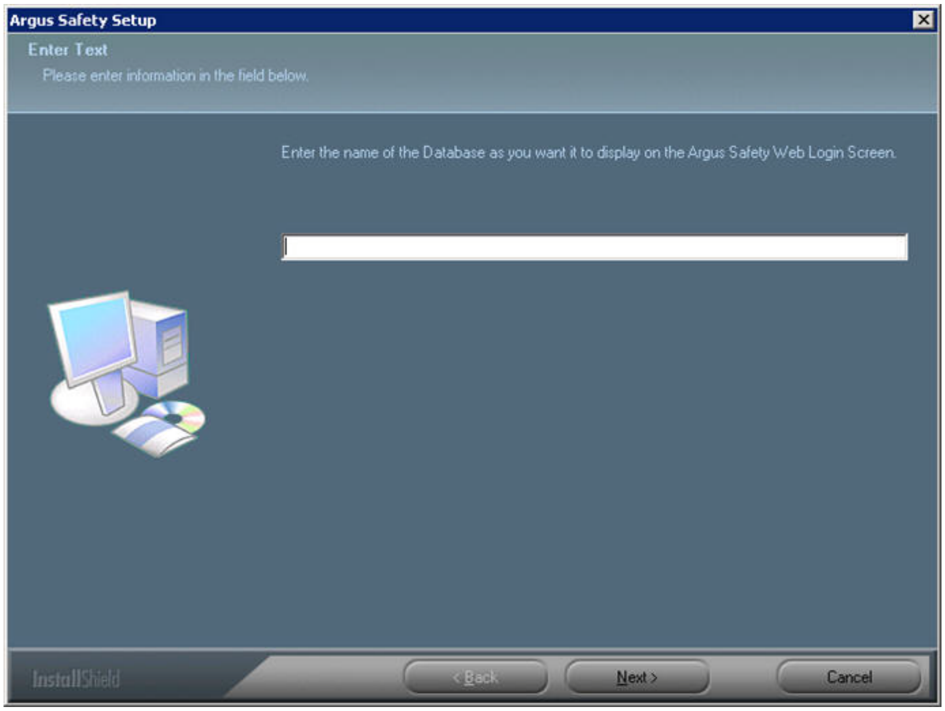
Select the setup type that best suits your needs.

Select the option where Argus Global Application option will be deployed.

● Argus Safety Web Server

○ Oracle Web Center

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.



Argus Safety Setup

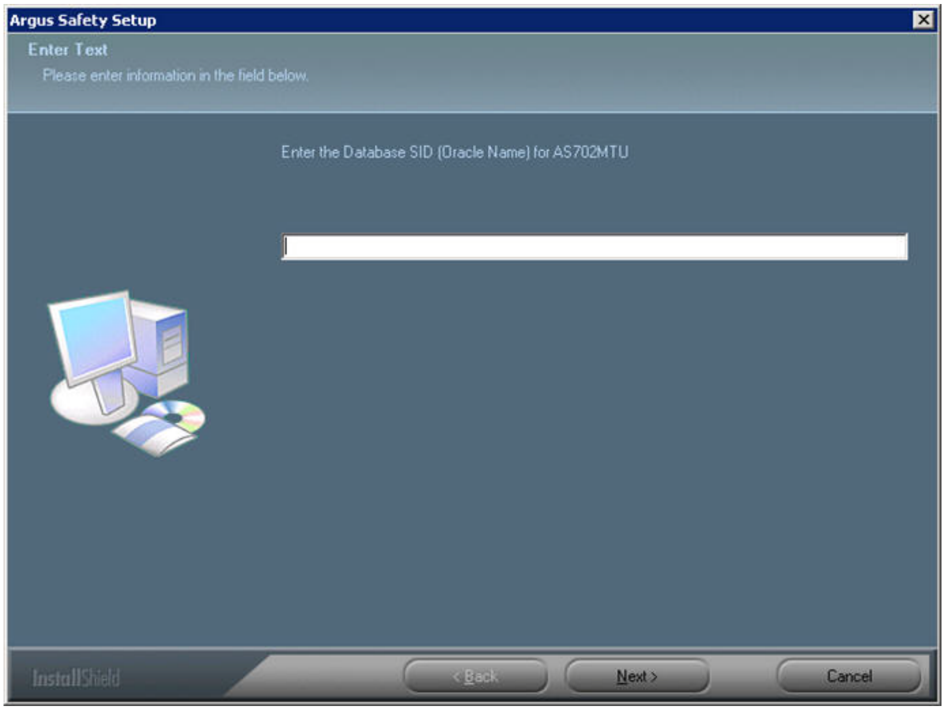
Enter Text

Please enter information in the field below.

Enter the name of the Database as you want it to display on the Argus Safety Web Login Screen.

15. Click **Next >** to continue.

16. When prompted to enter the database SID: Enter the database SID.

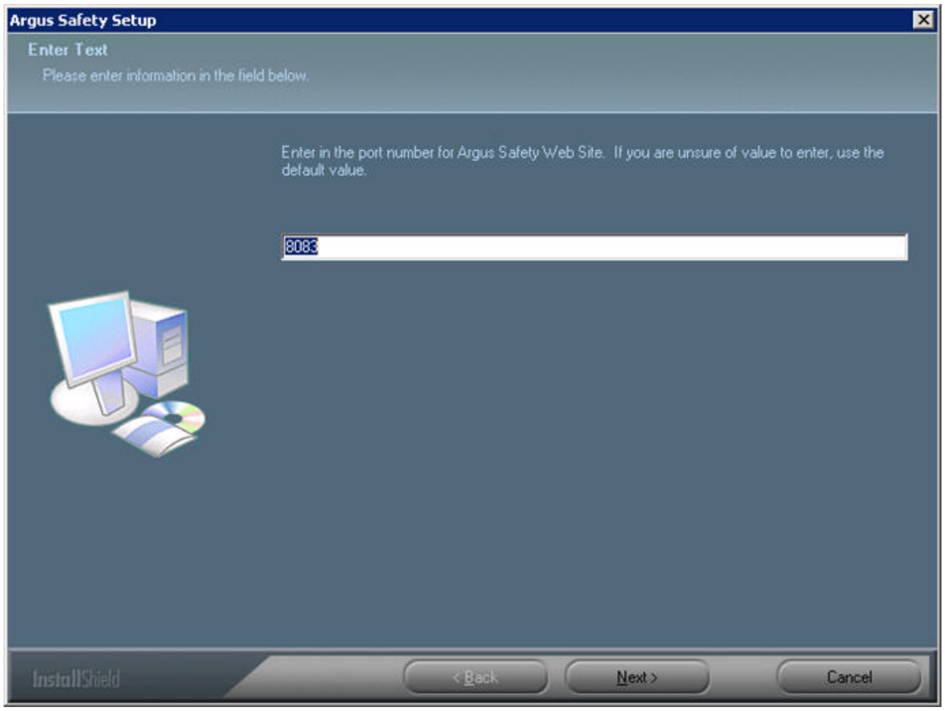


Enter the Database SID (Oracle Name) for AS702MTU

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).



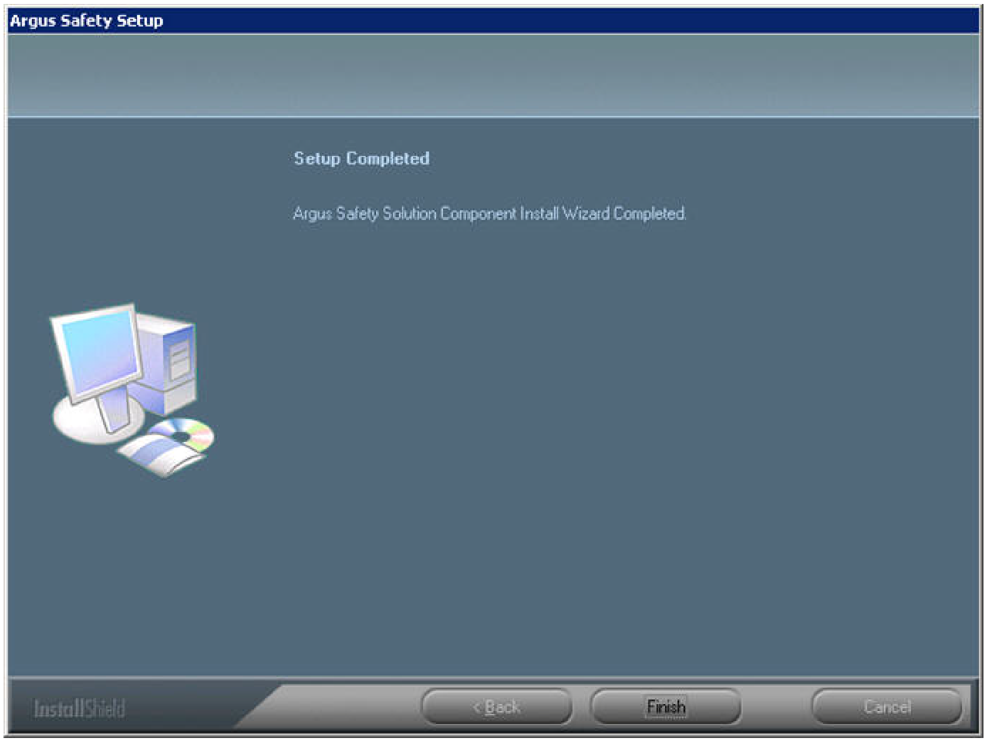
Enter in the port number for Argus Safety Web Site. If you are unsure of value to enter, use the default value.

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**.

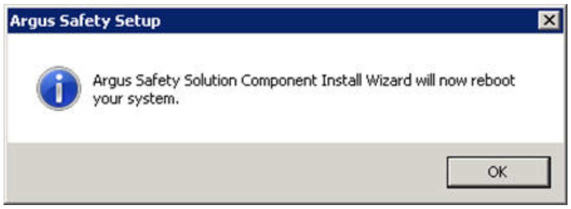


Argus Safety Setup

Setup Completed

Argus Safety Solution Component Install Wizard Completed.

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



Argus Safety Setup

Argus Safety Solution Component Install Wizard will now reboot your system.

Note: After installing Argus Safety Web, refer to the section The Argus Safety 8.0 Application Servers to set up the Argus Cryptography key.

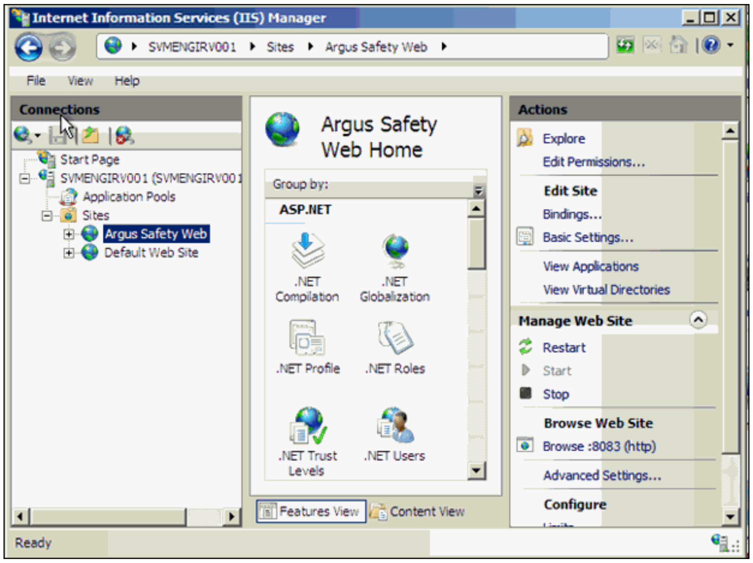
Configuring the IIS Manager for Windows 2008 and Windows 2012

Note: For Windows 2008 and Windows 2012, IIS 6 Management Compatibility and Application Development > ASP.NET/ASP roles must be installed.

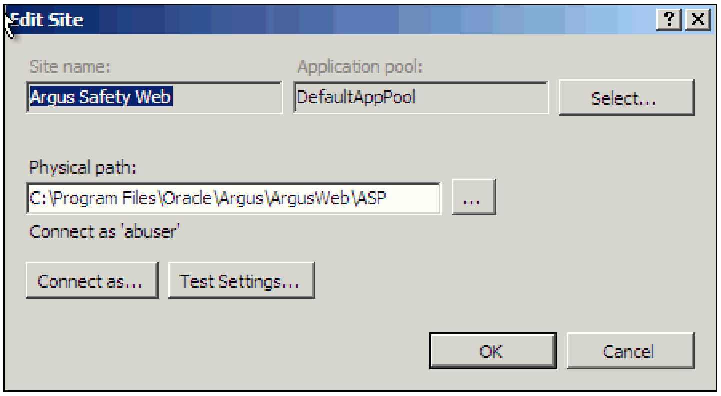
1. Select Start > Administrative Tools > Internet Information Services (IIS) Manager.

2. Expand the Connection Panel and open **Sites**.

3. Select Argus Safety Web.



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



Site name: Argus Safety Web

Application pool: DefaultAppPool

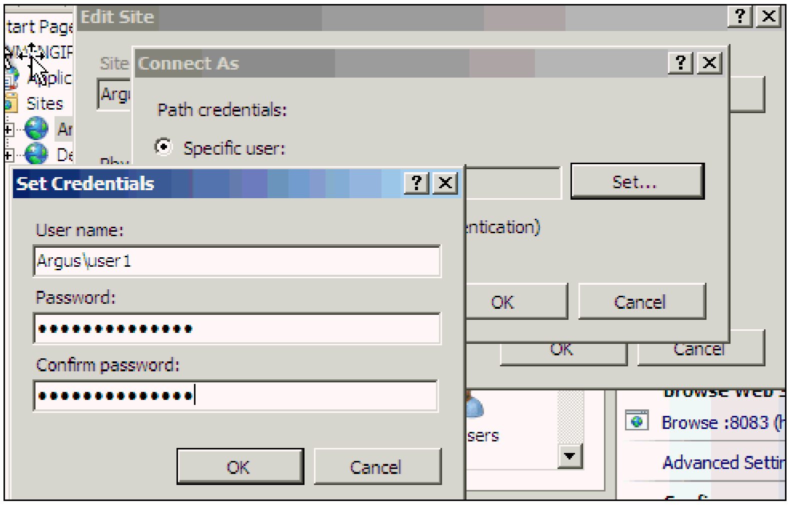
Physical path: C:\Program Files\Oracle\Argus\ArgusWeb\ASP

Connect as 'abuser'

5. Click on **Connect as…**

6. Click on **Specific User** and click on **Set**.

7. Enter Domain user name and password and click **OK**.

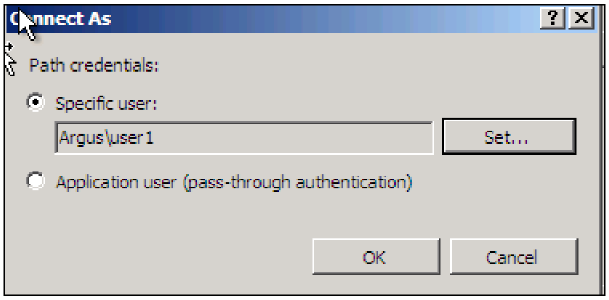


User name: Argus\user1

Password: ••••••••••••••

Confirm password: ••••••••••••••

8. Click **OK**.



Connect As

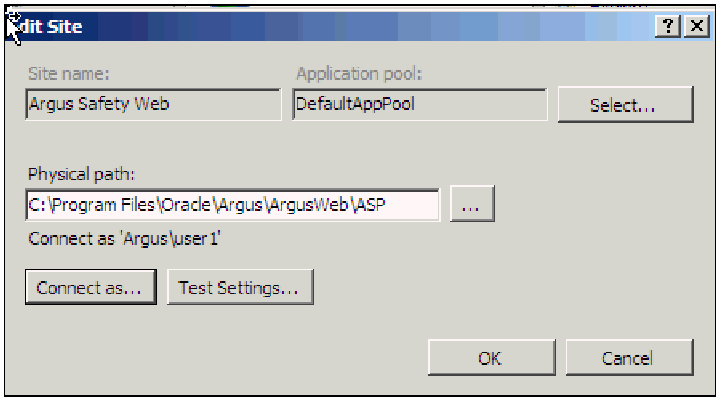
Path credentials:

● Specific user:

Argus\user1

○ Application user (pass-through authentication)

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



Edit Site

Site name: Argus Safety Web

Application pool: DefaultAppPool

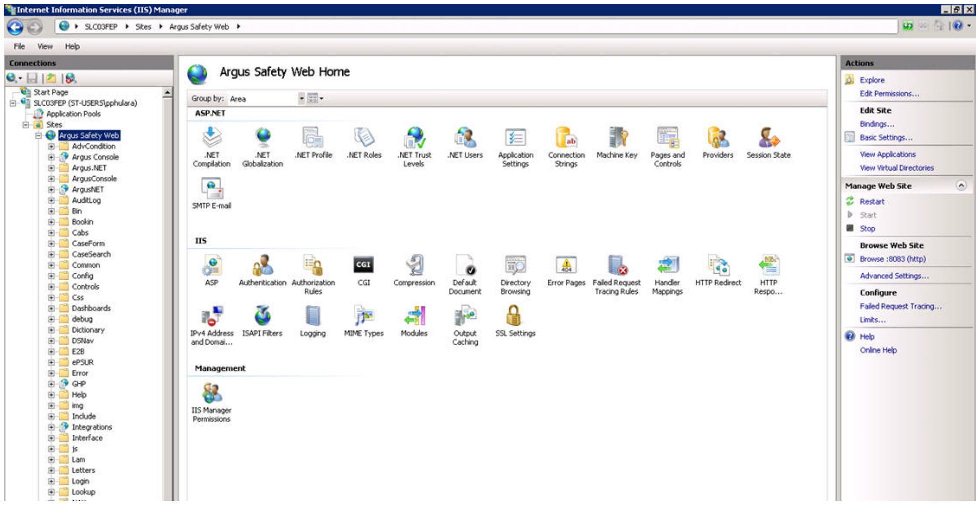
Physical path: C:\Program Files\Oracle\Argus\ArgusWeb\ASP

Connect as 'Argus\user1'

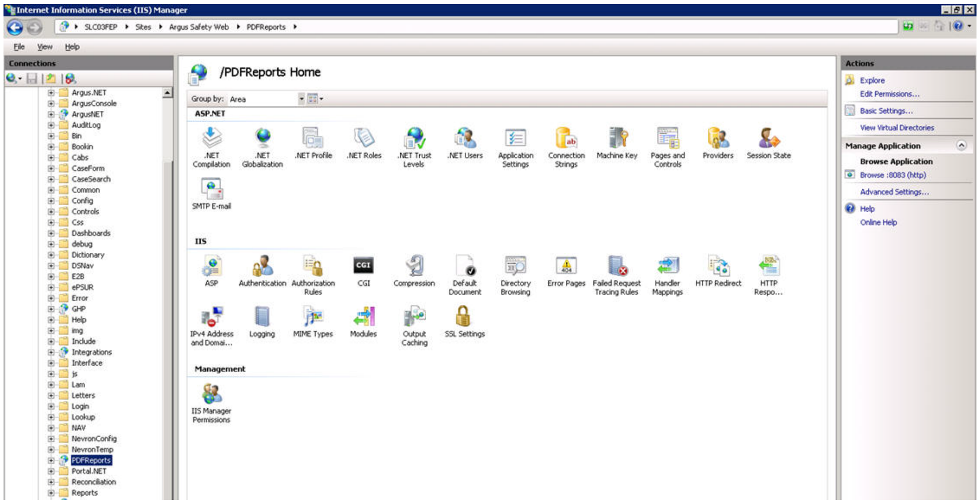
Connecting to a Domain Account on Windows 2008 and Windows 2012

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.



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.

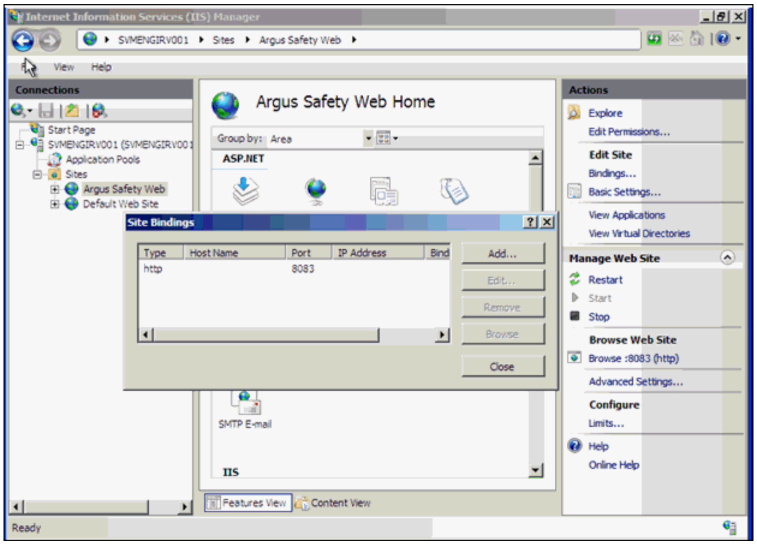
6. Repeat the above-mentioned steps for UploadedLetters, and Scanned_Images.

Enabling SSL Support for Windows 2008 and 2012

Use the following procedure to enable SSL support for Windows 2008 and 2012:

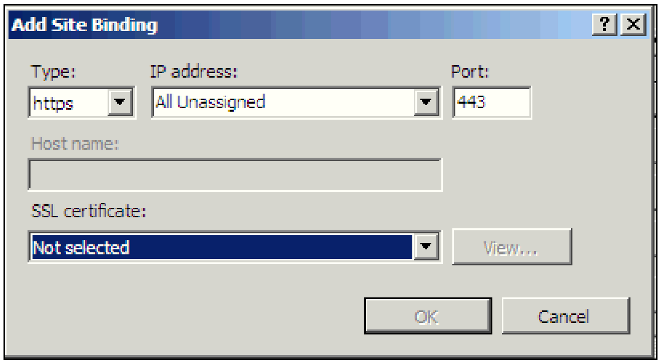
1. Obtain and install the SSL certificate.

2. Click Argus Safety Web > Bindings.



Type	Host Name	Port	IP Address	Bind
http		8083		

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



Type: https

IP address: All Unassigned

Port: 443

Host name:

SSL certificate: Not selected

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

1. 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).

5

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 Trusted Site
- Setting up Compatibility View with Internet Explorer

Adding the Argus Site as a Trusted Site

Use the following procedure to add the Argus site URL as a trusted site:

1. Open Internet Explorer.
2. Select **Tools > Internet Options**.
3. When the system displays the Internet Options dialog box.
4. When the system displays the Security tab: select **Local Intranet or Trusted Sites** and click **Sites**.
5. When the system displays the Trusted Sites dialog box.
6. Type the Argus site URL in the **Add this website to the zone** field.
7. Click **Add**.

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

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 URL.
4. Click **Add**.
5. Click **Close**.

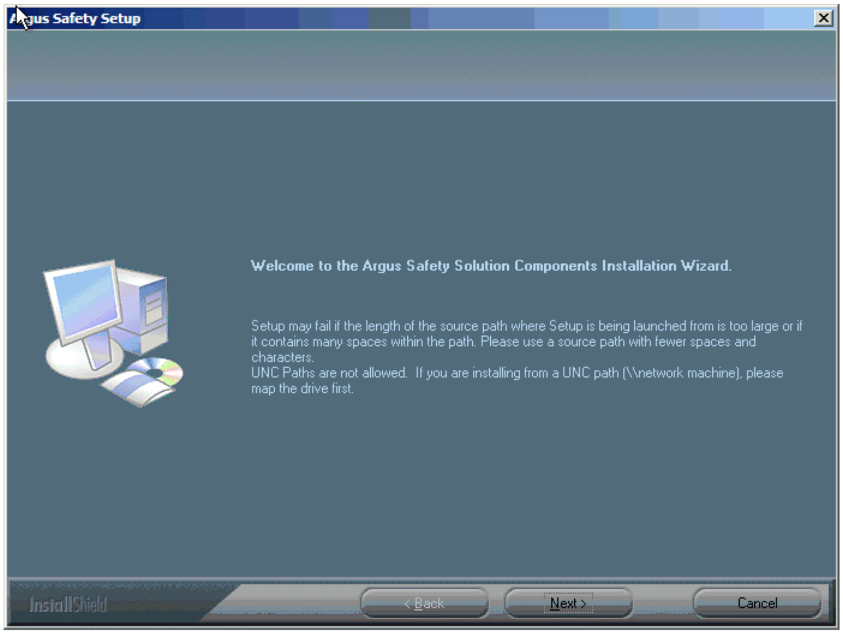
6 Installing Argus Safety Service

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.

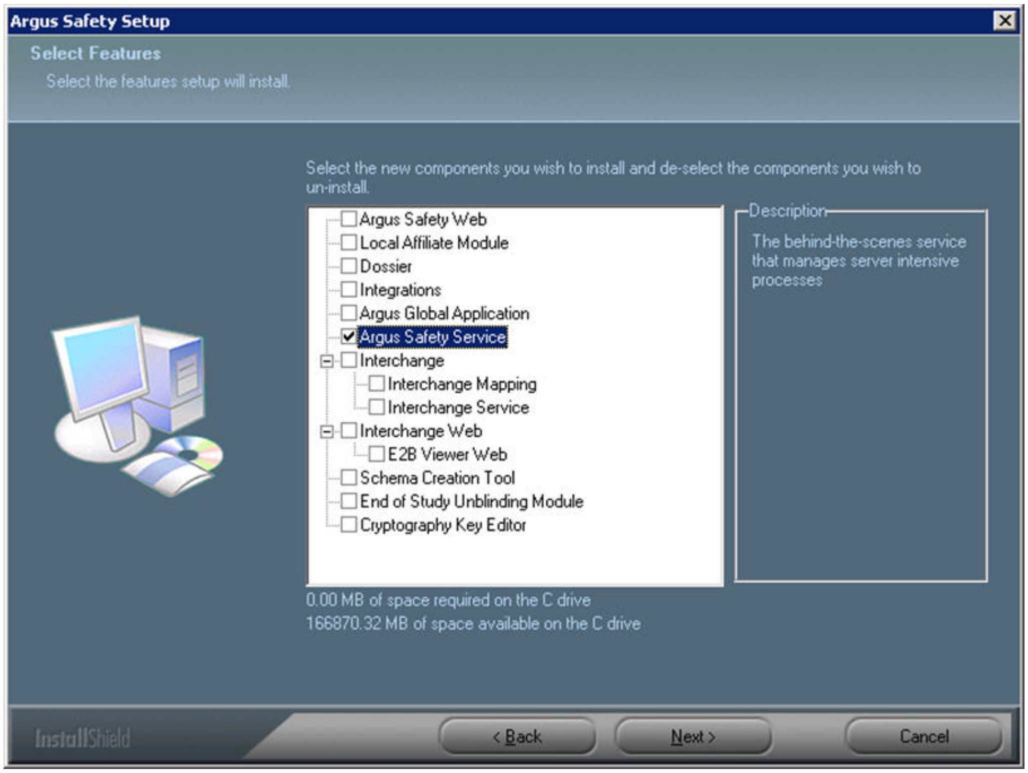


Welcome to the Argus Safety Solution Components Installation Wizard.

Setup may fail if the length of the source path where Setup is being launched from is too large or if it contains many spaces within the path. Please use a source path with fewer spaces and characters.
UNC Paths are not allowed. If you are installing from a UNC path (\\network machine), please map the drive first.

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.



Argus Safety Setup

Select Features

Select the features setup will install.

Select the new components you wish to install and de-select the components you wish to un-install.

- ☐ Argus Safety Web
- ☐ Local Affiliate Module
- ☐ Dossier
- ☐ Integrations
- ☐ Argus Global Application
- ☑ Argus Safety Service
- ☐ Interchange
  - ☐ Interchange Mapping
  - ☐ Interchange Service
- ☐ Interchange Web
  - ☐ E2B Viewer Web
- ☐ Schema Creation Tool
- ☐ End of Study Unblinding Module
- ☐ Cryptography Key Editor

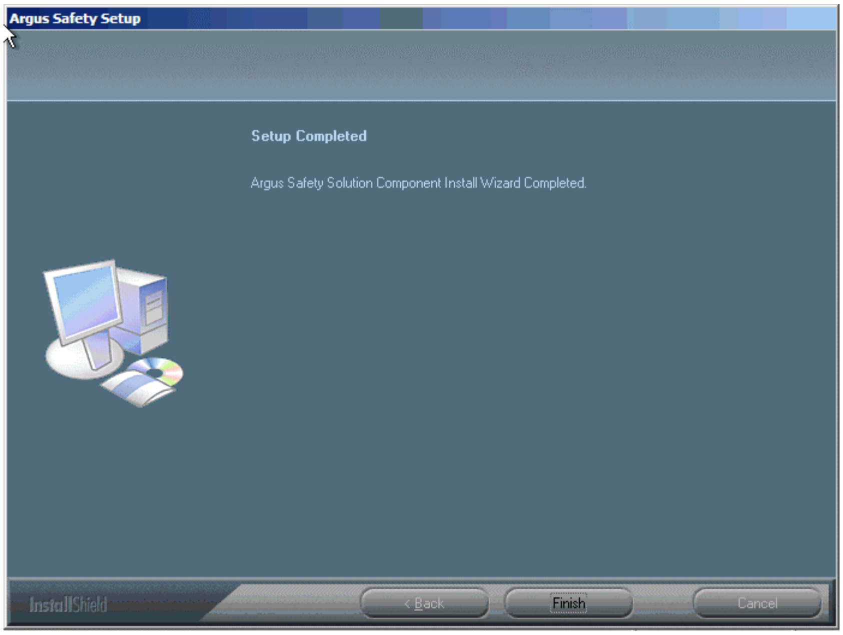
Description

The behind-the-scenes service that manages server intensive processes

0.00 MB of space required on the C drive

166870.32 MB of space available on the C drive

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**.

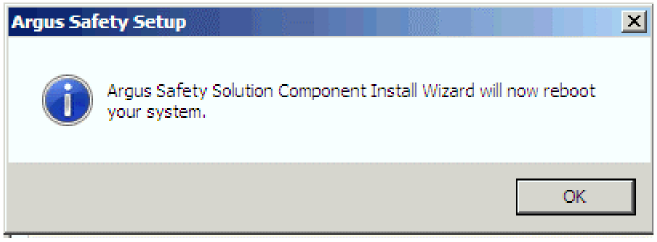


Argus Safety Setup

Setup Completed

Argus Safety Solution Component Install Wizard Completed.

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



Argus Safety Setup

Argus Safety Solution Component Install Wizard will now reboot your 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.

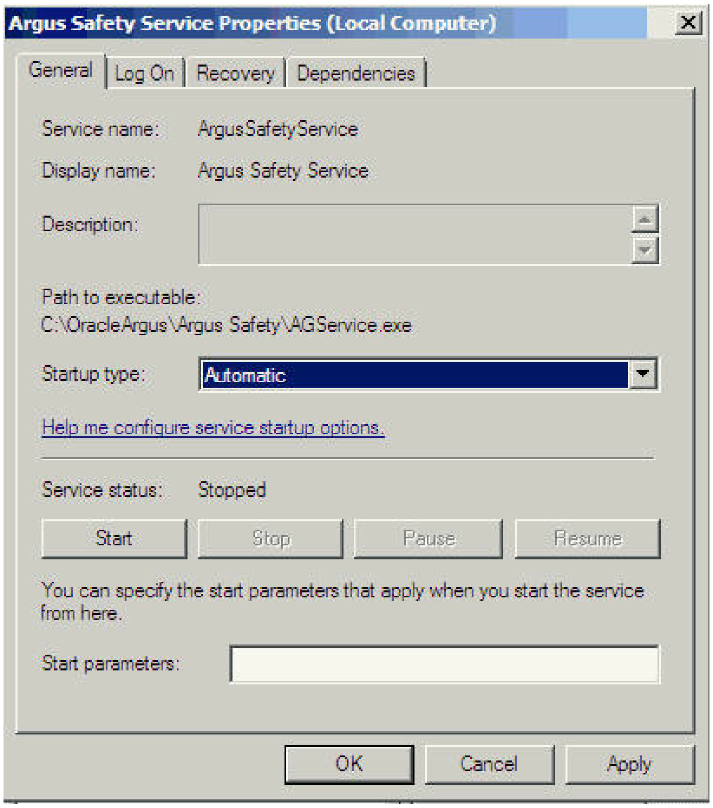
> **Note:** After installing Agus Safety Service, refer to the section The Argus Safety 8.0 Application Servers to set up the Argus Cryptography key and also to the section Generating Encrypted String from Clear Text on Configured User Cryptography Key to configure Argus Safety Service user passwords.

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:



Service name: ArgusSafetyService

Display name: Argus Safety Service

Description:

Path to executable:
C:\OracleArgus\Argus Safety\AGService.exe

Startup type: Automatic

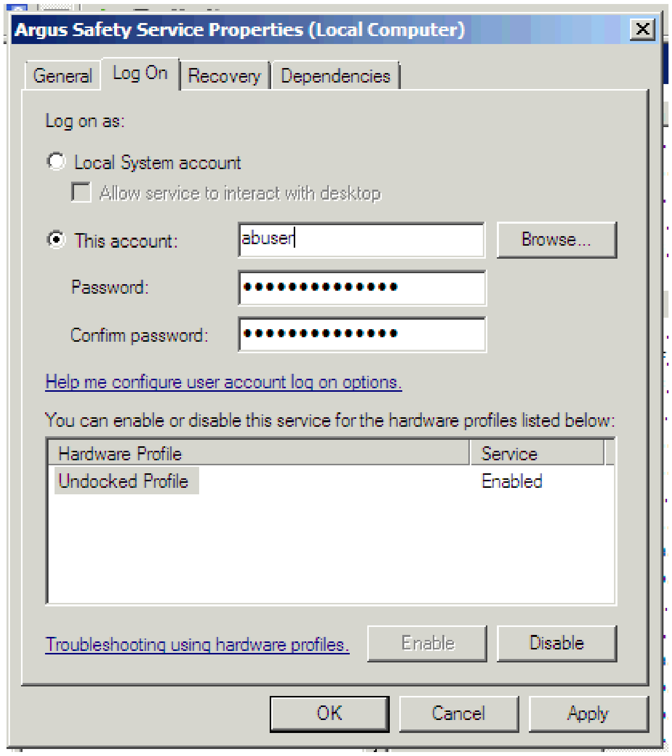
Help me configure service startup options.

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

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:



Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: abuser

Password: •••••••••••••••

Confirm password: •••••••••••••••

Help me configure user account log on options.

You can enable or disable this service for the hardware profiles listed below:

Hardware Profile	Service
Undocked Profile	Enabled

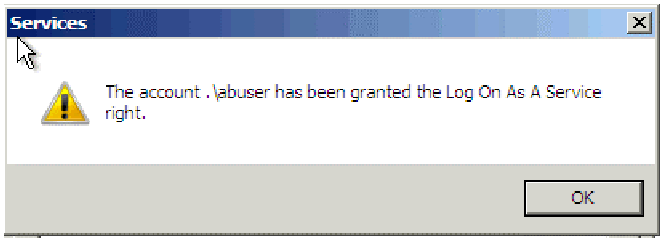
Troubleshooting using hardware profiles.

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**.



The account .\abuser has been granted the Log On As A Service right.

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
- Configuring Axway Synchrony for Binary File Transmission
- Configuring Axway Synchrony Community
- Adding a Node
- Configuring Axway Synchrony Certificates
- Configuring EVENTS.XML
- 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

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 - 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 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 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.
   - Click **Home**.

     The status of the node changes to **Running.**
8. 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 Pick a community page opens:

- Click the **Community name**.

6. When the Summary page opens:

   - Click the **Certificates** link.

7. When the Pick a 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:

   - Locate the **Or pick a task** section and click **Export this certificate**.

9. When the Choose the format you want to use for the certificate export page opens:

   - Click **Export certificate**.
   - Click the **Include all certificates in the certification path if possible** check box.
   - Click the **Cryptographic Message Syntax Standard PKCS #7** option button.

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 Pick a community page opens:

   - Click the **Community name**.

6. When the Summary page opens:

   - Click the **Certificates** link.

7. When the Pick a 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

Use the following procedure to configure EVENTS.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>

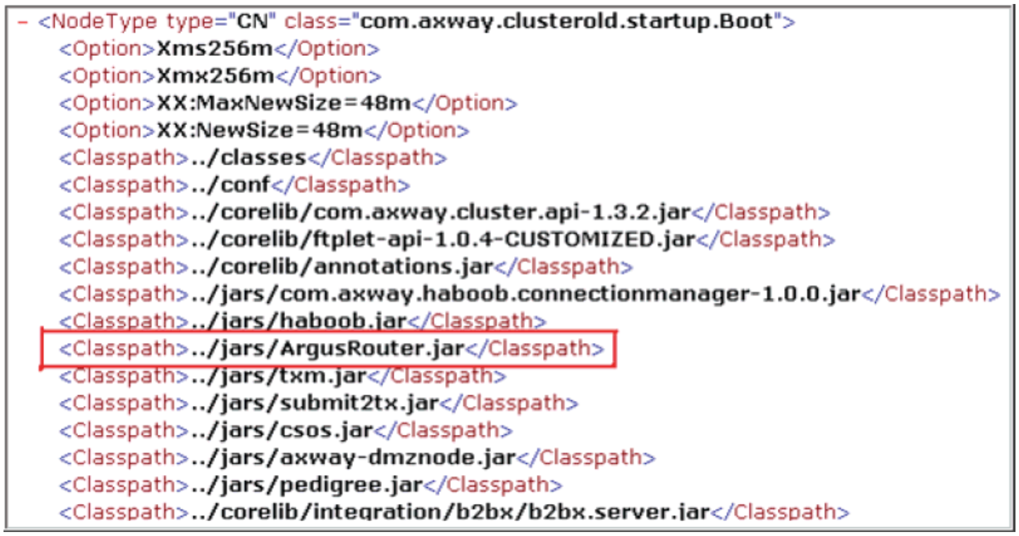
   </EventFilter>

   In order to re-enable logging to the MESSAGEEVENTSNAPHOTS table, the following event filter needs to be un-commented in the events.xml. This used to be enabled by default in Axway Synchrony versions prior to Axway Synchrony v5.4.

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

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:



```
- <NodeType type="CN" class="com.axway.clusterold.startup.Boot">
    <Option>Xms256m</Option>
    <Option>Xmx256m</Option>
    <Option>XX:MaxNewSize=48m</Option>
    <Option>XX:NewSize=48m</Option>
    <Classpath>../classes</Classpath>
    <Classpath>../conf</Classpath>
    <Classpath>../corelib/com.axway.cluster.api-1.3.2.jar</Classpath>
    <Classpath>../corelib/ftplet-api-1.0.4-CUSTOMIZED.jar</Classpath>
    <Classpath>../corelib/annotations.jar</Classpath>
    <Classpath>../jars/com.axway.haboob.connectionmanager-1.0.0.jar</Classpath>
    <Classpath>../jars/haboob.jar</Classpath>
    <Classpath>../jars/ArgusRouter.jar</Classpath>
    <Classpath>../jars/txm.jar</Classpath>
    <Classpath>../jars/submit2tx.jar</Classpath>
    <Classpath>../jars/csos.jar</Classpath>
    <Classpath>../jars/axway-dmznode.jar</Classpath>
    <Classpath>../jars/pedigree.jar</Classpath>
    <Classpath>../corelib/integration/b2bx/b2bx.server.jar</Classpath>
```

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.

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.

8

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".

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

The 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.

9

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:

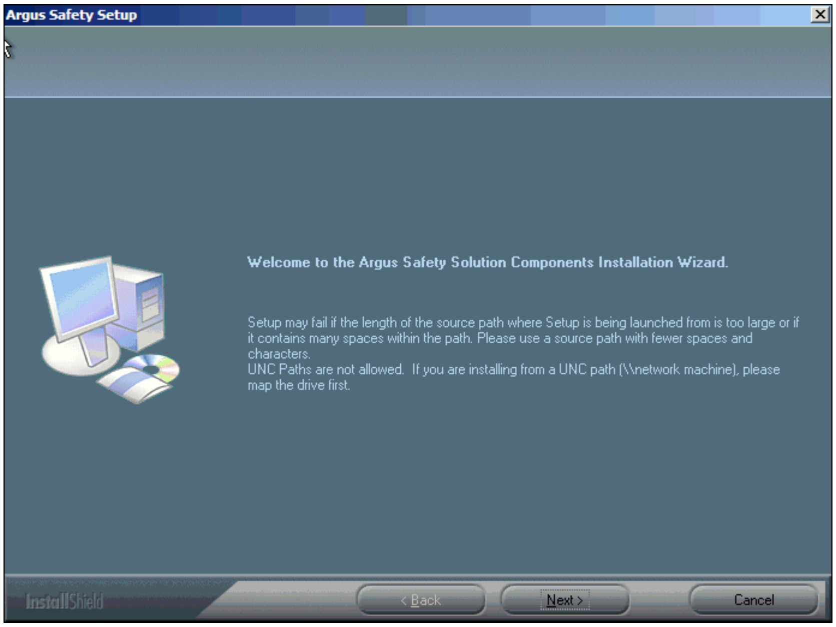
- Since Interchange Mapping has a user interface for configuring Interchange Service, it must be installed on the same system as Interchange Service. If they are not installed on the same system, you will be unable to access the user interface required to configure Interchange Service.
- You must also 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.

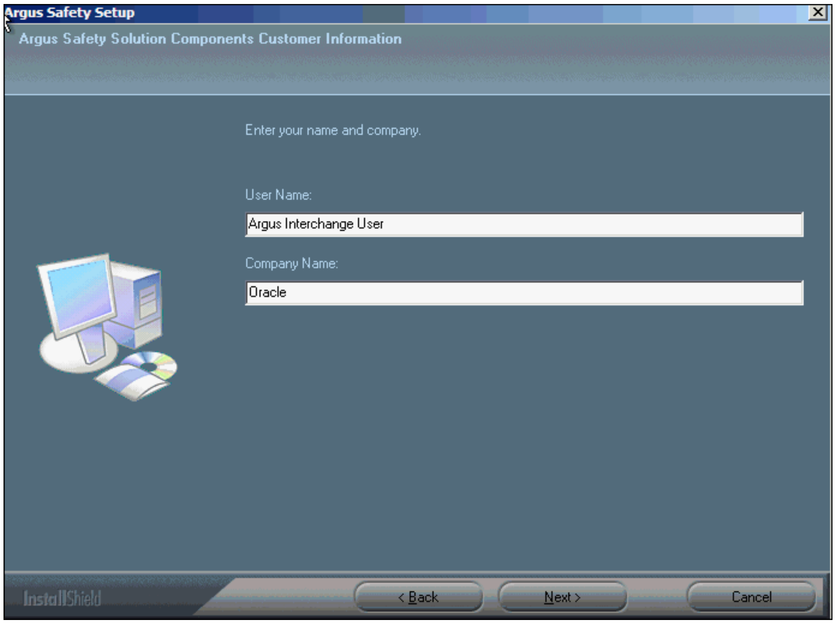


Argus Safety Setup

Welcome to the Argus Safety Solution Components Installation Wizard.

Setup may fail if the length of the source path where Setup is being launched from is too large or if it contains many spaces within the path. Please use a source path with fewer spaces and characters.
UNC Paths are not allowed. If you are installing from a UNC path (\\network machine), please map the drive first.

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



Argus Safety Setup

Argus Safety Solution Components Customer Information

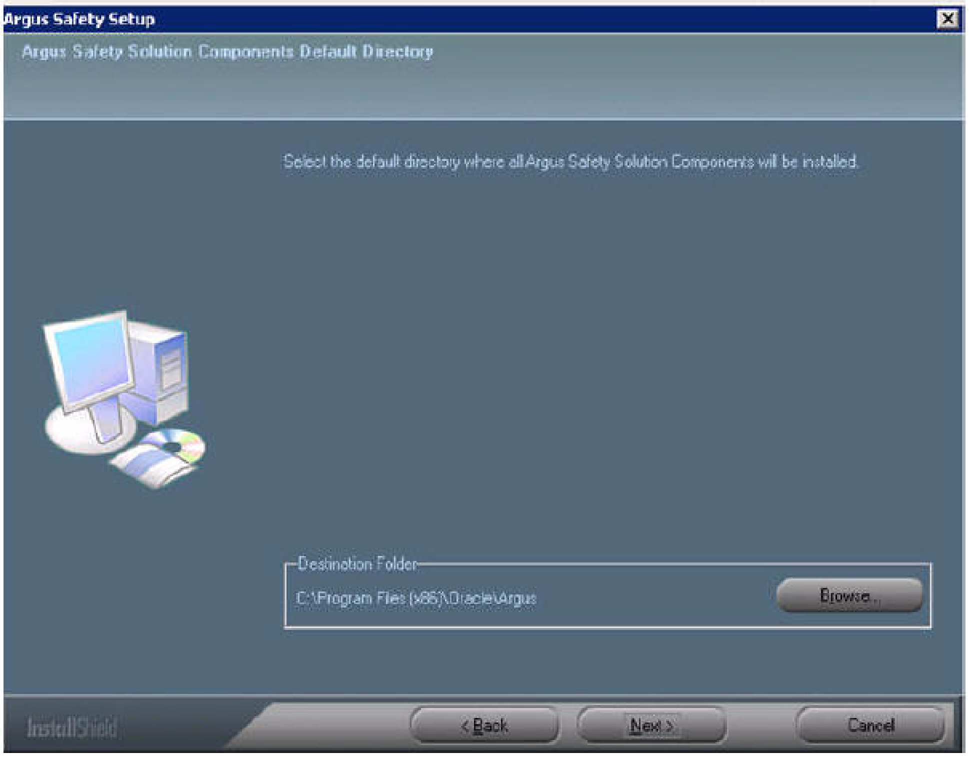
Enter your name and company.

User Name: Argus Interchange User

Company Name: Oracle

- 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:



Argus Safety Setup

Argus Safety Solution Components Default Directory

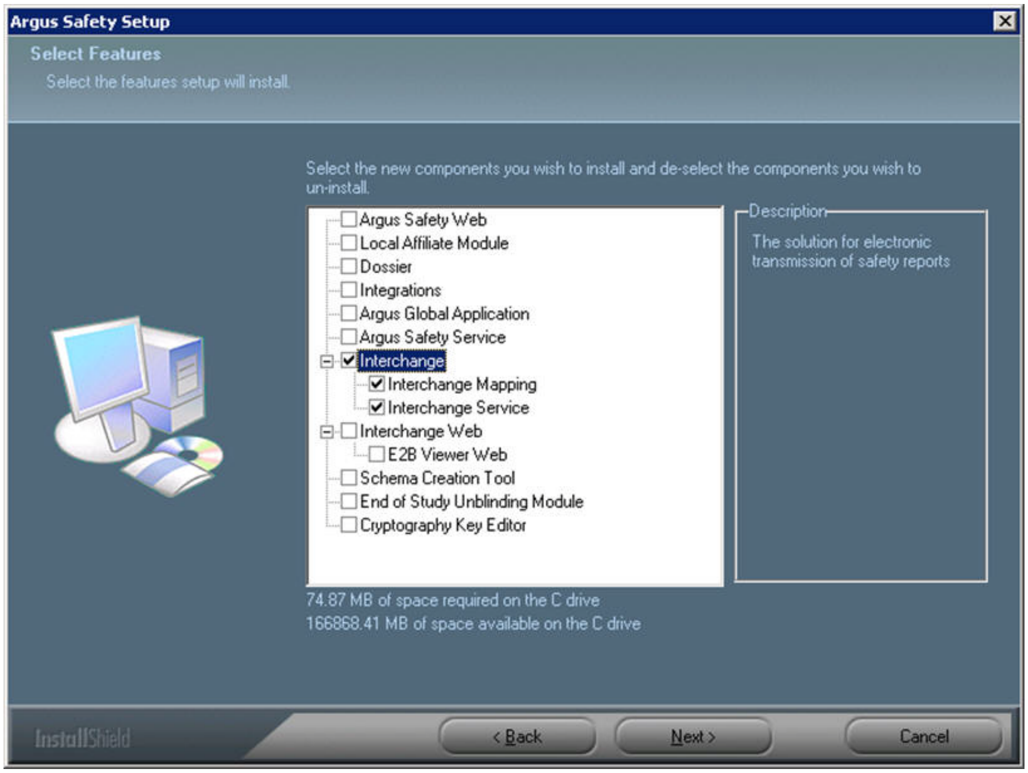
Select the default directory where all Argus Safety Solution Components will be installed.

Destination Folder

C:\Program Files (x86)\Oracle\Argus

- Click **Browse** to default installation directory for the Argus Safety Solution components.

5. When the wizard opens the dialog box:



Argus Safety Setup

Select Features

Select the features setup will install.

Select the new components you wish to install and de-select the components you wish to un-install.

- ☐ Argus Safety Web
- ☐ Local Affiliate Module
- ☐ Dossier
- ☐ Integrations
- ☐ Argus Global Application
- ☐ Argus Safety Service
- ☑ Interchange
  - ☑ Interchange Mapping
  - ☑ Interchange Service
- ☐ Interchange Web
  - ☐ E2B Viewer Web
- ☐ Schema Creation Tool
- ☐ End of Study Unblinding Module
- ☐ Cryptography Key Editor

Description

The solution for electronic transmission of safety reports

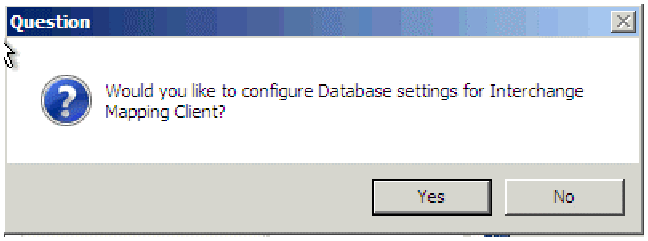
74.87 MB of space required on the C drive

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:

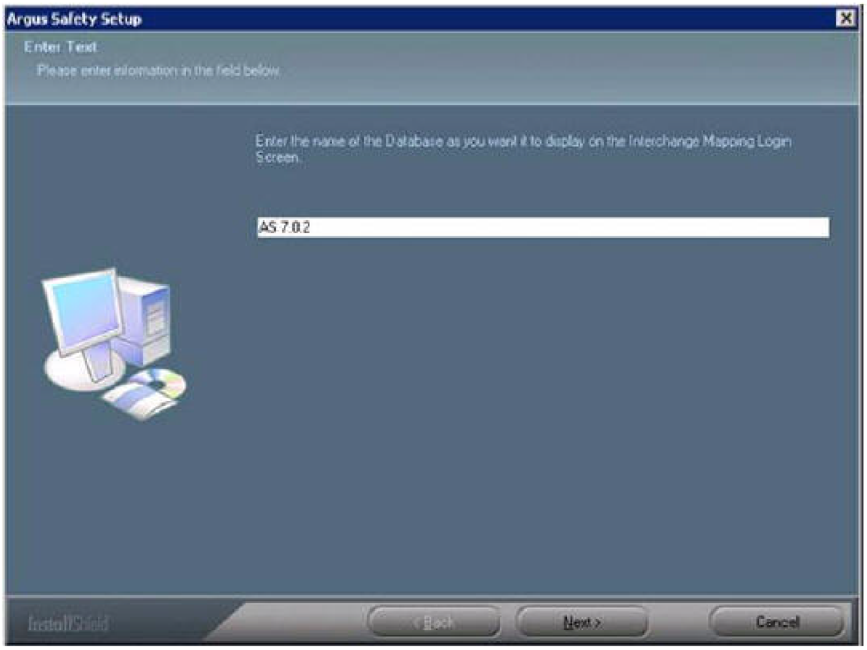


Question

Would you like to configure Database settings for Interchange Mapping Client?

- Click **Yes** to configure a database for Argus Interchange.

7. When prompted to enter a database name:



Argus Safety Setup

Enter Text

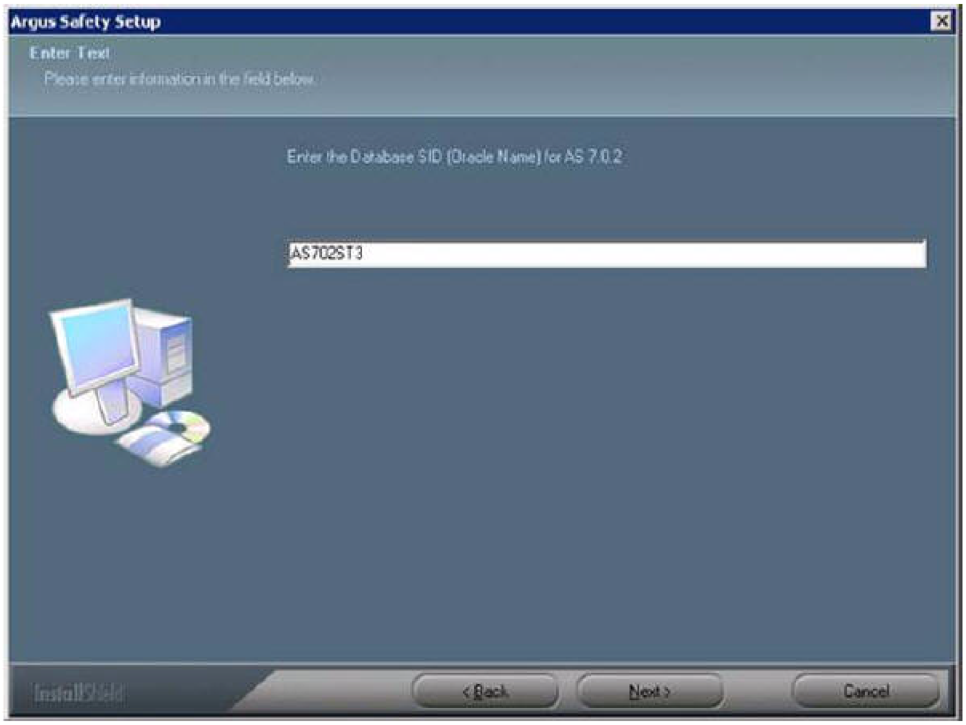
Please enter information in the field below.

Enter the name of the Database as you want it to display on the Interchange Mapping Login Screen.

AS 7.0.2

- 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 Text

Please enter information in the field below.

Enter the Database SID (Oracle Name) for AS 7.0.2

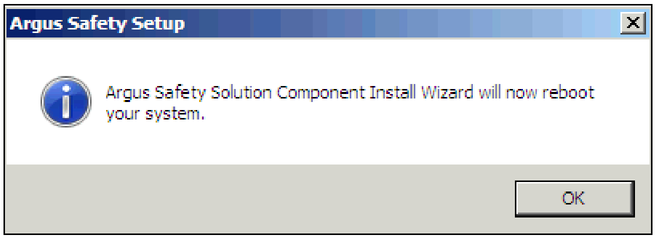
AS702ST3

   - 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:



Argus Safety Solution Component Install Wizard will now reboot your system.

11. Click **OK** to reboot.

> **Note:** After installing Interchange Service, refer to the section The Argus Safety 8.0 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.

10

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
- Validating the easyPDF 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/12c 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

1. 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="0314F7D9B94FF1F651069E4F36EE517D452537339935F9D7C2FA04843FA5E486"
   - 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="0314F7D9B94FF1F651069E4F36EE517D452537339935F9D7C2FA04843FA5E486"
  - 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.

Validating the easyPDF Installation

You must validate the easyPDF Installation for Change to Word 2007, 2010, and 2013.

Validating the easyPDF Installation for Word 2007, 2010, and 2013

Use the following procedure verify that easyPDF has installed correctly.

1. Open Mirosoft Word.
2. Select File > Word Options. go to file Menu > Word Option > Add-ins. Observe that **BCL easyPDF 7 (or 6) COM Add-in** is present. If it is not present, add it.
3. When the Word Options dialog box opens, click Add-Ins.
4. When the Add-Ins dialog box opens, verify that BCL easyPDF6 COM Add-in is present.
5. If it is not present, add it.

11

Enabling IIS HTTP Compression

This chapter describes how to enable IIS HTTP Compression on a Windows 2008 Server and 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 2008 and 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 2008 and 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 Explorer	Selecting this option will cache files only until the browser is closed. Upon closing the IE window, all cache will be expired. This option will provide some performance enhancement when a user visits the same page multiple times within a single browser session
Automatically	Selecting this option will allow IE to make a decision if a file should be cached or not. This option automatically performs the same function as "Every Time I Start Internet Explorer". In addition, after a file has been request so many time, IE will automatically cache the file even after the browser is closed. If the file has been cached and a new version of the file exists on the Web Server, the new version will be downloaded to the 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 cause problem with sites that have dynamic data and so this should not be used. Also, if a file has been updated on the server due to an upgrade, 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.

12
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 the following e-mail methods:

- SMTP

Argus Safety Service and Interchange Service use these e-mail methods in the following priority order:

1. SMTP

   SMTP is used 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.
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.
2. Select Reporting Destination.

3. Enter the e-mail address in the E-mail Address text box under Agent 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

1. 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

1. 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.

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.

13 Enabling and Configuring BIP Periodic Reports

Argus BIP 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 BIP Periodic reports.

It includes the following sections:

- Preparing BI Publisher Server
- Database Configuration
- Setting up the BI Publisher for Argus Safety
- Uploading the Argus Safety.xdrz file to BIP
- Integrating Argus Safety with BIP
- Argus Console-level Configurations
- Creating the Database Jobs

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 BIP 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 BIP 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: <password for the argus safety schema owner>.
- Enter BI Publisher Schema which is created: <the BIP Schema owner name created through the schema creation utility during Argus Safety db creation>.
- Enter Password for BIP user: <password of the BIP Schema owner>.
- Enter BIP Repository Instance name: <database SID of the BIP metadata repository database>.
- Enter BIP Repository User name (Default DEV_BIPLATFORM): <the DEV_BIPLATFORM user created in BIP metadata repository database>.
- Enter BIP Repository Password: (password for the DEV_BIPLATFORM user>.

Note: If you are using Argus Mart with BIP 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:

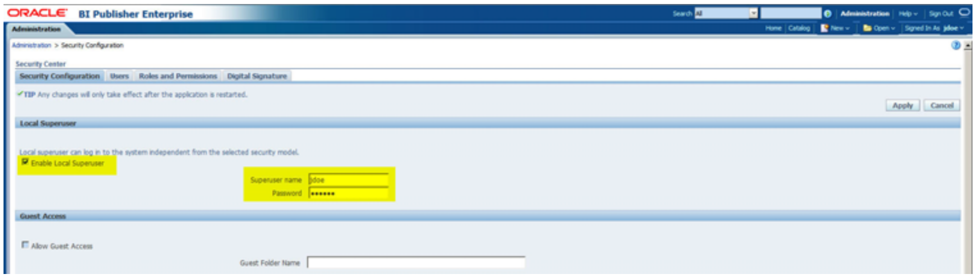
- Enabling a Local Superuser
- Configuring the Security Model
- Configuring Server Settings
- Creating Users and Assigning Roles
- Creating ASBIP JDBC Connection

13.4.1 Enabling a Local Superuser

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

To enable a local superuser:

1. Click **Administration**.
2. Under **Security Center**, click **Security Configuration**.
3. Under Local Superuser, select the box and enter the credentials for the Superuser, as shown.
4. Restart the BI Publisher service.



TIP Any changes will only take effect after the application is restarted.

Local superuser can log in to the system independent from the selected security model.

☑ Enable Local Superuser

Superuser name: jdoe

Password: ••••••

☐ Allow Guest Access

Guest Folder Name:

13.4.2 Configuring the Security Model

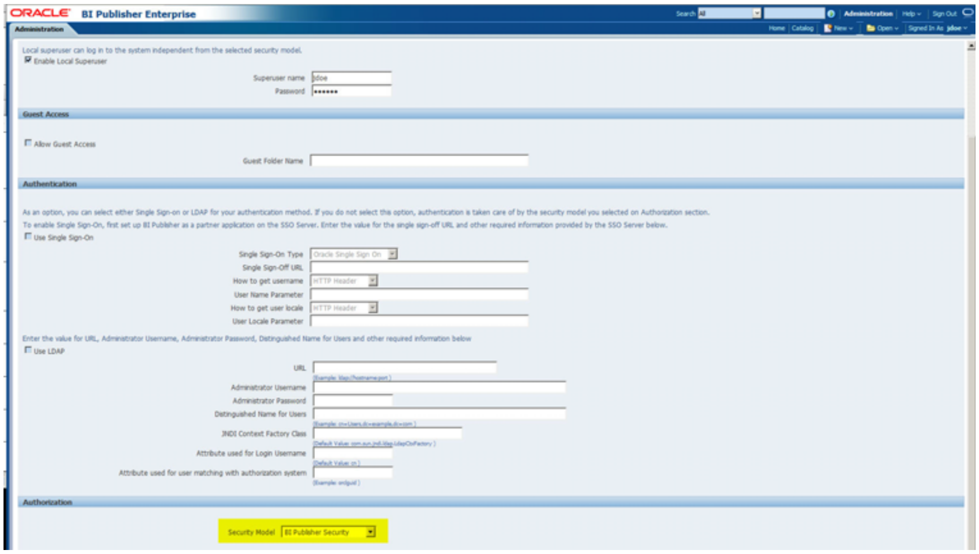
BI Publisher supports numerous security models. For Argus Safety 8.0, the following security models are supported:

- 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 default BI Publisher Security model. For more details about configuring the BI Publisher Security Model or Oracle Fusion Middleware Security set up, refer to the Extensibility Guide.



Local superuser can log in to the system independent from the selected security model.

☑ Enable Local Superuser

Superuser name: jdoe
Password: •••••••

Guest Access

☐ Allow Guest Access

Guest Folder Name:

Authentication

As an option, you can select either Single Sign-on or LDAP for your authentication method. If you do not select this option, authentication is taken care of by the security model you selected on Authorization section.

To enable Single Sign-On, first set up BI Publisher as a partner application on the SSO Server. Enter the value for the single sign-off URL and other required information provided by the SSO Server below.

☐ Use Single Sign-On

Single Sign-On Type: Oracle Single Sign On
Single Sign-Off URL:
How to get username: HTTP Header
User Name Parameter:
How to get user locale: HTTP Header
User Locale Parameter:

Enter the value for URL, Administrator Username, Administrator Password, Distinguished Name for Users and other required information below

☐ Use LDAP

URL: (Example: ldap://hostname:port)
Administrator Username:
Administrator Password:
Distinguished Name for Users: (Example: cn=Users,dc=example,dc=com)
JNDI Context Factory Class: (Default Value: com.sun.jndi.ldap.LdapCtxFactory)
Attribute used for Login Username: (Default Value: cn)
Attribute used for user matching with authorization system: (Example: orclguid)

Authorization

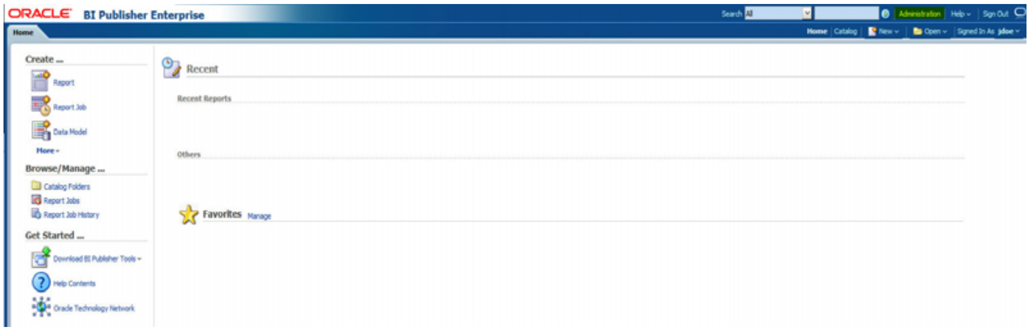
Security Model: BI Publisher Security

13.4.3 Configuring Server Settings

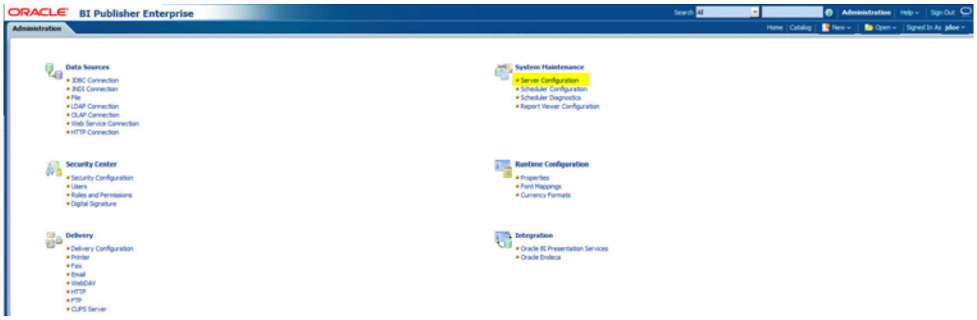
When using file systems such as NFS, Windows, or NAS for the repository, make sure that the file system is secured.

To configure the server settings for the BI Publisher Security Model, execute the following steps:

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



3. Click **Server Configuration** in the System Maintenance section as highlighted in the following figure.

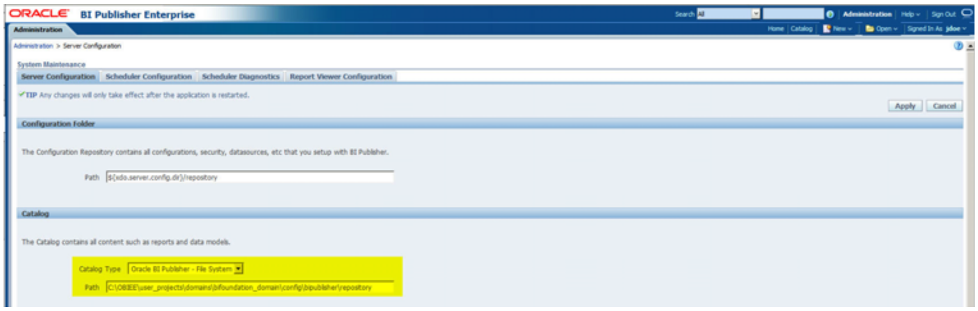


4. In the Catalog section, select **Oracle BI Publisher - File System** from the Catalog Type drop-down list. If the Catalog Type is not Oracle BI Publisher - File System, the folder level permission settings cannot be done in BIP. Refer to the Oracle Business Intelligence Developer's Guide for more information.

Note: Only Oracle BI Publisher - File System is supported in this release.

---

5. Enter the path where all BIP folders, data models, and BIP reports will be stored in the BIP server as highlighted in the following figure:



TIP Any changes will only take effect after the application is restarted.

The Configuration Repository contains all configurations, security, datasources, etc that you setup with BI Publisher.

Path: ${xdo.server.config.dir}/repository

The Catalog contains all content such as reports and data models.

Catalog Type: Oracle BI Publisher - File System

Path: C:\OBIEE\user_projects\domains\bifoundation_domain\config\bipublisher\repository

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

7. Restart your BI Publisher service.

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

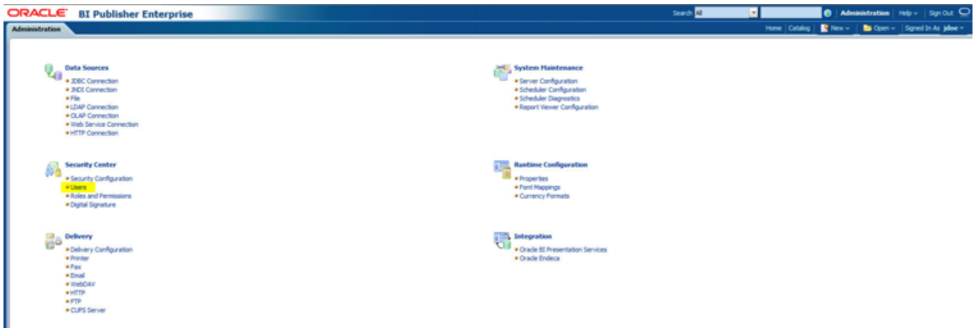
13.4.4 Creating Users and Assigning Roles

To create users and assign them roles in the BI Publisher Security Model, execute the following steps:

1. Log in to BIP using administrator credentials. This displays the BIP Home Page.

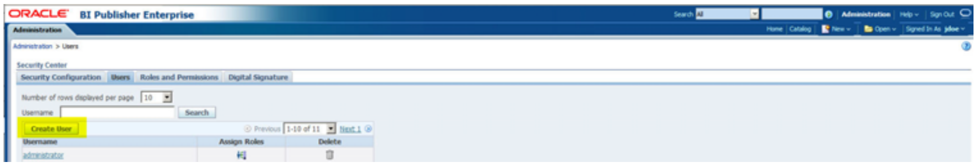
2. Click **Administration**.

3. Click **Users** under **Security Center**.



This displays the **Users** screen.

4. Click **Create User**.



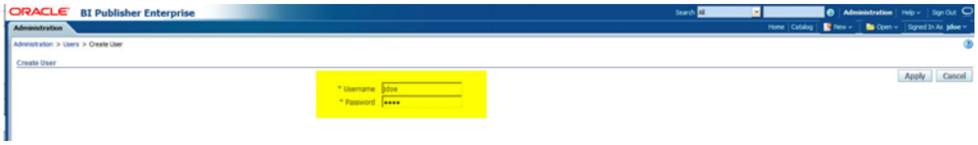
Number of rows displayed per page: 10

Username:

1-10 of 11

Username	Assign Roles	Delete
administrator		

This displays the **Create User** screen.

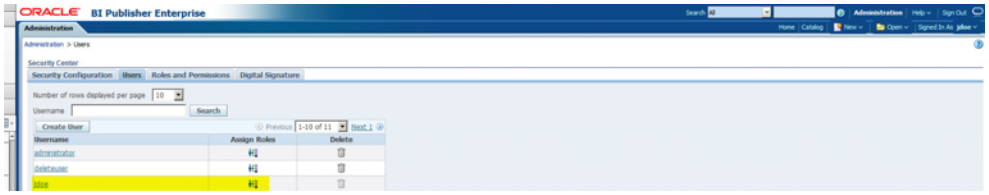


* Username: jdoe

* Password: ••••

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

   Once you have created the user, you need to assign the required roles to the user.
8. Click the **Assign Roles** icon corresponding to the user that you have created as highlighted in the following figure:



Number of rows displayed per page: 10

Username:

1-10 of 11

Username	Assign Roles	Delete
administrator		
deleteuser		
jdoe		

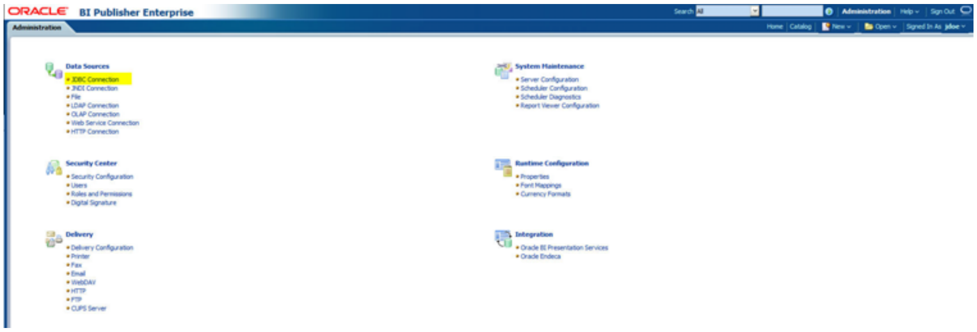
This displays the Assign Roles Screen for the user. The BIP system roles such as BI Publisher Administrator, BI Publisher Excel Analyzer, BI Publisher Online Analyzer, BI Publisher Developer, BI Publisher Scheduler, and BI Publisher Template Designer are available by default along with the custom roles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

13.4.5 Creating ASBIP JDBC Connection

> **Note:** If you are using the 12c database, you must make sure that the steps mentioned in Section 13.4.6, "Configuring12c Database Driver for BI Publisher 11g" are completed BEFORE creating a JDBC connection.
>
> 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.

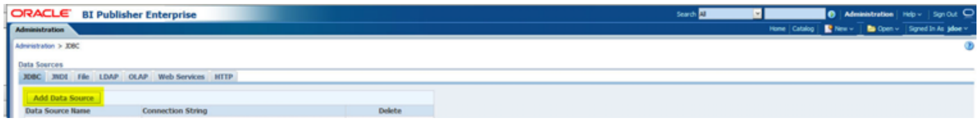
To connect the BIP and the database, execute the following steps:

1. Log on to BIP using the administrator credentials. This displays the BIP Home Page.
2. Click **Administration**.
3. Click **JDBC Connection** under **Data Sources**.



This displays the **Data Sources** screen.

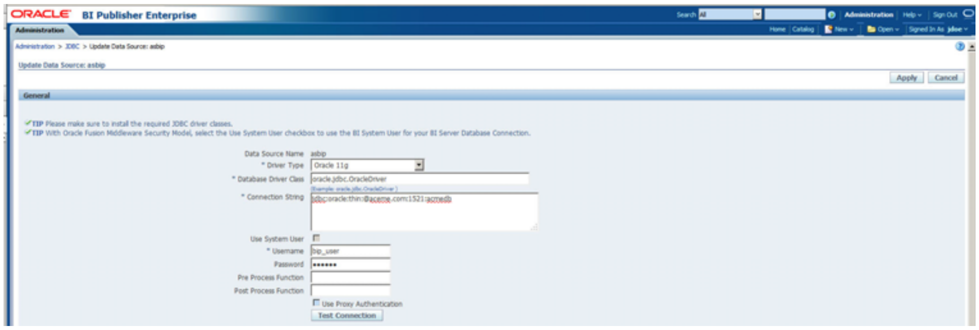
4. Click **Add Data Source**.



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

   - 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 the connection string in the **Connection String** field. 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**.

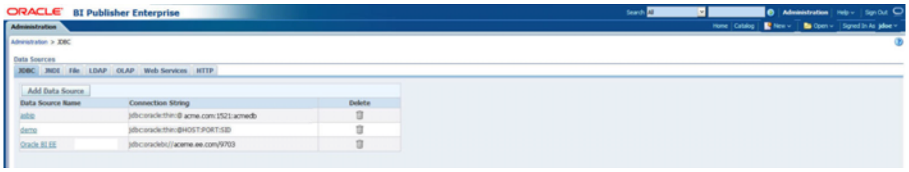

ORACLE BI Publisher Enterprise
Administration
Administration > JDBC > Update Data Source: asbip
Update Data Source: asbip
Apply
Cancel
General
Test Connection

TIP Please make sure to install the required JDBC driver classes.
TIP With Oracle Fusion Middleware Security Model, select the Use System User checkbox to use the BI System User for your BI Server Database Connection.

Data Source Name asbip
* Driver Type Oracle 11g
* Database Driver Class oracle.jdbc.OracleDriver
(Example: oracle.jdbc.OracleDriver)
* Connection String jdbc:oracle:thin:@aceme.com:1521:acmedb
Use System User ☐
* Username bip_user
Password ••••••
Pre Process Function
Post Process Function
☐ Use Proxy Authentication

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.



Data Source Name	Connection String	Delete
asbip	jdbc:oracle:thin:@ acme.com:1521:acmedb	🗑
demo	jdbc:oracle:thin:@HOST:PORT:SID	🗑
Oracle BI EE	jdbc:oraclebi://aceme.ee.com/9703	🗑

This successfully creates a connection between BIP and the database.

13.4.6 Configuring12c Database Driver for BI Publisher 11g

By default, the 12c driver type option is not shown in the list of drivers in BI Publisher JDBC creation screen.

This can be enabled by following any one of the following two options:

Option 1:

The 12c driver type could be added to the drop-down list, as follows:

1. Login to the BI Publisher Server and open the file located at the following location:

   BI_Home\user_projects\domains\bifoundation_domain\config\bipublisher\repository\Admin\DataSource\jdbcdefaults.xml

2. Add the following <defaultvalue> tag:

   ```
    <defaultvalue name="ORACLE"
      description="Oracle 12c"
       driver="oracle.jdbc.OracleDriver"
            url="jdbc:oracle:thin:@[host]:[port]/[sid]" />
   ```

   Instead of this method, one may also consider:

   ```
    <defaultvalue name="ORACLE"
       description="Oracle 12c"
       driver="oracle.jdbc.OracleDriver"
       url="jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_
   LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=host.com)(PORT=1521)))(CONNEC
   T_DATA=(SID=orcl)))" />
   ```

3. Save the file and restart the BI Publisher service.

Option 2:

The administrator can decide not to add the 12c driver type, but still retain the 11g driver itself.

However, the connection string should still be specified in the following way:

jdbc:oracle:thin:@[host]:[port]/[sid]

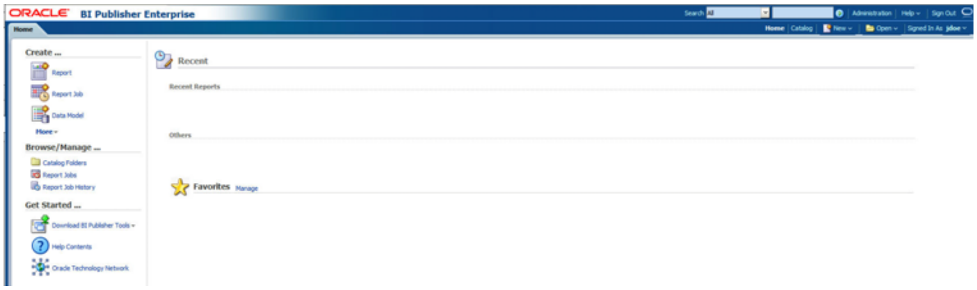
13.5 Uploading the Argus Safety.xdrz file to BIP

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

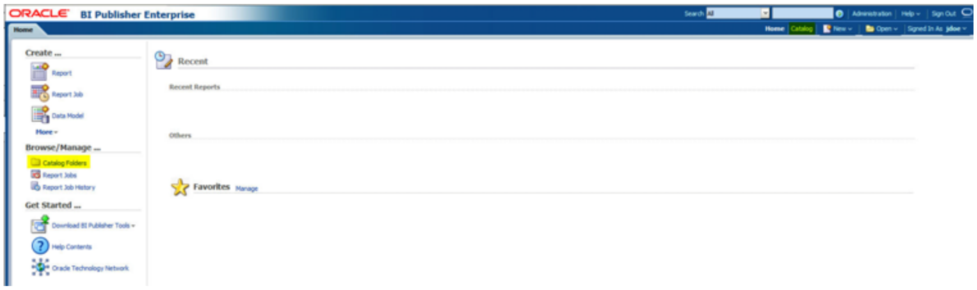
1. Copy the Argus Safety.xdrz file from the following location on the Argus Safety Web Server to the local file system:

   <Argus Installation Media>\SUPPORT\BIP

2. Log in to BIP using BI Admin User credentials. This displays the BIP Home Page as depicted in the following figure:

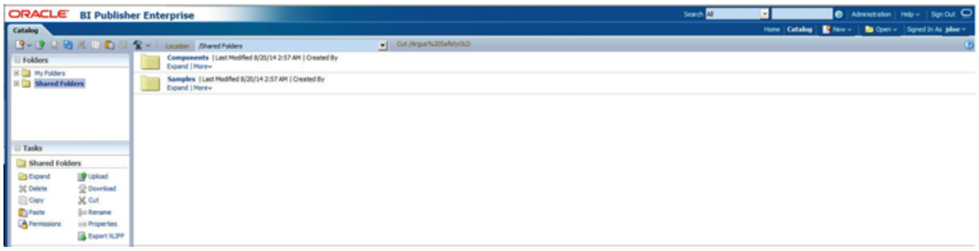


3. Click **Catalog**.

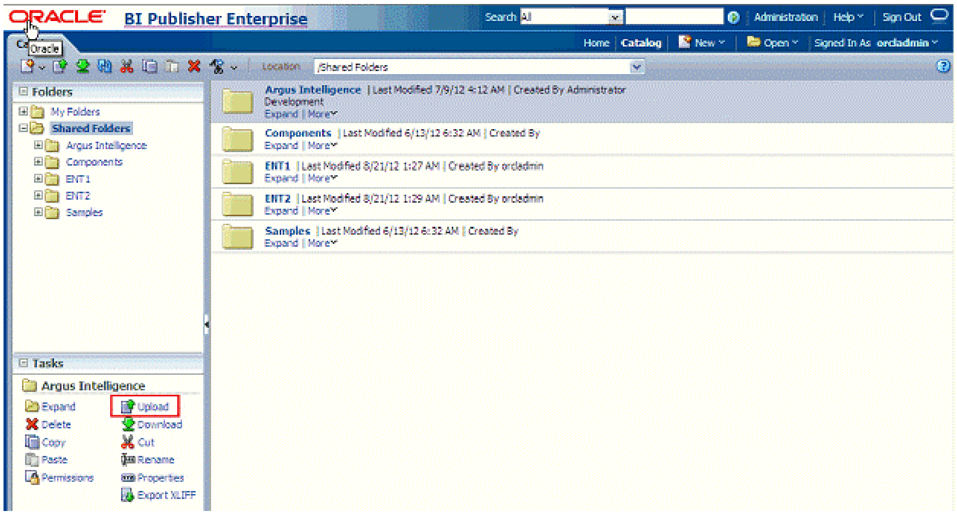


This displays the **Catalog** screen with the **Folders** and **Tasks** sections.

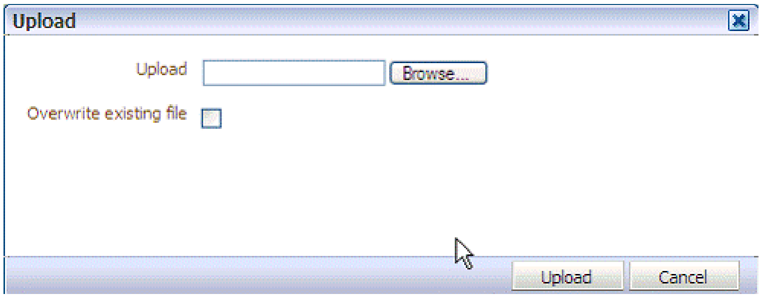
4. Click **Shared Folders** under **Folders**.



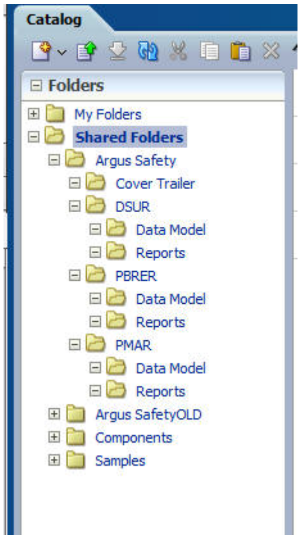
5. Click **Upload** under **Tasks**.



This displays the **Upload** dialog box.



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



13.6 Integrating Argus Safety with BIP

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 BIP 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.

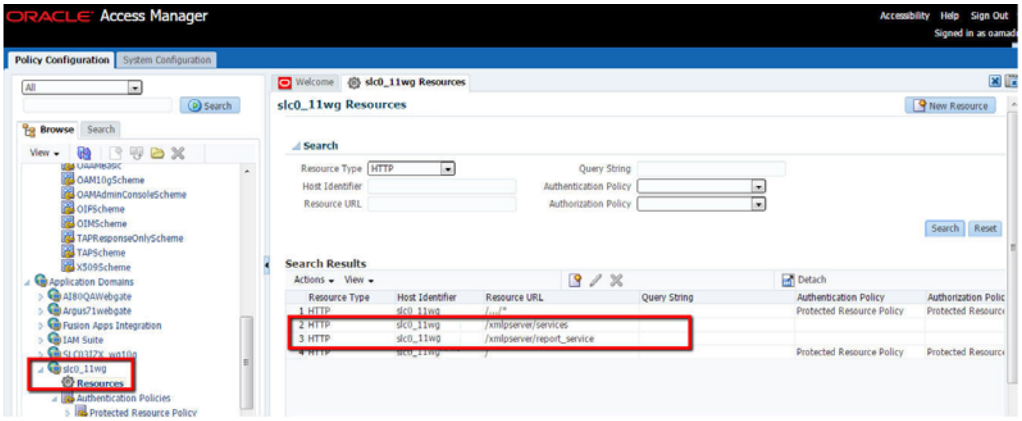
6. The following URLs need to be excluded from SSO (if SSO is enabled):

   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.



slc0_11wg Resources

Search

Resource Type: HTTP

Host Identifier:

Resource URL:

Query String:

Authentication Policy:

Authorization Policy:

	Resource Type	Host Identifier	Resource URL	Query String	Authentication Policy	Authorization Polic
1	HTTP	slc0_11wg	/.../*		Protected Resource Policy	Protected Resource
2	HTTP	slc0_11wg	/xmlpserver/services			
3	HTTP	slc0_11wg	/xmlpserver/report_service			
4	HTTP	slc0_11wg	/		Protected Resource Policy	Protected Resource

   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>

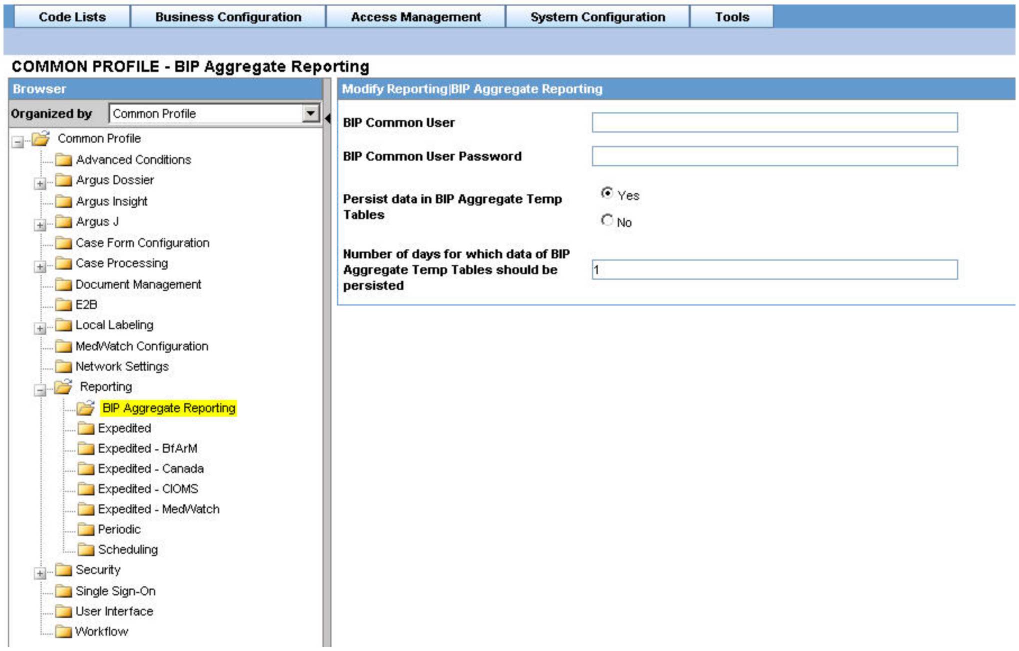
   d. Save the file and restart OHS Service.

13.7 Argus Console-level Configurations

To enable execution of the BIP 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**.



COMMON PROFILE - BIP Aggregate Reporting

Modify Reporting|BIP Aggregate Reporting

BIP Common User

BIP Common User Password

Persist data in BIP Aggregate Temp Tables ● Yes ○ No

Number of days for which data of BIP Aggregate Temp Tables should be persisted: 1

7. In the **BIP Common User** and **Password** fields, enter the username and password of a BIP user having administrative permissions. Save the changes. Make sure that the BIP User added here is not same as that of an actual Argus user. It can be a user which is available only for BIP, 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.

13.8 Configuring Code Lists

For BIP Reports to be run from Argus Safety, the BIP Report template path in the BIP 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:** The REPPATH value may be different based on the uploaded path of the templates in the BIP Server.

13.9 Creating the Database Jobs

A database job must be created for polling the BIP 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 BIP Schema User.

14

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 8.0
Database Server	(Same requirements as Argus Safety 8.0 Database Server) A Tablespace with 500MB free space to create EOSU Schema Argus 8.0 schema (This is a prerequisite for the EOSU package to be installed.)
Client Machine	Microsoft Windows 7 (32-bit) (English and Japanese) Oracle Client v11.2.0.4 Oracle ODAC 11.2.0.4 Microsoft .NET 3.5 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 2007 and 2010 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 8.0 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

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>	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. For example, for a database that is recognized as "Testing Database" in Argus Web Login screen and whose alias in the Oracle TNSNAMES.ORA file is "TESTDB", the entry will be <DBNAME id="TESTDB">Testing Database</DBNAME>.

XML Tag	Description
<LICENSE_KEY>	This tag contains the License Key value for the Argus application. Do not update this key unless Oracle Customer Support instructs 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\PDFReports\	This is the path for PDF Reports (Expedited/Periodic/Screen Prints etc.). In case of multiple web servers, this is a shared path on the network.
2	Workstation	MessageCachePath	c:\ArgusReports\MessageCache\	This is the shared path to save the system level cache such as data for LM tables, CMN Fields, etc. In case of multiple web servers, this is a shared path on the network. For use with Web Server.
3	Workstation	Upload	c:\ArgusReports\UploadedLetters\	This is the shared path for uploaded letters. In case of multiple web servers, this is a shared path on the network. For use with Web Server.

#	Section	Parameter	Sample Value	Description
4	Workstation	Template	C:\Program Files\Oracle\E2BViewer \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 Files\Adobe\Acrobat 7.0\Acrobat\Acrobat.exe	This is the path to the Acrobat Reader exe file.
6	Workstation	HELP	C:\App\Oracle\Documentation\	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 Utility. It specifies how often the Print Utility shall run to print reports to the 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 Utility. When this is set to 0, the AG Service Process Bulk Transmit Print, generates the report and directly prints the report to the printer. If set to 1, the Bulk Transmit Process creates the PDF in the Cache folder with an associated Batch file. The Print Utility then picks up the Batch File, prints the PDF to the printer and deletes the Batch Job File. For use with Transactional (AG) Server.
9	Workstation	ArgusInstallPath	C:\Program Files\Oracle\ArgusWeb\ ASP\	This refers to the path of the location where the ASP files are placed. For use with Web Server.
10	Workstation	SCANNED_ IMAGES	C:\Temp\Scanned_ Images	This is the location of files that are used by the "New Case from Image" functionality.
11	PDFReports	TempFileDeleteInterval	1	This key specifies how often the Argus Report Service should run to check for files to delete. By default, this service will delete files from paths specified for "Cache" and "Upload" parameters described above. The unit is in hours. The default value is 1.
12	PDFReports	HoursBeforeDelete	24	This key is used by Argus Report Service. This key specifies in hours, how old the file must be before it gets deleted. By default, this service will delete files from paths specified for "Cache" and "Upload" parameters described above. The default value is 1.
13	Argus Server	SQLTimes	1	This enables the Argus Web application to start creating log files for all the SQLs that are fired. These log files are created in C:\Temp folder and can be used for debugging.

#	Section	Parameter	Sample Value	Description
14	Argus Server	Pool_Initial_Size	3	This refers to the DB Connection Pool Initial Size. For use with Web Server.
15	Argus Server	Pool_Maximum_ Size	120	This refers to the DB Connection Pool Maximum Size. For use with Web Server.
16	Argus Server	Connection_Time_ 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_ Time	3	This refers to the connection wait time in seconds. An exception occurs if the system cannot obtain a DB connection in the given time. For use with Web Server.
18	Argus Server	PeriodicRptMaxRun Time	60000	This refers to the setting in the Argus.ini file that allows you to override the default Argusvr2a EXE timeout setting to approximately 16 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):

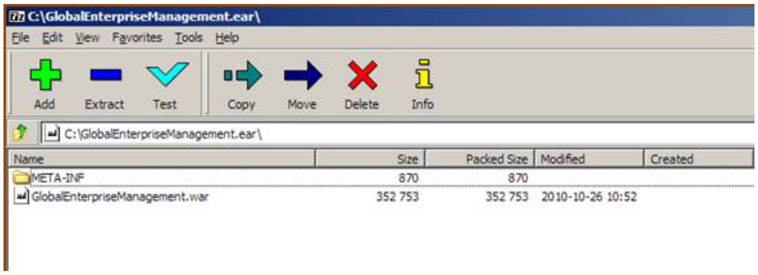
1. Start the Registry Editor on the IE client machine.
2. Locate the following sub-key: HKEY_CURRENT_ USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings.
3. In this sub-key, add the following DWORD entries with 14400000 (4 hours):
   - KeepAliveTimeout
   - ReceiveTimeout
   - ServerInfoTimeout

4. Restart the computer.

Deploying a Portlet on Oracle WebLogic Server

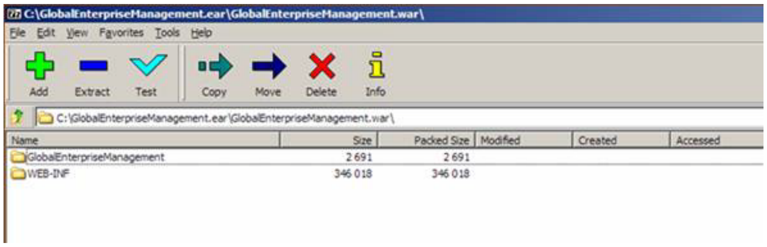
To deploy the portlets to the Oracle Portal Server, navigate to the Portlet Installation folder on the Web Server where the module was installed. Perform the following steps for each Portlet being installed.

1. Open the .ear file using a Zip utility. The zip program will open with files as seen below.


C:\GlobalEnterpriseManagement.ear\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
C:\GlobalEnterpriseManagement.ear\

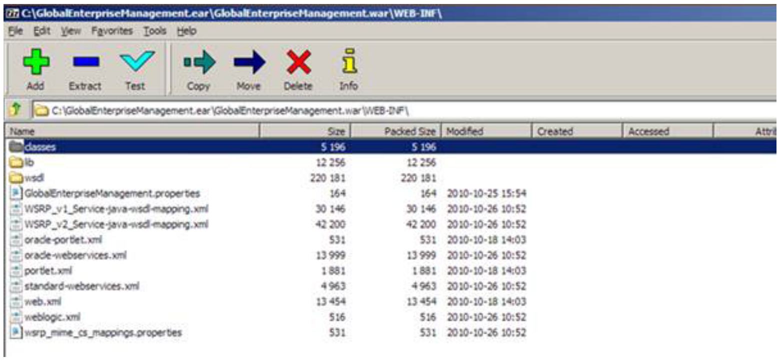
Name	Size	Packed Size	Modified	Created
META-INF	870	870		
GlobalEnterpriseManagement.war	352 753	352 753	2010-10-26 10:52	

2. Double click the .war file and you will see the following screen. Double Click the WEB-INF folder.


C:\GlobalEnterpriseManagement.ear\GlobalEnterpriseManagement.war\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
C:\GlobalEnterpriseManagement.ear\GlobalEnterpriseManagement.war\

Name	Size	Packed Size	Modified	Created	Accessed
GlobalEnterpriseManagement	2 691	2 691			
WEB-INF	346 018	346 018			

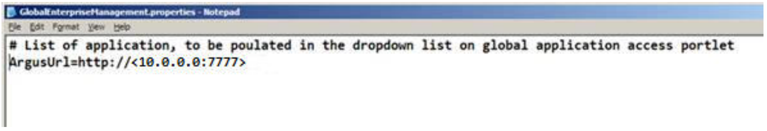
3. Double click the file **portletname.properties** where portletname is the name of the portlet ear file under modification.


C:\GlobalEnterpriseManagement.ear\GlobalEnterpriseManagement.war\WEB-INF\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
C:\GlobalEnterpriseManagement.ear\GlobalEnterpriseManagement.war\WEB-INF\

Name	Size	Packed Size	Modified	Created	Accessed	Attri
classes	5 196	5 196				
lib	12 256	12 256				
wsdl	220 181	220 181				
GlobalEnterpriseManagement.properties	164	164	2010-10-25 15:54			
WSRP_v1_Service-java-wsdl-mapping.xml	30 146	30 146	2010-10-26 10:52			
WSRP_v2_Service-java-wsdl-mapping.xml	42 200	42 200	2010-10-26 10:52			
oracle-portlet.xml	531	531	2010-10-18 14:03			
oracle-webservices.xml	13 999	13 999	2010-10-26 10:52			
portlet.xml	1 881	1 881	2010-10-18 14:03			
standard-webservices.xml	4 963	4 963	2010-10-26 10:52			
web.xml	13 454	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.

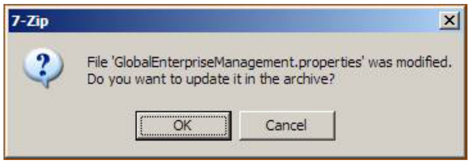

GlobalEnterpriseManagement.properties - Notepad
File Edit Format View Help

```
# List of application, to be poulated in the dropdown list on global application access portlet
ArgusUrl=http://<10.0.0.0:7777>
```

Note: Make sure there is no space between the tokens "ArgusUrl", "=" and the actual URL value.

---

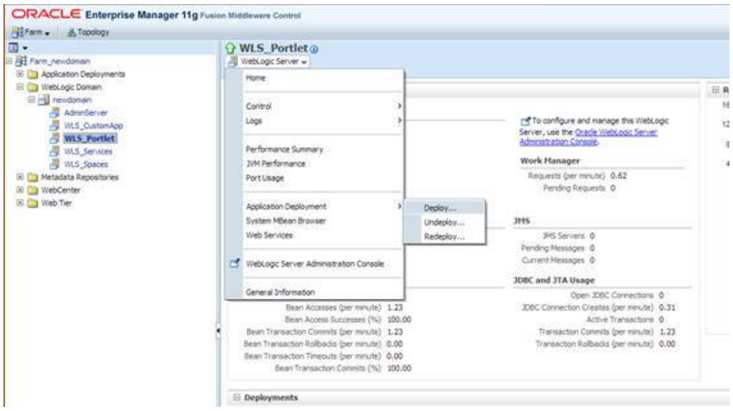
5. Save the changes to the properties file and close it. Close the 7-zip manager window and press OK to save the changes in the archive. You are now ready to deploy the ear file.



7-Zip

File 'GlobalEnterpriseManagement.properties' was modified.
Do you want to update it in the archive?

6. 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**.



To configure and manage this WebLogic Server, use the Oracle WebLogic Server Administration Console.

Work Manager

Requests (per minute) 0.62
Pending Requests 0

JMS

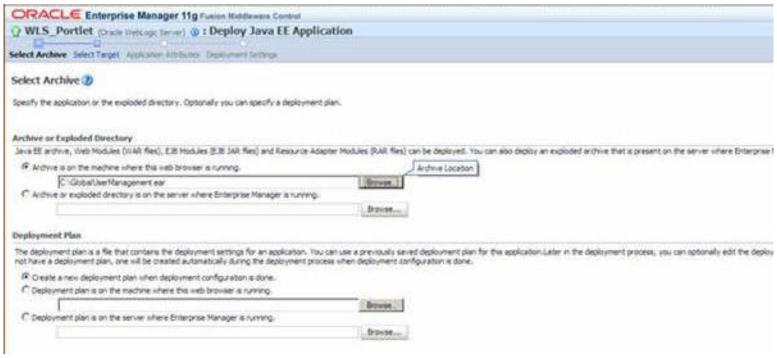
JMS Servers 0
Pending Messages 0
Current Messages 0

JDBC and JTA Usage

Open JDBC Connections 0
JDBC Connection Creates (per minute) 0.31
Active Transactions 0
Transaction Commits (per minute) 1.23
Transaction Rollbacks (per minute) 0.00

Bean Accesses (per minute) 1.23
Bean Access Successes (%) 100.00
Bean Transaction Commits (per minute) 1.23
Bean Transaction Rollbacks (per minute) 0.00
Bean Transaction Timeouts (per minute) 0.00
Bean Transaction Commits (%) 100.00

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 Middleware Control
WLS_Portlet (Oracle WebLogic Server) : Deploy Java EE Application
Select Archive
Select Target
Application Attributes
Deployment Settings
Archive Location
Browse...

Select Archive

Specify the application or the exploded directory. Optionally you can specify a deployment plan.

Archive or Exploded Directory

Java EE archive, Web Modules (WAR files), EJB Modules (EJB JAR files) and Resource Adapter Modules (RAR files) can be deployed. You can also deploy an exploded archive that is present on the server where Enterprise

● Archive is on the machine where this web browser is running.

C:\GlobalUserManagement.ear

○ Archive or exploded directory is on the server where Enterprise Manager is running.

Deployment Plan

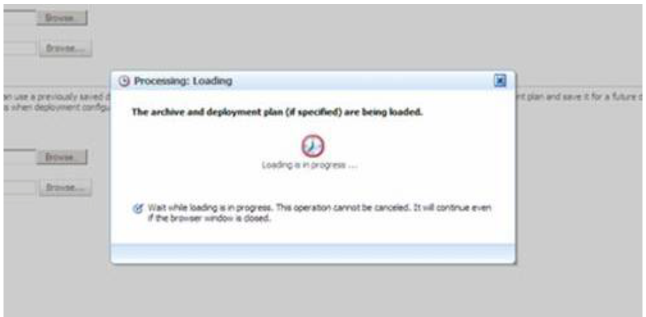
The deployment plan is a file that contains the deployment settings for an application. You can use a previously saved deployment plan for this application.Later in the deployment process, you can optionally edit the deploy not have a deployment plan, one will be created automatically during the deployment process when deployment configuration is done.

● Create a new deployment plan when deployment configuration is done.

○ Deployment plan is on the machine where this web browser is running.

○ Deployment plan is on the server where Enterprise Manager is running.

8. The Portlet will now get uploaded to the server.

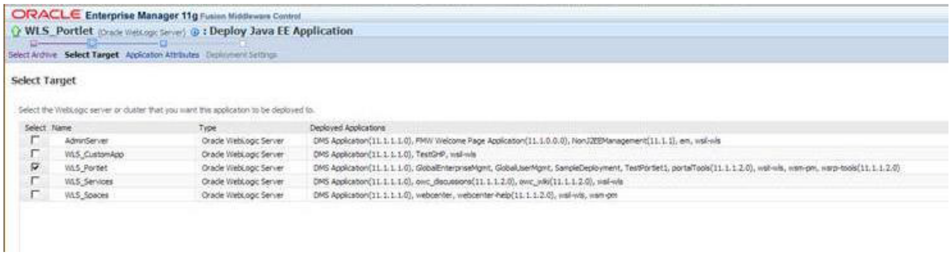


The archive and deployment plan (if specified) are being loaded.

Loading is in progress ...

Wait while loading is in progress. This operation cannot be canceled. It will continue even if the browser window is closed.

9. Once the Portlet is uploaded, by default **WLS_Portlet** will be selected. If not then select and click **Next**.

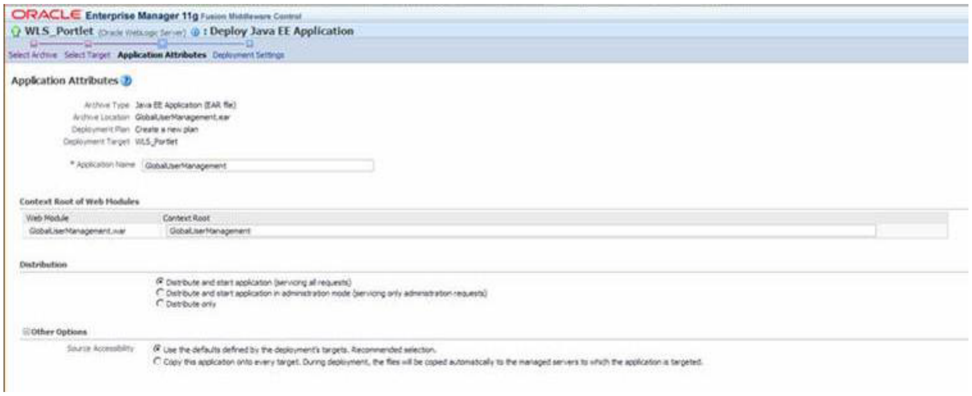

ORACLE Enterprise Manager 11g Fusion Middleware Control
WLS_Portlet (Oracle WebLogic Server) : Deploy Java EE Application
Select Archive
Select Target
Application Attributes
Deployment Settings

Select Target

Select the WebLogic server or cluster that you want this application to be deployed to.

Select	Name	Type	Deployed Applications
□	AdminServer	Oracle WebLogic Server	DMS Application(11.1.1.1.0), FMW Welcome Page Application(11.1.0.0.0), NonJ2EEManagement(11.1.1), em, wsil-wls
□	WLS_CustomApp	Oracle WebLogic Server	DMS Application(11.1.1.1.0), TestGHP, wsil-wls
☑	WLS_Portlet	Oracle WebLogic Server	DMS Application(11.1.1.1.0), GlobalEnterpriseMgmt, GlobalUserMgmt, SampleDeployment, TestPortlet1, portalTools(11.1.1.2.0), wsil-wls, wsrp-pm, wsrp-tools(11.1.1.2.0)
□	WLS_Services	Oracle WebLogic Server	DMS Application(11.1.1.1.0), owc_discussions(11.1.1.2.0), owc_wiki(11.1.1.2.0), wsil-wls
□	WLS_Spaces	Oracle WebLogic Server	DMS Application(11.1.1.1.0), webcenter, webcenter-help(11.1.1.2.0), wsil-wls, wsrp-pm

10. Do not change the default selection. Click **Next.**


ORACLE Enterprise Manager 11g Fusion Middleware Control
WLS_Portlet (Oracle WebLogic Server) : Deploy Java EE Application
Select Archive
Select Target
Application Attributes
Deployment Settings

Application Attributes

Archive Type Java EE Application (EAR file)
Archive Location GlobalUserManagement.ear
Deployment Plan Create a new plan
Deployment Target WLS_Portlet

* Application Name GlobalUserManagement

Context Root of Web Modules

Web Module	Context Root
GlobalUserManagement.war	GlobalUserManagement

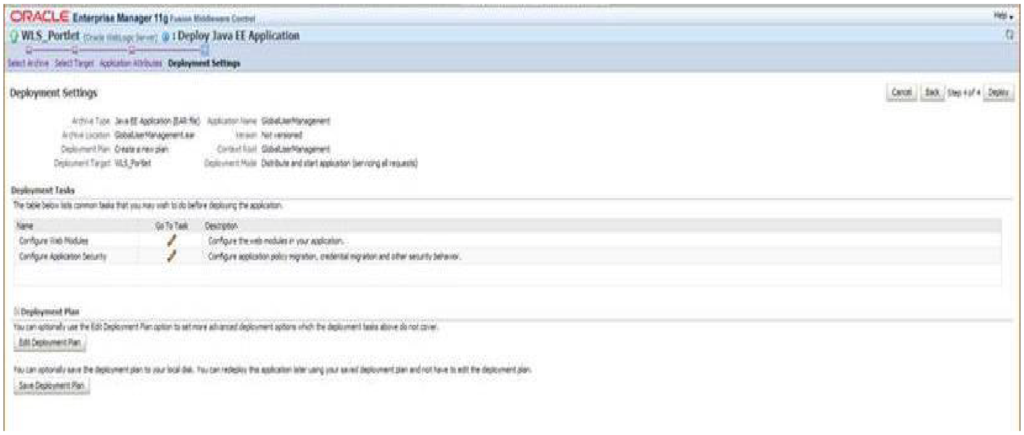
Distribution

● Distribute and start application (servicing all requests)
○ Distribute and start application in administration mode (servicing only administration requests)
○ Distribute only

Other Options

Source Accessibility ● Use the defaults defined by the deployment's targets. Recommended selection.
○ Copy this application onto every target. During deployment, the files will be copied automatically to the managed servers to which the application is targeted.

11. Click **Deploy** on the last screen to publish the Portlet. Verify that the Portlet was deployed successfully in the Status.


ORACLE Enterprise Manager 11g Fusion Middleware Control
Help
WLS_Portlet (Oracle WebLogic Server) : Deploy Java EE Application
Select Archive
Select Target
Application Attributes
Deployment Settings
Cancel
Back
Step 4 of 4
Deploy

Deployment Settings

Archive Type Java EE Application (EAR file) Application Name GlobalUserManagement
Archive Location GlobalUserManagement.ear Version Not versioned
Deployment Plan Create a new plan Context Root GlobalUserManagement
Deployment Target WLS_Portlet Deployment Mode Distribute and start application (servicing all requests)

Deployment Tasks

The table below lists common tasks that you may wish to do before deploying the application.

Name	Go To Task	Description
Configure Web Modules	✎	Configure the web modules in your application.
Configure Application Security	✎	Configure application policy migration, credential migration and other security behavior.

Deployment Plan

You can optionally use the Edit Deployment Plan option to set more advanced deployment options which the deployment tasks above do not cover.

You can optionally save the deployment plan to your local disk. You can redeploy the application later using your saved deployment plan and not have to edit the deployment 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.

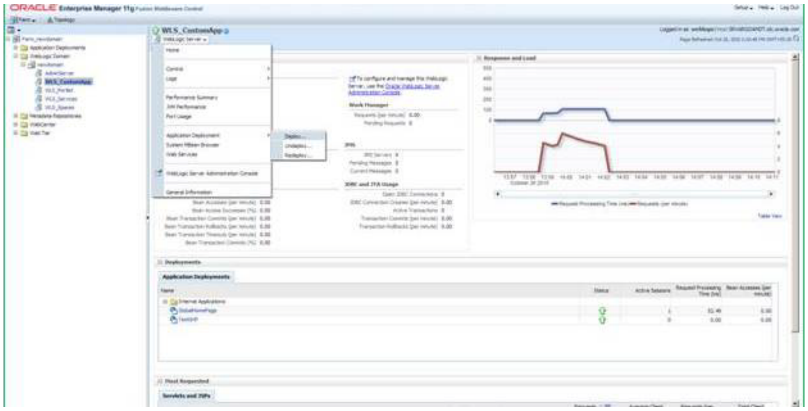
Deploy Company Logo

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.

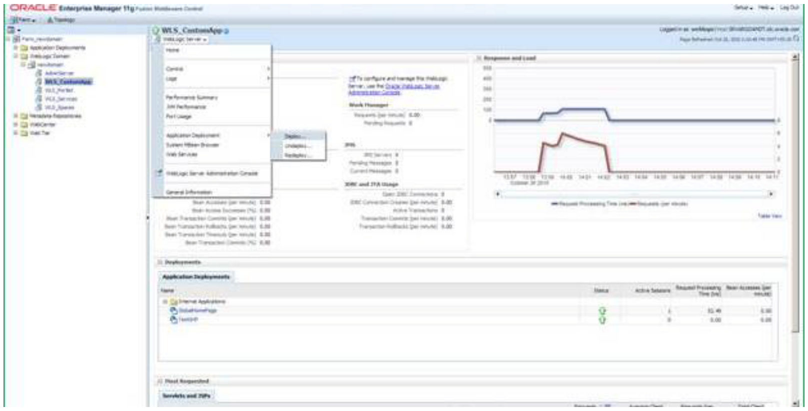
Pre-Deployment Configuration

Now, perform the following steps to deploy the global home application on the Weblogic Server.

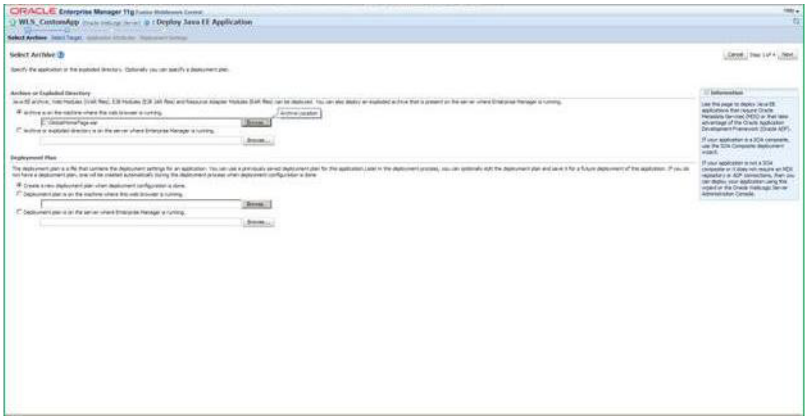
1. Log in to the Enterprise Manager Admin console. In the left hand tree navigation, select **WebLogic Domain**>**Your Domain**>**WLS_CustomApp** in the left hand tree navigation. The WLS_CustomApp is the name of the server that we have created to deploy Global Home Page. Click the menu just below the name of the server as shown below. Navigate to **Application Deployment** > **Deploy**.



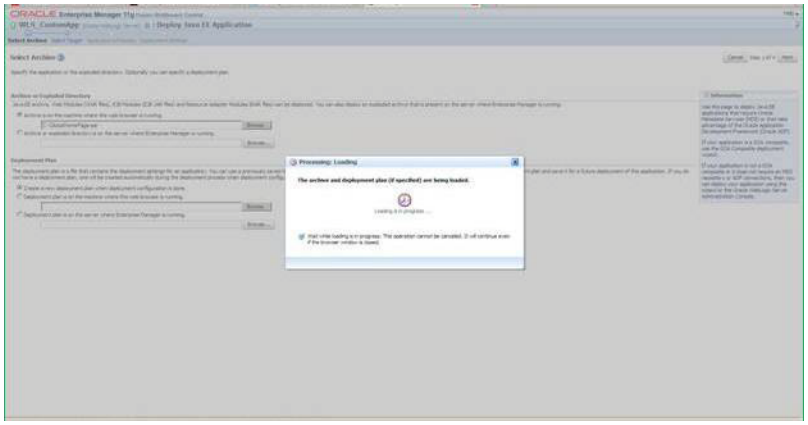
2. Log in to the Enterprise Manager Admin console. In the left hand tree navigation, select **WebLogic Domain**>**Your Domain**>**WLS_CustomApp** in the left hand tree navigation. The WLS_CustomApp is the name of the server that we have created to deploy Global Home Page. Click the menu just below the name of the server as shown below. Navigate to **Application Deployment** > **Deploy**.



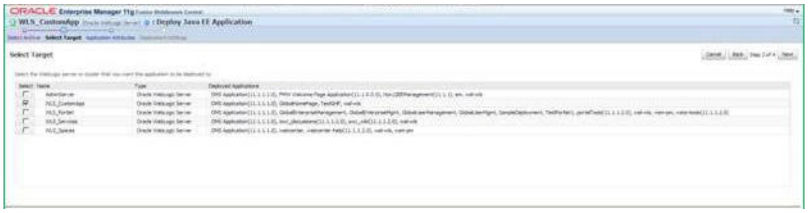
3. The following screen appears. Browse for the application. ear file and click **Next**.



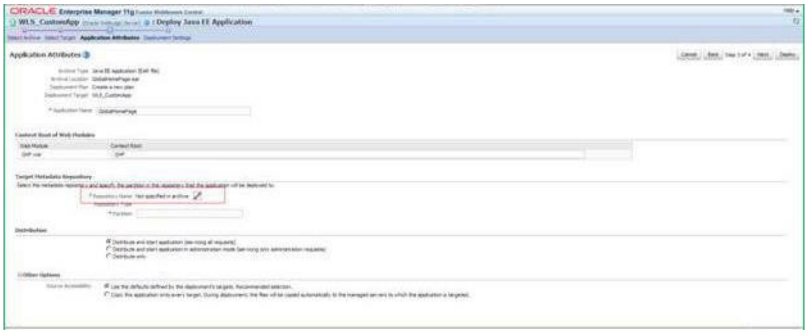
4. Wait for the progressing dialog to finish.



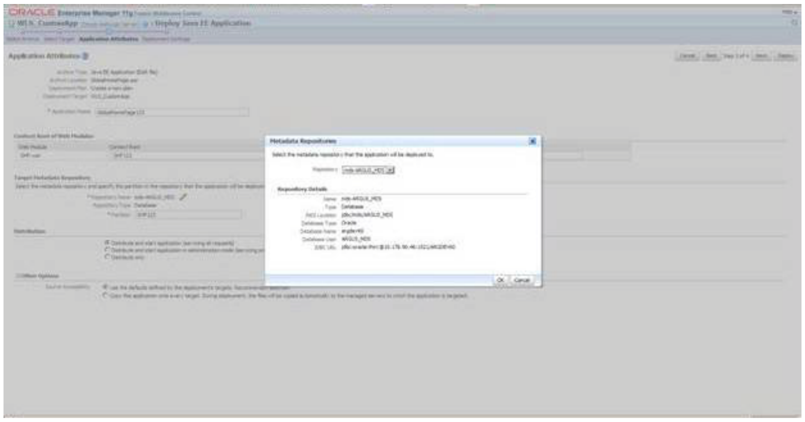
5. After modal dialogue is completed, you will see a screen for selecting targets. By default **WLS_CustomApp** will be selected, if not then select and click **Next**.



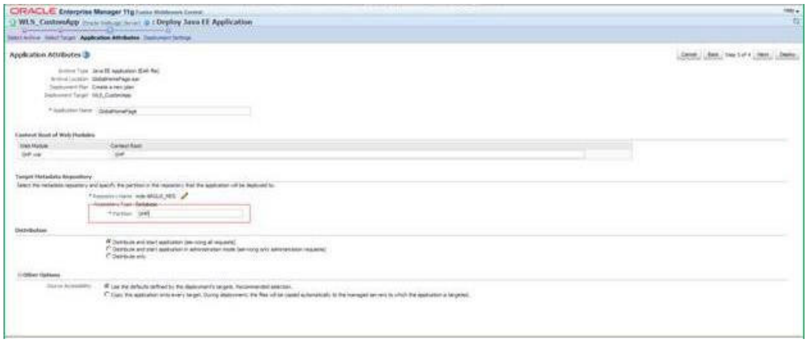
6. Click the “pencil” icon in the **Target Metadata Repository** section.



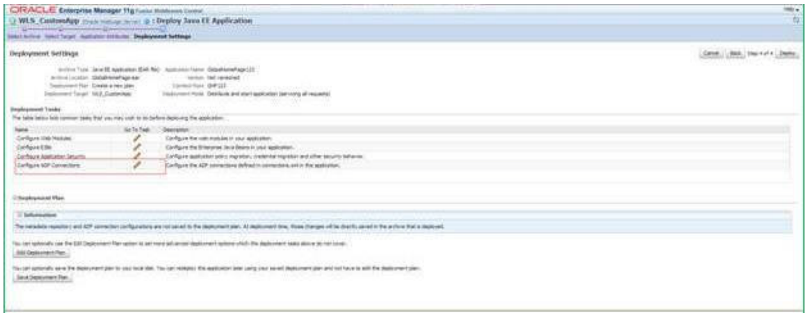
7. A modal dialog appears that allows you to specify the metadata repository for this application. Choose a metadata repository and click **OK**.



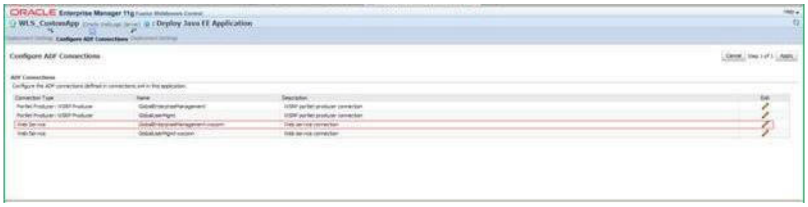
8. Specify the **partition** value. You may choose any value but Oracle recommends using the application name itself as the partition value. Click **Next**.



9. In the Configure ADF connections section, click **pencil** icon, you will be redirected to the Configure ADF connections screen.

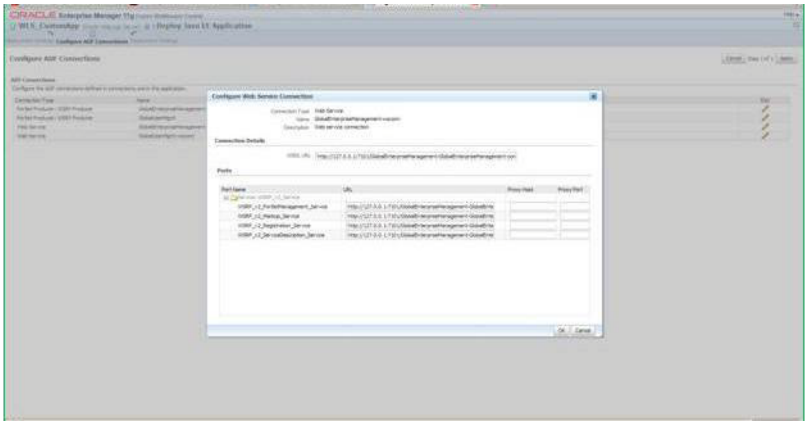


10. In the Configure ADF connections screen, modify the web service connection. Click the **pencil** icon to edit the ADF connection settings.

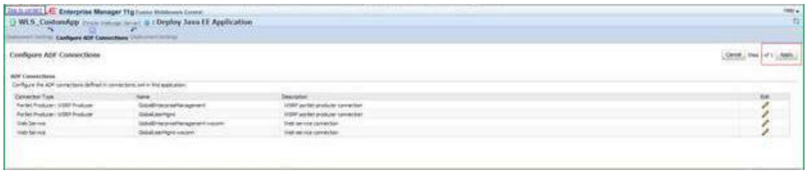

ORACLE Enterprise Manager 11g
WLS_CustomApp
Deploy Java EE Application
Configure ADF Connections

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


Enterprise Manager 11g
WLS_CustomApp
Deploy Java EE Application
Configure ADF Connections
Configure Web Service Connection
Connection Details
Ports
OK
Cancel

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.



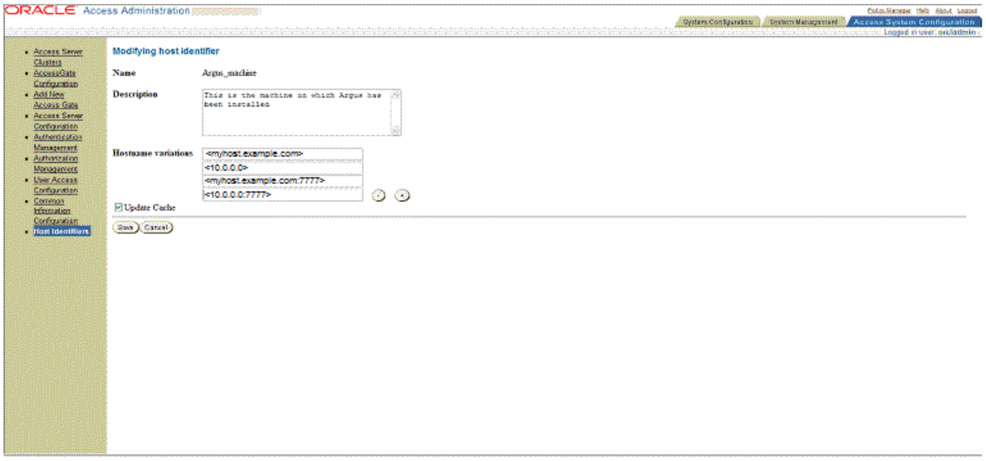
Configuring SSO in Oracle Access Manager 10g

This section describes how to configure SSO in the Oracle Access Manager (OAM) 10g. 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:

1. Navigate to the Access System console of OAM and click the **Access System Configuration** tab. Click **Host Identifiers** on the left panel. Provide the Fully Qualified Domain Name (FQDN), IP Address and both entries along with port numbers of the Argus Web Server machine. Click **Save**. For example:
   - <myhost.example.com>
   - <myhost.example.com:7777>
   - <10.0.0.0>
   - <10.0.0.0:7777>


ORACLE Access Administration
Policy Manager Help About Logout
System Configuration
System Management
Access System Configuration
Logged in user: orcladmin
Access Server Clusters
AccessGate Configuration
Add New Access Gate
Access Server Configuration
Authentication Management
Authorization Management
User Access Configuration
Common Information Configuration
Host Identifiers
Save
Cancel

Modifying host identifier

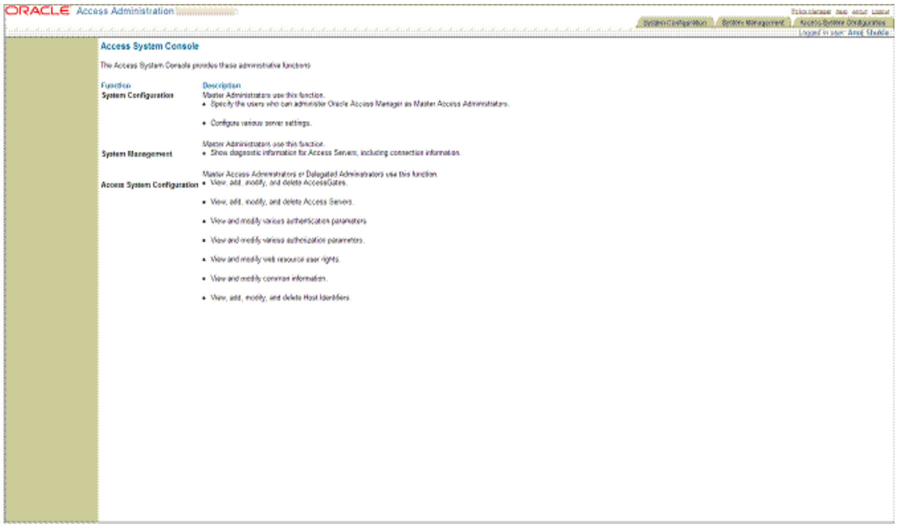
Name: Argus_machine

Description: This is the machine on which Argus has been installed

Hostname variations:
<myhost.example.com>
<10.0.0.0>
<myhost.example.com:7777>
<10.0.0.0:7777>

☑ Update Cache

2. In the Access System console of OAM, click **Access System Configuration**.


ORACLE Access Administration
Policy Manager Help About Logout
System Configuration
System Management
Access System Configuration
Logged in user: Anuj Shukla

Access System Console

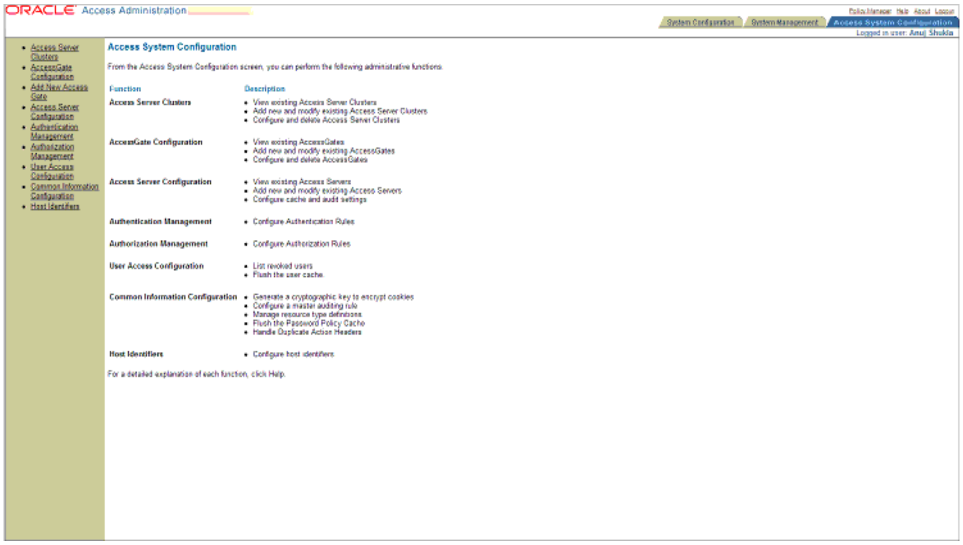
The Access System Console provides these administrative functions

Function | Description
System Configuration | Master Administrators use this function.
- Specify the users who can administer Oracle Access Manager as Master Access Administrators.
- Configure various server settings.

System Management | Master Administrators use this function.
- Show diagnostic information for Access Servers, including connection information.

Access System Configuration | Master Access Administrators or Delegated Administrators use this function.
- View, add, modify, and delete AccessGates.
- View, add, modify, and delete Access Servers.
- View and modify various authentication parameters.
- View and modify various authorization parameters.
- View and modify web resource user rights.
- View and modify common information.
- View, add, modify, and delete Host Identifiers.

3. Click **Add New Access Gate** link on left panel.


ORACLE Access Administration
Policy Manager Help About Logout
System Configuration
System Management
Access System Configuration
Logged in user: Anuj Shukla
Access Server Clusters
AccessGate Configuration
Add New Access Gate
Access Server Configuration
Authentication Management
Authorization Management
User Access Configuration
Common Information Configuration
Host Identifiers

Access System Configuration

From the Access System Configuration screen, you can perform the following administrative functions

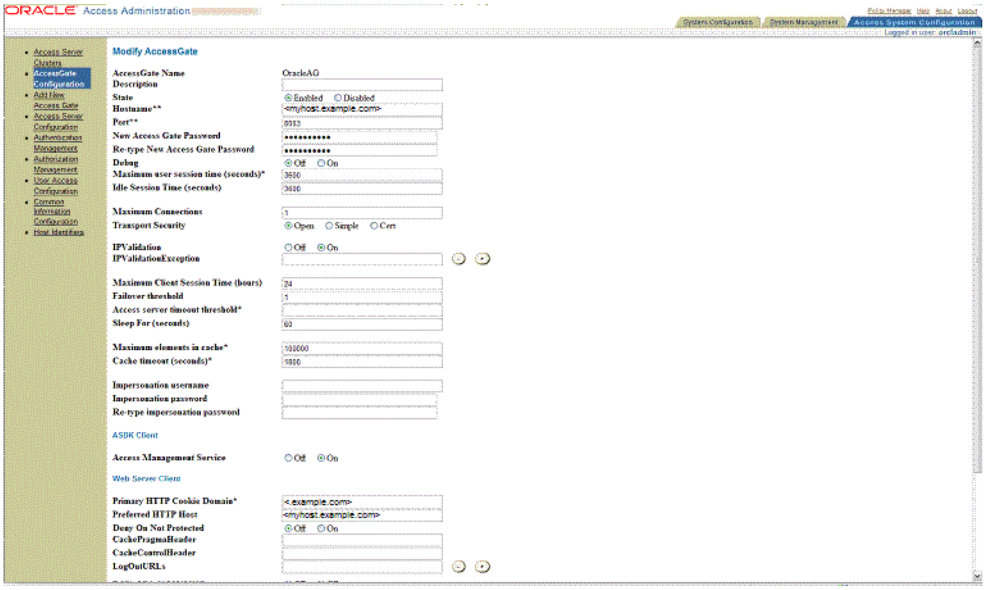
Function	Description
Access Server Clusters	• View existing Access Server Clusters • Add new and modify existing Access Server Clusters • Configure and delete Access Server Clusters
AccessGate Configuration	• View existing AccessGates • Add new and modify existing AccessGates • Configure and delete AccessGates
Access Server Configuration	• View existing Access Servers • Add new and modify existing Access Servers • Configure cache and audit settings
Authentication Management	• Configure Authentication Rules
Authorization Management	• Configure Authorization Rules
User Access Configuration	• List revoked users • Flush the user cache
Common Information Configuration	• Generate a cryptographic key to encrypt cookies • Configure a master auditing rule • Manage resource type definitions • Flush the Password Policy Cache • Handle Duplicate Action Headers
Host Identifiers	• Configure host identifiers

For a detailed explanation of each function, click Help.

4. Provide details like access gate name, port, and password. Also, enter the following details:

   - **Hostname** - provide the FQDN of the Argus Web Server where you will install webgate.
   - **Access Management Service** - select **On**. To enable a smooth installation, it is essential that this option is selected as On.
   - **Primary HTTP 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 HTTP Host** - provide the same value as **Hostname**.
   - **CachePragmaHeader** - enter value as private
   - **CacheControlHeader** - enter value as private

   Once you have entered all the above details, click **Save** to add the webgate.


ORACLE Access Administration
Policy Manager Help About Logout
System Configuration
System Management
Access System Configuration
Logged in user: orcladmin
Access Server Clusters
AccessGate Configuration
Add New Access Gate
Access Server Configuration
Authentication Management
Authorization Management
User Access Configuration
Common Information Configuration
Host Identifiers

Modify AccessGate

AccessGate Name	OracleAG
Description	
State	● Enabled ○ Disabled
Hostname**	<myhost.example.com>
Port**	8083
New Access Gate Password	••••••••••
Re-type New Access Gate Password	••••••••••
Debug	● Off ○ On
Maximum user session time (seconds)*	3600
Idle Session Time (seconds)	3600
Maximum Connections	1
Transport Security	● Open ○ Simple ○ Cert
IPValidation	○ Off ● On
IPValidationException	
Maximum Client Session Time (hours)	24
Failover threshold	1
Access server timeout threshold*	
Sleep For (seconds)	60
Maximum elements in cache*	100000
Cache timeout (seconds)*	1800
Impersonation username	
Impersonation password	
Re-type impersonation password	

ASDK Client

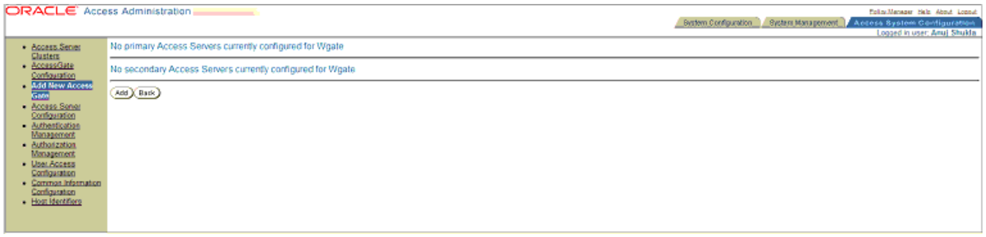
Access Management Service	○ Off ● On

Web Server Client

Primary HTTP Cookie Domain*	<.example.com>
Preferred HTTP Host	<myhost.example.com>
Deny On Not Protected	● Off ○ On
CachePragmaHeader	
CacheControlHeader	
LogOutURLs	

5. You will see the message *Please associate an Access Server or Access Server Cluster with this AccessGate*.

6. Click **List Access Servers**. The following screen appears:

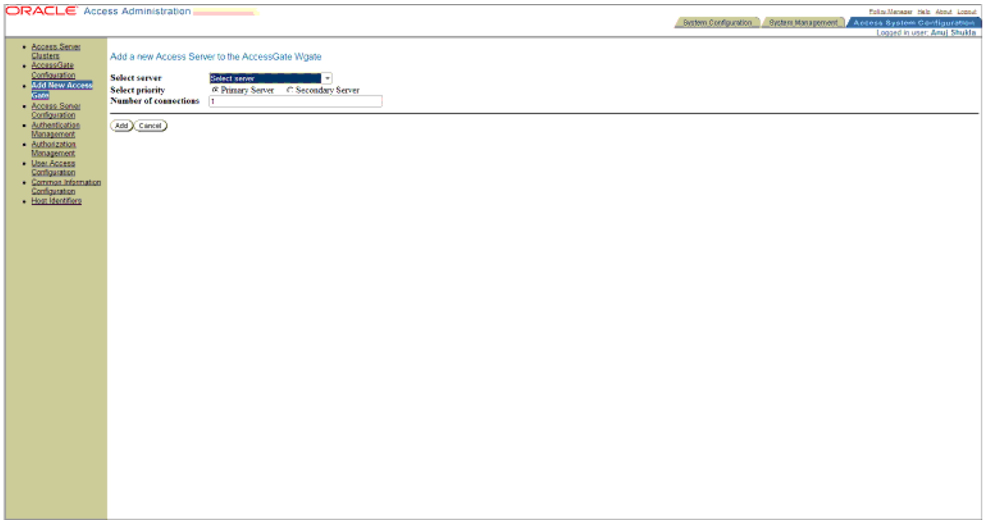

ORACLE Access Administration
Policy Manager Help About Logout
System Configuration
System Management
Access System Configuration
Logged in user: Anuj Shukla
Access Server Clusters
AccessGate Configuration
Add New Access Gate
Access Server Configuration
Authentication Management
Authorization Management
User Access Configuration
Common Information Configuration
Host Identifiers
Add
Back

No primary Access Servers currently configured for Wgate

No secondary Access Servers currently configured for Wgate

7. Click **Add**. Select an access server from the drop-down and click add to associate webgate with access server.

> **Note:** The access servers in this list will appear based on the access servers installed in the OAM image or installation that you have. Do not attempt adding Access Servers from OAM Console.


ORACLE Access Administration
Policy Manager Help About Logout
System Configuration
System Management
Access System Configuration
Logged in user: Anuj Shukla
Access Server Clusters
AccessGate Configuration
Add New Access Gate
Access Server Configuration
Authentication Management
Authorization Management
User Access Configuration
Common Information Configuration
Host Identifiers
Add
Cancel

Add a new Access Server to the AccessGate Wgate

Select server: Select server

Select priority: ● Primary Server ○ Secondary Server

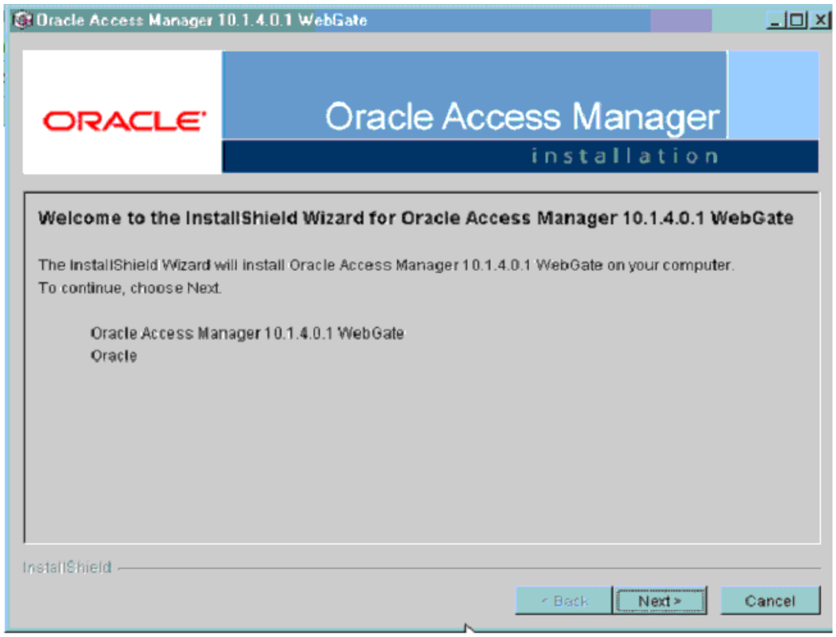
Number of connections: 1

8. Navigate to the Argus Web Server Machine, that is the machine where you have installed Argus. Run the installer for Webgate.

Installing WebGate

Following is the procedure to install WebGate:

1. Run the file `Oracle_Access_Manager10_1_4_3_0_Win32_ISAPI_WebGate.exe`. The following screen appears. Click **Next**.

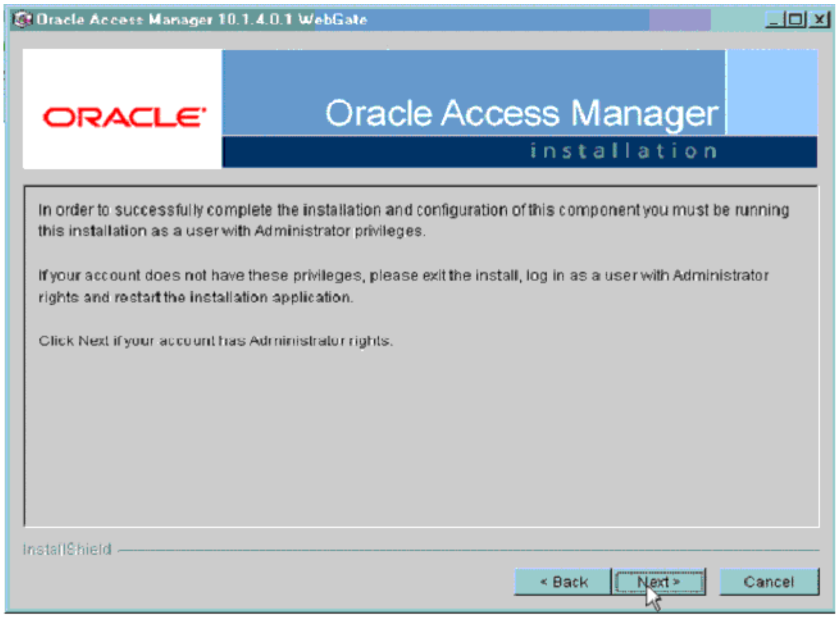


Welcome to the InstallShield Wizard for Oracle Access Manager 10.1.4.0.1 WebGate

The InstallShield Wizard will install Oracle Access Manager 10.1.4.0.1 WebGate on your computer.
To continue, choose Next.

Oracle Access Manager 10.1.4.0.1 WebGate
Oracle

2. You must have administrative privileges to run the installation. If you are logged in as a different user, you must exit the installation, log in as the Administrator and then restart the installation. When the following screen appears, click **Next**.

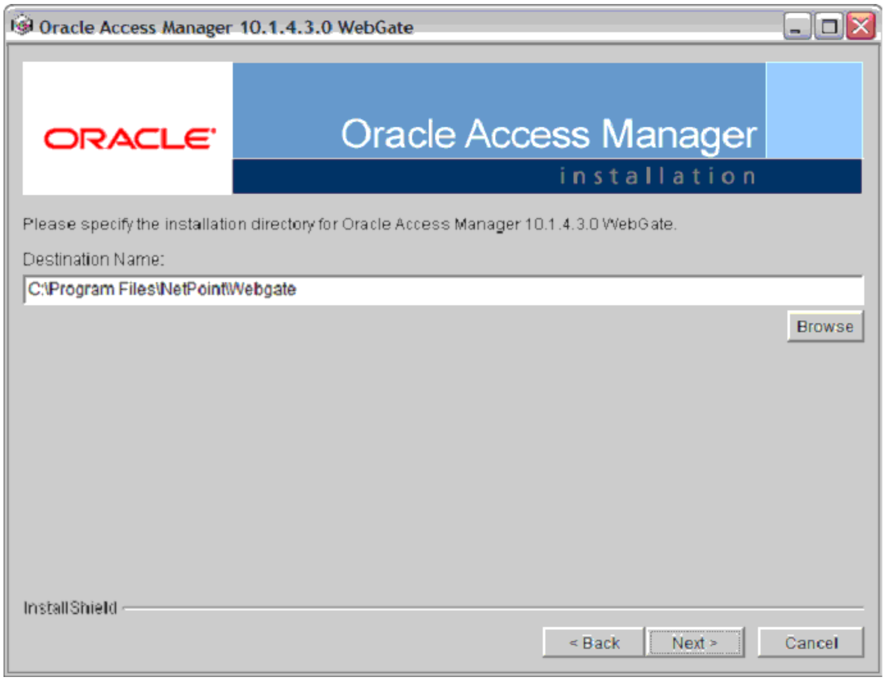


In order to successfully complete the installation and configuration of this component you must be running this installation as a user with Administrator privileges.

If your account does not have these privileges, please exit the install, log in as a user with Administrator rights and restart the installation application.

Click Next if your account has Administrator rights.

3. In the **Destination Name**, set the installation directory and click **Next**.

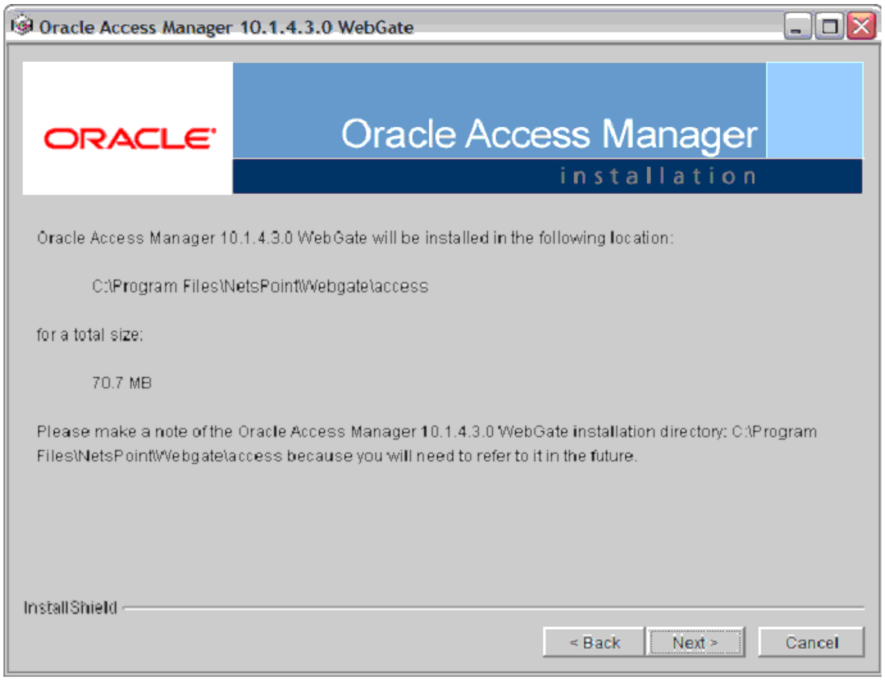


Please specify the installation directory for Oracle Access Manager 10.1.4.3.0 WebGate.

Destination Name:

C:\Program Files\NetPoint\Webgate

4. Review the location to which WebGate for IIS is getting installed and the total disk space it will take for the installation. Then click **Next**.



Oracle Access Manager 10.1.4.3.0 WebGate will be installed in the following location:

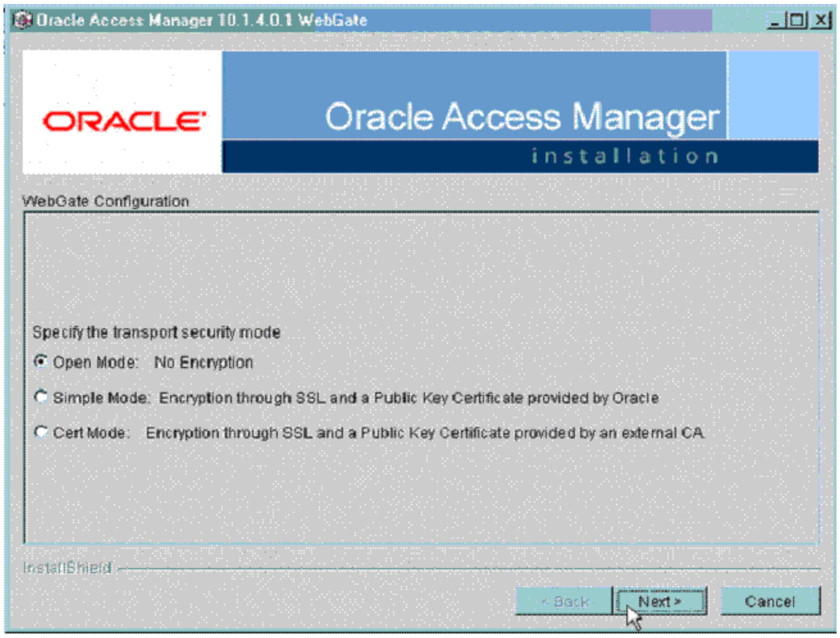
C:\Program Files\NetsPoint\Webgate\access

for a total size:

70.7 MB

Please make a note of the Oracle Access Manager 10.1.4.3.0 WebGate installation directory: C:\Program Files\NetsPoint\Webgate\access because you will need to refer to it in the future.

5. The installer begins copying the WebGate files for IIS. Now select **Open Mode: No encryption** for the transport security mode and click **Next**.



Specify the transport security mode

● Open Mode: No Encryption

○ Simple Mode: Encryption through SSL and a Public Key Certificate provided by Oracle

○ Cert Mode: Encryption through SSL and a Public Key Certificate provided by an external CA

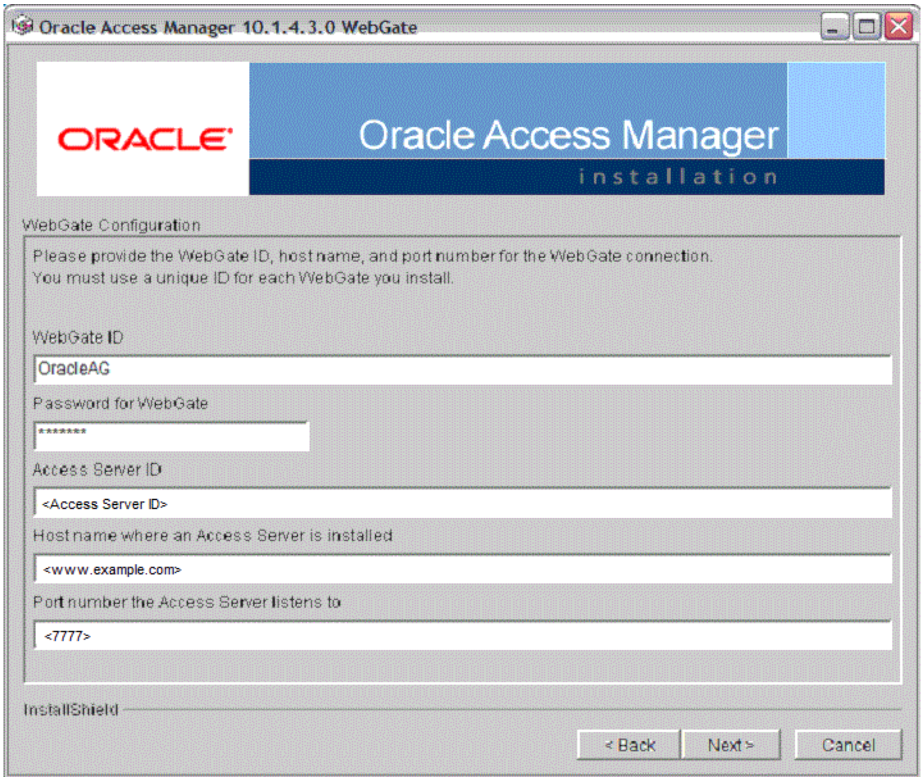
6. Provide the following details and click **Next**.

Table 15–1 Values for WebGate configuration

Parameter	Description
WebGate ID	Name of the webgate.
Password	Password for the webgate.
Access Server ID	Name of the access server that is configured in access server console.

Table 15–1 (Cont.) Values for WebGate configuration

Parameter	Description
Host name	FQDN of the machine where the access server is installed.
Port number	Port of the access server



WebGate Configuration

Please provide the WebGate ID, host name, and port number for the WebGate connection.
You must use a unique ID for each WebGate you install.

WebGate ID: OracleAG

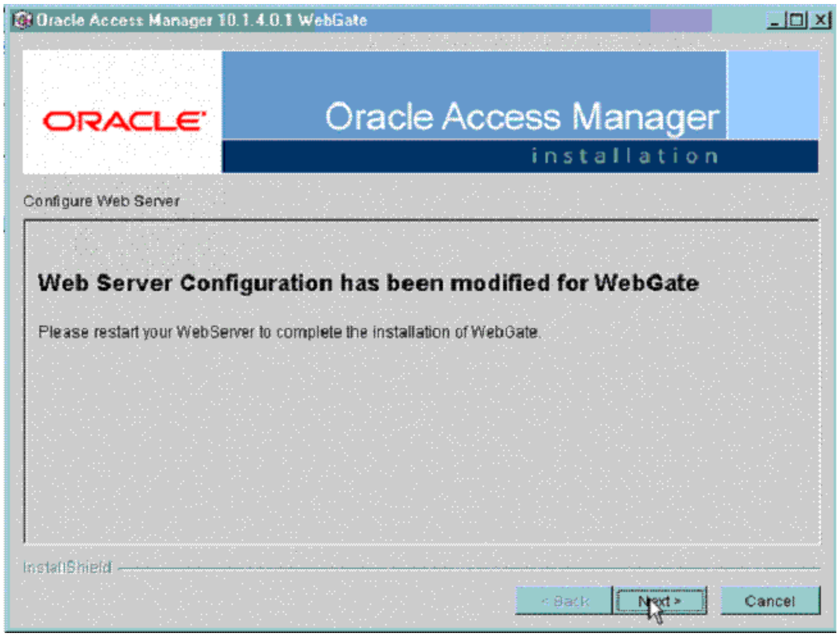
Password for WebGate: *******

Access Server ID: <Access Server ID>

Host name where an Access Server is installed: <www.example.com>

Port number the Access Server listens to: <7777>

7. The following screen appears:

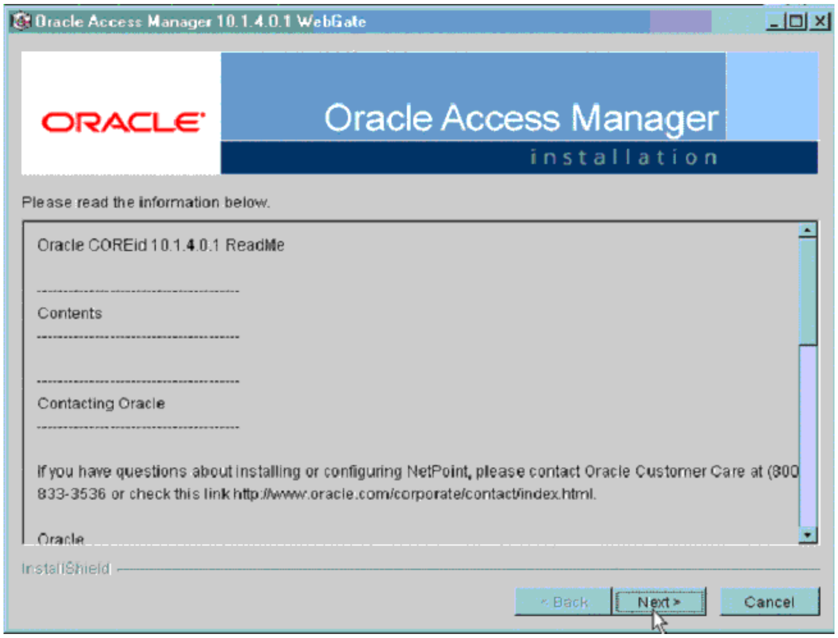


Configure Web Server

Web Server Configuration has been modified for WebGate

Please restart your WebServer to complete the installation of WebGate.

8. Review the Readme page and click **Next**.



Please read the information below.

Oracle COREid 10.1.4.0.1 ReadMe

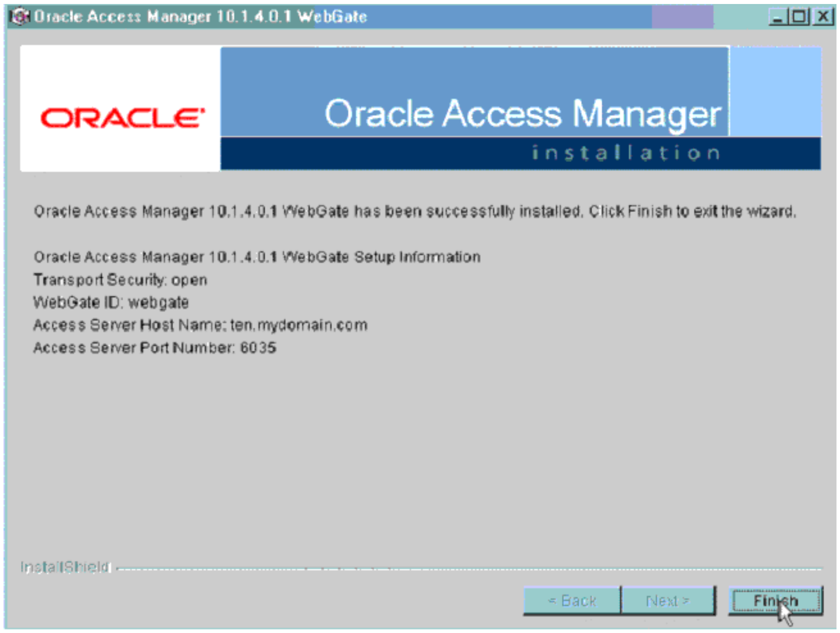
Contents

Contacting Oracle

If you have questions about installing or configuring NetPoint, please contact Oracle Customer Care at (800 833-3536 or check this link http://www.oracle.com/corporate/contact/index.html.

Oracle

9. You can review the WebGate for IIS configuration settings and click **Finish**.



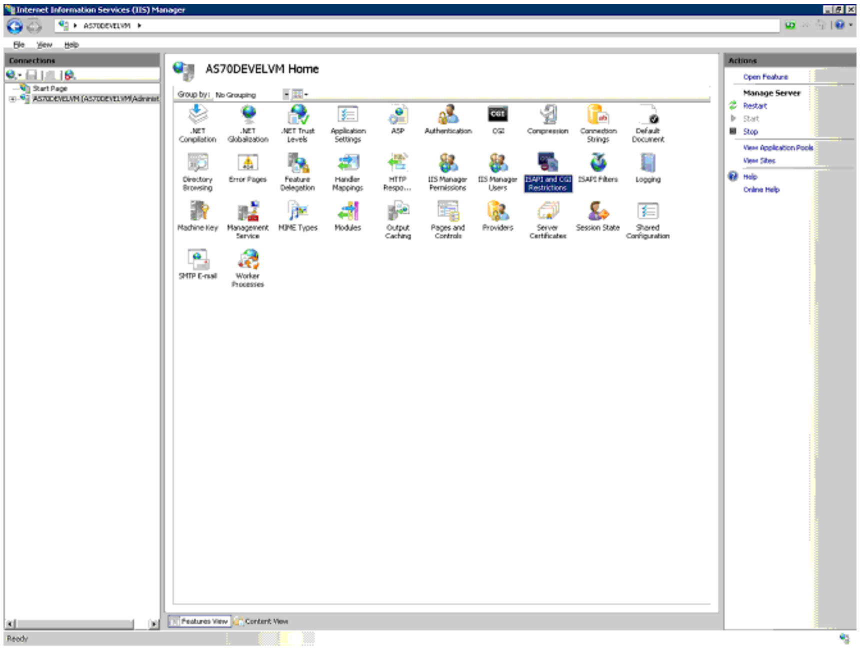
Oracle Access Manager 10.1.4.0.1 WebGate has been successfully installed. Click Finish to exit the wizard.

Oracle Access Manager 10.1.4.0.1 WebGate Setup Information
Transport Security: open
WebGate ID: webgate
Access Server Host Name: ten.mydomain.com
Access Server Port Number: 6035

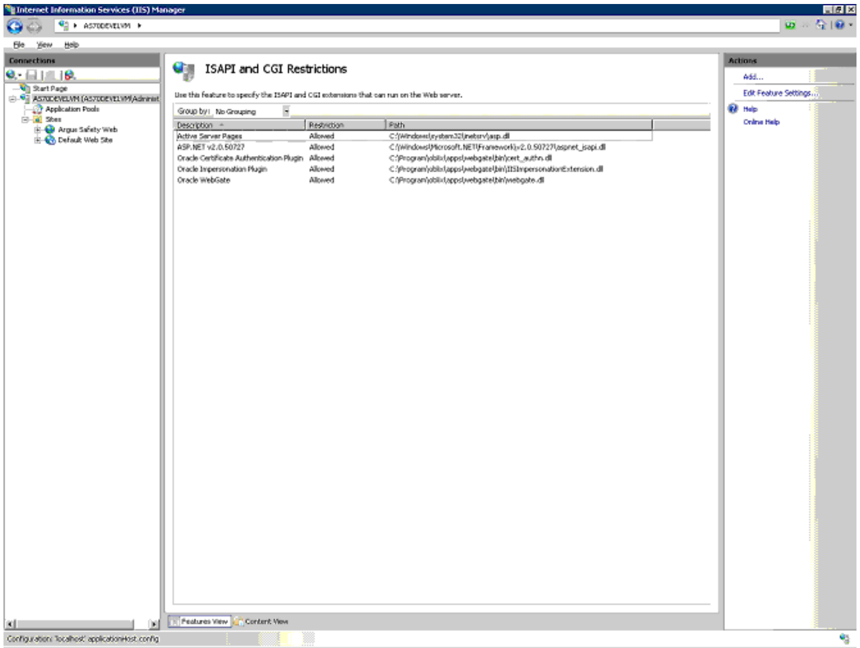
Configuring WebGate on Windows Server 2008 and Windows Server 2012

This section describes the procedure to install WebGate on Windows Server 2008 and Windows Server 2012. Before following this procedure, ensure that you have already installed webgate on Windows 2008 and Windows 2012 servers.

1. Open IIS manager and navigate to the top level node. On the home page, double click **ISAPI and CGI restrictions** to open the feature.



2. The following screen appears:



ISAPI and CGI Restrictions

Use this feature to specify the ISAPI and CGI extensions that can run on the Web server.

Description	Restriction	Path
Active Server Pages	Allowed	C:\Windows\system32\inetsrv\asp.dll
ASP.NET v2.0.50727	Allowed	C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll
Oracle Certificate Authentication Plugin	Allowed	C:\Program\oblix\apps\webgate\bin\cert_authn.dll
Oracle Impersonation Plugin	Allowed	C:\Program\oblix\apps\webgate\bin\IISImpersonationExtension.dll
Oracle WebGate	Allowed	C:\Program\oblix\apps\webgate\bin\webgate.dll

3. You have to correct the path for the following DLLs to reflect the path where you have installed the WebGate. To do this, double click the DLL entry and you will see the **Edit ISAPI or GCI Restrictions** dialog box as shown below. In this dialog box, enter the path given in the following table and click **OK**.

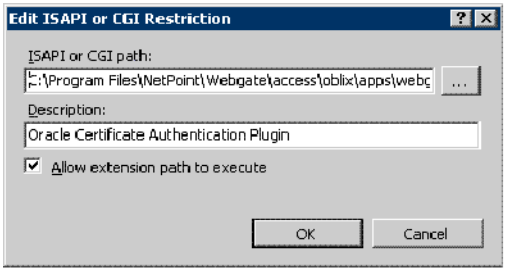
Table 15–2 Default path for DLL

DLL Name	Default Installation Path
Oracle Certificate Authentication Plugin	`C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\cert_authn.dll`

Table 15–2 (Cont.) Default path for DLL

DLL Name	Default Installation Path
Oracle Impersonation Plugin	`C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\IISImpersonationExtension.dll`
Oracle WebGate	`C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\webgate.dll`

> **Note:** For Windows 2008 R2 and Windows 2012 R2, the DLLs must be manually added by clicking on the Add link in the right-most pane.

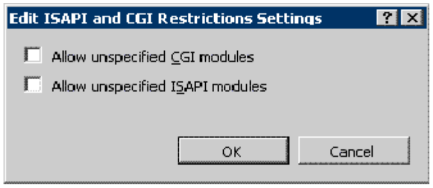


ISAPI or CGI path: C:\Program Files\NetPoint\Webgate\access\oblix\apps\webg

Description: Oracle Certificate Authentication Plugin

☑ Allow extension path to execute

4. Click **Edit Feature Settings** in the **Actions** panel in the right. The following dialog box appears:

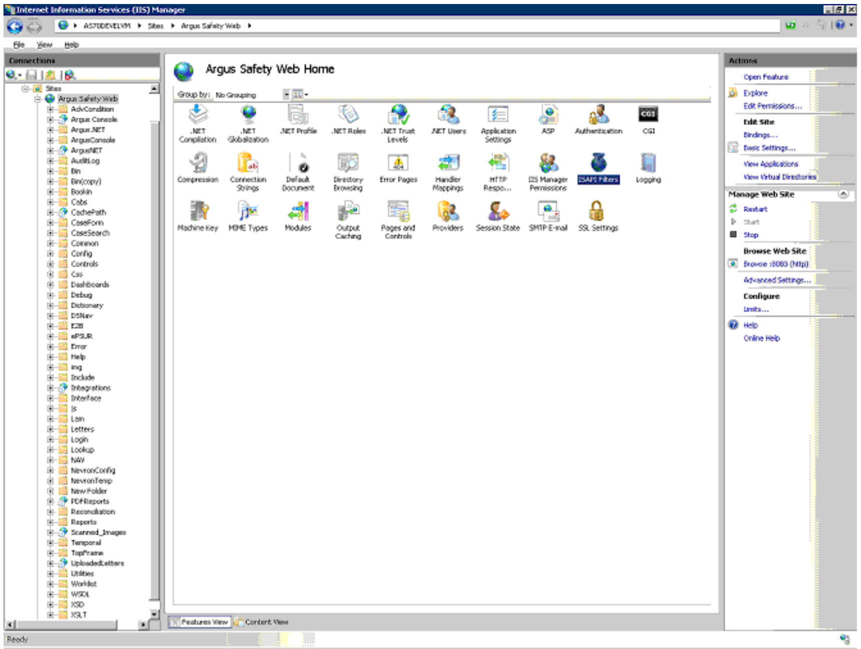


☐ Allow unspecified CGI modules

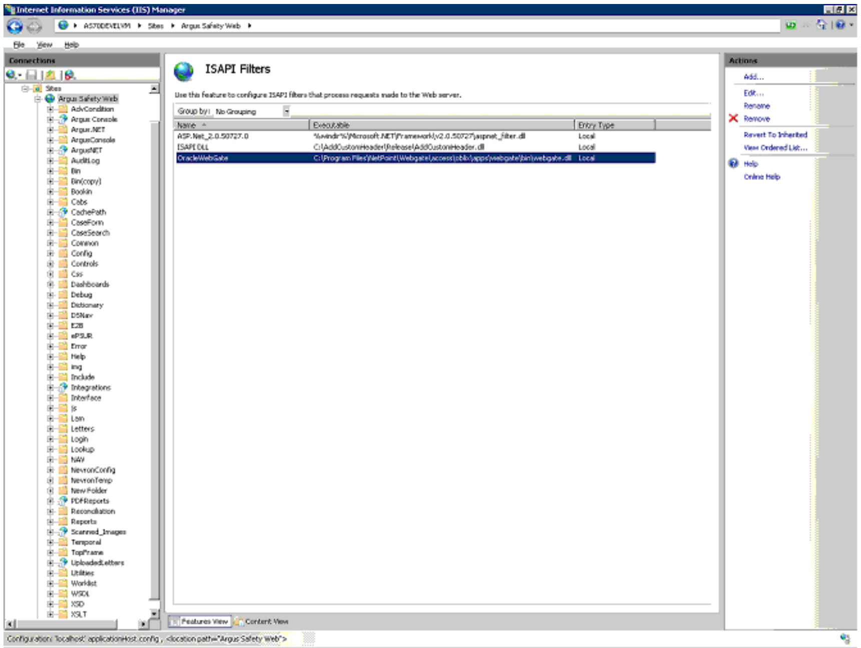
☐ Allow unspecified ISAPI modules

5. Check both the boxes and click **OK**.

6. Click **Argus Safety Web** node, which will open the home page for the application as shown below.



7. Click **ISAPI Filters** and the following screen appears:



Use this feature to configure ISAPI filters that process requests made to the Web server.

Name	Executable	Entry Type
ASP.Net_2.0.50727.0	%windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_filter.dll	Local
ISAPI DLL	C:\AddCustomHeader\Release\AddCustomHeader.dll	Local
OracleWebGate	C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\webgate.dll	Local

Configuration: 'localhost' applicationHost.config , <location path="Argus Safety Web">

8. Double click **OracleWebGate** and enter the path to where you have installed WebGate. The default path is `C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\webgate.dll`

9. You will now have to remove the `<add segment="bin"/>` entry from applicationhost.config file. Take a backup of the file before you make the following changes:

   a. Navigate to `Windows\System32\inetsrv\config` and open the applicationHost.config file.

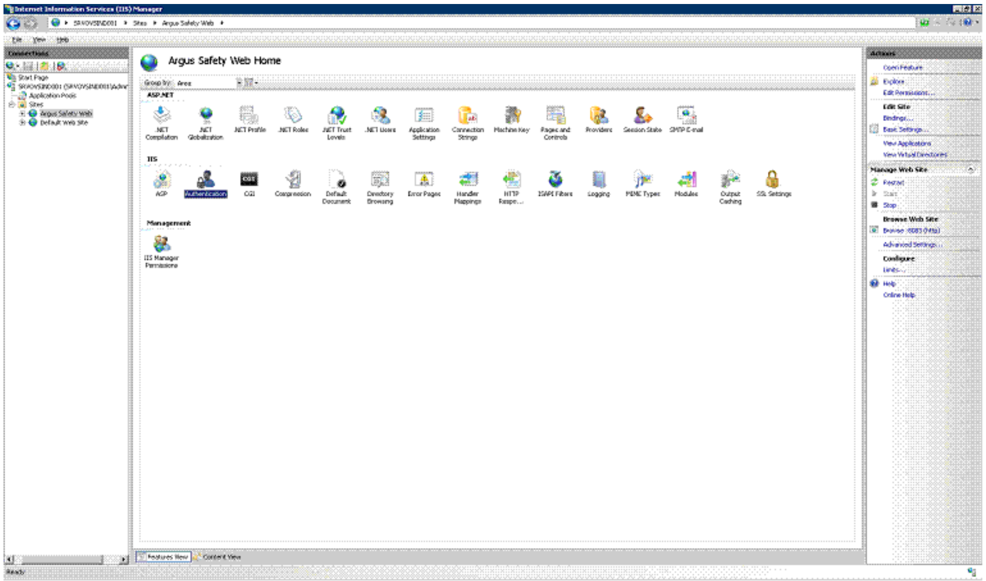
   b. Search for the `<hiddenSegments>` module.

c. Remove the entry `<add segment="bin"/>` if it is present.

d. Save the file.

10. Restart IIS for the changes to take effect.

After restarting IIS, open IIS Manager and navigate to **Sites** > **Argus Safety Web** > **Authentication** as per the screenshot below:

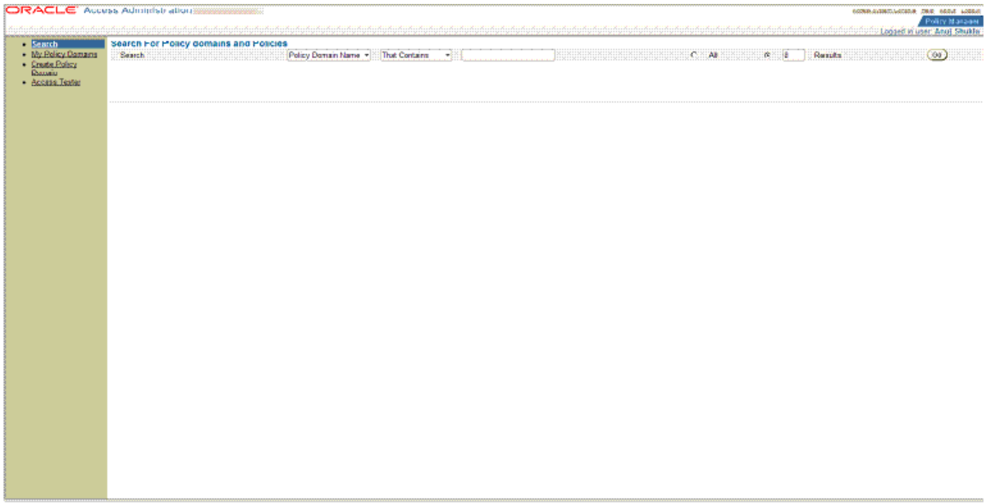


Right click on **Windows Authentication** and check if it is enabled. If yes, then disable it. This completes the WebGate installation on Windows Server 2008 and Windows Server 2012.

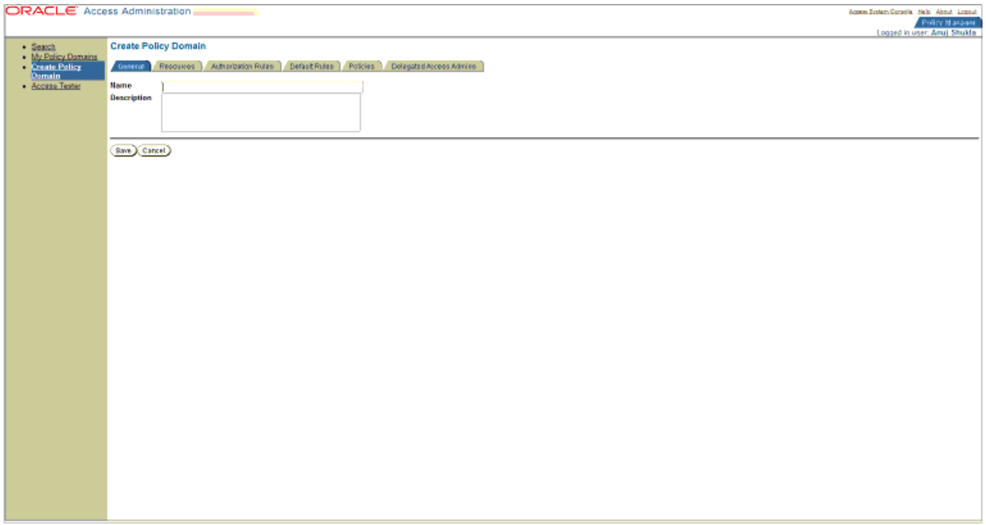
Protecting Files in the Argus Directory

This section describes the procedure to create a policy to protect files under the Argus directory.

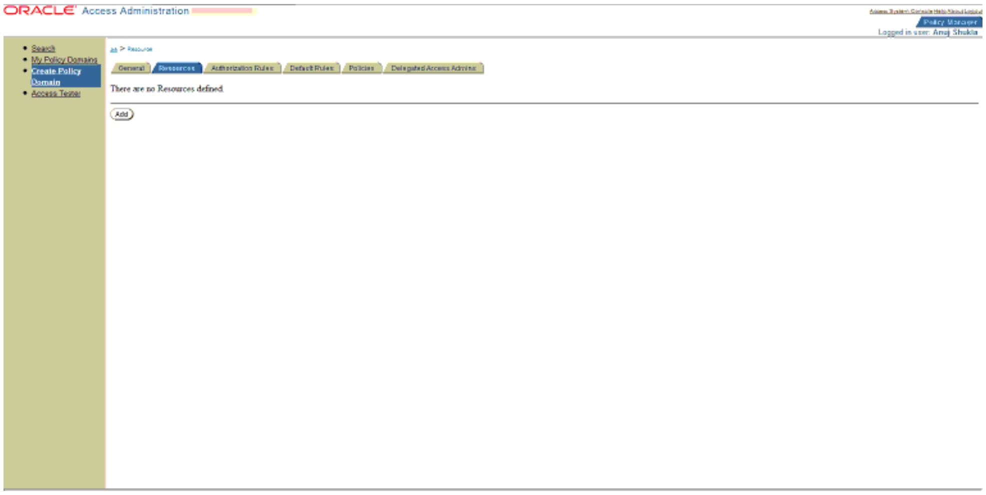
1. Navigate to the policy manager console and click **Create Policy Domain**.



2. Under the **General** tab provide a name and description and click **Save**.

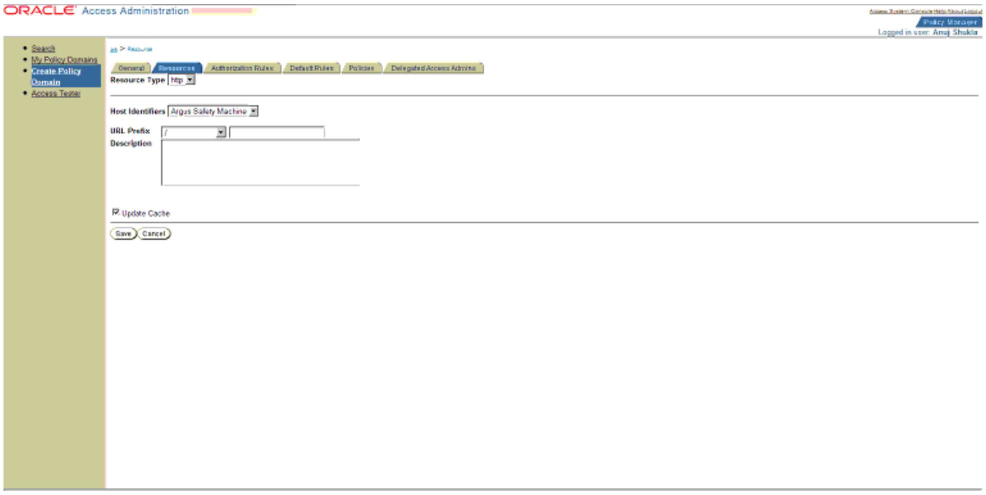


3. Click the **Resource** tab and then click **Add**.



There are no Resources defined.

4. Select **Host Identifier** from the drop-down list and select **URL Prefix** as / and provide a description. Click **Save**.



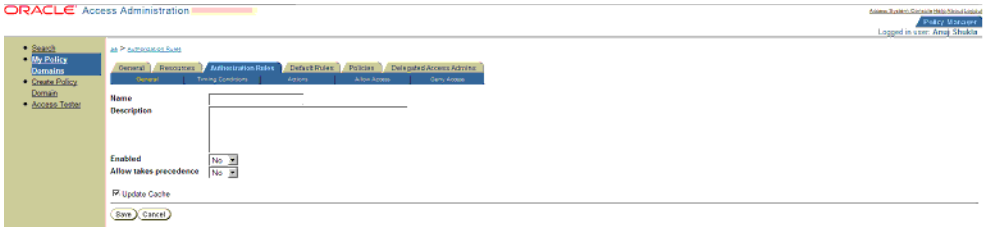
Resource Type: http

Host Identifiers: Argus Safety Machine

URL Prefix: /

☑ Update Cache

5. Click the **Authorization Rules** tab and select the **General** sub tab.



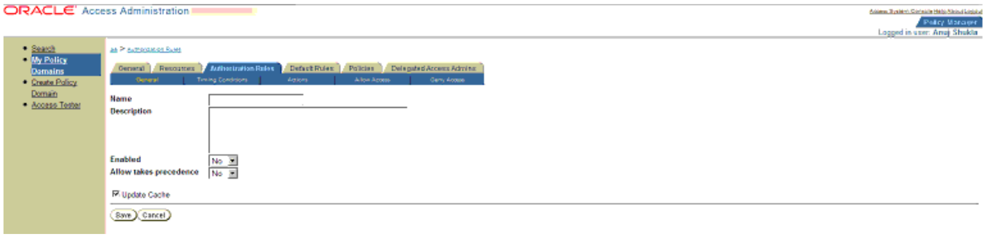
Enabled: No

Allow takes precedence: No

☑ Update Cache

6. Enter the following details in this tab and click **Save**:

   - **Name** - Enter an appropriate name for the rule.
   - **Description** - Enter a description for the rule.
   - **Enabled** - Select **Yes** from the drop-down list.
   - **Allow takes precedence** - Select **Yes** from the drop-down list.

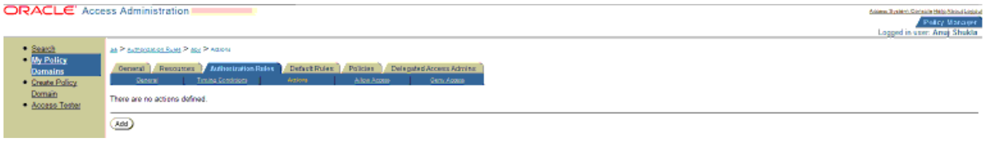


Enabled: No

Allow takes precedence: No

☑ Update Cache

7. Click the **Actions** sub tab, and then click **Add**.

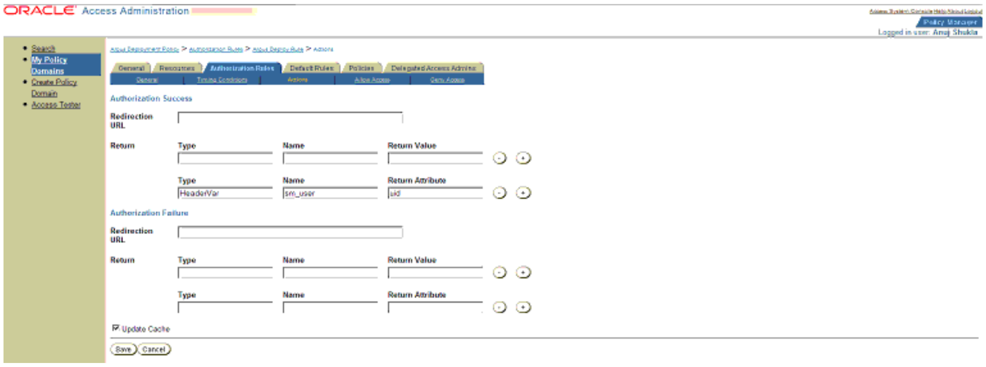


There are no actions defined.

8. In the **Authorization Success** section under **Return**, enter the following values and click **Save**:

Table 15–3 Values for Return field

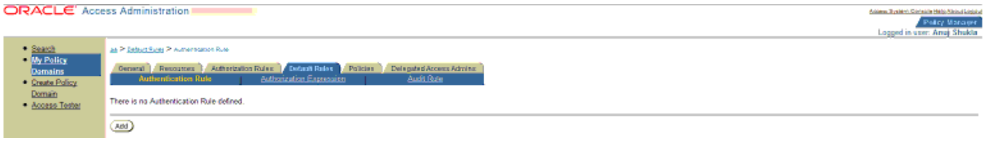
Field name	Value
Type	HeaderVar
Name	SM_USER
Return Attribute	uid



Authorization Success — Return: Type: HeaderVar | Name: sm_user | Return Attribute: uid

☑ Update Cache

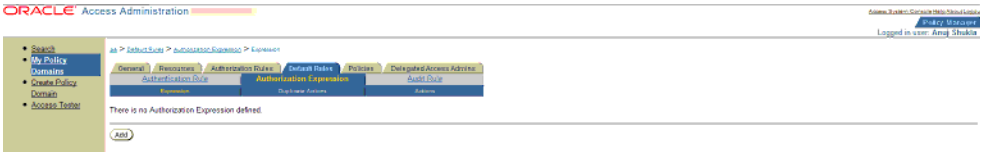
9. Navigate to **Default Rules** > **Authentication Rule**. Click **Add**.



There is no Authentication Rule defined.

10. Enter details for Name and decsription and select Authentication Scheme as **Oracle Access and Identity Basic Over LDAP**. Click **Save**.

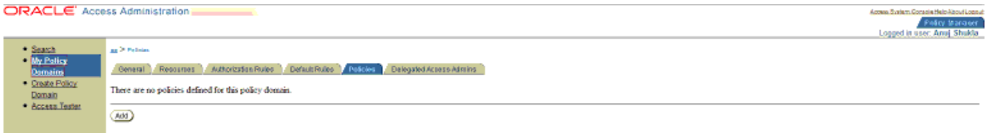
11. Click the **Authorization Expression** sub tab and click **Add**.



There is no Authorization Expression defined.

12. Select **Authorization Rule** from the drop-down. Click **Add** and then click **Save**.

13. Click **Policies** and then click **Add**.



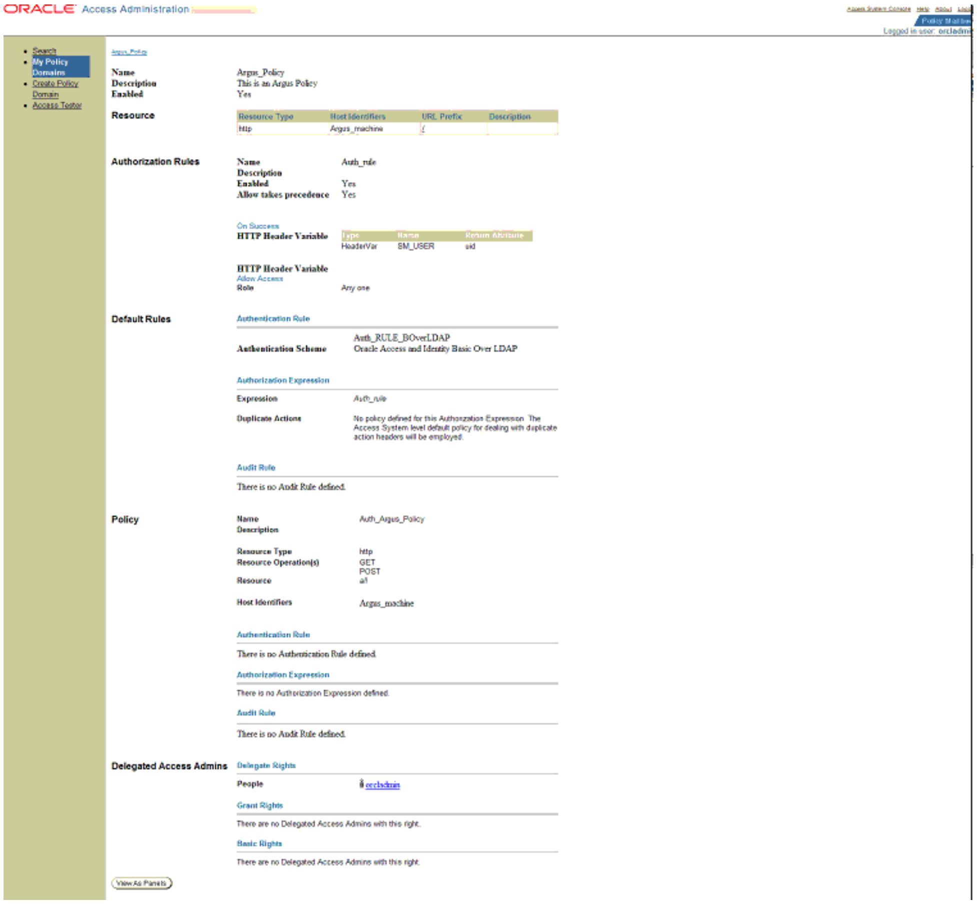
There are no policies defined for this policy domain.

14. Provide the following details and click **Save**:

   - **Name** - Name of the policy.
   - **Description** - Description of the policy.
   - **Resource type** - Select as http.
   - **Resource Operation(s)** - Select as Get and Post.

15. Now restart the Identity service and Access service. Also restart the IIS Argus Web Server. This completes the webgate installation and SSO policy configuration.

After you have completed the above steps your policy will appear as shown below:



Name	Argus_Policy
Description	This is an Argus Policy
Enabled	Yes

Resource

Resource Type	Host Identifiers	URL Prefix	Description
http	Argus_machine	/	

Authorization Rules

Name	Auth_rule
Description	
Enabled	Yes
Allow takes precedence	Yes

On Success

HTTP Header Variable

Type	Name	Return Attribute
HeaderVar	SM_USER	uid

HTTP Header Variable

Allow Access

Role: Any one

Default Rules

Authentication Rule

Authentication Scheme: Auth_RULE_BOverLDAP
Oracle Access and Identity Basic Over LDAP

Authorization Expression

Expression: Auth_rule

Duplicate Actions: No policy defined for this Authorization Expression. The Access System level default policy for dealing with duplicate action headers will be employed.

Audit Rule

There is no Audit Rule defined.

Policy

Name	Auth_Argus_Policy
Description	
Resource Type	http
Resource Operation(s)	GET POST
Resource	a/l
Host Identifiers	Argus_machine

Authentication Rule

There is no Authentication Rule defined.

Authorization Expression

There is no Authorization Expression defined.

Audit Rule

There is no Audit Rule defined.

Delegated Access Admins

Delegate Rights

People: orcladmin

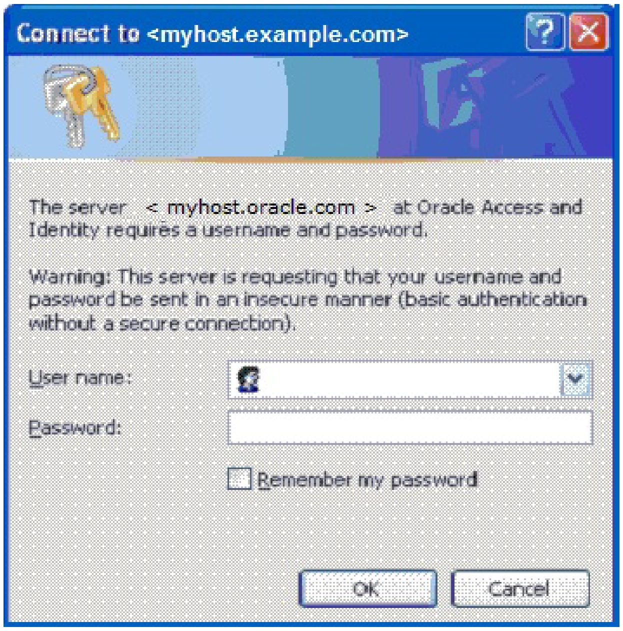
Grant Rights

There are no Delegated Access Admins with this right.

Basic Rights

There are no Delegated Access Admins with this right.

To verify if you have correctly configured the policy check for the following prompt when you open the Argus URL:



The server < myhost.oracle.com > at Oracle Access and Identity requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name:

Password:

□ Remember my password

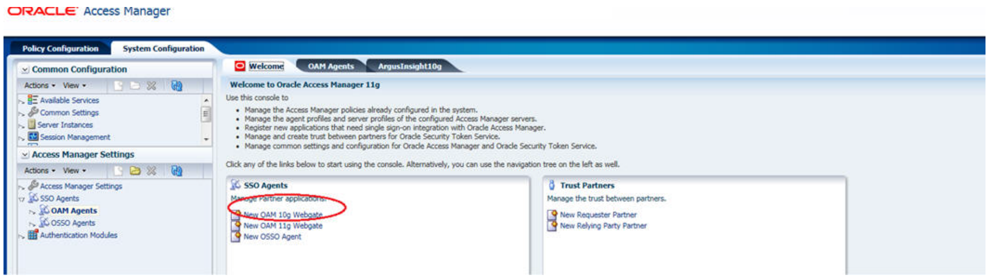
Configuring SSO in Oracle Access Manager 11g

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:

1. Navigate to the **System Configuration** tab of OAM and select the **New OAM 10g Webgate** link.



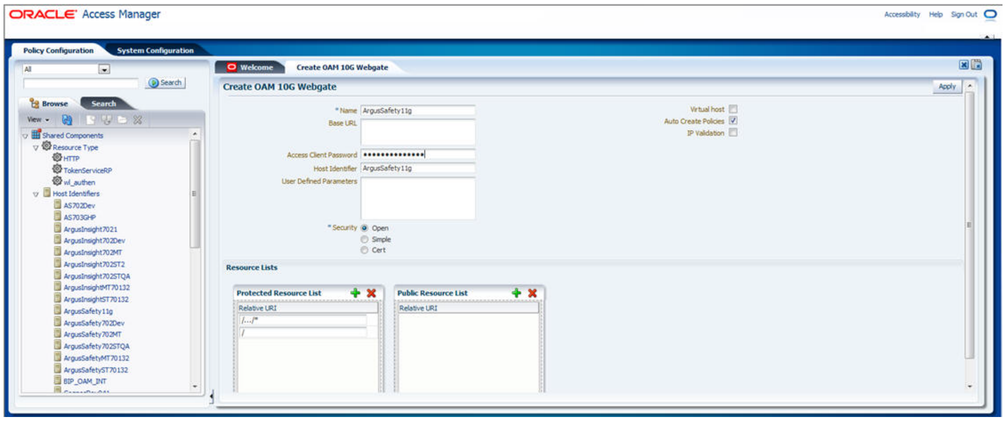
Welcome to Oracle Access Manager 11g

Use this console to

- Manage the Access Manager policies already configured in the system.
- Manage the agent profiles and server profiles of the configured Access Manager servers.
- Register new applications that need single sign-on integration with Oracle Access Manager.
- Manage and create trust between partners for Oracle Security Token Service.
- Manage common settings and configuration for Oracle Access Manager and Oracle Security Token Service.

Click any of the links below to start using the console. Alternatively, you can use the navigation tree 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**.



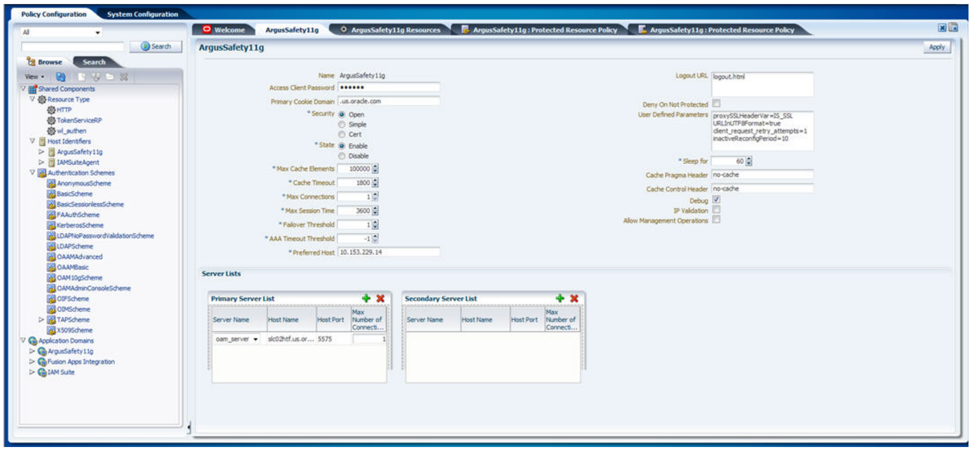
Create OAM 10G Webgate

* Name	ArgusSafety11g
Base URL	
Access Client Password	•••••••••••••••
Host Identifier	ArgusSafety11g
User Defined Parameters	
* Security	● Open ○ Simple ○ Cert
Virtual host	□
Auto Create Policies	☑
IP Validation	□

Protected Resource List

Relative URI
/.../*
/

3. The following screen is displayed:



ArgusSafety11g

Name ArgusSafety11g

Access Client Password ••••••

Primary Cookie Domain .us.oracle.com

* Security ● Open ○ Simple ○ Cert

* State ● Enable ○ Disable

* Max Cache Elements 100000

* Cache Timeout 1800

* Max Connections 1

* Max Session Time 3600

* Failover Threshold 1

* AAA Timeout Threshold -1

* Preferred Host 10.153.229.14

Logout URL logout.html

Deny On Not Protected □

User Defined Parameters proxySSLHeaderVar=IS_SSL URLInUTF8Format=true client_request_retry_attempts=1 inactiveReconfigPeriod=10

* Sleep for 60

Cache Pragma Header no-cache

Cache Control Header no-cache

Debug ☑

IP Validation □

Allow Management Operations □

Server Lists

Primary Server List

Server Name	Host Name	Host Port	Max Number of Connecti...
oam_server	slc02htf.us.or...	5575	1

Secondary Server List

Server Name	Host Name	Host Port	Max Number of Connecti...

Note: Refresh the Host Identifier list to view the newly created Webgate within the Policy Configuration tab.

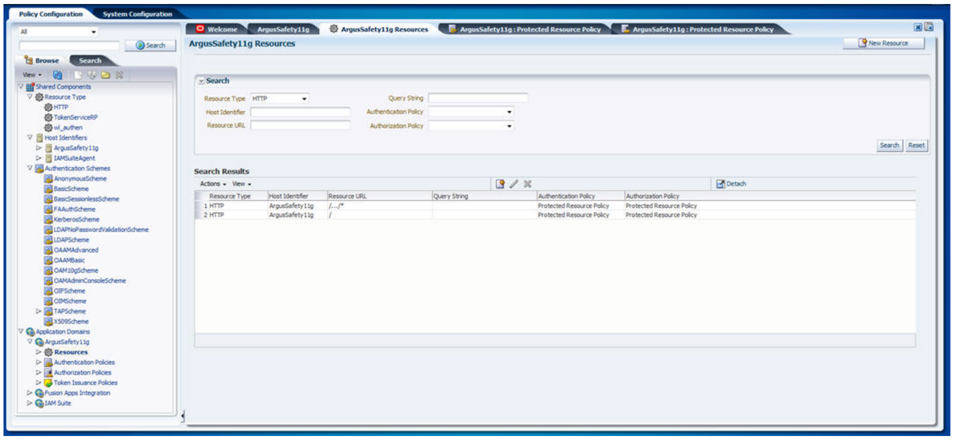
Provide details such as Primary Cookie Domain and Preferred Host, as shown above and click **Apply**:

- **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:



ArgusSafety11g Resources

Search

Resource Type HTTP

Host Identifier

Resource URL

Query String

Authentication Policy

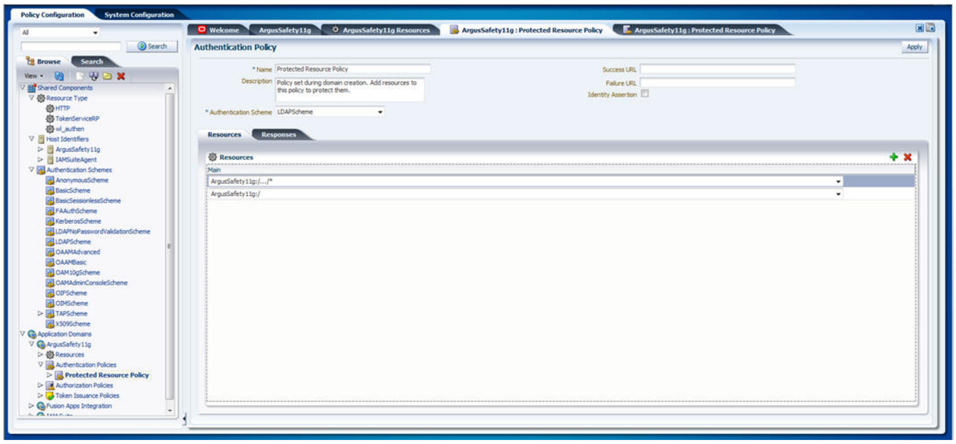
Authorization Policy

Search Results

	Resource Type	Host Identifier	Resource URL	Query String	Authentication Policy	Authorization Policy
1	HTTP	ArgusSafety11g	/.../*		Protected Resource Policy	Protected Resource Policy
2	HTTP	ArgusSafety11g	/		Protected Resource Policy	Protected Resource Policy

5. Expand the **Authentication Policies** under the newly created Webgate.

   Double-click the **Protected Resource Policy**. The following screen appears:



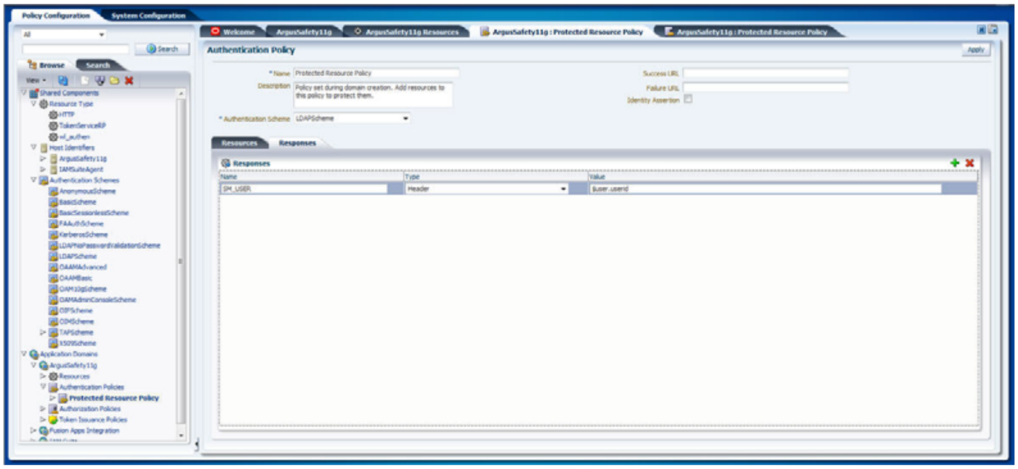
Authentication Policy

- *Name: Protected Resource Policy
- Description: Policy set during domain creation. Add resources to this policy to protect them.
- *Authentication Scheme: LDAPScheme
- Success URL:
- Failure URL:
- Identity Assertion: □

Resources

Main
ArgusSafety11g:/…/*
ArgusSafety11g:/

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:



Authentication Policy

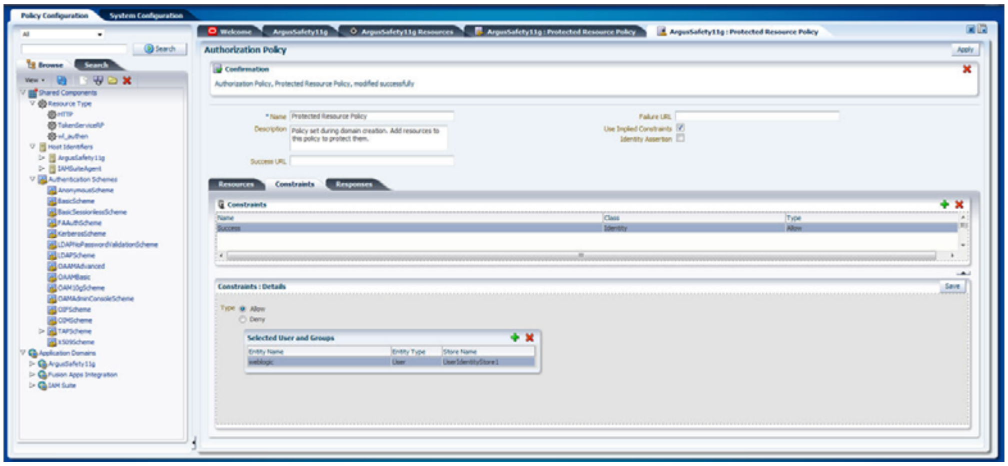
- *Name: Protected Resource Policy
- Description: Policy set during domain creation. Add resources to this policy to protect them.
- *Authentication Scheme: LDAPScheme

Responses

Name	Type	Value
SM_USER	Header	$user.userid

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

Confirmation

Authorization Policy, Protected Resource Policy, modified successfully

- *Name: Protected Resource Policy
- Description: Policy set during domain creation. Add resources to this policy to protect them.
- Success URL:
- Failure URL:
- Use Implied Constraints: ☑
- Identity Assertion: □

Constraints

Name	Class	Type
Success	Identity	Allow

Constraints : Details

Type: ● Allow ○ Deny

Selected User and Groups

Entity Name	Entity Type	Store Name
weblogic	User	UserIdentityStore1

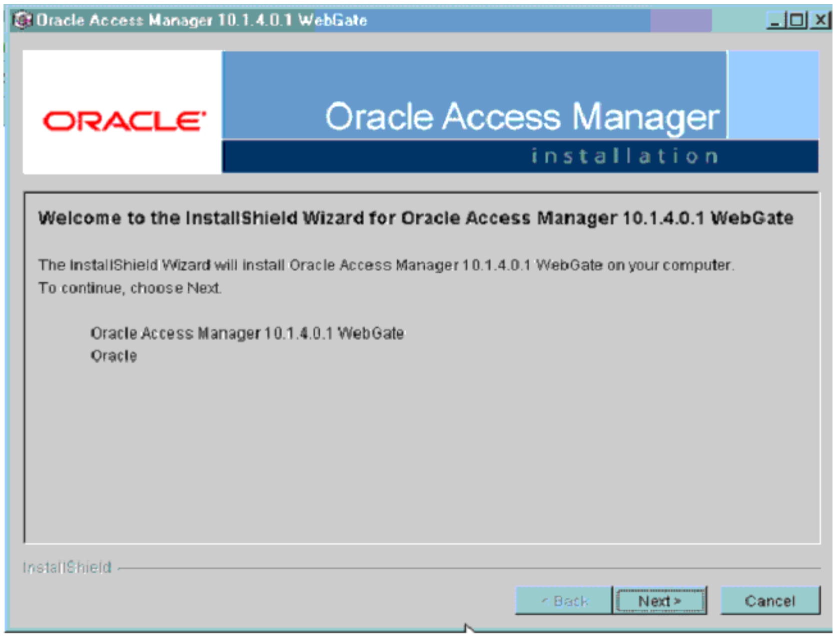
Note: All the names under the Constraints tab with **Type** as **Allow** can access the Argus Safety Server where Webgate has been installed. Select the **Type** as **Deny** if a user should be denied access to the Argus Safety Server where Webgate has been installed.

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.

Installing WebGate

Following is the procedure to install WebGate:

1. Run the file `Oracle_Access_Manager10_1_4_3_0_Win32_ISAPI_WebGate.exe`. The following screen appears. Click **Next**.

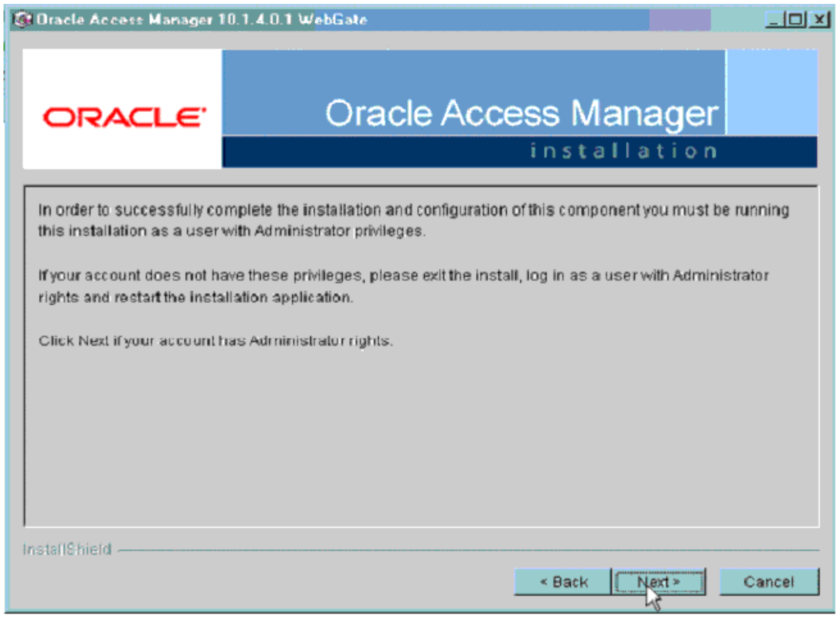


Welcome to the InstallShield Wizard for Oracle Access Manager 10.1.4.0.1 WebGate

The InstallShield Wizard will install Oracle Access Manager 10.1.4.0.1 WebGate on your computer.
To continue, choose Next.

Oracle Access Manager 10.1.4.0.1 WebGate
Oracle

2. You must have administrative privileges to run the installation. If you are logged in as a different user, you must exit the installation, log in as the Administrator and then restart the installation. When the following screen appears, click **Next**.

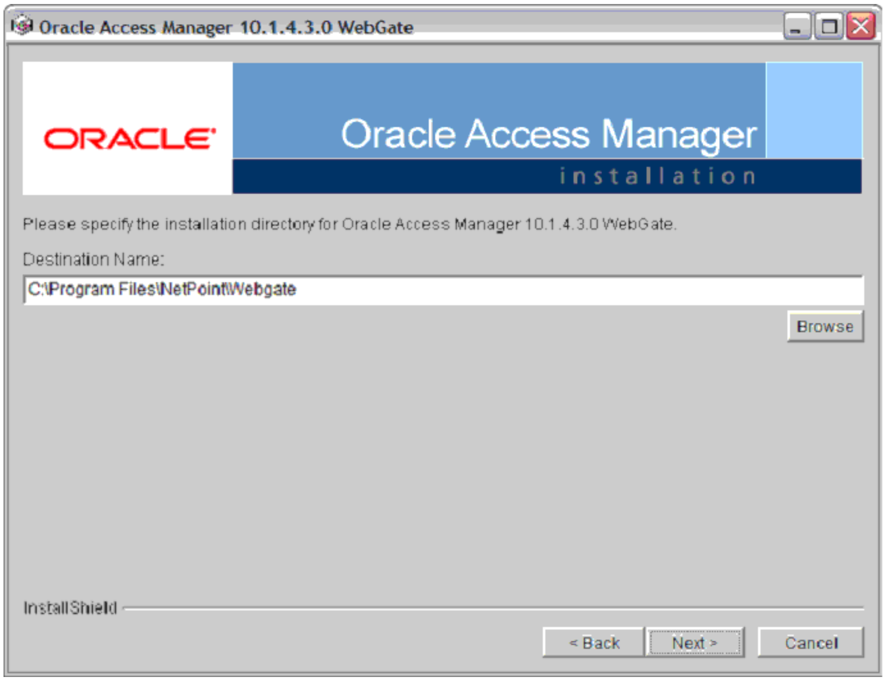


In order to successfully complete the installation and configuration of this component you must be running this installation as a user with Administrator privileges.

If your account does not have these privileges, please exit the install, log in as a user with Administrator rights and restart the installation application.

Click Next if your account has Administrator rights.

3. In the **Destination Name**, set the installation directory and click **Next**.

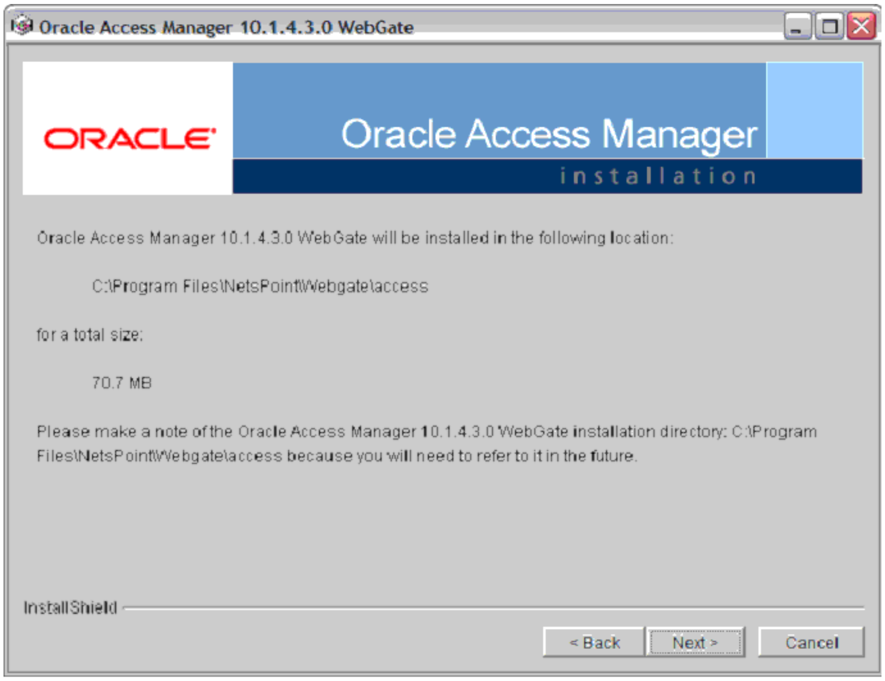


Please specify the installation directory for Oracle Access Manager 10.1.4.3.0 WebGate.

Destination Name:

C:\Program Files\NetPoint\Webgate

4. Review the location to which WebGate for IIS is getting installed and the total disk space it will take for the installation. Then click **Next**.



Oracle Access Manager 10.1.4.3.0 WebGate will be installed in the following location:

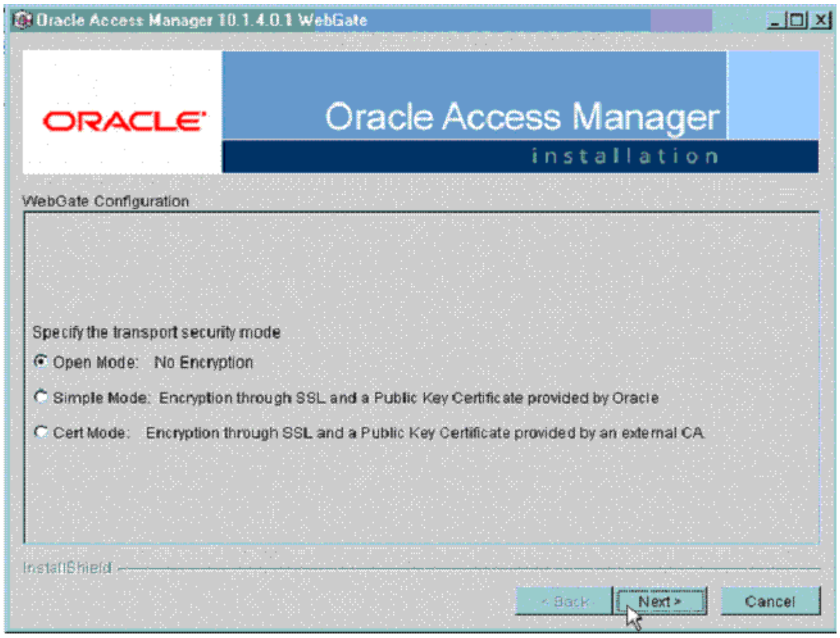
C:\Program Files\NetsPoint\Webgate\access

for a total size:

70.7 MB

Please make a note of the Oracle Access Manager 10.1.4.3.0 WebGate installation directory: C:\Program Files\NetsPoint\Webgate\access because you will need to refer to it in the future.

5. The installer begins copying the WebGate files for IIS. Now select **Open Mode: No encryption** for the transport security mode and click **Next**.



Specify the transport security mode

● Open Mode: No Encryption

○ Simple Mode: Encryption through SSL and a Public Key Certificate provided by Oracle

○ Cert Mode: Encryption through SSL and a Public Key Certificate provided by an external CA

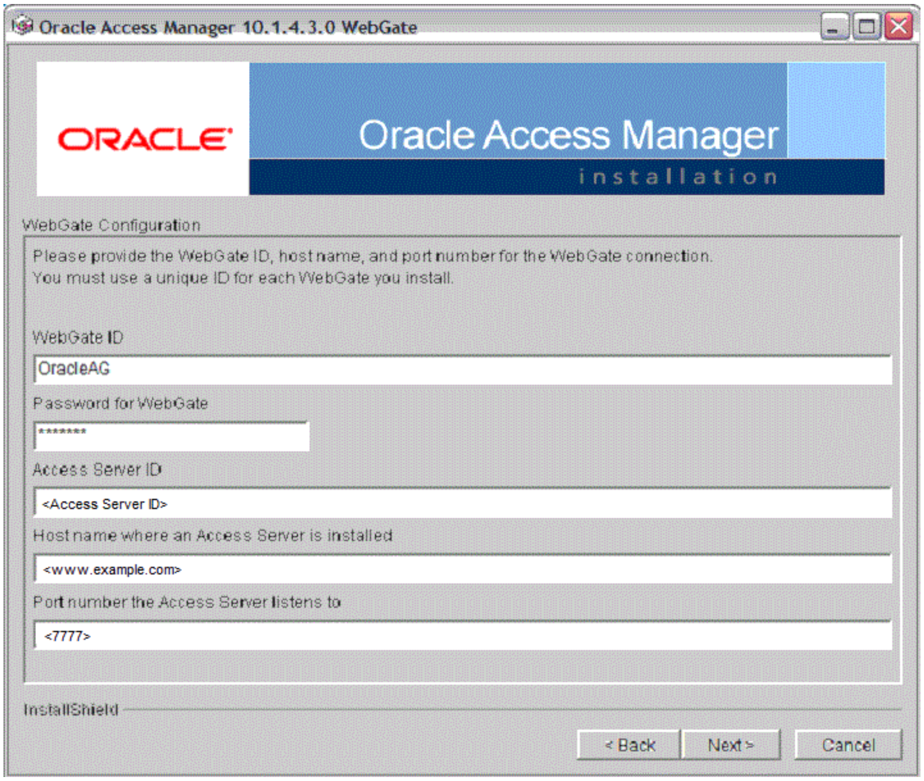
6. Provide the following details and click **Next**.

Table 15–4 Values for WebGate configuration

Parameter	Description
WebGate ID	Name of the webgate.
Password	Password for the webgate.
Access Server ID	Name of the access server that is configured in access server console.

Table 15–4 (Cont.) Values for WebGate configuration

Parameter	Description
Host name	FQDN of the machine where the access server is installed.
Port number	Port of the access server



WebGate Configuration

Please provide the WebGate ID, host name, and port number for the WebGate connection.
You must use a unique ID for each WebGate you install.

WebGate ID: OracleAG

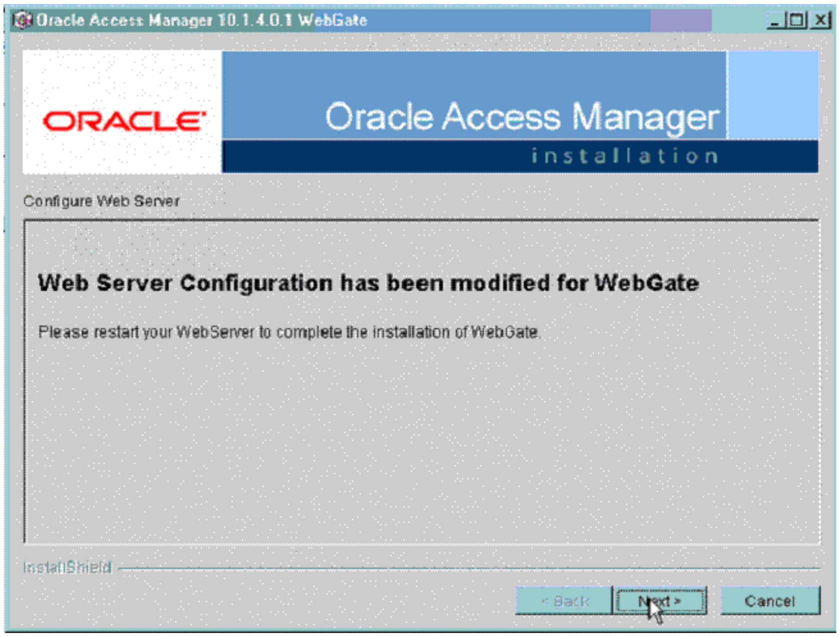
Password for WebGate: *******

Access Server ID: <Access Server ID>

Host name where an Access Server is installed: <www.example.com>

Port number the Access Server listens to: <7777>

7. The following screen appears:

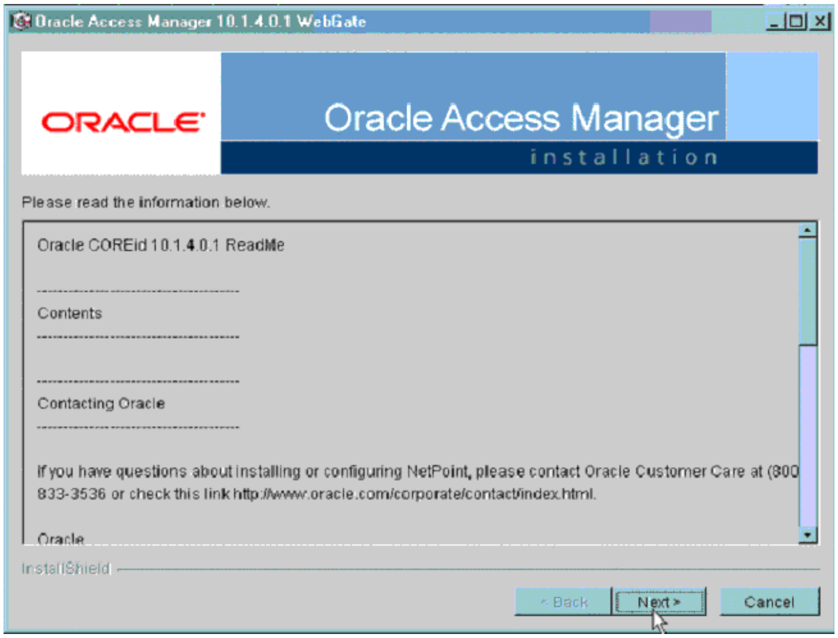


Configure Web Server

Web Server Configuration has been modified for WebGate

Please restart your WebServer to complete the installation of WebGate.

8. Review the Readme page and click **Next**.



Please read the information below.

Oracle COREid 10.1.4.0.1 ReadMe

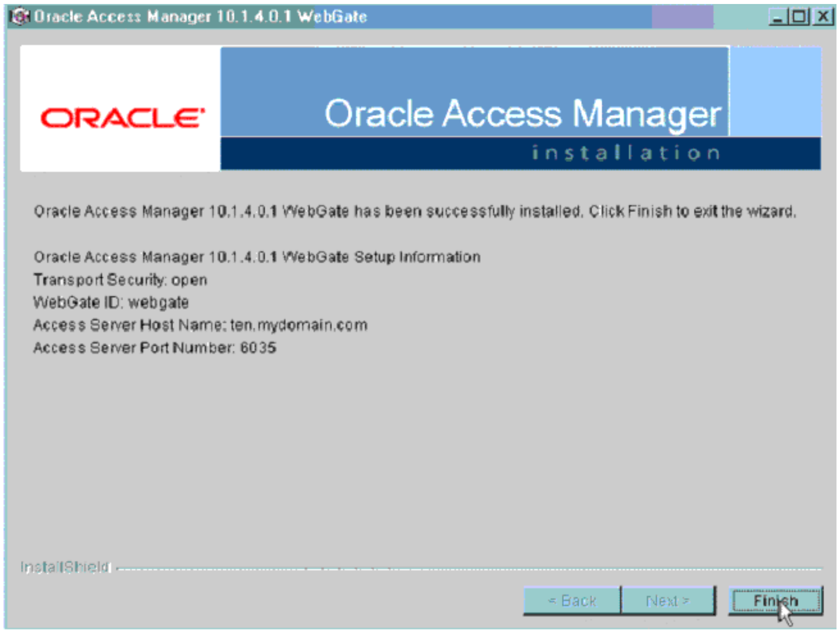
Contents

Contacting Oracle

If you have questions about installing or configuring NetPoint, please contact Oracle Customer Care at (800 833-3536 or check this link http://www.oracle.com/corporate/contact/index.html.

Oracle

9. You can review the WebGate for IIS configuration settings and click **Finish**.



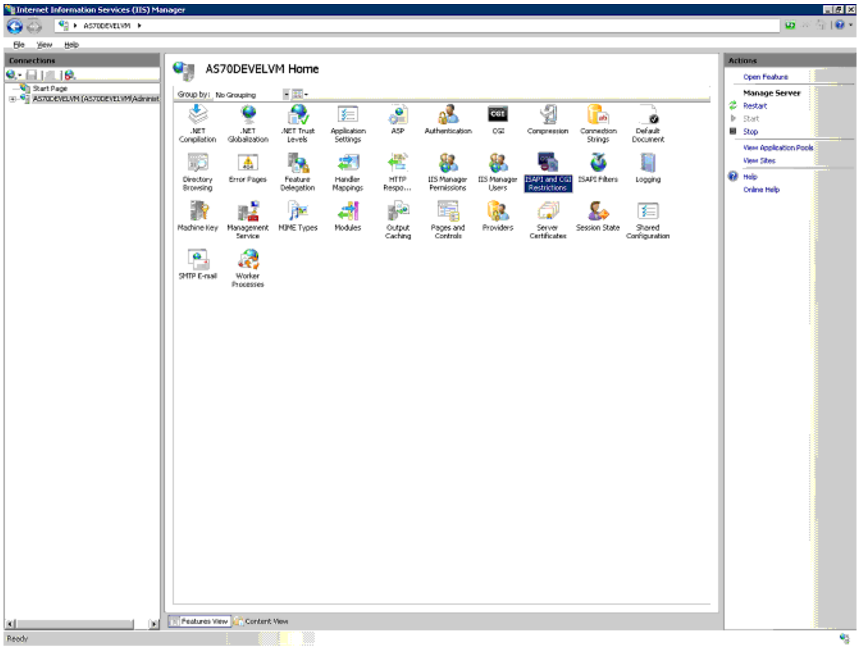
Oracle Access Manager 10.1.4.0.1 WebGate has been successfully installed. Click Finish to exit the wizard.

Oracle Access Manager 10.1.4.0.1 WebGate Setup Information
Transport Security: open
WebGate ID: webgate
Access Server Host Name: ten.mydomain.com
Access Server Port Number: 6035

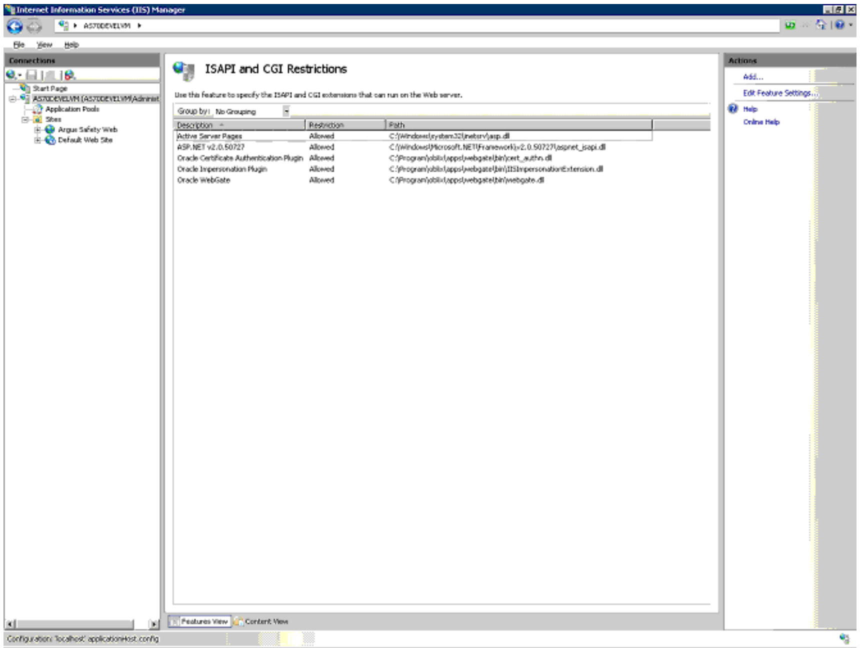
Configuring WebGate on Windows Server 2008 and Windows Server 2012

This section describes the procedure to install WebGate on Windows Server 2008 and Windows Server 2012. Before following this procedure, ensure that you have already installed webgate on Windows 2008 and Windows 2012 servers.

1. Open IIS manager and navigate to the top level node. On the home page, double click **ISAPI and CGI restrictions** to open the feature.



2. The following screen appears:



ISAPI and CGI Restrictions

Use this feature to specify the ISAPI and CGI extensions that can run on the Web server.

Group by: No Grouping

Description	Restriction	Path
Active Server Pages	Allowed	C:\Windows\system32\inetsrv\asp.dll
ASP.NET v2.0.50727	Allowed	C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll
Oracle Certificate Authentication Plugin	Allowed	C:\Program\oblix\apps\webgate\bin\cert_authn.dll
Oracle Impersonation Plugin	Allowed	C:\Program\oblix\apps\webgate\bin\IISImpersonationExtension.dll
Oracle WebGate	Allowed	C:\Program\oblix\apps\webgate\bin\webgate.dll

3. You have to correct the path for the following DLLs to reflect the path where you have installed the WebGate. To do this, double click the DLL entry and you will see the **Edit ISAPI or GCI Restrictions** dialog box as shown below. In this dialog box, enter the path given in the following table and click **OK**.

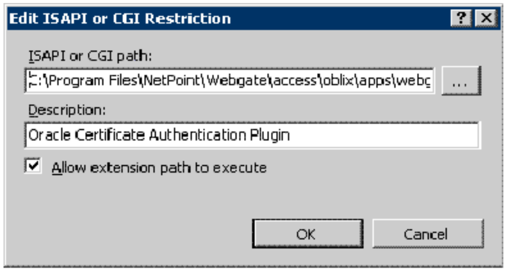
Table 15–5 Default path for DLL

DLL Name	Default Installation Path
Oracle Certificate Authentication Plugin	`C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\cert_authn.dll`

Table 15–5 (Cont.) Default path for DLL

DLL Name	Default Installation Path
Oracle Impersonation Plugin	`C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\IISImpersonationExtension.dll`
Oracle WebGate	`C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\webgate.dll`

Note: For Windows 2008 R2 and Windows 2012 R2, the DLLs must be manually added by clicking on the Add link in the right-most pane.

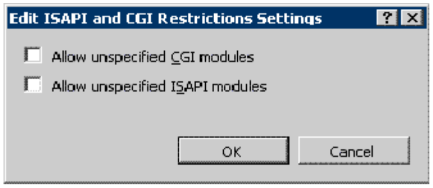

Edit ISAPI or CGI Restriction

ISAPI or CGI path: C:\Program Files\NetPoint\Webgate\access\oblix\apps\webg

Description: Oracle Certificate Authentication Plugin

☑ Allow extension path to execute

4. Click **Edit Feature Settings** in the **Actions** panel in the right. The following dialog box appears:

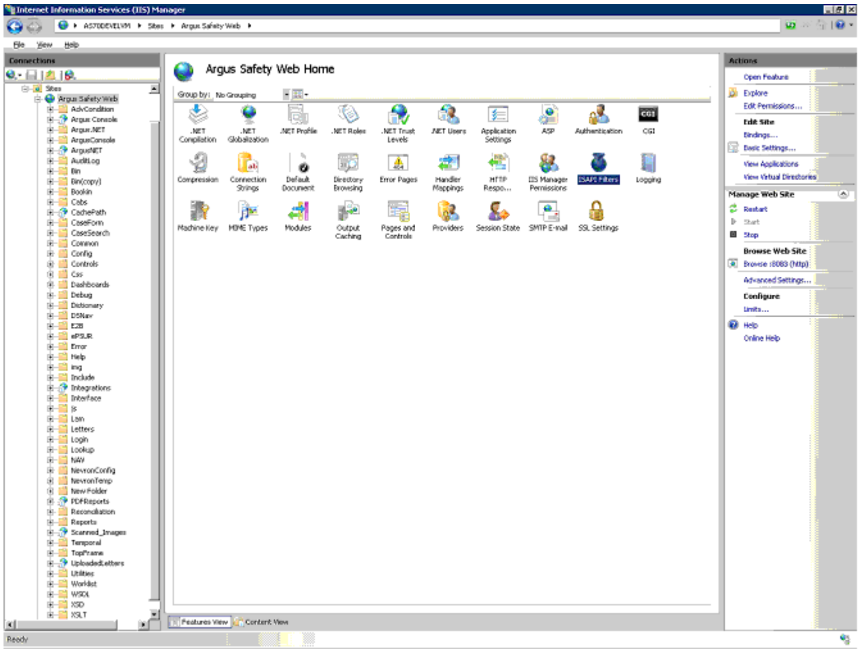

Edit ISAPI and CGI Restrictions Settings

☐ Allow unspecified CGI modules

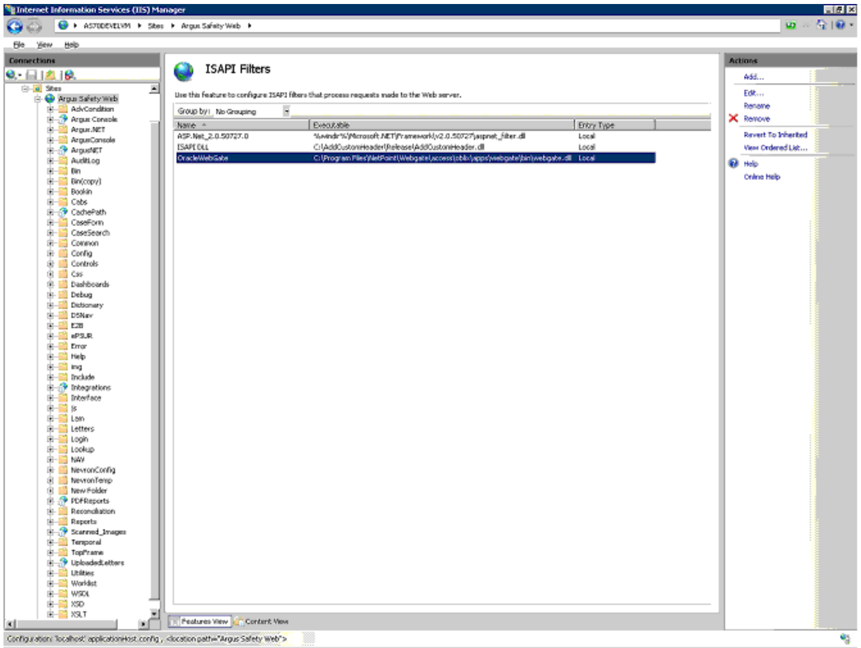
☐ Allow unspecified ISAPI modules

5. Check both the boxes and click **OK**.

6. Click **Argus Safety Web** node, which will open the home page for the application as shown below.



7. Click **ISAPI Filters** and the following screen appears:



ISAPI Filters

Use this feature to configure ISAPI filters that process requests made to the Web server.

Group by: No Grouping

Name	Executable	Entry Type
ASP.Net_2.0.50727.0	%windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_filter.dll	Local
ISAPI DLL	C:\AddCustomHeader\Release\AddCustomHeader.dll	Local
OracleWebGate	C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\webgate.dll	Local

Configuration: 'localhost' applicationHost.config , <location path="Argus Safety Web">

8. Double click **OracleWebGate** and enter the path to where you have installed WebGate. The default path is `C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\webgate.dll`

9. You will now have to remove the `<add segment="bin"/>` entry from applicationhost.config file. Take a backup of the file before you make the following changes:

   a. Navigate to `Windows\System32\inetsrv\config` and open the applicationHost.config file.

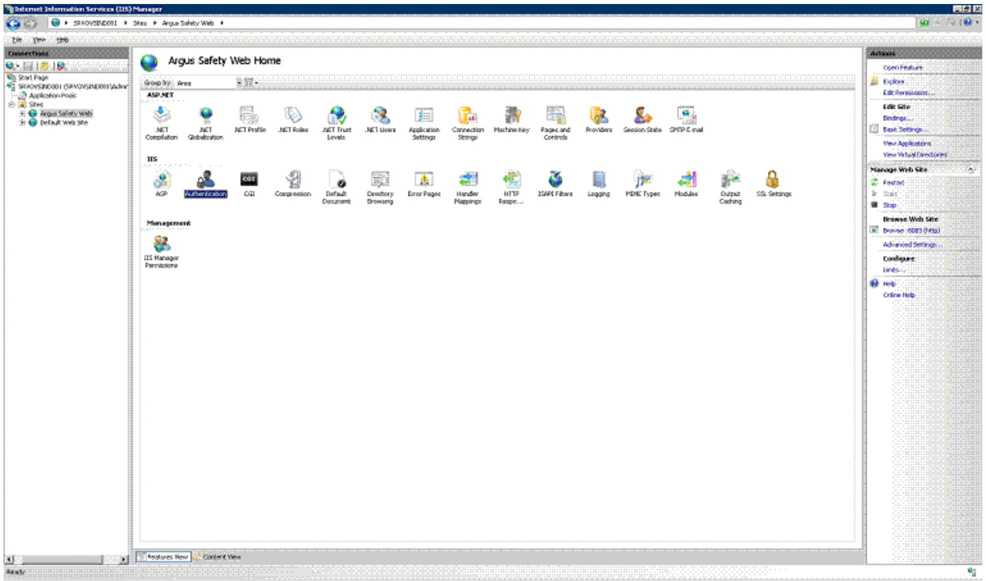
   b. Search for the `<hiddenSegments>` module.

c. Remove the entry `<add segment="bin"/>` if it is present.

d. Save the file.

10. Restart IIS for the changes to take effect.

After restarting IIS, open IIS Manager and navigate to **Sites** > **Argus Safety Web** > **Authentication** as per the screenshot below:

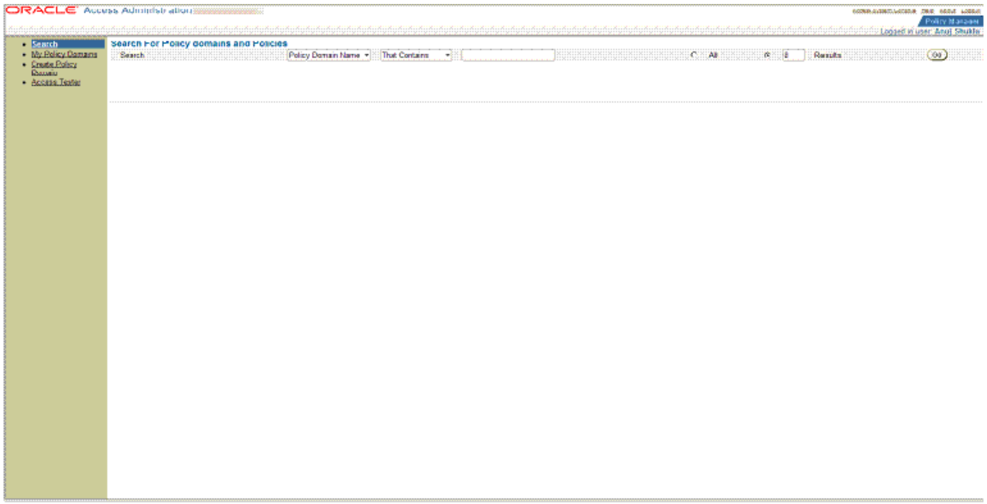


Right click on **Windows Authentication** and check if it is enabled. If yes, then disable it. This completes the WebGate installation on Windows Server 2008 and Windows Server 2012.

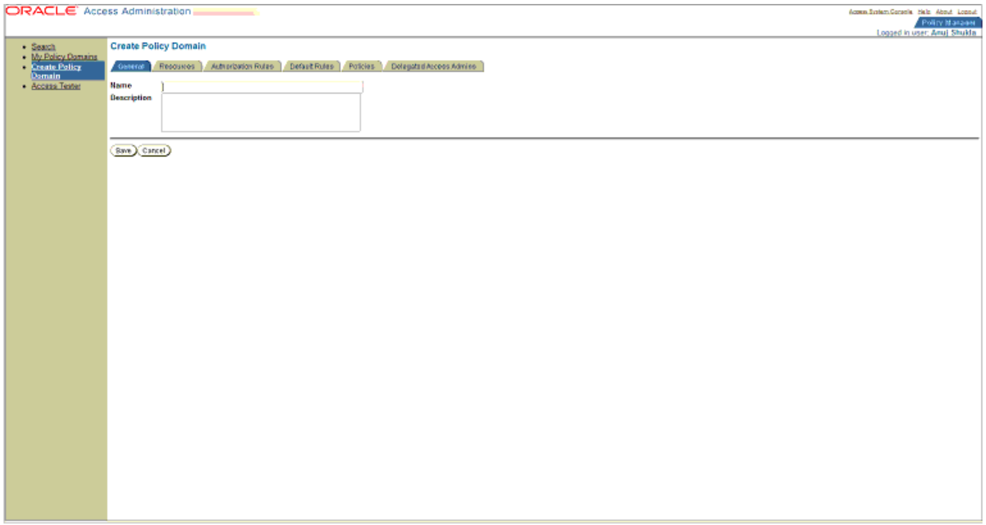
Protecting Files in the Argus Directory

This section describes the procedure to create a policy to protect files under the Argus directory.

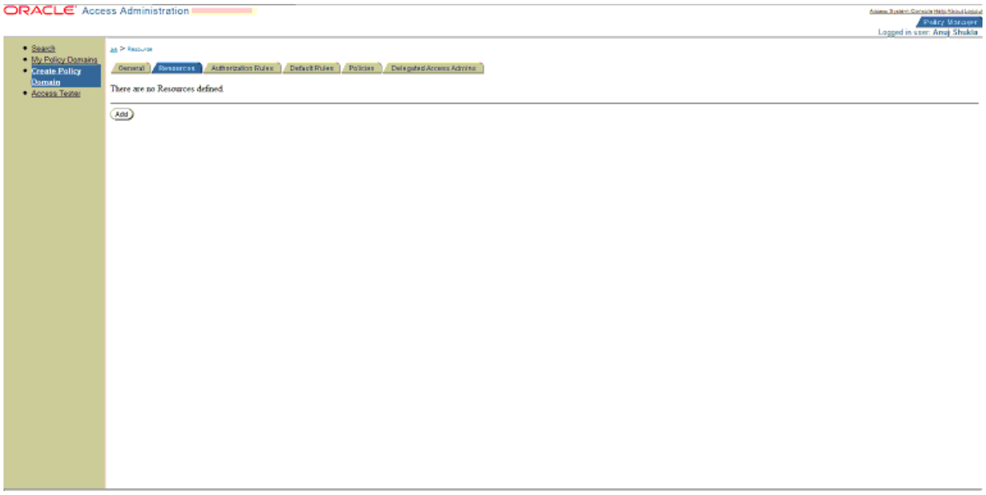
1. Navigate to the policy manager console and click **Create Policy Domain**.



2. Under the **General** tab provide a name and description and click **Save**.

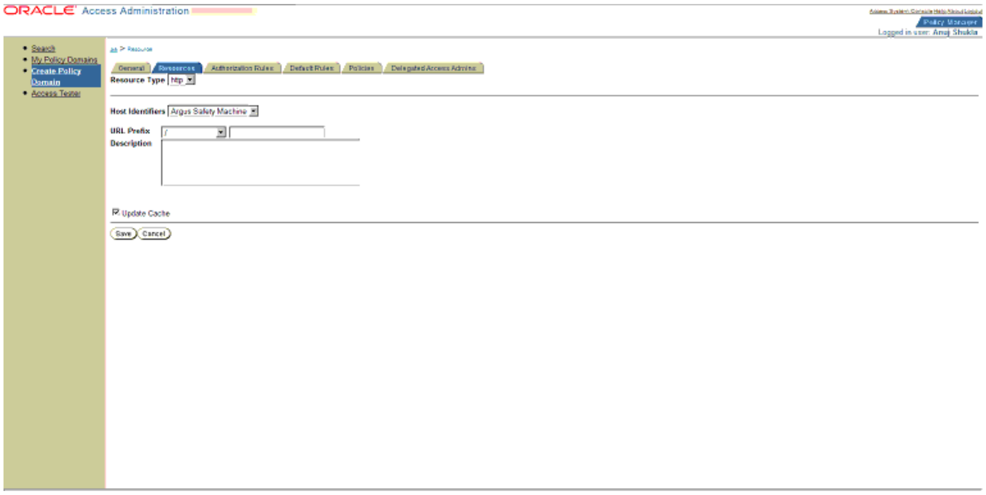


3. Click the **Resource** tab and then click **Add**.



There are no Resources defined.

4. Select **Host Identifier** from the drop-down list and select **URL Prefix** as / and provide a description. Click **Save**.



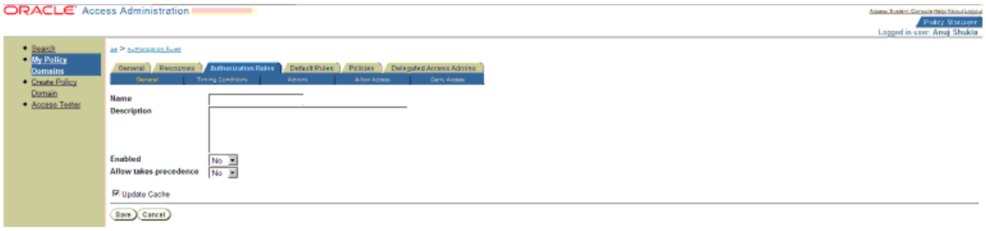
Resource Type: http

Host Identifiers: Argus Safety Machine

URL Prefix: /

☑ Update Cache

5. Click the **Authorization Rules** tab and select the **General** sub tab.



Name

Description

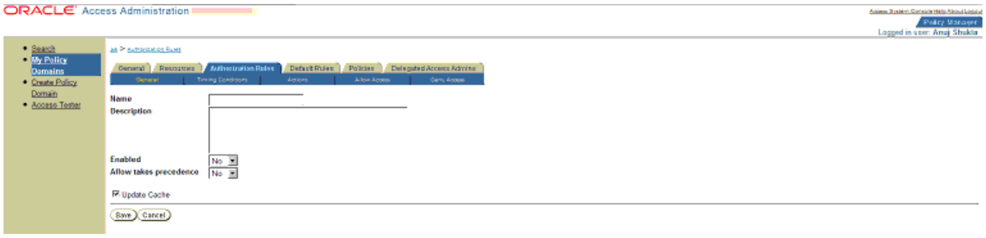
Enabled: No

Allow takes precedence: No

☑ Update Cache

6. Enter the following details in this tab and click **Save**:

- **Name** - Enter an appropriate name for the rule.
- **Description** - Enter a description for the rule.
- **Enabled** - Select **Yes** from the drop-down list.
- **Allow takes precedence** - Select **Yes** from the drop-down list.



Name

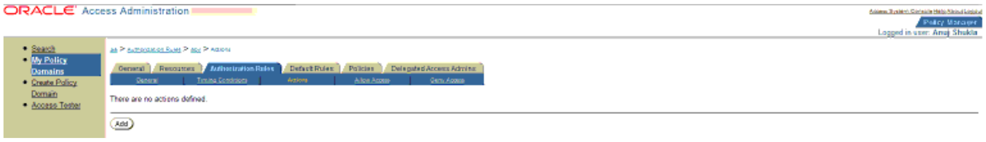
Description

Enabled: No

Allow takes precedence: No

☑ Update Cache

7. Click the **Actions** sub tab., and click **Add**.

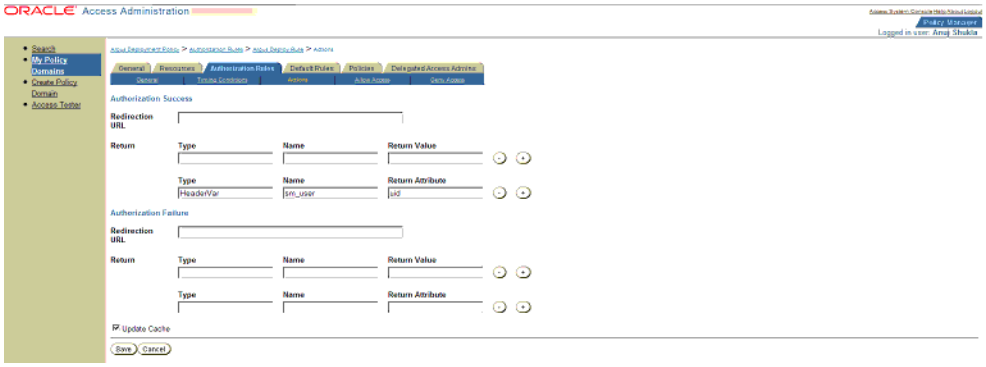


There are no actions defined.

8. In the **Authorization Success** section under **Return**, enter the following values and click **Save**:

Table 15–6 Values for Return field

Field name	Value
Type	HeaderVar
Name	SM_USER
Return Attribute	uid



Authorization Success

Redirection URL

Return — Type / Name / Return Value

Type: HeaderVar — Name: sm_user — Return Attribute: uid

Authorization Failure

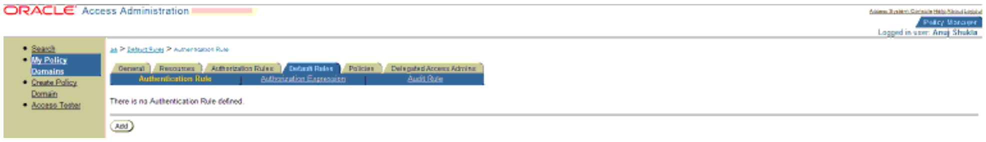
Redirection URL

Return — Type / Name / Return Value

Type / Name / Return Attribute

☑ Update Cache

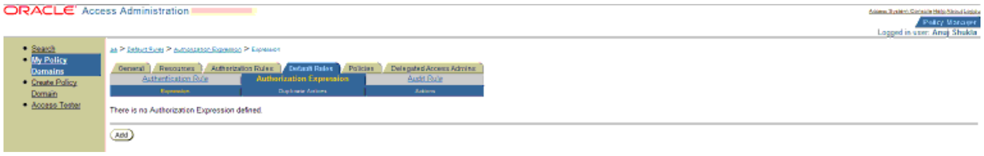
9. Navigate to **Default Rules** > **Authentication Rule**. Click **Add**.



There is no Authentication Rule defined.

10. Enter details for Name and decsription and select Authentication Scheme as **Oracle Access and Identity Basic Over LDAP**. Click **Save**.

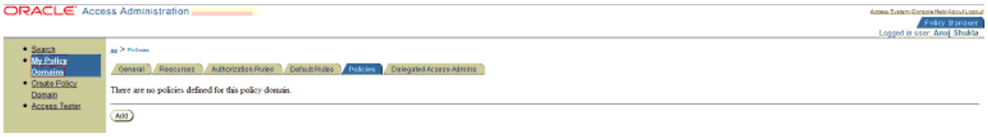
11. Click the **Authorization Expression** sub tab and click **Add**.



There is no Authorization Expression defined.

12. Select **Authorization Rule** from the drop-down. Click **Add** and then click **Save**.

13. Click **Policies** and then click **Add**.

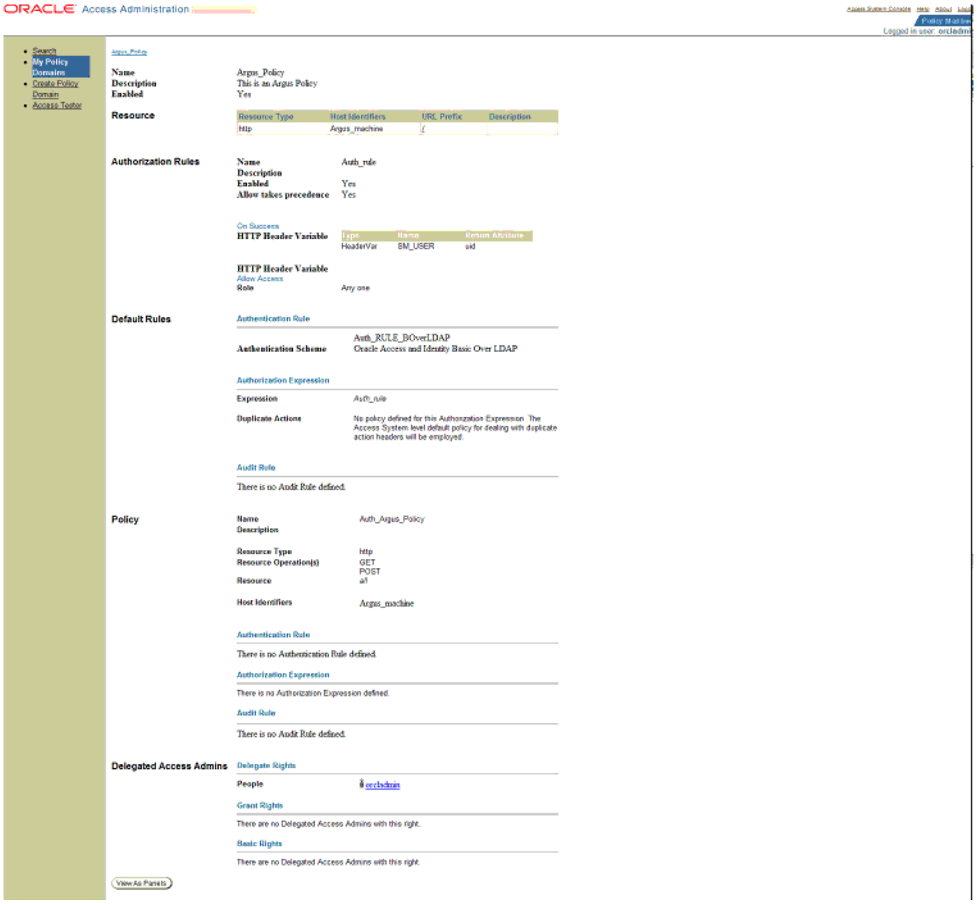


There are no policies defined for this policy domain.

14. Provide the following details and click **Save**:
    - **Name** - Name of the policy.
    - **Description** - Description of the policy.
    - **Resource type** - Select as http.
    - **Resource Operation(s)** - Select as Get and Post.

15. Now restart the Identity service and Access service. Also restart the IIS Argus Web Server. This completes the webgate installation and SSO policy configuration.

After you have completed the above steps your policy will appear as shown below:



Name Argus_Policy
Description This is an Argus Policy
Enabled Yes

Resource

Resource Type	Host Identifiers	URL Prefix	Description
http	Argus_machine	/	

Authorization Rules

Name Auth_rule
Description
Enabled Yes
Allow takes precedence Yes

On Success
HTTP Header Variable

Type	Name	Return Attribute
HeaderVar	SM_USER	uid

HTTP Header Variable
Allow Access
Role Any one

Default Rules

Authentication Rule

Auth_RULE_BOverLDAP
Authentication Scheme Oracle Access and Identity Basic Over LDAP

Authorization Expression

Expression *Auth_rule*

Duplicate Actions No policy defined for this Authorization Expression. The Access System level default policy for dealing with duplicate action headers will be employed.

Audit Rule

There is no Audit Rule defined.

Policy

Name Auth_Argus_Policy
Description

Resource Type http
Resource Operation(s) GET
POST
Resource all

Host Identifiers Argus_machine

Authentication Rule

There is no Authentication Rule defined.

Authorization Expression

There is no Authorization Expression defined.

Audit Rule

There is no Audit Rule defined.

Delegated Access Admins

Delegate Rights

People orcladmin

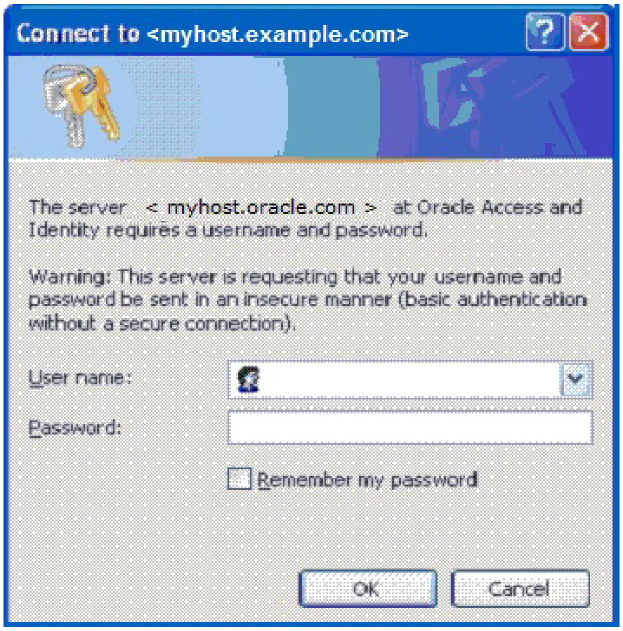
Grant Rights

There are no Delegated Access Admins with this right.

Basic Rights

There are no Delegated Access Admins with this right.

To verify if you have correctly configured the policy check for the following prompt when you open the Argus URL:



The server < myhost.oracle.com > at Oracle Access and Identity requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

☐ Remember my password

Installation and Configuration of Oracle Web Tier Suite

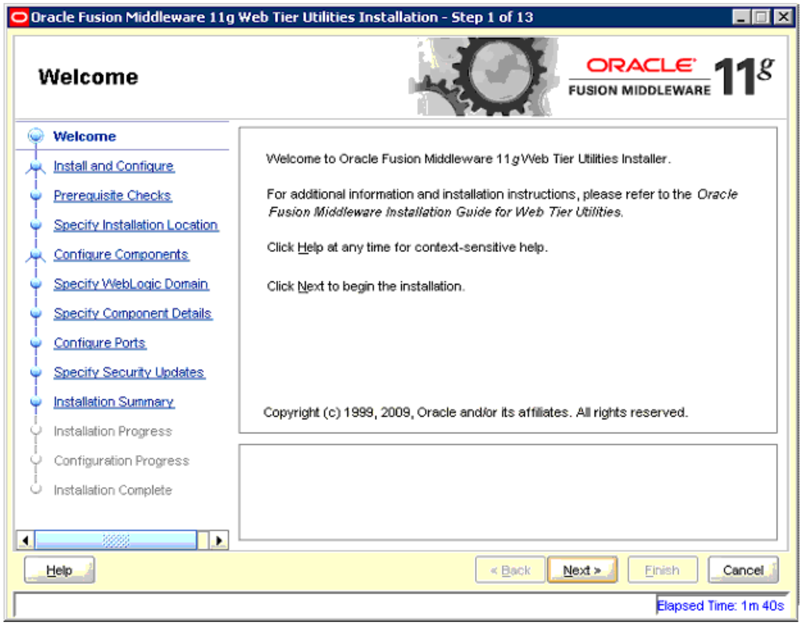
The Oracle Web Tier Suite consists of following products:

- 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

Welcome to Oracle Fusion Middleware 11*g* Web Tier Utilities Installer.

For additional information and installation instructions, please refer to the *Oracle Fusion Middleware Installation Guide for Web Tier Utilities.*

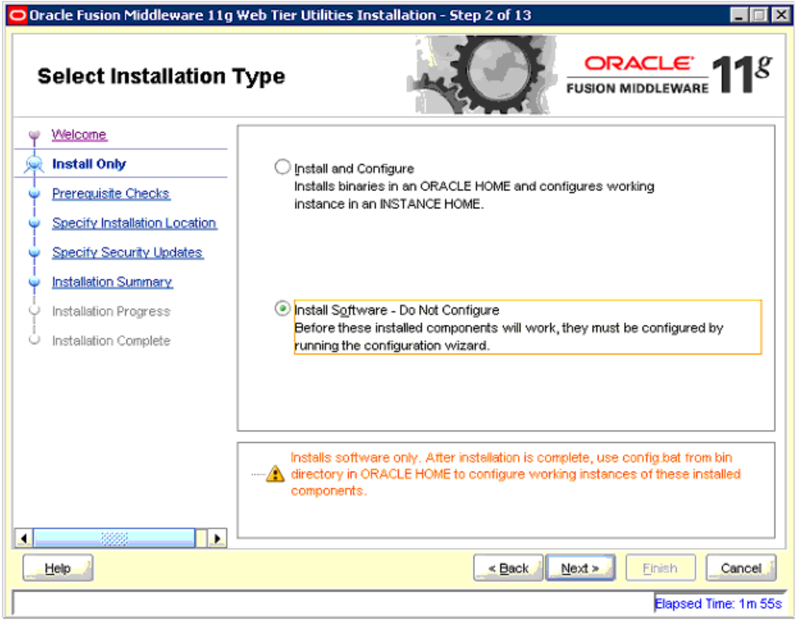
Click Help at any time for context-sensitive help.

Click Next to begin the installation.

Copyright (c) 1999, 2009, Oracle and/or its affiliates. All rights reserved.

Elapsed Time: 1m 40s

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

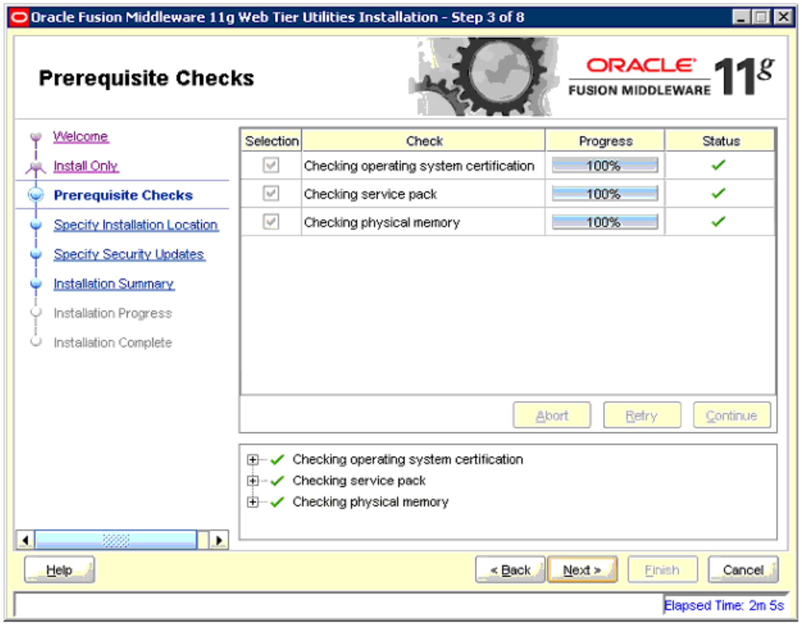
○ Install and Configure
Installs binaries in an ORACLE HOME and configures working instance in an INSTANCE HOME.

● Install Software - Do Not Configure
Before these installed components will work, they must be configured by running the configuration wizard.

Installs software only. After installation is complete, use config.bat from bin directory in ORACLE HOME to configure working instances of these installed components.

Elapsed Time: 1m 55s

4. In the next screen, the installer performs Prerequisite Checks. Click **Next** to continue.



Oracle Fusion Middleware 11g Web Tier Utilities Installation - Step 3 of 8

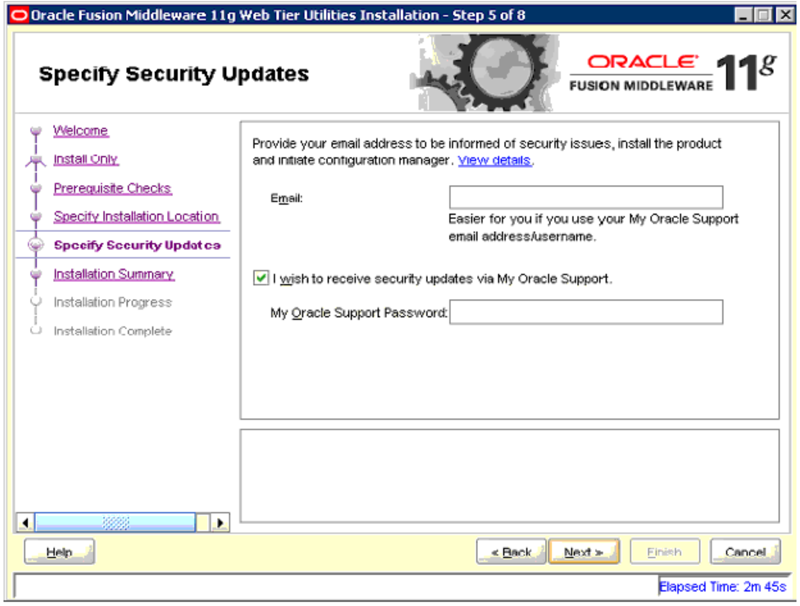
Prerequisite Checks

Selection	Check	Progress	Status
☑	Checking operating system certification	100%	✓
☑	Checking service pack	100%	✓
☑	Checking physical memory	100%	✓

⊞ ✓ Checking operating system certification
⊞ ✓ Checking service pack
⊞ ✓ Checking physical memory

Elapsed Time: 2m 5s

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 Updates

Provide your email address to be informed of security issues, install the product and initiate configuration manager. View details.

Email:

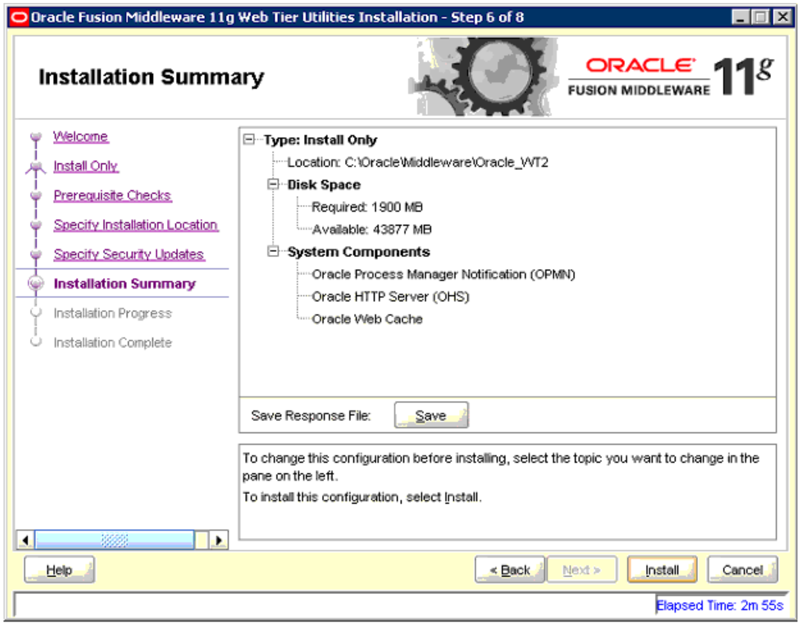
Easier for you if you use your My Oracle Support email address/username.

☑ I wish to receive security updates via My Oracle Support.

My Oracle Support Password:

Elapsed Time: 2m 45s

6. On the installation summary screen, click **Install**. This will install Oracle Web Tier.



Oracle Fusion Middleware 11g Web Tier Utilities Installation - Step 6 of 8

Installation Summary

- Type: Install Only
  - Location: C:\Oracle\Middleware\Oracle_WT2
  - Disk Space
    - Required: 1900 MB
    - Available: 43877 MB
  - System Components
    - Oracle Process Manager Notification (OPMN)
    - Oracle HTTP Server (OHS)
    - Oracle Web Cache

Save Response File: Save

To change this configuration before installing, select the topic you want to change in the pane on the left.

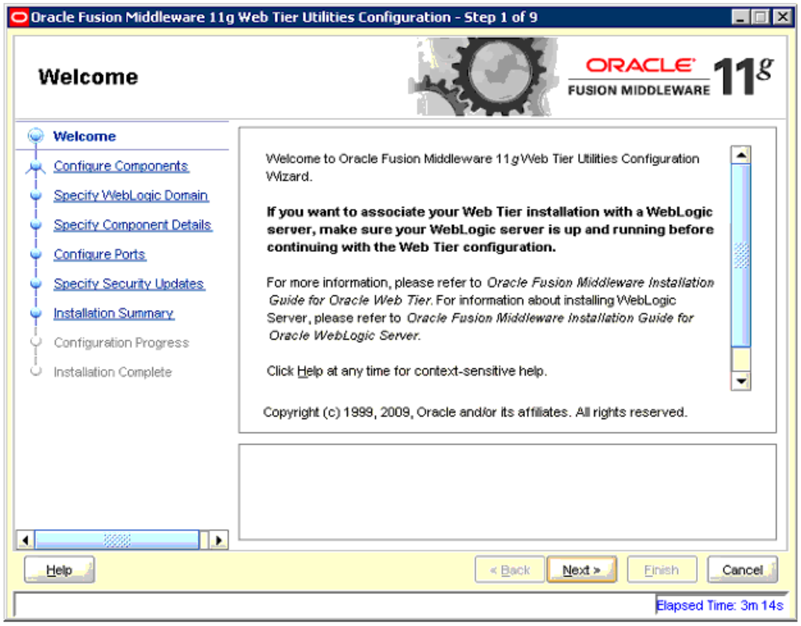
To install this configuration, select Install.

Elapsed Time: 2m 55s

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.



Oracle Fusion Middleware 11g Web Tier Utilities Configuration - Step 1 of 9

Welcome

Welcome to Oracle Fusion Middleware 11g Web Tier Utilities Configuration Wizard.

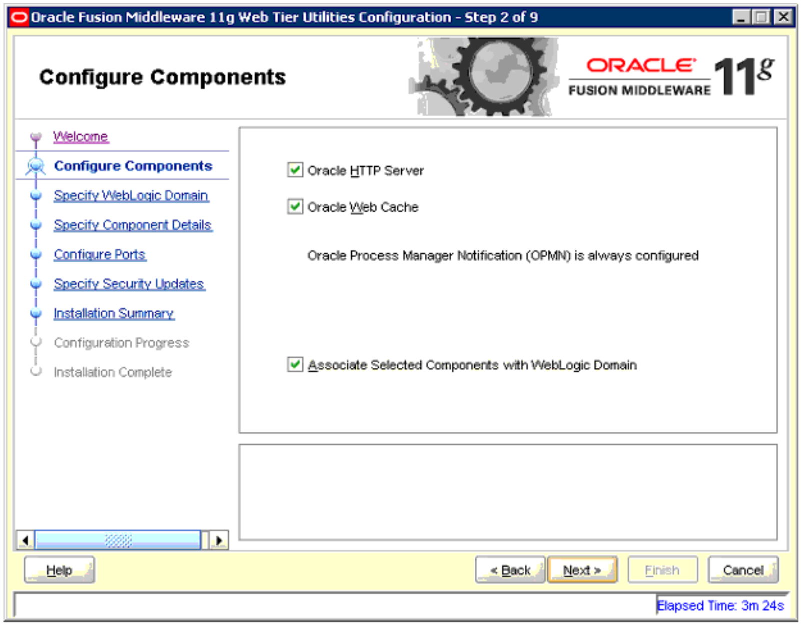
If you want to associate your Web Tier installation with a WebLogic server, make sure your WebLogic server is up and running before continuing with the Web Tier configuration.

For more information, please refer to *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*. For information about installing WebLogic Server, please refer to *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

Click Help at any time for context-sensitive help.

Copyright (c) 1999, 2009, Oracle and/or its affiliates. All rights reserved.

2. In the next screen, click **Next**.



Oracle Fusion Middleware 11g Web Tier Utilities Configuration - Step 2 of 9

Configure Components

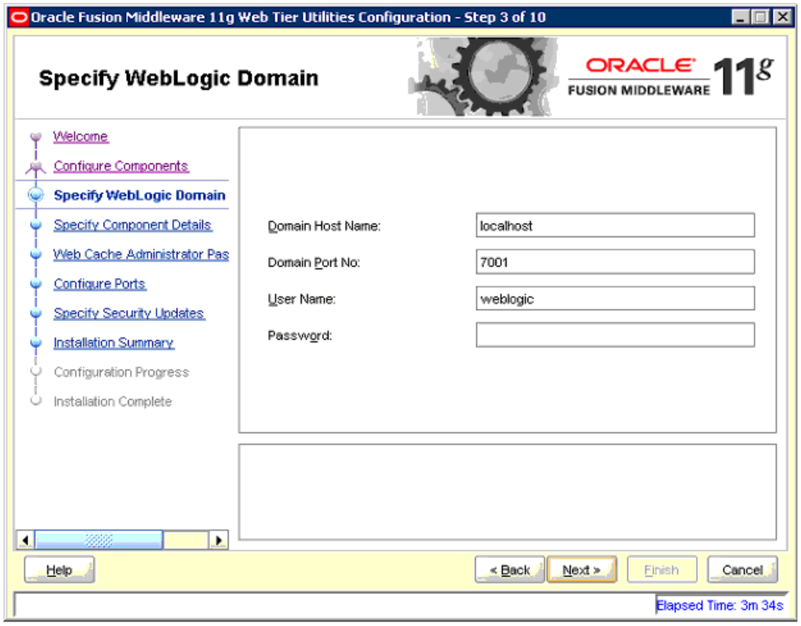
☑ Oracle HTTP Server

☑ Oracle Web Cache

Oracle Process Manager Notification (OPMN) is always configured

☑ Associate Selected Components with WebLogic Domain

3. Enter details of the weblogic server and click **Next**.


Oracle Fusion Middleware 11g Web Tier Utilities Configuration - Step 3 of 10

Specify WebLogic Domain

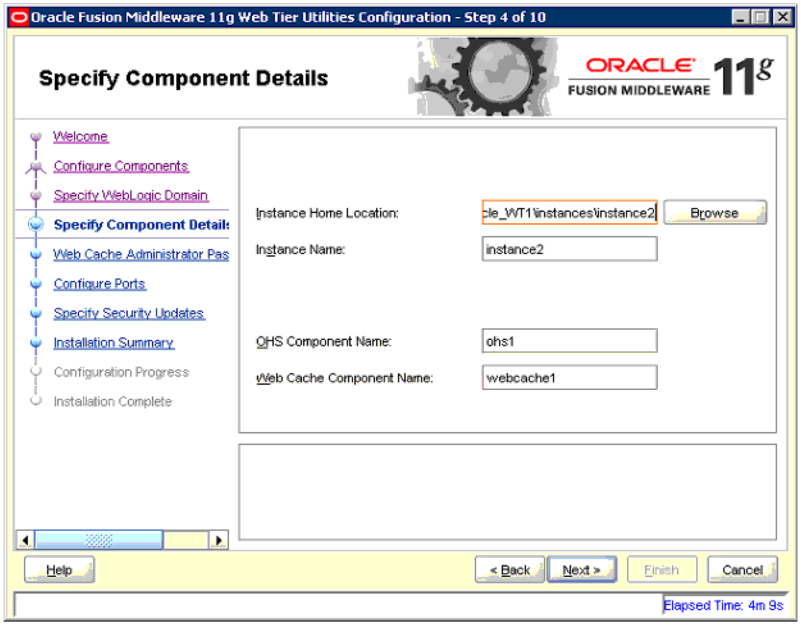
Domain Host Name: localhost

Domain Port No: 7001

User Name: weblogic

Password:

4. In the next screen, click **Next**.


Oracle Fusion Middleware 11g Web Tier Utilities Configuration - Step 4 of 10

Specify Component Details

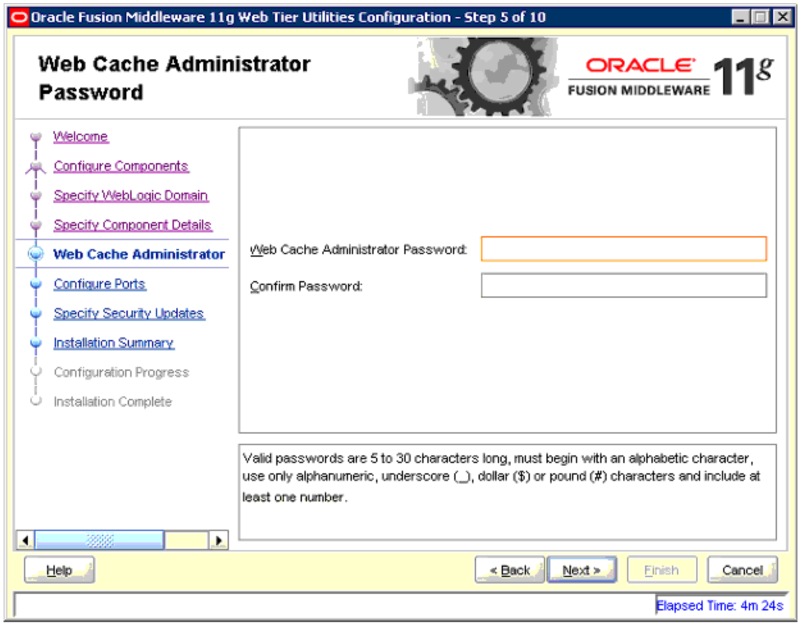
Instance Home Location: :le_WT1\instances\instance2

Instance Name: instance2

OHS Component Name: ohs1

Web Cache Component Name: webcache1

5. Enter a password for Web Cache and click **Next**.



Web Cache Administrator Password:

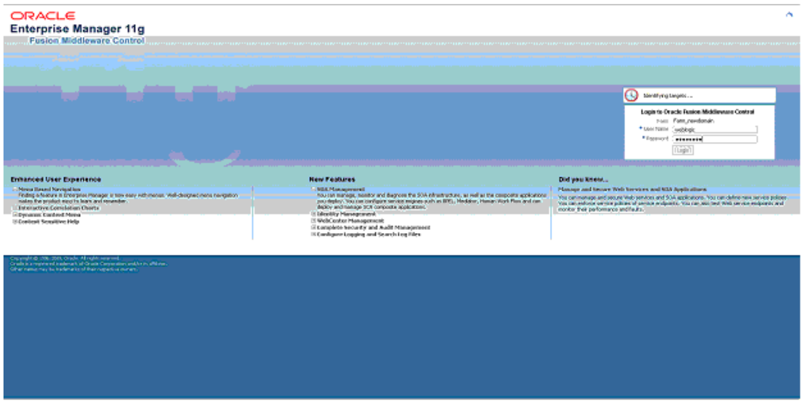
Confirm Password:

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.

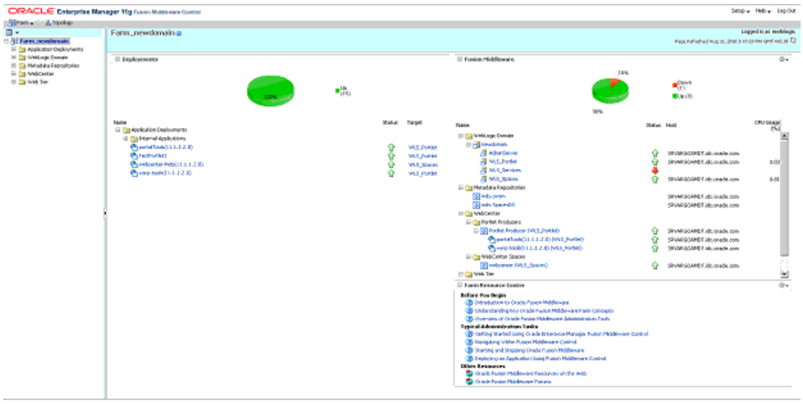
6. Select auto configuration port in the Configure Ports screen. Click **Next**.

7. Skip security updates for now and then click **Next** to continue configuring the Web Tier.

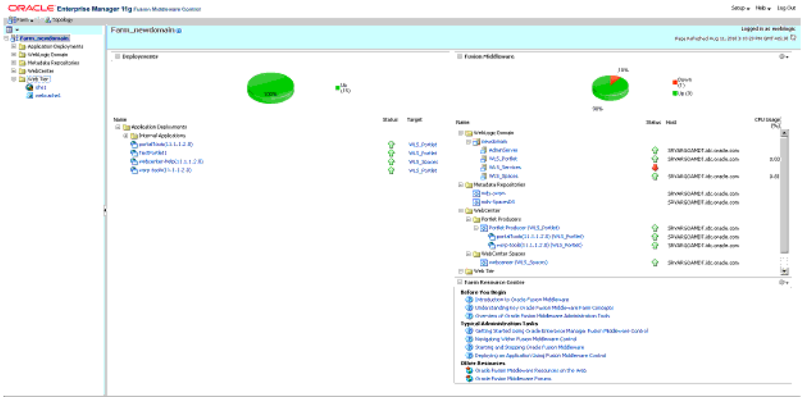
8. After the configuration, navigate to http://localhost:7001/em. This will open the Enterprise Management console for Fusion Middleware as shown below. Log in using the same credentials as that of the WebLogic server.



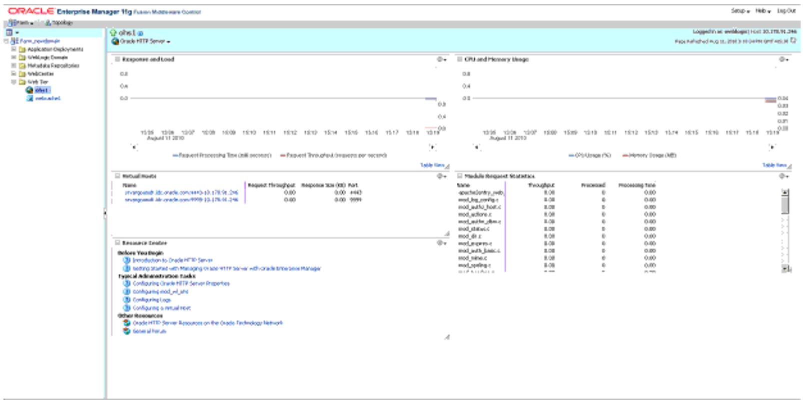
9. Click the Web Tier node on the left.



10. Click the name of the OHS instance that you have created during installation. In the following example, the OHS instance is ohs1.



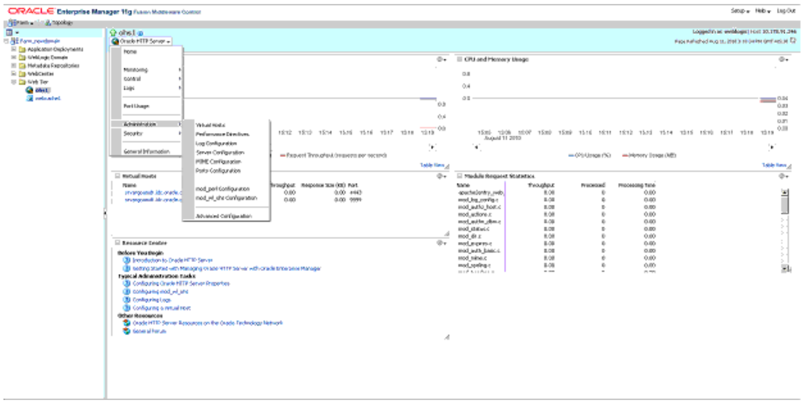
11. You will see all the details related to Oracle Http server on this console.


ORACLE Enterprise Manager 11g Fusion Middleware Control
ohs1
Oracle HTTP Server
Response and Load
CPU and Memory Usage
Virtual Hosts
Module Request Statistics
Resource Center
Before You Begin
Introduction to Oracle HTTP Server
Typical Administration Tasks
Configuring Oracle HTTP Server Properties
Configuring mod_wl_ohs
Configuring Logs
Other Resources

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.



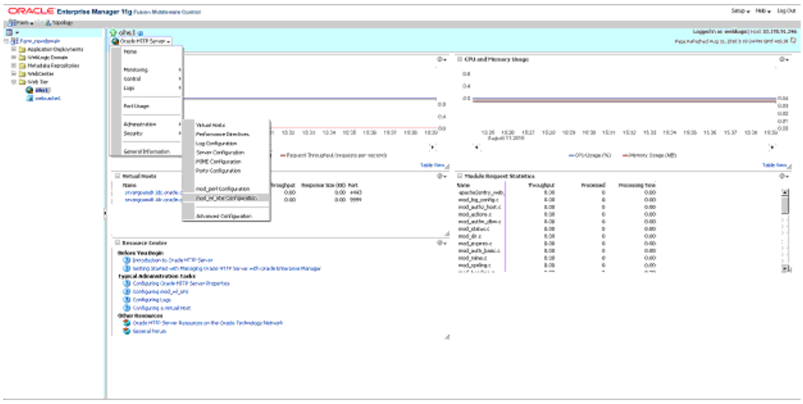
This menu allows you to perform the following administrative tasks:

- 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.

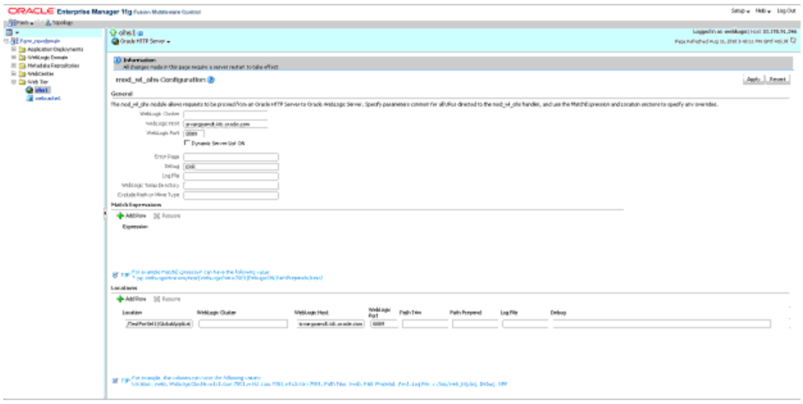
Configuring Oracle Http Server as Reverse Proxy Server for WebLogic

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.



3. The following screen appears:



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.

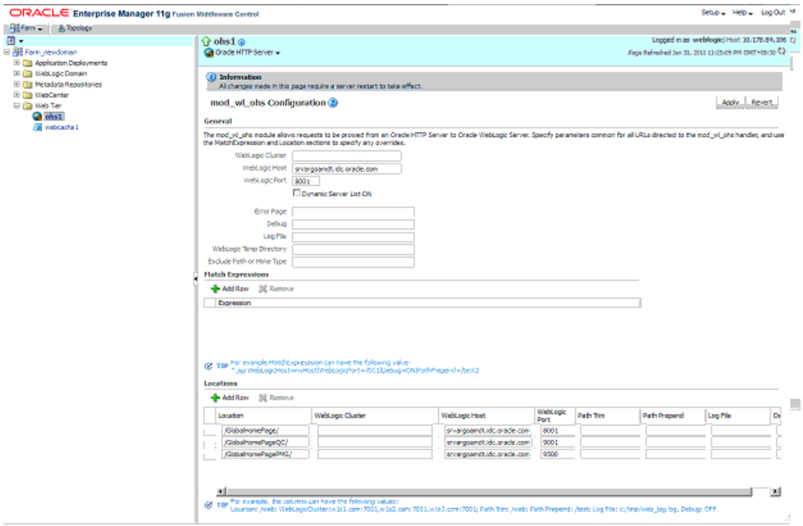
In the Locations Section:

- 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/GlobalHome`, 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.



Information
All changes made in this page require a server restart to take effect.

mod_wl_ohs Configuration

General

The mod_wl_ohs module allows requests to be proxied from an Oracle HTTP Server to Oracle WebLogic Server. Specify parameters common for all URLs directed to the mod_wl_ohs handler, and use the MatchExpression and Location sections to specify any overrides.

WebLogic Cluster	
WebLogic Host	srvargoandt.idc.oracle.com
WebLogic Port	8001
	□ Dynamic Server List ON
Error Page	
Debug	
Log File	
WebLogic Temp Directory	
Exclude Path or Mime Type	

Match Expressions

Expression

TIP For example MatchExpression can have the following value:
*.jsp WebLogicHost=myHost|WebLogicPort=7001|Debug=ON|PathPrepend=/test2

Locations

Location	WebLogic Cluster	WebLogic Host	WebLogic Port	Path Trim	Path Prepend	Log File
/GlobalHomePage/		srvargoandt.idc.oracle.com	8001			
/GlobalHomePageQC/		srvargoandt.idc.oracle.com	9001			
/GlobalHomePagePMG/		srvargoandt.idc.oracle.com	9500			

TIP For example, the columns can have the following values:
Location: /web; WebLogicCluster:w1s1.com:7001,w1s2.com:7001,w1s3.com:7001; Path Trim: /web; Path Prepend: /test; Log File: c:/tmp/web_log.log, Debug: OFF

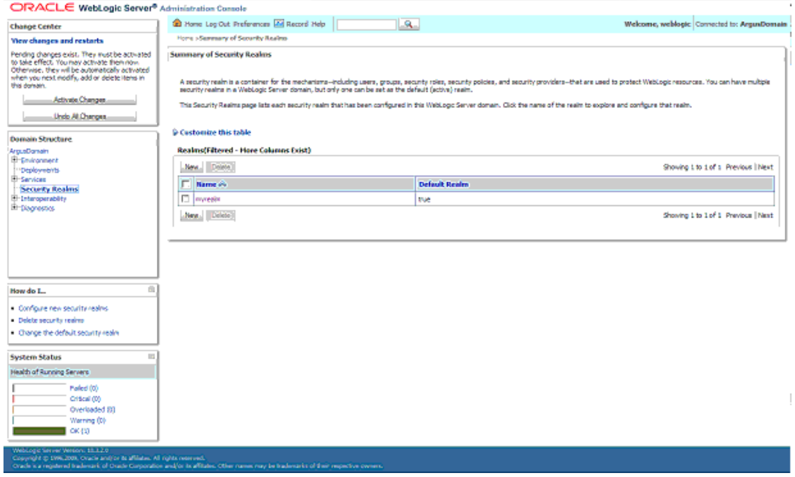
Configuring the WebCenter Security Provider for Identity Assertion

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.



Pending changes exist. They must be activated to take effect. You may activate them now. Otherwise, they will be automatically activated when you next modify, add or delete items in this domain.

Summary of Security Realms

A security realm is a container for the mechanisms—including users, groups, security roles, security policies, and security providers—that are used to protect WebLogic resources. You can have multiple security realms in a WebLogic Server domain, but only one can be set as the default (active) realm.

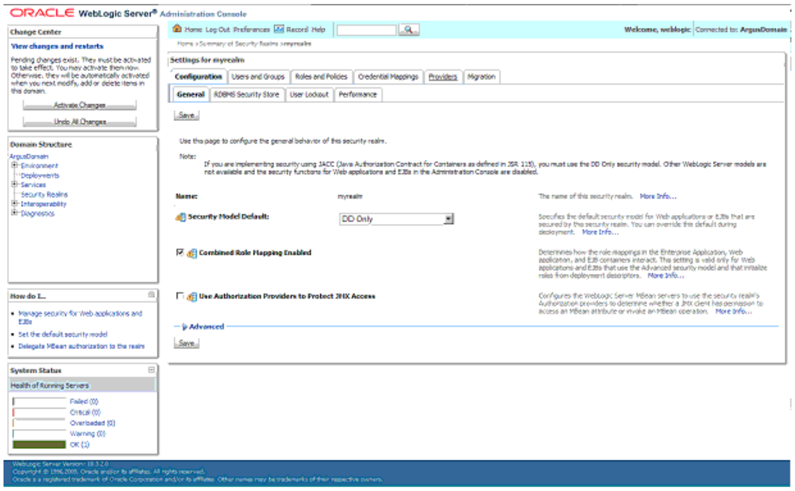
This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

WebLogic Server Version: 10.3.2.0
Copyright © 1996,2009, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

2. Navigate to Providers > Authentication. Click **New** to create a new provider.



Pending changes exist. They must be activated to take effect. You may activate them now. Otherwise, they will be automatically activated when you next modify, add or delete items in this domain.

Settings for myrealm

Use this page to configure the general behavior of this security realm.

Note: If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.

Name: myrealm — The name of this security realm. More Info...

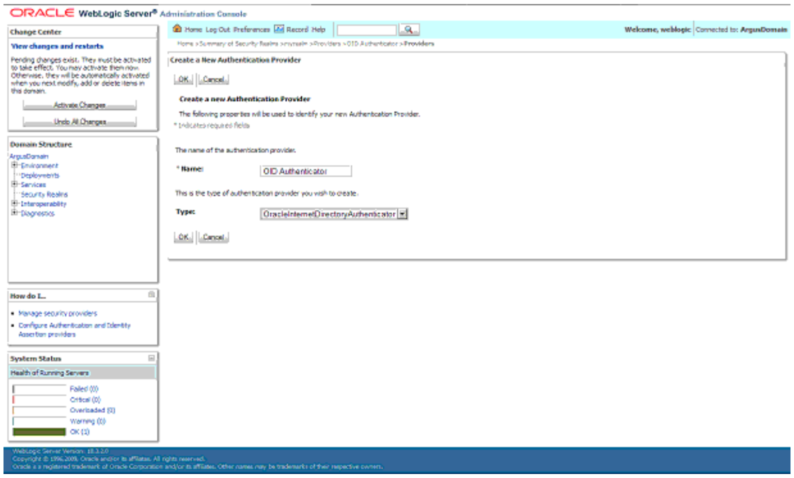
Security Model Default: DD Only — Specifies the default security model for Web applications or EJBs that are secured by this security realm. You can override this default during deployment. More Info...

☑ Combined Role Mapping Enabled — Determines how the role mappings in the Enterprise Application, Web application, and EJB containers interact. This setting is valid only for Web applications and EJBs that use the Advanced security model and that initialize roles from deployment descriptors. More Info...

☐ Use Authorization Providers to Protect JMX Access — Configures the WebLogic Server MBean servers to use the security realm's Authorization providers to determine whether a JMX client has permission to access an MBean attribute or invoke an MBean operation. More Info...

WebLogic Server Version: 10.3.2.0
Copyright © 1996,2009, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

3. Enter **Name** as OID Authenticator and select **type** from the drop-down as OracleInternetDirectoryAuthenticator. Click OK.


ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: ArgusDomain
Home >Summary of Security Realms >myrealm >Providers >OID Authenticator >Providers
Change Center
View changes and restarts
Activate Changes
Undo All Changes
Domain Structure
ArgusDomain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Manage security providers
Configure Authentication and Identity Assertion providers
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (1)
OK
Cancel

Pending changes exist. They must be activated to take effect. You may activate them now. Otherwise, they will be automatically activated when you next modify, add or delete items in this domain.

Create a New Authentication Provider

Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.
* Indicates required fields

The name of the authentication provider.

* Name: OID Authenticator

This is the type of authentication provider you wish to create.

Type: OracleInternetDirectoryAuthenticator

WebLogic Server Version: 10.3.2.0
Copyright © 1996,2009, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

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:

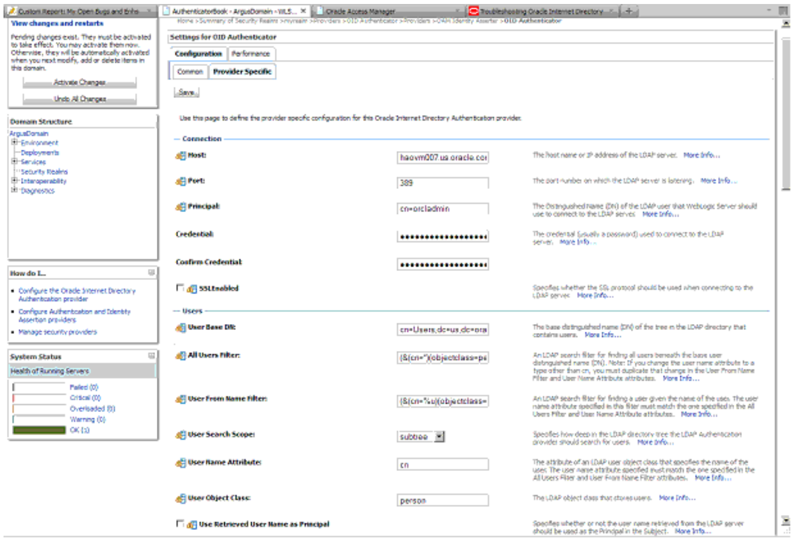
Table 15–7 Values for the Providers Specific tab

Parameter Name	Description	Sample Value
Host	LDAP Hostname	i<myhost.vm.example.com>
Port	LDAP Port	389
Principal	LDAP admin principal	cn=orcladmin
Credential	Password for admin principal (password of cn=orcladmin)	
User Base DN	User Search Base - This value can be obtained by checking the Users realm DN from OID	For example, cn=Users,dc=idc,dc=oracle, dc=com

Table 15–7 (Cont.) Values for the Providers Specific tab

Parameter Name	Description	Sample Value
All Users Filter	Set as `(&(uid=*)(objectclass=person))`	`(&(uid=*)(objectclass=person))`
User Name Attribute	Set to "uid" from "cn"	uid
Group Base DN - Group search base - Same as User Base DN	Group Search Base - The DN used to search the Group, can be checked by Groups DN in OID	For example, cn=Groups,dc=idc,dc=oracle,dc=com

Retain the default values for the remaining attributes. Click **Save**.



Custom Report: My Open Bugs and Enha...
AuthenticatorBook - ArgusDomain - WLS...
Oracle Access Manager
Troubleshooting Oracle Internet Directory
Home >Summary of Security Realms >myrealm >Providers >OID Authenticator >Providers >OAM Identity Asserter >OID Authenticator
View changes and restarts
Activate Changes
Undo All Changes
Domain Structure
ArgusDomain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Configure the Oracle Internet Directory Authentication provider
Configure Authentication and Identity Assertion providers
Manage security providers
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (1)
Configuration
Performance
Common
Provider Specific
Save
More Info...

Pending changes exist. They must be activated to take effect. You may activate them now. Otherwise, they will be automatically activated when you next modify, add or delete items in this domain.

Settings for OID Authenticator

Use this page to define the provider specific configuration for this Oracle Internet Directory Authentication provider.

— Connection

Host: haovm007.us.oracle.co — The host name or IP address of the LDAP server.

Port: 389 — The port number on which the LDAP server is listening.

Principal: cn=orcladmin — The Distinguished Name (DN) of the LDAP user that WebLogic Server should use to connect to the LDAP server.

Credential: •••••••••••••••••• — The credential (usually a password) used to connect to the LDAP server.

Confirm Credential: ••••••••••••••••••

□ SSLEnabled — Specifies whether the SSL protocol should be used when connecting to the LDAP server.

— Users

User Base DN: cn=Users,dc=us,dc=ora — The base distinguished name (DN) of the tree in the LDAP directory that contains users.

All Users Filter: (&(cn=*)(objectclass=pe — An LDAP search filter for finding all users beneath the base user distinguished name (DN). Note: If you change the user name attribute to a type other than cn, you must duplicate that change in the User From Name Filter and User Name Attribute attributes.

User From Name Filter: (&(cn=%u)(objectclass= — An LDAP search filter for finding a user given the name of the user. The user name attribute specified in this filter must match the one specified in the All Users Filter and User Name Attribute attributes.

User Search Scope: subtree — Specifies how deep in the LDAP directory tree the LDAP Authentication provider should search for users.

User Name Attribute: cn — The attribute of an LDAP user object class that specifies the name of the user. The user name attribute specified must match the one specified in the All Users Filter and User From Name Filter attributes.

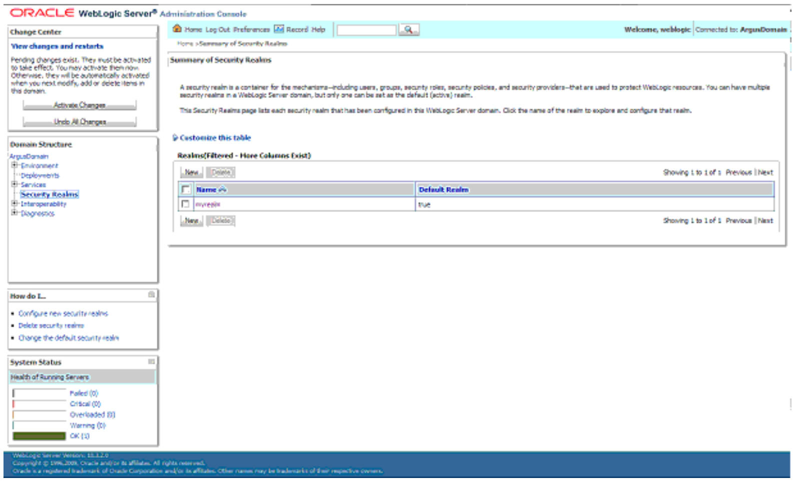
User Object Class: person — The LDAP object class that stores users.

□ 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.

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.



ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic | Connected to: ArgusDomain
Home >Summary of Security Realms
Change Center
View changes and restarts
Activate Changes
Undo All Changes
Domain Structure
ArgusDomain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Configure new security realms
Delete security realms
Change the default security realm
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (1)
Customize this table
New
Delete
Showing 1 to 1 of 1 Previous | Next

Pending changes exist. They must be activated to take effect. You may activate them now. Otherwise, they will be automatically activated when you next modify, add or delete items in this domain.

Summary of Security Realms

A security realm is a container for the mechanisms—including users, groups, security roles, security policies, and security providers—that are used to protect WebLogic resources. You can have multiple security realms in a WebLogic Server domain, but only one can be set as the default (active) realm.

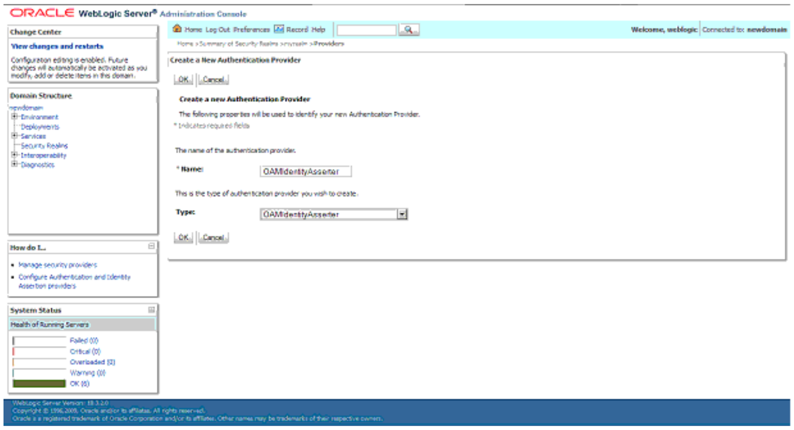
This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

Realms(Filtered - More Columns Exist)

□	Name	Default Realm
□	myrealm	true

WebLogic Server Version: 10.3.2.0
Copyright © 1996,2009, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

2. Click the Providers tab to see list of providers.
3. Click **New**. Enter name as OAMIdentity Asserter and select type as OAMIdentityAsserter.


ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: newdomain
Home >Summary of Security Realms >myrealm >Providers
Change Center
View changes and restarts
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.
Domain Structure
newdomain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Manage security providers
Configure Authentication and Identity Assertion providers
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (6)
OK
Cancel
WebLogic Server Version: 10.3.2.0
Copyright © 1996,2009, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Create a New Authentication Provider

Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.

* Indicates required fields

The name of the authentication provider.

* Name: OAMIdentityAsserter

This is the type of authentication provider you wish to create.

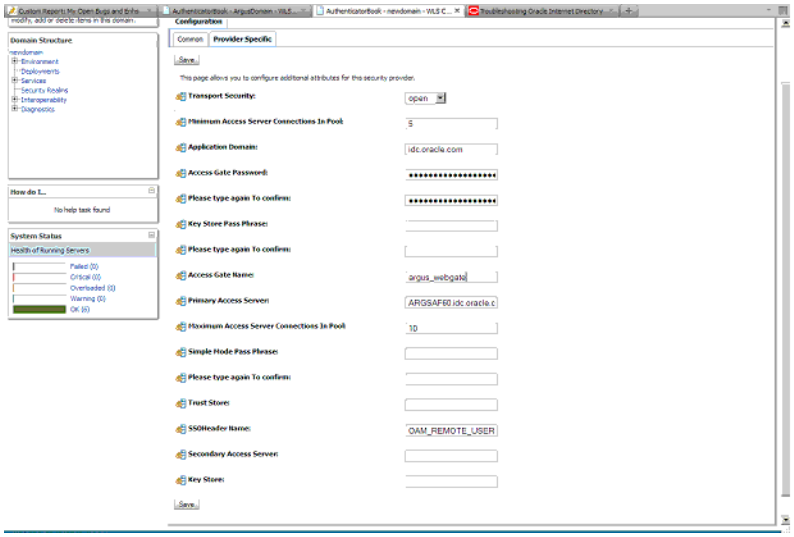
Type: OAMIdentityAsserter

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:

Table 15–8 Values for Provider sub tab

Parameter Name	Description	Sample Value
Transport Security	Encryption type for Access Gate communication	Open
Primary Access Server	Provide OAM server endpoint information in HOST:PORT format	<myhost.idc.example.com:7777>
Access Gate Name	Copy the Access Gate name from the AG created from Step 3.	<myhost.example.com>_AG
Access Gate Password	Type the Access Gate Password configured in access system console	

Retain the default values for the remaining attributes.



This page allows you to configure additional attributes for this security provider.

Transport Security:	open
Minimum Access Server Connections In Pool:	5
Application Domain:	idc.oracle.com
Access Gate Password:	••••••••••••••••••
Please type again To confirm:	••••••••••••••••••
Key Store Pass Phrase:	
Please type again To confirm:	
Access Gate Name:	argus_webgate
Primary Access Server:	ARGSAF60.idc.oracle.c
Maximum Access Server Connections In Pool:	10
Simple Mode Pass Phrase:	
Please type again To confirm:	
Trust Store:	
SSOHeader Name:	OAM_REMOTE_USER
Secondary Access Server:	
Key Store:	

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:

> **Note:** Use these steps to configure Internet Explorer v8.0 and v9.0.

1. Open Internet Explorer v8.0.
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:
   - Locate the Multimedia section.
   - Clear the following check boxes:
     – **Show image download placeholders**
     – **Smart image dithering**
   - Select the **Show Pictures** check box.
   - Clear the **Enable Automatic Image Resizin**g 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 2008 and 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

16

Argus Integrations

This chapter provides information about the Argus Integrations and includes discussions of the following:

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: If Integration is hosted under IIS 7.0, the following command line utility needs to be run as an administrator:

"%windir%\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\ServiceModelReg.exe" -r -y

This command line utility updates the script maps at the IIS metabase roots to ensure the hosted service .svc file is recognized by IIS 7.0.

Note: After installing Argus Integrations, refer to the section The Argus Safety 8.0 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 (outbound)	WHO Drug web service interface provides a mechanism to integrate customer hosted WHO Coding systems with Argus Safety via web services.
Lot Query (outbound)	Lot Number web service interface provides a mechanism to integrate customer hosted central product information systems with Argus Safety via web services
Product Study License(PSL) - (inbound)	PSL web service interface provides a mechanism to integrate customer central system to push/query PSL data 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
Type	An enumeration (currently either "Request" or "Response") 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 outbound message payload and is not required as part of 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">
   00000000-0000-0000-3100-0060000000f0
  </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/v1.1"
     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>
    <b: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 site
conditions</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
   0-0000-0000-7600-0060000000f3
  </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>
    <b: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 Name	Description
MEDICAL_ DICTIONARY	The MEDICAL_DICTIONARY node is the first child node identifying MedDRA integration
Action	An enumeration supporting the following values (currently only one): Auto This attribute will be present in the request when a full hierarchy is required to be passed back to auto encode the term without using the MedDRA Browser. With an "Auto" message, the system requires that an LLT Term be passed in the request. If the full Hierarchy is not found / returned, the system will open the MedDRA Browsers and display the LLTs returned for manual encoding by the user using the local MedDRA instance. If multiple paths are returned, the Primary SOC path will be used.
Source	An enumerated value that specifies additional information that may be required for coding based on origination as follows: ■ Reaction Case Form | Patient Tab | Patient Tab | Other Relevant History | Reaction Case Form | Patient Tab | Parent Tab | Other Relevant History | Reaction ■ Indication Case Form | Patient Tab | Patient Tab | Other Relevant History | Indication Case Form | Patient Tab | Parent Tab | Other Relevant History | Indication ■ Condition should be verbatim Case Form | Patient Tab | Patient Tab | Other Relevant History | Verbatim Case Form | Patient Tab | Parent Tab | Other Relevant History | Verbatim ■ Lab Console | Code Lists | Lab Test Type
Description	Case Form | Events Tab | Event Tab | Description to be Coded Case Form | Events Tab | Death Information | Cause of Death and Autopsy Results | Description as Reported
Diagnosis	Argus Case Form | Analysis Tab | Analysis Tab| Company Diagnosis Syndrome
Term(v 1.0)	The TERM node specifies the information about a specific term that is either being looked up or populated with data and supports 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 Primary SOC path for the selected term. In the event that multiple terms are returned for a MedDRA level, this attribute is only available on the Primary Term
PATHS/PATH (version 1.0)	MedDRA Hierarchy with English Terms only
PATHS/PATH (Version 1.1)	MedDRA Hierarchy with English and Japanese Terms

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>
    <b: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
   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_ DICTIONARY	First Child node under SAFETY_MESSAGE which represents the WHO Drug Dictionary integration
DRUG/DRUG_ NAME	WHO Drug Name that needs to be searched in central WHO Drug Coding system.

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_ 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"
  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>
     <tnsb: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>
    <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>
        <tns:CUSTOM tns:Name="Thermisol" tns:Metadata="Thermisol
Indicator">15</tns:CUSTOM>
        <tns: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
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 ■ EXPIRATION_DATE

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 name	Description
LOT_LOOKUP	First Child node under SAFETY_MESSAGE which represents the Lot Number integration.
LOT	■ LOT Number ■ Expiration Date ■ Custom Provides a mechanism **Name**: Attribute value is used to identify Case Form field that is to be populated with data in the node **Metadata**: 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:attribute>
  </xsl:when>
  <xsl:when test=".='Albumin'">
    <xsl:attribute name="CaseField">CASE_DOSE_REGIMENS_UD_TEXT_3,CASE_
DOSE_REGIMENS_UD_TEXT_4</xsl:attribute>
  </xsl:when>
 </xsl:choose>
</xsl:template>
```

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

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>12US000000001</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>12US000000001</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.

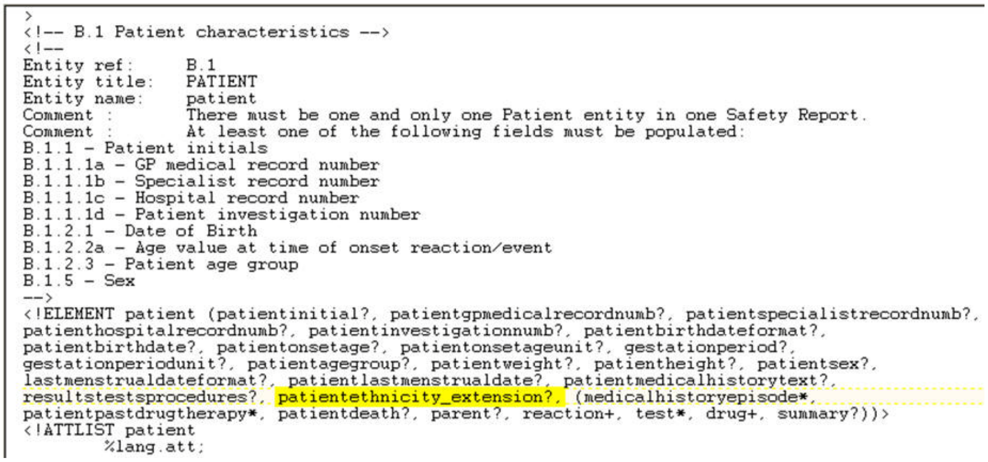
1. Log on to ESM Mapping Utility.
2. Select a **Profile** from the drop-down list.

   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

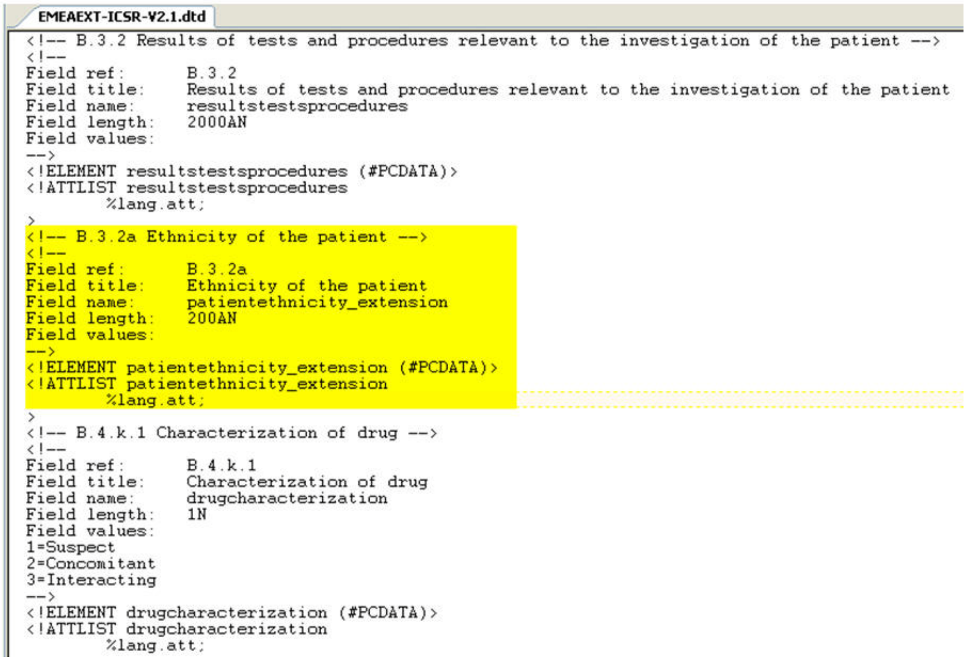
The following steps in this section will add the Extension element in the DTD file.

1. 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:



```
>
<!-- B.1 Patient characteristics -->
<!--
Entity ref:     B.1
Entity title:   PATIENT
Entity name:    patient
Comment :       There must be one and only one Patient entity in one Safety Report.
Comment :       At least one of the following fields must be populated:
B.1.1 - Patient initials
B.1.1.1a - GP medical record number
B.1.1.1b - Specialist record number
B.1.1.1c - Hospital record number
B.1.1.1d - Patient investigation number
B.1.2.1 - Date of Birth
B.1.2.2a - Age value at time of onset reaction/event
B.1.2.3 - Patient age group
B.1.5 - Sex
-->
<!ELEMENT patient (patientinitial?, patientgpmedicalrecordnumb?, patientspecialistrecordnumb?,
patienthospitalrecordnumb?, patientinvestigationnumb?, patientbirthdateformat?,
patientbirthdate?, patientonsetage?, patientonsetageunit?, gestationperiod?,
gestationperiodunit?, patientagegroup?, patientweight?, patientheight?, patientsex?,
lastmenstrualdateformat?, patientlastmenstrualdate?, patientmedicalhistorytext?,
resultstestsprocedures?, patientethnicity_extension?, (medicalhistoryepisode*,
patientpastdrugtherapy*, patientdeath?, parent?, reaction+, test*, drug+, summary?))>
<!ATTLIST patient
        %lang.att;
```

3. Add the element details as an individual entity, as highlighted in the following image:



```
<!-- B.3.2 Results of tests and procedures relevant to the investigation of the patient -->
<!--
Field ref:      B.3.2
Field title:    Results of tests and procedures relevant to the investigation of the patient
Field name:     resultstestsprocedures
Field length:   2000AN
Field values:
-->
<!ELEMENT resultstestsprocedures (#PCDATA)>
<!ATTLIST resultstestsprocedures
        %lang.att;
>
<!-- B.3.2a Ethnicity of the patient -->
<!--
Field ref:      B.3.2a
Field title:    Ethnicity of the patient
Field name:     patientethnicity_extension
Field length:   200AN
Field values:
-->
<!ELEMENT patientethnicity_extension (#PCDATA)>
<!ATTLIST patientethnicity_extension
        %lang.att;
>
<!-- B.4.k.1 Characterization of drug -->
<!--
Field ref:      B.4.k.1
Field title:    Characterization of drug
Field name:     drugcharacterization
Field length:   1N
Field values:
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"
5. 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;
```

17

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 8.0

Whether you are upgrading to Argus Safety 8.0 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 8.0 Database

Prior to creating a 8.0 database or upgrading to a 8.0 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 8.0 Application Servers

After the application servers have been installed with 8.0, 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.

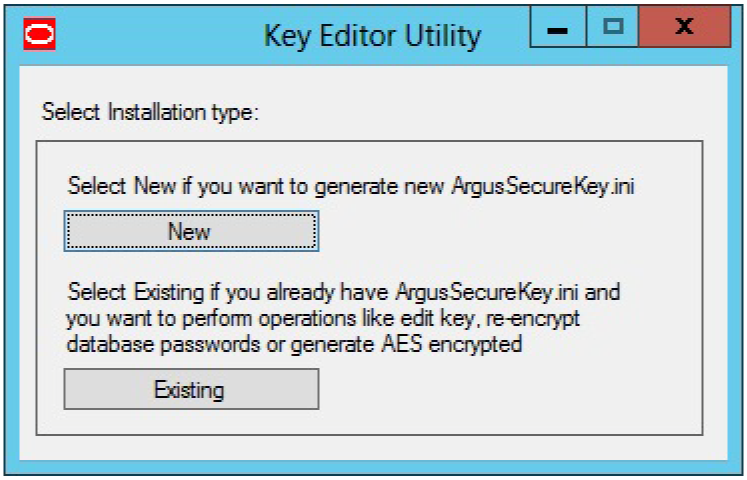
Generating a New Cryptography Key

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.



Key Editor Utility

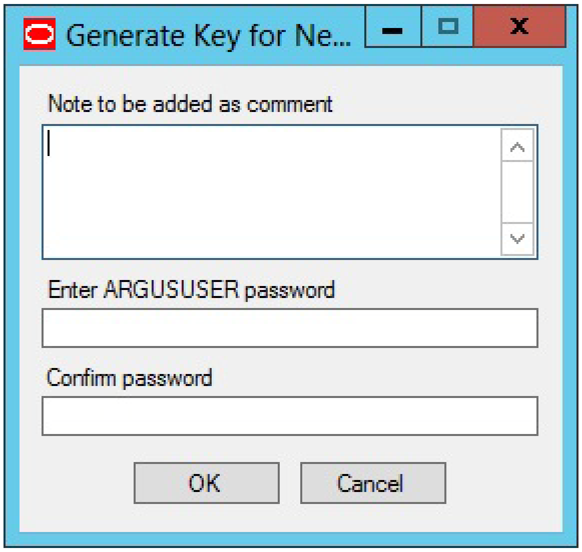
Select Installation type:

Select New if you want to generate new ArgusSecureKey.ini

Select Existing if you already have ArgusSecureKey.ini and you want to perform operations like edit key, re-encrypt database passwords or generate AES encrypted

2. Click **New**.

   The following screen appears.



3. In the **Note to be added as comment** field, enter a comment that will be saved in the ArgusSecureKey.ini. This can be any form of metadata, such as why this key was generated or for what environments it is used.

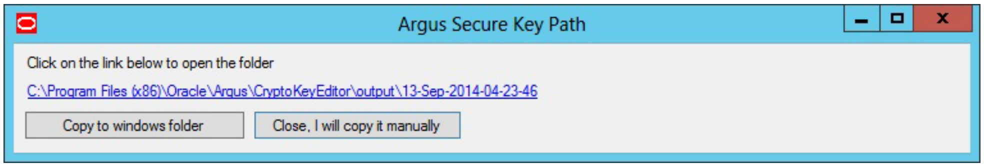
4. In the **Enter ARGUSUSER password** field, enter the password for the database user called ARGUSUSER.

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.



Click on the link below to open the folder

C:\Program Files (x86)\Oracle\Argus\CryptoKeyEditor\output\13-Sep-2014-04-23-46

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

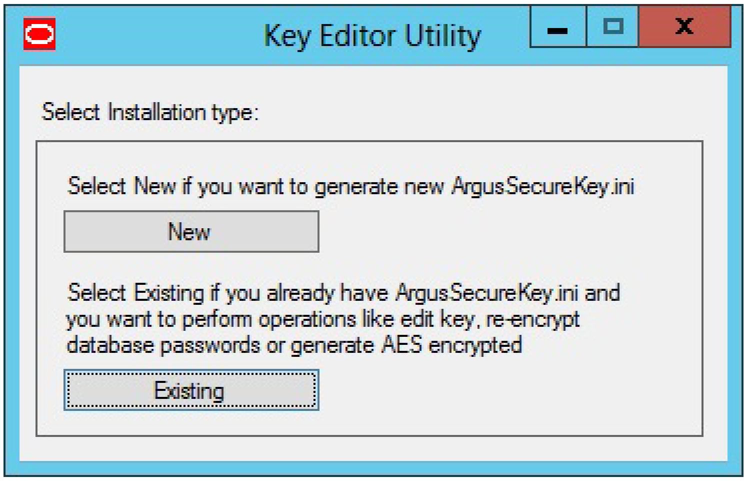
Resetting the ARGUSUSER Password

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.



Key Editor Utility

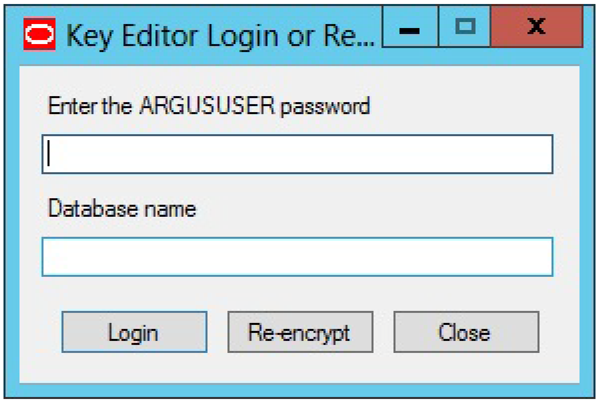
Select Installation type:

Select New if you want to generate new ArgusSecureKey.ini

Select Existing if you already have ArgusSecureKey.ini and you want to perform operations like edit key, re-encrypt database passwords or generate AES encrypted

2. Click **Existing**.

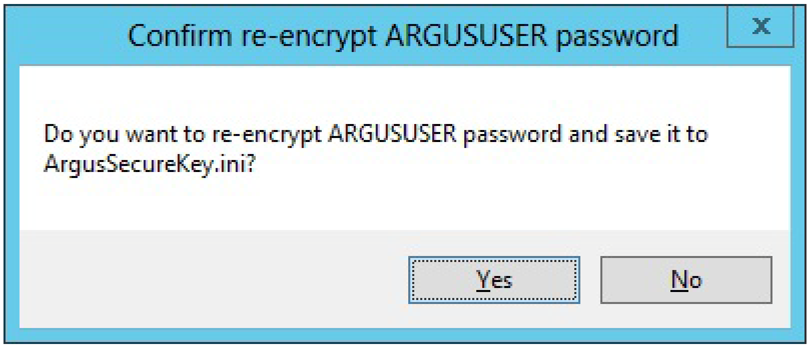
   The Key Editor Login or Re-encrypt ARGUSUSER screen appears.



Key Editor Login or Re...

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.



Confirm re-encrypt ARGUSUSER password

Do you want to re-encrypt ARGUSUSER password and save it to ArgusSecureKey.ini?

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.

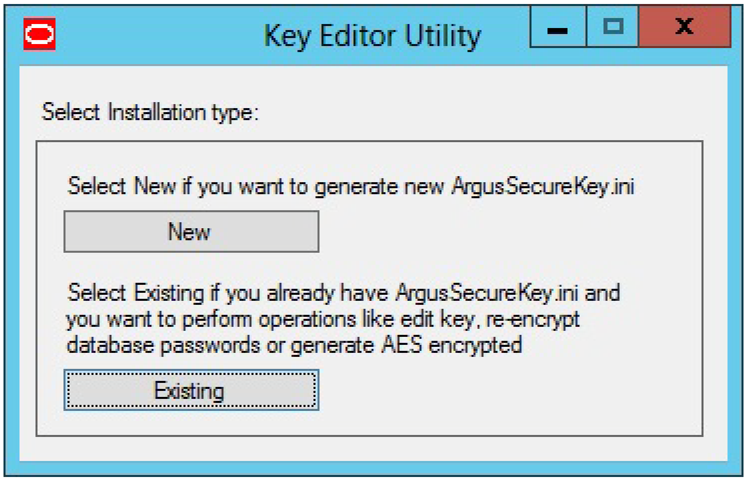
Editing Keys

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

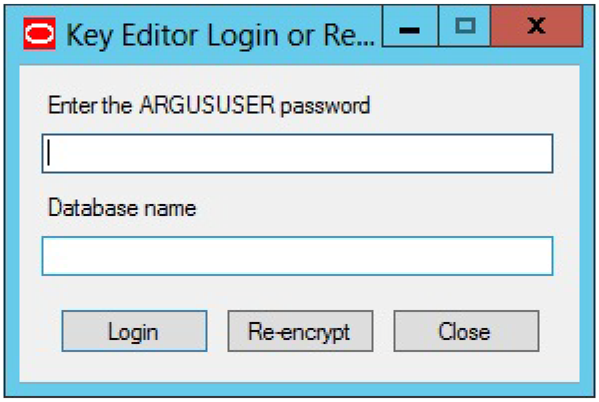
Select Installation type:

Select New if you want to generate new ArgusSecureKey.ini

Select Existing if you already have ArgusSecureKey.ini and you want to perform operations like edit key, re-encrypt database passwords or generate AES encrypted

2. Click **Existing**.

   The Key Editor Login or Re-encrypt ARGUSUSER screen appears.

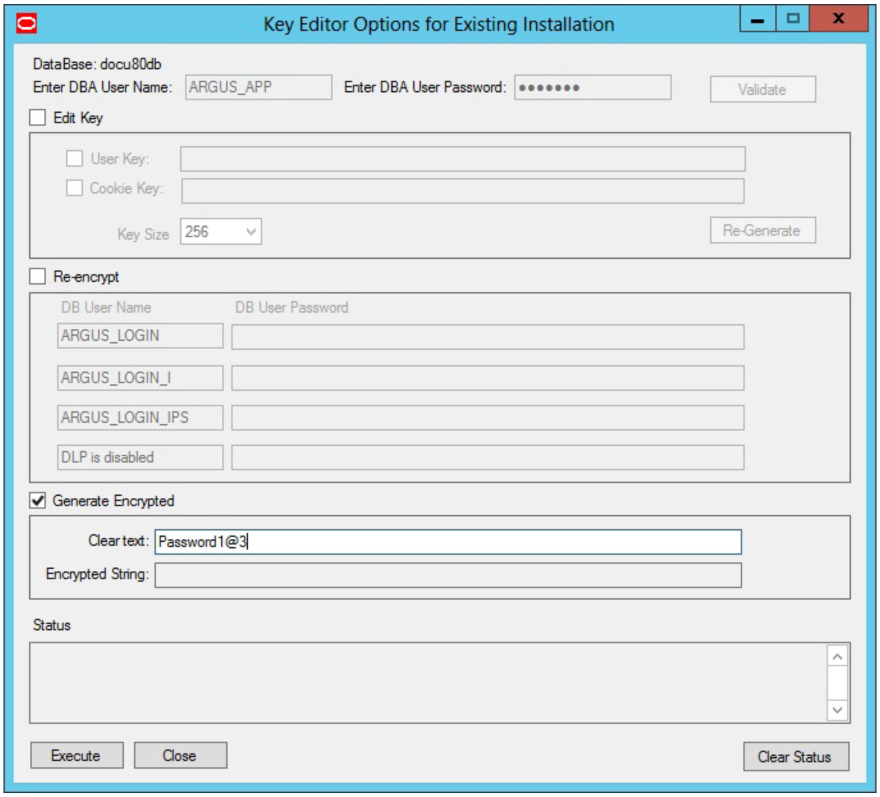


3. In the **Enter the ARGUSUSER password** field, enter the password for the database user called ARGUSUSER.

4. Enter the name of the database in the **Database name** field.

5. Click **Login**.

   The Key Editor Options for Existing Installation screen appears.



DataBase: docu80db

Enter DBA User Name: ARGUS_APP   Enter DBA User Password: •••••••

□ Edit Key

□ User Key:

□ Cookie Key:

Key Size 256

□ Re-encrypt

DB User Name	DB User Password
ARGUS_LOGIN	
ARGUS_LOGIN_I	
ARGUS_LOGIN_IPS	
DLP is disabled	

☑ Generate Encrypted

Clear text: Password1@3

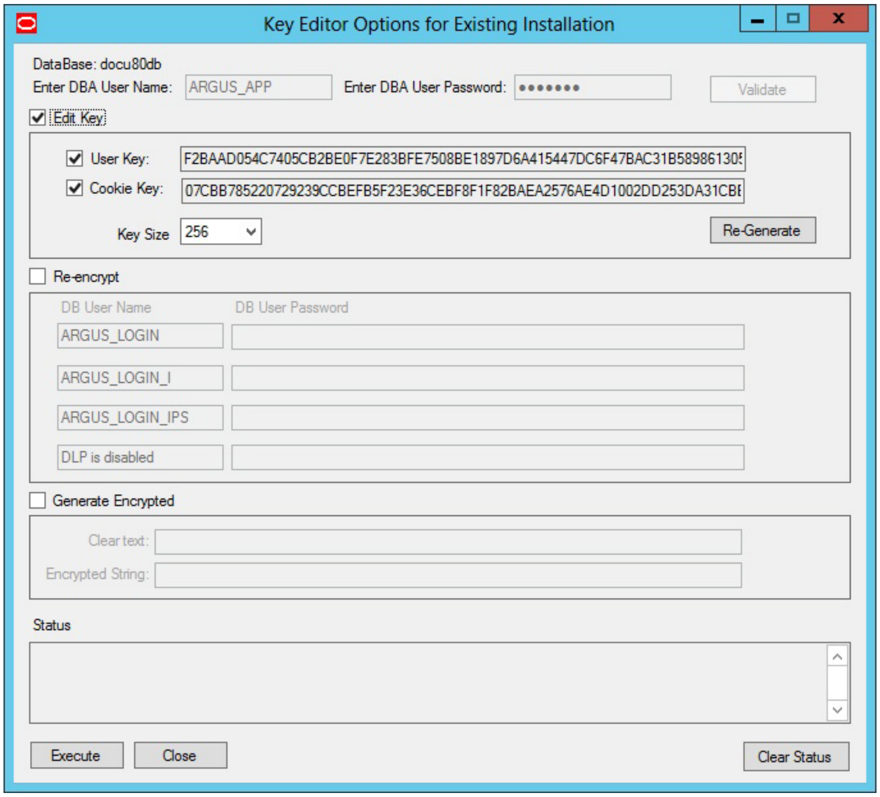
Encrypted String:

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 Editor Options for Existing Installation

DataBase: docu80db

Enter DBA User Name: ARGUS_APP Enter DBA User Password: ●●●●●●●● Validate

☑ Edit Key

☑ User Key: F2BAAD054C7405CB2BE0F7E283BFE7508BE1897D6A415447DC6F47BAC31B58986130

☑ Cookie Key: 07CBB785220729239CCBEFB5F23E36CEBF8F1F82BAEA2576AE4D1002DD253DA31CB

Key Size 256 Re-Generate

☐ Re-encrypt

DB User Name	DB User Password
ARGUS_LOGIN	
ARGUS_LOGIN_I	
ARGUS_LOGIN_IPS	
DLP is disabled	

☐ Generate Encrypted

Clear text:

Encrypted String:

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.

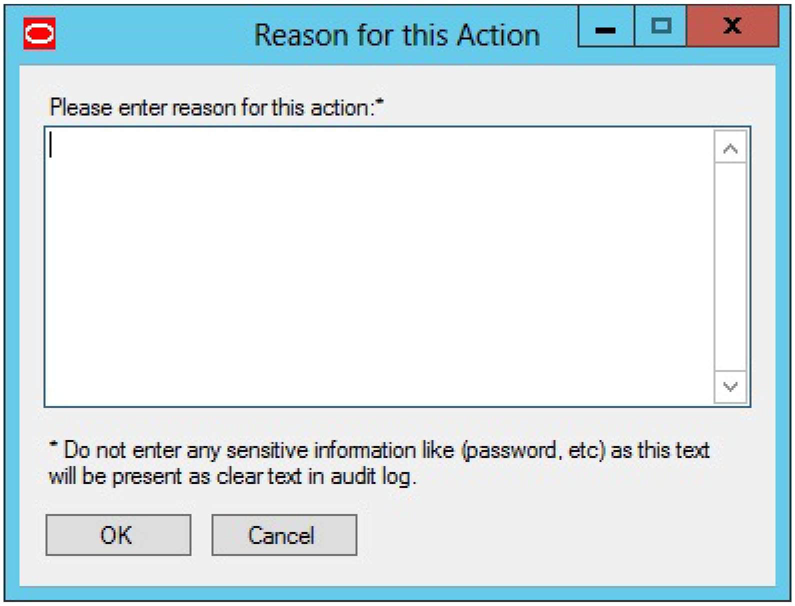
10. Change the Key Size drop-down list value, if you wish to change the key size. Key Size is measured in bits of the key used in a cryptographic algorithm.

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.


Reason for this Action

Please enter reason for this action:*

* Do not enter any sensitive information like (password, etc) as this text will be present as clear text in audit log.

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.

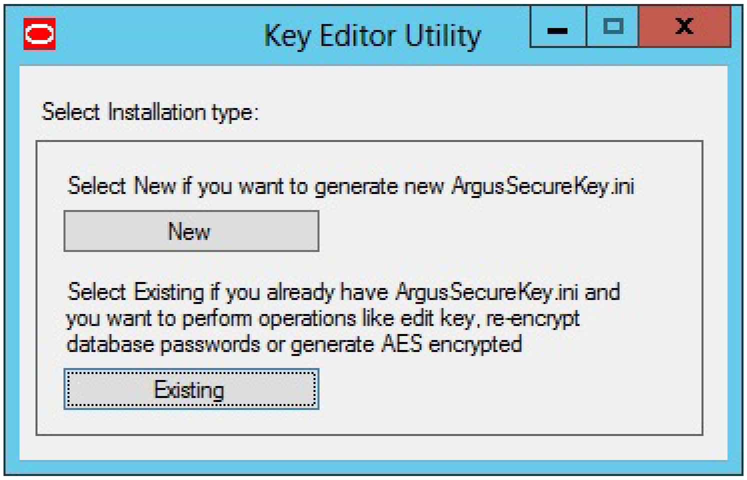
Re-encrypting Common User Passwords

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.

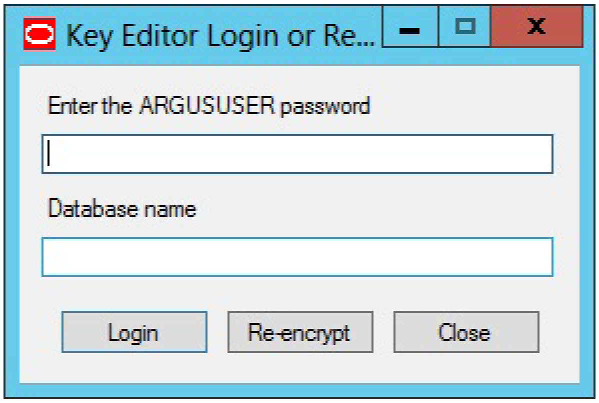


Select New if you want to generate new ArgusSecureKey.ini

Select Existing if you already have ArgusSecureKey.ini and you want to perform operations like edit key, re-encrypt database passwords or generate AES encrypted

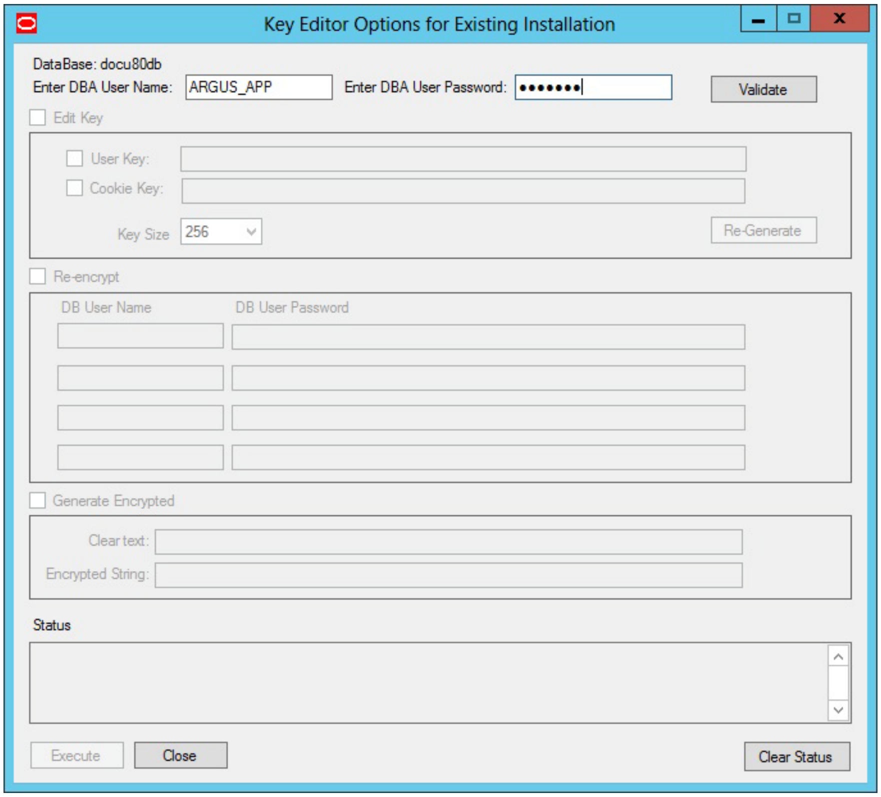
2. Click **Existing**.

   The Key Editor Login or Re-encrypt ARGUSUSER screen appears.



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.



Key Editor Options for Existing Installation

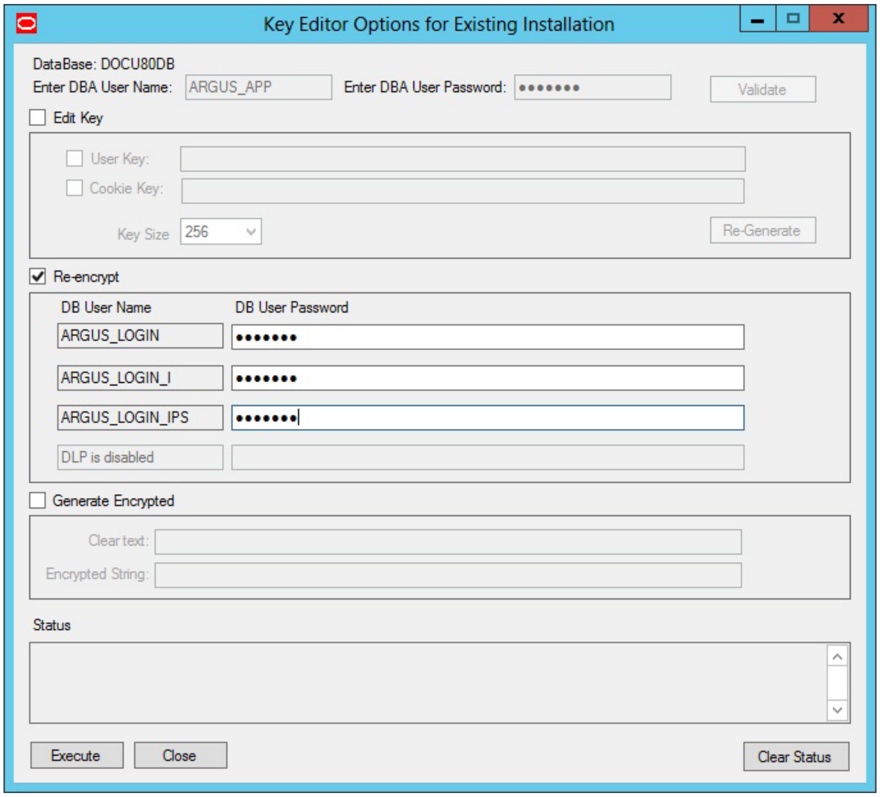
DataBase: docu80db

Enter DBA User Name: ARGUS_APP

Enter DBA User Password: •••••••

Key Size 256

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 Editor Options for Existing Installation

DataBase: DOCU80DB

Enter 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 Password
ARGUS_LOGIN	•••••••
ARGUS_LOGIN_I	•••••••
ARGUS_LOGIN_IPS	•••••••
DLP is disabled	

□ Generate Encrypted

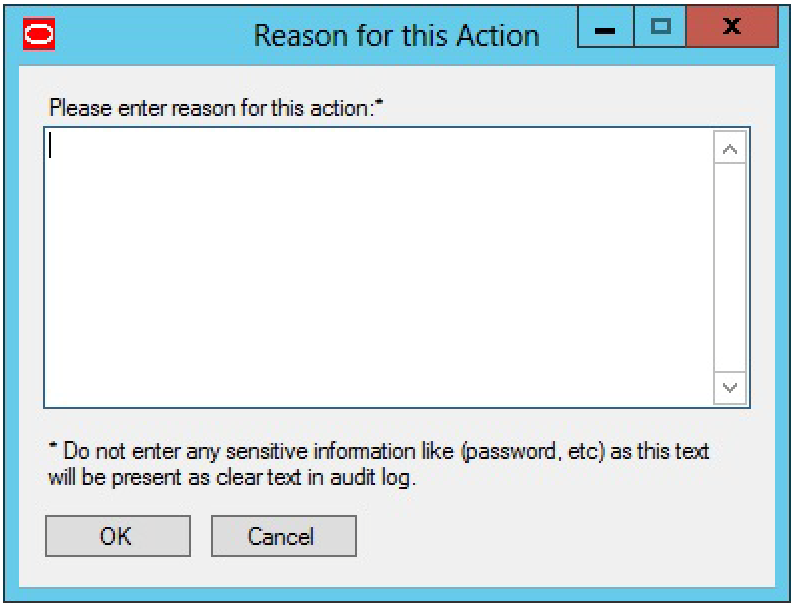
Clear text:

Encrypted String:

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

Please enter reason for this action:*

* Do not enter any sensitive information like (password, etc) as this text will be present as clear text in audit log.

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.

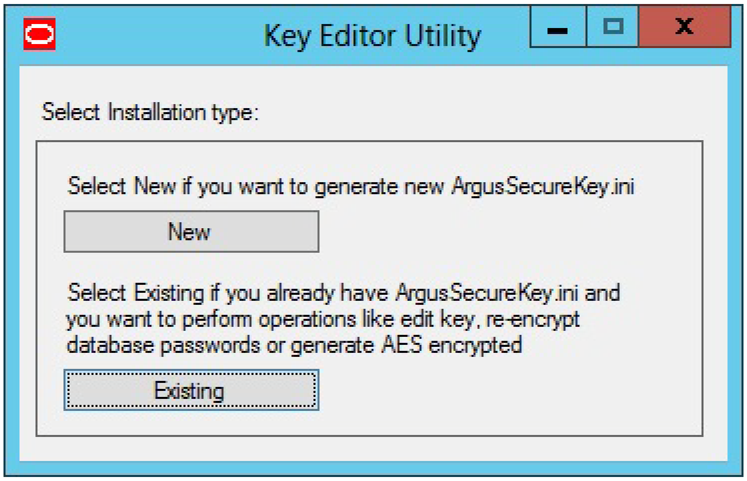
Generating Encrypted String from Clear Text on Configured User Cryptography Key

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

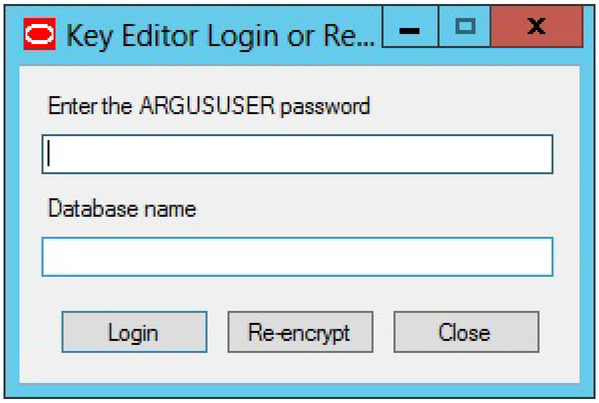
Select Installation type:

Select New if you want to generate new ArgusSecureKey.ini

Select Existing if you already have ArgusSecureKey.ini and you want to perform operations like edit key, re-encrypt database passwords or generate AES encrypted

2. Click **Existing**.

   The Key Edit Login screen appears.



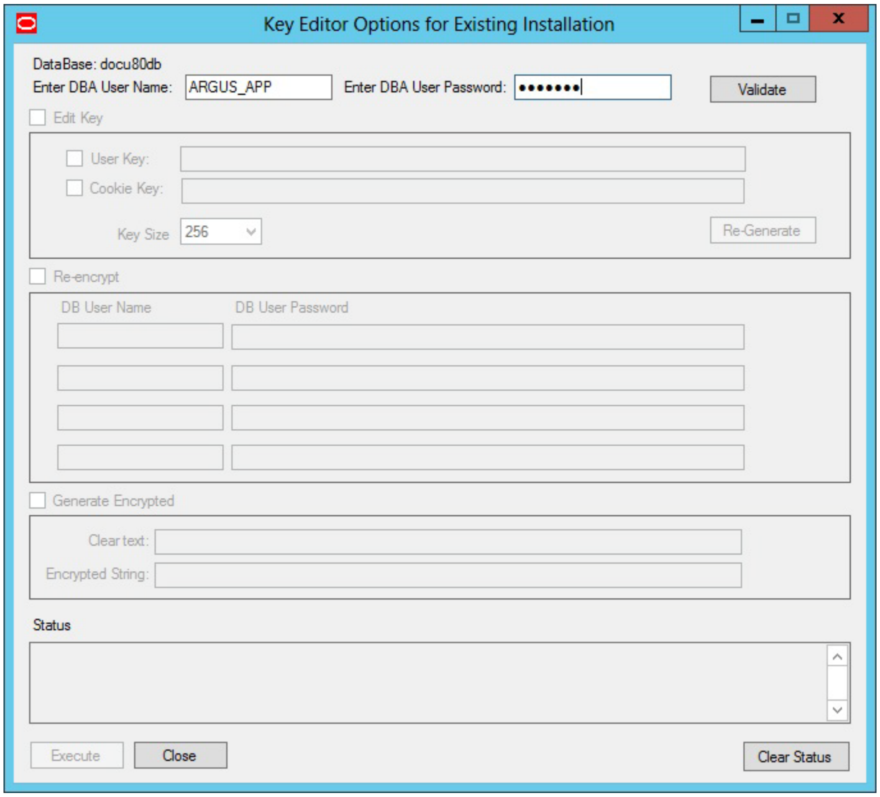
Key Editor Login or Re...

Enter the ARGUSUSER password

Database name

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.


Key Editor Options for Existing Installation

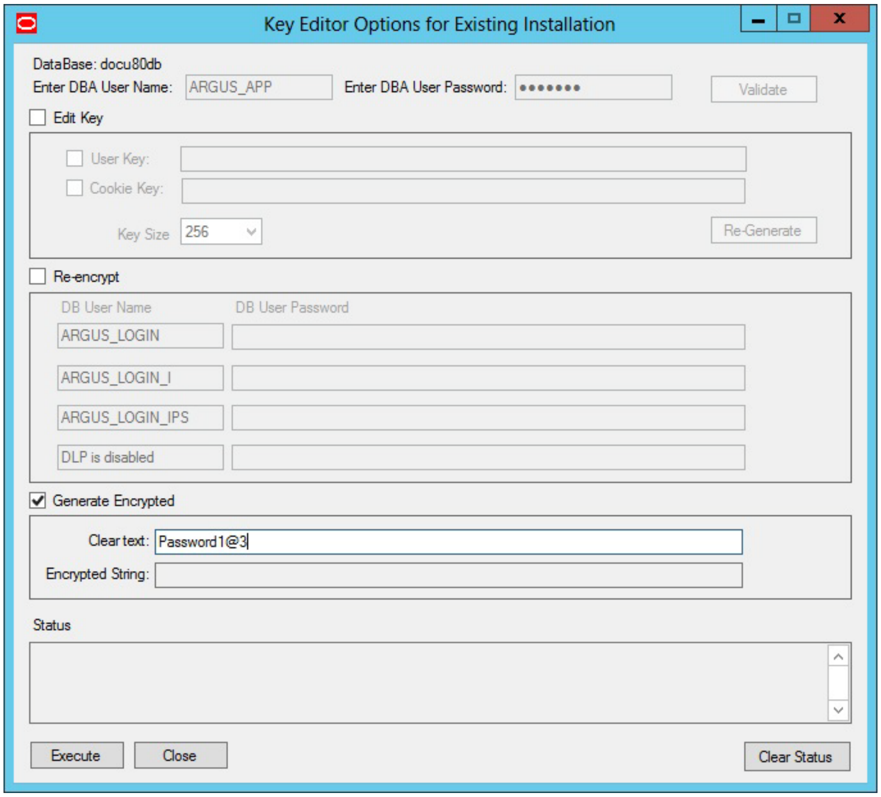
DataBase: docu80db

Enter DBA User Name: ARGUS_APP

Enter DBA User Password: •••••••

Key Size 256

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.



Key Editor Options for Existing Installation

DataBase: docu80db

Enter 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 Password
ARGUS_LOGIN	
ARGUS_LOGIN_I	
ARGUS_LOGIN_IPS	
DLP is disabled	

☑ Generate Encrypted

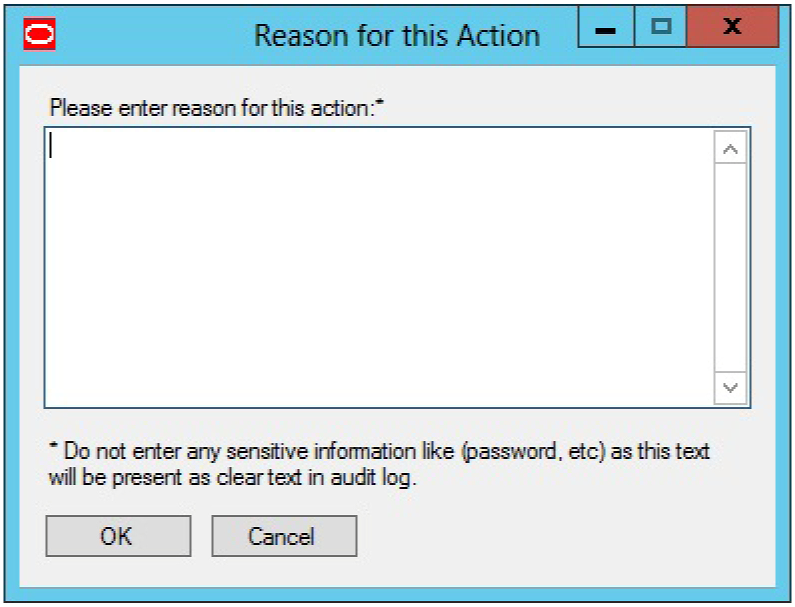
Clear text: Password1@3

Encrypted String:

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

Please enter reason for this action:*

* Do not enter any sensitive information like (password, etc) as this text will be present as clear text in audit log.

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:
4. 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

A

Third Party Attributions

This Appendix provides information about third party software.

Aspose

This software or website utilizes or contains material that is © 2003-2008 Aspose Pty Ltd (http://www.aspose.com), all rights reserved.

Dundas

This software or website utilizes or contains material that is © 1994-2000 Dundas Software Ltd., all rights reserved.

Telerik

This software or website utilizes or contains material that is copyright © 2002-2012 Telerik. All rights reserved.

/n software IPWorks

This software or website utilizes or contains material that is Copyright (c) 2013 /n software inc. All rights reserved.

Adobe Acrobat

The Argus Safety module in requires the use of Adobe Acrobat software. Before installing this application, you must purchase and install Adobe Acrobat.

Important: Oracle does not ship the Adobe Acrobat licenses along with these products. You must purchase the Adobe Acrobat license directly from Adobe or the recognized resellers.

EMC Documentum

The Argus Safety module may optionally use EMC Documentum software. When using EMC Documentum, before installing this application, you must purchase and install EMC Documentum.

Important: Oracle does not ship the EMC Documentum licenses along with these products. You must purchase the EMC Documentum license directly from EMC or the recognized resellers.

ICH

The ICH policy is that the materials provided on the ICH website are made available for public use, reproduction or distribution, provided that a clear reference to ICH as the copyright holder is made. In case of any adaptation or modification of the materials, the changes made to the original materials must be clearly labeled and any impression that these changes are endorsed by the ICH must be avoided. The above-mentioned permissions do not apply to third party content which may be included in some ICH materials. Any third party content included in ICH materials will be clearly identified. Permission for public use, reproduction, distribution or modification of such third party content must be obtained directly from the relevant third party.

In the case of ICH Implementation Guides containing third party material from HL7, HL7 has granted ICH permission for this use. Users may republish these ICH Implementation Guides in the form they appear on the ICH website without infringing HL7 copyright. However permission must be obtained directly from HL7 for any further use or modification of this material.

MedDRA MSSO

The Argus Safety module may optionally use MedDRA MSSO data. When using MedDRA MSSO, before installing this application, you must purchase a license to use MedDRA MSSO.

Important: Oracle does not ship the MedDRA MSSO licenses along with these products. You must purchase the MedDRA MSSO license directly from Northrop Grumman or the recognized resellers.

Microsoft Office

The Argus Safety module in requires the use of Microsoft Office software. Before installing this application, you must purchase and install Microsoft Office.

Important: Oracle does not ship the Microsoft Office licenses along with these products. You must purchase the Microsoft Office license directly from Microsoft or the recognized resellers.

OpenText RightFax

The Argus Safety module may optionally use OpenText RightFax software. When using OpenText RightFax, before installing this application, you must purchase and install OpenText RightFax.

Important: Oracle does not ship the OpenText RightFax licenses along with these products. You must purchase the OpenText RightFax license directly from OpenText or the recognized resellers.

WHO Drug Dictionary

The Argus Safety module may optionally use WHO Drug Dictionary data. When using WHO Drug Dictionary, before installing this application, you must purchase a license to use WHO Drug Dictionary.

Important: Oracle does not ship the WHO Drug Dictionary licenses along with these products. You must purchase the WHO Drug Dictionary license directly from the World Health Organization or the recognized resellers.

Microsoft Anti-XSS and Enterprise Library

Microsoft Public License (Ms-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

   The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

   A "contribution" is the original software, or any additions or changes to the software.

   A "contributor" is any person that distributes its contribution under this license.

   "Licensed patents" are a contributor's patent claims that read directly on its contribution

2. Grant of Rights

   a. Copyright Grant—Subject to the terms of this license, including the license conditions and limitations in Section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create

   b. Patent Grant—Subject to the terms of this license, including the license conditions and limitations in Section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

   a. No Trademark License—This license does not grant you rights to use any contributors' name, logo, or trademarks.

   b. If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

   c. If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

   d. If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

   e. The software is licensed "as-is". You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

Apache Log4net

This product includes software developed by The Apache Software Foundation (http://www.apache.org/).

Please read the LICENSE files present in the root directory of this distribution.

1. The names "log4net" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission.

   For written permission, contact: apache@apache.org

2. Include the following License ONLY ONCE in the documentation even if there are multiple products licensed under the license.

3. The following applies to all products licensed under the Apache 2.0 License:

   You may not use the identified files except in compliance with the Apache License, Version 2.0 (the "License.")

   You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

   A copy of the license is also reproduced below.

   Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

   See the License for the specific language governing permissions and limitations under the License.

   Apache License

   Version 2.0, January 2004

   http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions

   "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Section 1through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

   "Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

   "Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   a. You must give any other recipients of the Work or Derivative Works a copy of this License; and

   b. You must cause any modified files to carry prominent notices stating that You changed the files; and

   c. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the

Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

d. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any

other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at `http://www.apache.org/licenses/LICENSE-2.0`.

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Prototype JavaScript Framework

Prototype JavaScript Framework, version 1.5.0 (c) 2005-2007 Sam Stephenson

Prototype is freely distributable under the terms of an MIT-Style license. For details, see the Prototype website: `http://www.prototype.conio.net/`

Copyright (c) 2005-2007 Sam Stephenson

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

PDFlib GmbH

cryptsoft:

Copyright (C) 1995-1997 Eric Young (`eay@cryptsoft.com`). All rights reserved.

This package is an SSL implementation written by Eric Young. The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the ARC4, RSA, lhash, DES, etc., code; not just the SSL code.

The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (`tjh@cryptsoft.com`).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (`eay@cryptsoft.com`)"

   The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (`tjh@cryptsoft.com`)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence].

Expat 2.0.0:

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper.

Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the"Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

ICClib 2.0.2:

Copyright (c) 1997-2002 Graeme W. Gill.

Permission is hereby granted, to use, copy, modify, distribute, and sell this software and its associated documentation files (the "Software") for any purpose without fee, provided that:

1. The above copyright notices and this permission notice accompany all source code copies of the Software and related documentation, and
2. If executable code based on the Software only is distributed, then the accompanying documentation must aknowledge that "this software is based in part on the work of Graeme W. Gill", and
3. It is accepted that Graeme W. Gill (the "Author") accepts NO LIABILITY for damages of any kind. The Software is provided without fee by the Author "AS-IS" and without warranty of any kind, express, implied or otherwise, including without limitation, any warranty of merchantability or fitness for a particular purpose, and
4. These conditions apply to any software derived from or based on the Software, not just to the unmodified library, and
5. Except as contained in this notice, or in the required acknowledgment, the name of the Author, or the name of any organization or company affiliated with the Author may not be used in any advertising or publicity relating to the Software, without the specific, prior written permission of the Author.

ICU 4.0.1:

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1995-2008 International Business Machines Corporation and others. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

Koblas GIF Reader:

Copyright 1990 - 1994, David Koblas. (`koblas@netcom.com`)

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. This software is provided "AS IS" without express or implied warranty.

Libjpeg 6b:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-1998, Thomas G. Lane. All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

1. If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.
2. If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".
3. Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.)

So far as we are aware, there are no patent restrictions on the remaining code.

Libpng 1.2.36:

If you modify Libpng you may insert additional notices immediately following

this sentence.

- libpng versions 1.2.6, August 15, 2004, through 1.2.36, May 7, 2009, are Copyright (c) 2004, 2006-2009 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as Libpng-1.2.5 with the following individual added to the list of Contributing Authors:
  - Cosmin Truta
- libpng versions 1.0.7, July 1, 2000, through 1.2.5, October 3, 2002, are Copyright (c) 2000-2002 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as Libpng-1.0.6 with the following individuals added to the list of Contributing Authors:
  - Simon-Pierre Cadieux
  - Eric S. Raymond
  - Gilles Vollant

  and with the following additions to the disclaimer:

  There is no warranty against interference with your enjoyment of the library or against infringement. There is no warranty that our efforts or the library will fulfill any of your particular purposes or needs. This library is provided with all faults, and the entire risk of satisfactory quality, performance, accuracy, and effort is with the user
- libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c) 1998, 1999, 2000 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-0.96, with the following individuals added to the list of Contributing Authors:
  - Tom Lane
  - Glenn Randers-Pehrson
  - Willem van Schaik
- l libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996, 1997 Andreas Dilger Distributed according to the same disclaimer and license as libpng-0.88, with the following individuals added to the list of Contributing Authors:
  - John Bowler
  - Kevin Bracey

   - Sam Bushell
   - Magnus Holmgren
   - Greg Roelofs
   - Tom Tanner

- libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc. For the purposes of this copyright and license, Contributing Authors is defined as the following set of individuals:
   - Andreas Dilger
   - Dave Martindale
   - Guy Eric Schalnat
   - Paul Schmidt
   - Tim Wegner

The PNG Reference Library is supplied AS IS. The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.
2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.
3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

Libtiff 3.7.4:

Copyright (c) 1988-1997 Sam Leffler.

Copyright (c) 1991-1997 Silicon Graphics, Inc.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that (i) the above copyright notices and this permission notice appear in all copies of the software and related documentation, and (ii) the names of Sam Leffler and Silicon Graphics may not be used in any advertising or publicity relating to the software without the specific, prior written permission of Sam Leffler and Silicon Graphics.

THE SOFTWARE IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SAM LEFFLER OR SILICON GRAPHICS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE

POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

OpenSSL:

Copyright (c) 1998-2002 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names *OpenSSL Toolkit* and *OpenSSL Project* must not be used to endorse or promote products derived from this software without prior written permission. For written permission, contact: openssl-core@openssl.org.
5. Products derived from this software may not be called OpenSSL nor may OpenSSL appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OPENSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RSA MD5 Message Digest:

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

sRGB ICC Color Profile:

To anyone who acknowledges that the file "sRGB Color Space Profile.icm" is provided "AS IS" WITH NO EXPRESS OR IMPLIED WARRANTY: p.rmission to use, copy and distribute this file for any purpose is hereby granted without fee, provided that the file is not changed including the HP copyright notice tag, and that the name of Hewlett-Packard Company not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Hewlett-Packard Company makes no representations about the suitability of this software for any purpose.

zlib 1.2.3:

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly	Mark Adler
`jloup@gzip.org`	`madler@alumni.caltech.edu`

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files:

- `http://www.ietf.org/rfc/rfc1950.txt` (zlib format)
- `http://www.ietf.org/rfc/rfc1951.txt` (deflate format)
- `http://www.ietf.org/rfc/rfc1952.txt` (gzip format)