

Oracle Argus Safety

Installation Guide

Release 7.0.3

E40575-02

October 2015

Oracle Argus Safety Installation Guide, Release 7.0.3

E40575-02

Copyright © 2013, 2015 Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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

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

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

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

Contents

Preface	x
Intended Audience.....	x
Documentation Accessibility	xi
About This Book.....	xi
Related Documents	xii
Revision History	xii
Checking My Oracle Support	xii
Conventions	xiii
1 Introduction	
General Installation and Software Requirements	1-1
Pre-Requirement Installation Order	1-1
Argus Safety Database Server Installation Requirements.....	1-2
Argus Safety Web Server Installation Requirements.....	1-3
Argus Safety Report Server Installation Requirements.....	1-4
Argus Transaction Server Installation Requirements.....	1-5
Argus Interchange Server Requirements.....	1-6
Argus Safety Web Client Installation Requirements	1-6
Argus End of Study Unblinding Tool (EOSU) Installation Requirements.....	1-7
Argus Safety Hardware Topology	1-7
Recommended Hardware Topology for a Small Company	1-8
Recommended Hardware Topology for a Mid-sized Company	1-8
Recommended Hardware Topology for a Large Company	1-9
General Pre-Installation Tasks	1-9
Installation Process Overview	1-10
2 Starting the Installation	
Getting Started.....	2-1
Installing the Files Required to View Japanese Text.....	2-1
3 Installing the Argus Safety Database	
Overview.....	3-1
Schemas Required for Database Instances	3-2
Argus Safety Instance Database Schemas.....	3-2
Axway Synchrony Database Instance (Optional).....	3-2

Setting up Oracle Parameters	3-2
Oracle 11g Database Settings.....	3-2
Argus Safety Database Instance Parameters.....	3-3
Additional Database Setup Information.....	3-3
GMT Offset Calculation	3-3
Prerequisites for New Schema Creation	3-4
Creating the Argus Safety Database Schema	3-5
XDB Schema Installation Requirement for Interchange	3-5
Installing the Schema Creation Tool	3-5
Creating the Tablespaces	3-6
Creating the Schema	3-7
Loading Factory Data	3-11
Enabling and Disabling Oracle Text	3-12
Enabling Oracle Text	3-12
Disabling Oracle Text	3-13
Implementing Table Partitioning	3-14
Working with the MedDRA and MedDRA J Dictionaries	3-14
Loading the MedDRA Dictionary	3-15
Overwriting an Existing MedDRA Dictionary	3-16
Recoding Events.....	3-18
Loading the J Drug Dictionary	3-20
Overwriting an Existing J Drug Dictionary	3-21
Loading the WHO-DRUG Dictionary	3-22
Loading the WHO-Drug Dictionary to New Tables.....	3-22
Loading the WHO-Drug Dictionary Using the Overwrite Option.....	3-24
To Load the WHO-Drug Dictionary using the Format C Option.....	3-25
Validating the Argus Safety Database	3-26
Enabling and Disabling DLP	3-28
Creating the Tablespaces.....	3-28
Enabling DLP.....	3-28
Disabling DLP.....	3-31
Upgrading the Argus Safety Database	3-32
Database Upgrade Procedure (with or without DLP) from AS 7.0.2 to AS 7.0.3	3-33
Merging a Single Enterprise Safety Database into a Multi-tenant Database	3-38
Prerequisites to Running the Merge Export Step	3-38
Prerequisites to Running the Merge Import Step.....	3-38
Completing the Merge Process	3-39
Merge Export	3-39
Exporting the dmp File Copy to the Target Database Server.....	3-39
Merge Import.....	3-39
Manual Dictionary Synchronization.....	3-40
Copy Configuration Tool	3-41

4 Installing Argus Safety Web

Installing Argus Safety Web	4-1
Adding the Argus Site as a Trusted Site	4-9
Configuring the IIS Manager for Windows 2008.....	4-9

Connecting to a Domain Account on Windows 2008	4-11
Enabling SSL Support for Windows 2008	4-12
Configuring Load Balancer in Argus Web	4-13
Set up Argus Web Load Balancer IP Address	4-13
Set up Load Balanced Folders	4-14
Set up Shared Network Directory	4-14
Installing Argus Report Server.....	4-14
Recommended Changes in IIS 7.5 on the Report Server	4-15
Securing Sensitive Configuration and Operational Data	4-17
Configuring Identity in the IIS Application Pools.....	4-17
Resetting IIS	4-18
5 Installing Argus Safety Service	
Starting Argus Safety Service	5-3
Setting up RightFax	5-6
6 Installing and Configuring EDI Gateway	
Creating an Axway Synchrony Database Instance	6-1
Installing Axway Synchrony Interchange	6-2
Starting the Axway Synchrony Server	6-2
Configuring Axway Synchrony Interchange	6-2
Configuring Axway Synchrony for Binary File Transmission	6-4
Configuring Axway Synchrony Community	6-5
Registering with the Axway Synchrony Community	6-5
Adding a Partner to the Axway Synchrony Community	6-6
Registering the Receiver's Community on the Sender Server	6-7
Adding a Node	6-7
Configuring Axway Synchrony Certificates	6-8
Configuring Receiver Axway Synchrony Certificates	6-8
Configuring Sender Axway Synchrony Certificates	6-9
Configuring EVENTS.XML	6-10
Testing Communication	6-13
7 Installing and Configuring Interchange	
Installing Interchange Service	7-1
Configuring Interchange Service	7-5
Transmitting E2B Attachments	7-6
Accessing EDI Gateway Shared Folders.....	7-6
Configuring the Interchange Service.INI File	7-6
8 Performing Post-installation Checks	
Post-Installation Tasks	8-1
General Checklist	8-1
Configuring Argus Safety Windows Service to run as a Domain User	8-2
Configure Worklist Intake	8-2

RelsysWindowsService.exe.config	8-2
Service.config.....	8-3
Intake.config	8-3
IIS Checklist	8-4
.INI File Checklist.....	8-5
Service Checklist.....	8-5
Verifying the Web Server Installation and IIS Configurations.....	8-5
Verifying IIS 7 Configuration	8-6
Configure and Verify the Dossier Installation	8-6
Configuring the Dossier Application	8-6
Verifying the Dossier Installation.....	8-7
Verify Files installed on Middle Tier Servers:.....	8-8
Verifying the Documentum Installation.....	8-8
Validating the easyPDF Installation.....	8-10
Validating the easyPDF Installation for Word 2007 and Word 2010.....	8-10

9 Enabling IIS HTTP Compression

IIS Web Page Compression	9-1
HTTP Compression.....	9-1
Known Effects of Enabling Compression.....	9-1
How to Enable HTTP Compression	9-2
IIS Caching Settings	9-2
IIS Caching	9-2
Known Effects of Enabling Caching.....	9-2
How to Enable Caching.....	9-2
Local Internet Explorer (IE) Client Caching Settings.....	9-3
IE Client Caching.....	9-3
IE Client Caching Tab Options.....	9-3
How to Enable IE Caching.....	9-4

10 Configuring E-mail

About E-mail Configuration	10-1
Configuring SMTP.....	10-1
Using the SMTP Configuration Utility	10-1
Functions Affected by SMTP	10-2
Bulk Report Transmit E-mail	10-2
Autosignal E-mail	10-3
Fax E-mail.....	10-3
Fax Status E-mail.....	10-3
Priority E-mail	10-3
Dossier Notification E-mail	10-3
E-mail Sent by Interchange Service	10-3

11 Installing End of Study Unblinding

EOSU Hardware/Software Requirements	11-1
How to Install the EOSU Utility.....	11-2

12 Other Tasks

Configuring the Argus.xml File	12-1
Configuring the Argus.ini File	12-2
Increasing the Internet Explorer Timeout Setting to Run Reports	12-4
Deploying a Portlet on Oracle WebLogic Server	12-5
Deploying the Global Home Application on a WebLogic Server	12-8
Configure Global Homepage Properties File.....	12-8
Update Global Homepage Properties File	12-9
Deploy Company Logo.....	12-9
Pre-Deployment Configuration	12-9
Configuring SSO in Oracle Access Manager 10g	12-14
Installing WebGate.....	12-18
Configuring WebGate on Windows Server 2008	12-23
Protecting Files in the Argus Directory	12-27
Configuring SSO in Oracle Access Manager 11g	12-33
Installing WebGate.....	12-36
Configuring WebGate on Windows Server 2008	12-41
Protecting Files in the Argus Directory	12-45
Installation and Configuration of Oracle Web Tier Suite	12-52
Installing Oracle Web Tier	12-53
Configuring Oracle Web Tier	12-55
Oracle Http Server Administration	12-59
Configuring Oracle Http Server as Reverse Proxy Server for WebLogic	12-59
Configuring the WebCenter Security Provider for Identity Assertion	12-61
Configuring the Oracle Internet Directory Authenticator	12-61
Configuring the OAM Identity Asserter	12-64
Configuring the Default Authenticator and Setting the Order of Providers	12-66
Setting EXTRA_JAVA_PROPERTIES for WebLogic Domain	12-66
Installation Maintenance Tasks	12-67
Installing New Components.....	12-67
Uninstalling Components	12-68
Removing All Components	12-68
Web Client Tips	12-69
Clearing Oracle Temp Files	12-70
Configuring easyPDF	12-71
Setting Up easyPDF	12-71
Setting up Microsoft Office.....	12-72
Using Display PDF in Browser	12-72
Setting Printer Defaults	12-73
Argus Configuration Files	12-73

13 Argus Integrations

Installing Argus Integrations	13-1
Resetting IIS	13-3
Overview: Argus Web Service Interface	13-3
Argus Web Service Interface Framework.....	13-4

Basic Configuration Overview	13-4
Outbound Interface.....	13-4
Inbound Interface	13-5
Safety Message Overview	13-5
MedDRA Interface	13-5
Overview	13-5
MedDRA Encoding Safety Message Example	13-6
Request (V 1.1).....	13-6
Response (V 1.1)	13-7
Request (V 1.0).....	13-9
Response (V 1.0)	13-10
MedDRA Dictionary: XML Schema	13-12
Request: MEDDRA_Request	13-12
Request: MEDDRA_Response	13-14
Flow of MedDRA Auto Encoding	13-14
Configuration.....	13-14
Product License Study Interface	13-15
WHO Drug Coding Interface	13-16
Overview	13-16
WHO Drug Coding Safety Message Example	13-17
Request	13-17
Response.....	13-18
WHO Drug Coding: XML Schema	13-20
Request: WHODrug_Request	13-21
Response: WHODrug_Response	13-21
Flow of Drug Dictionary Coding.....	13-21
Configuration.....	13-22
Lot Number Interface	13-22
Overview	13-22
Lot Number Safety Message Example	13-23
Request	13-23
Response.....	13-24
Lot Number: XML Schema	13-25
Request: Lot_Request	13-25
Response: Lot_Response	13-26
Flow of Lot Validation.....	13-27
Configuration.....	13-27
Transformation	13-28
Worklist Intake	13-29
Flow of Worklist Intake.....	13-29
Worklist Intake Safety Message Example.....	13-30
Configuration.....	13-32
Literature Intake	13-32
Flow of Literature Intake.....	13-33
Configuration.....	13-33
Metadata Configuration.....	13-33
Extended E2B Interface	13-34

E2B Mapping Updates.....	13-34
Adding Extension Elements to DTD.....	13-35
Prepare Factory Data for Extension Elements	13-36
Create Business Logic for Extension Elements	13-38
Configure Reporting Destination for Extension Profile	13-38
Extension Elements Sample XML.....	13-39
Extension Elements Sample Import PL/SQL Block.....	13-39

14 Argus Password Management - Cryptography Tool

Cryptography Tool Overview	14-1
Installing or Upgrading to Argus Safety 7.0.3	14-1
The Argus Safety 7.0.3 Database.....	14-2
The Argus Safety 7.0.3 Application Servers.....	14-2
Generating a New Cryptography Key	14-2
Resetting Password / Changing the Cryptography Key	14-3
Resetting the ARGUSUSER Password.....	14-4
Editing Keys.....	14-5
Re-encrypting Common User Passwords.....	14-8
Generating Encrypted String from Clear Text on Configured User Cryptography Key ...	14-11
Resetting the Environment if ArgusSecureKey.ini is Lost.....	14-14

A Third Party Attributions

Preface

This guide describes installing — or upgrading to — Oracle Argus Safety 7.0.3. Keep this guide; you perform some of these tasks once, but others you repeat 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 lacks 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
- 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

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

Chapter 2, "Starting the Installation"

This section provides information about starting the installation.

Chapter 3, "Installing the Argus Safety Database"

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

Chapter 4, "Installing Argus Safety Web"

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

Chapter 5, "Installing Argus Safety Service"

This section provides instructions on installing Argus Safety Service.

Chapter 6, "Installing and Configuring EDI Gateway"

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

Chapter 7, "Installing and Configuring Interchange"

This section describes how to install and configure Interchange.

Chapter 8, "Performing Post-installation Checks"

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

Chapter 9, "Enabling IIS HTTP Compression"

This section describes how to enable IIS HTTP Compression on Windows 2008 Server.

Chapter 10, "Configuring E-mail"

This section provides information about configuring E-mail.

Chapter 11, "Installing End of Study Unblinding"

This section describes how to install the EOSU Utility.

Chapter 12, "Other Tasks"

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

Chapter 13, "Argus Integrations"

This section provides information about the Argus Integrations.

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 UI/CH DTD 2.1 Mapping Reference Guide*

Revision History

This is the second version of the release notes.

Version #	Description
2	Updated Argus Transaction Server Installation and Interchange Server Requirements.
1	Original Version.

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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Introduction

This section includes the following information:

- [General Installation and Software Requirements](#)
- [Pre-Requisite Installation Order](#)
- [Argus Safety Hardware Topology](#)
- [General Pre-Installation Tasks](#)
- [Installation Process Overview](#)

General Installation and Software Requirements

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

- Argus Safety Database Server
- Argus Safety Web Server
- Argus Safety Report Server
- Argus Transaction Server
- Argus Interchange Server
- Argus Safety Web Client
- Argus End of Study Unblinding Tool

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
- 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, please 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>
```

Argus Safety Database Server Installation Requirements

The following table describes Argus Safety Database Server Configuration.

Argus Safety Database Server Software Requirements	Requirement Description
Operating System	Windows 2008 SP2 Standard/Enterprise (32-bit) Windows 2008 R2 SP1 Standard/Enterprise (64-bit) Oracle Enterprise Linux X86/86-64 (Version 5.5.0.0.0/5.7.0.0/6.2 UEK) Sun Solaris 10/11 (English version for all above OS)
Database Server	Oracle Database Server (Standard/Enterprise - AL32UTF8 character set) - Version 11.2.0.3 (32/64-bit) Oracle Advanced Security Transparent Data Encryption (TDE)* (Optional) Oracle Advanced Security Network Encryption (Optional)

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

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

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

Argus Safety Database Server Hardware Requirements				
Requirements	Small	Mid-Sized	Large	Very Large
RAM	4 -- 8 GB	8 - 16 GB	16 - 32 GB	16 - 32 GB
CPU	Equivalent to 2 - 4 Dual Core, 3GHz	Equivalent to 4 - 8 Dual Core, 3GHz	Equivalent to 16 Dual Core, 3GHz	Equivalent to 16 Dual Core, 3GHz
Virtualization	Oracle Virtual Machine - OVM 2.2.1/2.2.2 (Optional)			
Others	Exadata 11g R2 (Optional) RAC 11g R2 (Optional)			

Argus Safety Web Server Installation Requirements

The following table lists the hardware and software installation requirements for the Argus Safety Web Server.

Requirement Type	Requirement Description
Software	<p>Windows 2008 SP2 Standard/Enterprise (32-bit)</p> <p>Windows 2008 R2 SP1 Standard/Enterprise (64-bit)</p> <p>(English version for all above OS)</p> <p>Oracle Standard/Enterprise Client, Version 11.2.0.3 (32-bit only)</p> <p>Oracle 11.2.0.3 OLE Objects</p> <p>Oracle ODP.net 11.2.0.3</p> <p>Oracle ODAC 11.2.0.3</p> <p>Oracle Access Manager 11g (Optional)</p> <p>WebGate 10.1.4.3 (Optional - Required only for SSO Integration with Oracle Access Manager)</p> <p>LDAP/LDAPS 3.0 (Optional)</p> <p>Adobe Acrobat Reader, (Version 9.x, 10)</p> <p>Microsoft Internet Explorer, Version 8.0/9.0</p> <p>Microsoft Word 2007/2010 (32-bit)</p> <p>(Optional - Required only if the Argus Dossier module is to be used)</p> <p>IIS, Version 7.0</p> <p>IIS Version 7.5 (Windows 2008 R2 on 64-bit) (IIS 6.0 compatibility pack should also be installed)</p> <p>E-mail Support - SMTP</p> <p>Microsoft XML Parser 6.0</p> <p>Visual C++ 2008 SP1 Runtime</p> <p>Microsoft .NET 3.5 Framework</p> <p>Documentum DFC, Version 6.5, 6.7 SP2 (64-bit)/SP3 (Optional - Required only when Documentum is used)</p>

Requirement Type	Requirement Description
Hardware	WebCenter 11.1.1.4 (on WebLogic 10.3.4)
	(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).
	1 Dual Core CPU X 3 GHz, 4 GB Memory/CPU (Small)
	2 Dual Core CPUs X 3 GHz, 4 GB Memory/CPU (Medium/Large)
	Physical Server or Oracle Virtual Machine 2.2.1/2.2.2
	Minimum Resolution 1280X1024

Argus Safety Report Server Installation Requirements

The following table lists the hardware and software installation requirements for the Argus Safety Report Server.

Note: The Report Server is an optional component meant to offload the report generation process from the Web Server. If the Report Server is not set up, the Web Server itself handles the report generation load.

Requirement Type	Requirement Description
Software	Windows 2008 SP2 Standard/Enterprise (32-bit)
	Windows 2008 R2 SP1 Standard/Enterprise (64-bit)
	(English version for all above OS)
	Oracle Standard/Enterprise Client, Version 11.2.0.3 (32-bit only)
	Oracle 11.2.0.3 OLE Objects
	Oracle ODP.net 11.2.0.3
	Oracle ODAC 11.2.0.3
	Oracle Access Manager 11g (Optional)
	WebGate 10.1.4.3 (Optional - Required only for SSO Integration with Oracle Access Manager)
	LDAP/LDAPS 3.0 (Optional)
	Adobe Acrobat Reader, (Version 9.x, 10)
	Microsoft Internet Explorer, Version 8.0/9.0
	Microsoft Word 2007/2010 (32-bit)
	(Optional - Required only if the Argus Dossier module is to be used)
	IIS, Version 7.0
	IIS Version 7.5 (Windows 2008 R2 on 64-bit)
	E-mail Support - SMTP
Microsoft XML Parser 6.0	
Visual C++ 2008 SP1 Runtime	
Microsoft .NET 3.5 Framework	

Requirement Type	Requirement Description
Hardware	1 Dual Core CPU X 3 GHz, 4 GB Memory/CPU (Small) 2 Dual Core CPUs X 3 GHz, 4 GB Memory/CPU (Medium/Large) Physical Server or Oracle Virtual Machine 2.2.1/2.2.2 Minimum Resolution 1280X1024

Argus Transaction Server Installation Requirements

The following table lists the hardware and software installation requirements for the Argus Transaction Server.

Requirement Type	Requirement Description
Software	Windows 2008 SP2 Standard/Enterprise (32-bit) Windows 2008 R2 SP1 Standard/Enterprise (64-bit) (English version for all above OS) RightFax 9.4 (Optional - Required for faxing Expedited Reports) Oracle Standard/Enterprise Client, Version 11.2.0.3 (32-bit only) Oracle 11.2.0.3 OLE Objects Oracle ODP.net 11.2.0.3 Oracle ODAC 11.2.0.3 IIS Version 7.0 IIS Version 7.5 (Windows 2008 R2 on 64-bit) (Optional - Required only if the Integrations module is to be used) E-mail Support - SMTP Microsoft Excel/Word - 2007/2010 (32-bit) Microsoft XML Parser 6.0 Visual C++ 2008 SP1 Runtime Microsoft Visual Basic Power Packs 3.0 (Required for Interchange Mapping Utility) Microsoft .NET 3.5 Framework Axway Synchrony, Version 5.9 SP1, 5.10 (64-bit) (Optional - Required for E2B Report Exchange) Documentum DFC, Version 6.5, 6.7 SP2 (64-bit)/SP3 (Optional - Required only when using Documentum with AG Service and/or Interchange Service) Adobe Acrobat Reader, (Version 9.x, 10) LDAP/LDAPS 3.0 (Optional - Required for Interchange Mapping Utility)
Hardware	1 Dual Core CPU X 3 GHz, 4GB Memory/CPU (Small) 2 Dual Core CPUs X 3 GHz, 4 GB Memory/CPU (Medium/Large) Physical Server or Oracle Virtual Machine 2.2.1/2.2.2 Minimum Resolution 1280X1024

Note:

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

Argus Interchange Server Requirements

The following table lists the hardware and software installation requirements for the Argus Interchange Transaction Server.

Note: 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.

Requirement Type	Requirement Description
Software	<p>Windows 2008 SP2 Standard/Enterprise (32-bit)</p> <p>Windows 2008 R2 SP1 Standard/Enterprise (64-bit)</p> <p>(English version for all above OS)</p> <p>Oracle Standard/Enterprise Client, Version 11.2.0.3 (32-bit only)</p> <p>Oracle 11.2.0.3 OLE Objects</p> <p>Oracle ODP.net 11.2.0.3</p> <p>Oracle ODAC 11.2.0.3</p> <p>E-mail Support - SMTP</p> <p>Microsoft Excel/Word - 2007/2010 (32-bit)</p> <p>Microsoft XML Parser 6.0</p> <p>Visual C++ 2008 SP1 Runtime</p> <p>Microsoft Visual Basic Power Packs 3.0 (Required for Interchange Mapping Utility)</p> <p>Microsoft .NET 3.5 Framework</p> <p>Axway Synchrony, Version 5.9, 5.10 SP1 (64-bit) (Optional - Required for E2B Report Exchange)</p> <p>Documentum DFC, Version 6.5, 6.7 SP2 (64-bit)/SP3 (Optional - Required only when using Documentum with Interchange Service)</p> <p>LDAP/LDAPS 3.0 (Optional - Required for Interchange Mapping Utility)</p>
Hardware	<p>1 Dual Core CPU X 3 GHz, 4 GB Memory/CPU (Small)</p> <p>2 Dual Core CPUs X 3 GHz, 4 GB Memory/CPU (Medium/Large)</p> <p>Physical Server or Oracle Virtual Server 2.2.1 / 2.2.2</p> <p>Minimum Resolution 1280X1024</p>

Argus Safety Web Client Installation Requirements

The following table lists the hardware and software installation requirements for the Argus Safety Web Client.

Requirement Type	Requirement Description
Software	Windows 7 (64-bit) (English and Japanese) Windows XP Pro SP3 (32-bit) (English and Japanese) Microsoft Internet Explorer 8.0/9.0 (32-bit) (English versions on English OS and Japanese versions on Japanese OS) Microsoft Excel/Word - 2007/2010 (32-bit) (English versions on English OS and Japanese versions on Japanese OS) Adobe Acrobat Reader (32-bit), (Version 9.x, 10) (English versions on English OS and Japanese versions on Japanese OS)
Hardware	Pentium IV, 3 GHz, 2 GB RAM (minimum) Minimum Resolution 1280X1024

On the web client system, a new window may open (instead of opening in the same application window) when you try to view a 2007 Microsoft Office program document from the Argus Application in Windows Internet Explorer 8 or Internet Explorer 9. Please refer to the following Microsoft article for more information and workaround:
<http://support.microsoft.com/kb/927009>

Argus End of Study Unblinding Tool (EOSU) Installation Requirements

The following table lists the hardware and software installation requirements for the Argus End of Study Unblinding Tool (EOSU).

Requirement Type	Requirement Description
Software	Microsoft Windows XP SP3 Microsoft Windows 7 Microsoft Windows 2008 SP2 Standard/Enterprise (32-bit) Microsoft Windows 2008 R2 SP1 Standard/Enterprise (64-bit) Oracle Standard/Enterprise Client, Version 11.2.0.3 (32-bit only) Oracle OLE Objects 11.2.0.3 Oracle ODAC 11.2.0.3 Microsoft Excel 2007 / 2010 (32-bit) Visual C++ 2008 SP1 Runtime LDAP/LDAPS 3.0 (Optional)
Hardware	1 Dual Core CPU x 3Ghz, 4 GB RAM Minimum Resolution 1280 x 1024

Argus Safety Hardware Topology

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

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

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

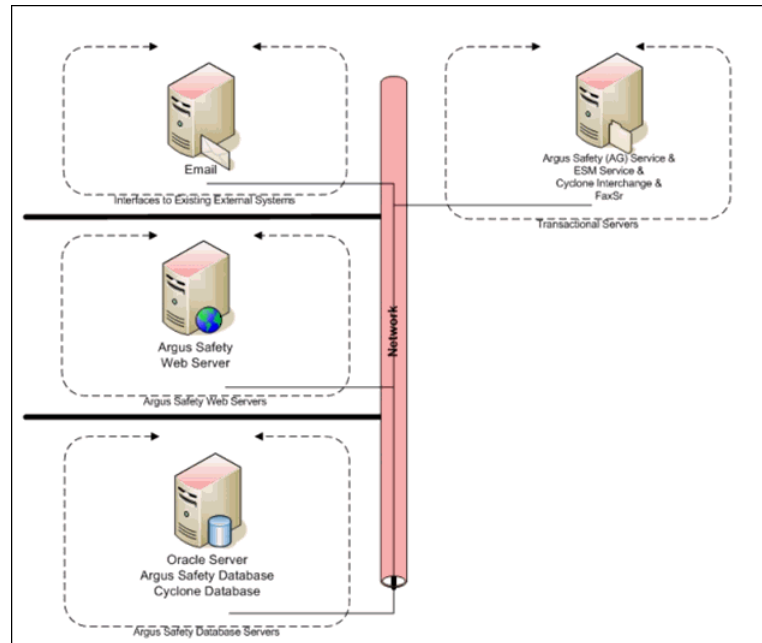
Small Company: A small company is a company that has from 1 to 50 concurrent users and fewer than 200 new cases reported each month.

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

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

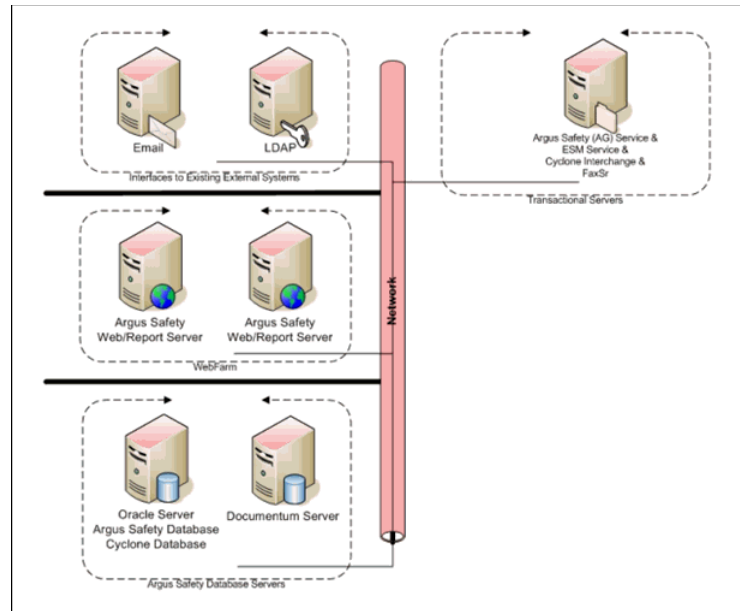
Recommended Hardware Topology for a Small Company

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



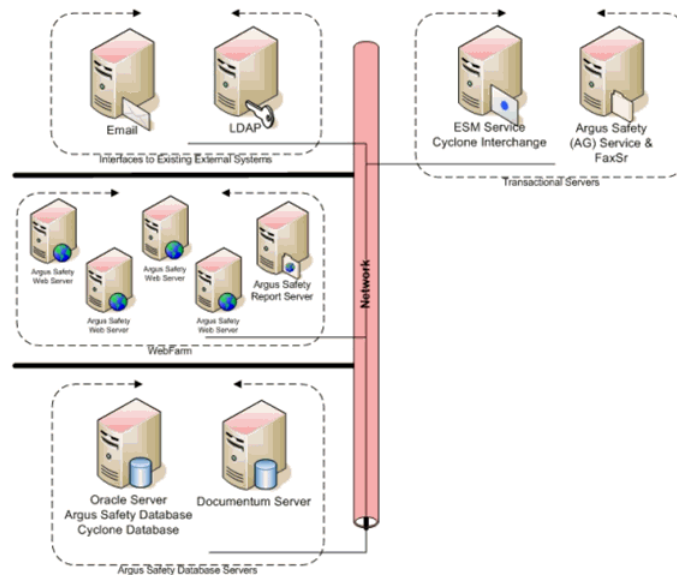
Recommended Hardware Topology for a Mid-sized Company

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



Recommended Hardware Topology for a Large Company

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



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.

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, please refer to the chapter 3 – Installing the Argus Safety Database. To install Argus Safety application, please 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. Please make sure you have sufficient free disk space for installing the language packs.

Installing the Argus Safety Database

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

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

Overview

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

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

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

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.
- **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.
- **DLP Schema:**
This is optional. You can create this schema if DLP 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 11g Database Settings

The tables in this section list the suggested parameters, configurations, and/or settings for an Oracle 11g 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, connect to ARGUS Safety database as a SYS user.

Note: If other DBA user used instead of SYSTEM then change SYSTEM to the name of DBA user.

Define user_dba=SYSTEM

Note: The DBMS_RLS package should be granted to a DBA user, only in case of multi-tenant environments.

GRANT EXECUTE ON SYS.UTL_FILE TO XDB;

GRANT EXECUTE ON SYS.DBMS_SCHEDULER TO &user_dba. WITH GRANT OPTION;

GRANT EXECUTE ON SYS.DBMS_OBFUSCATION_TOOLKIT TO &user_dba. WITH GRANT OPTION;

GRANT EXECUTE ON SYS.UTL_FILE TO &user_dba. WITH GRANT OPTION;

GRANT EXECUTE ON SYS.DBMS_RANDOM TO &user_dba. WITH GRANT OPTION;

GRANT SELECT ON SYS.ALL_SOURCE TO &user_dba. WITH GRANT OPTION;

GRANT EXECUTE on SYS.DBMS_RLS TO &user_dba. WITH GRANT OPTION;

GRANT EXECUTE on SYS.DBMS_LOCK TO &user_dba. WITH GRANT OPTION;

GRANT EXECUTE ON SYS.DBMS_JOB TO &user_dba. WITH GRANT OPTION;

GRANT EXECUTE ON SYS.DBMS_LOB TO &user_dba. WITH GRANT OPTION;

REVOKE EXECUTE ON SYS.DBMS_OBFUSCATION_TOOLKIT FROM PUBLIC;

REVOKE EXECUTE ON SYS.UTL_FILE FROM PUBLIC;

```
REVOKE EXECUTE ON SYS.DBMS_RANDOM FROM PUBLIC;
REVOKE SELECT ON SYS.ALL_SOURCE FROM PUBLIC;
```

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. Please 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: You must ensure to disable the UAC 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: from the screen and click **Next**.
 - 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:

- 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 redisplay 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.
- Locate the Oracle Licensing Option and select the applicable licensing option.
- 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.

- 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 disabled.
 - 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:

Tablespace Creation				
Tablespaces:	Small Model	Medium Model	Large Model	Complete Path and Datafile
ARGUS_AEXP_DATA_01	667M	1213M	2272M	I:\oradata\SOFD70\ARGUS_AEXP_DATA_01.dbf
ARGUS_AEXP_INDEX_01	60M	99M	142M	I:\oradata\SOFD70\ARGUS_AEXP_INDEX_01.dbf
ARGUS_AL_DATA_01	62M	208M	520M	I:\oradata\SOFD70\ARGUS_AL_DATA_01.dbf
ARGUS_AL_INDEX_01	60M	92M	132M	I:\oradata\SOFD70\ARGUS_AL_INDEX_01.dbf
ARGUS_DATA_01	971M	2924M	3088M	I:\oradata\SOFD70\ARGUS_DATA_01.dbf
ARGUS_DATA_02	737M	4621M	2782M	I:\oradata\SOFD70\ARGUS_DATA_02.dbf
ARGUS_DATA_03	480M	650M	1210M	I:\oradata\SOFD70\ARGUS_DATA_03.dbf
ARGUS_DATA_04	477M	762M	1425M	I:\oradata\SOFD70\ARGUS_DATA_04.dbf
ARGUS_DATA_05	276M	434M	814M	I:\oradata\SOFD70\ARGUS_DATA_05.dbf
ARGUS_INDEX_01	617M	1287M	2761M	I:\oradata\SOFD70\ARGUS_INDEX_01.dbf
ARGUS_INDEX_02	1251M	9297M	5380M	I:\oradata\SOFD70\ARGUS_INDEX_02.dbf
ARGUS_INDEX_03	571M	720M	1240M	I:\oradata\SOFD70\ARGUS_INDEX_03.dbf
ARGUS_INDEX_04	272M	367M	592M	I:\oradata\SOFD70\ARGUS_INDEX_04.dbf
ARGUS_INDEX_05	459M	713M	1976M	I:\oradata\SOFD70\ARGUS_INDEX_05.dbf
ARGUS_INDEX_06	167M	291M	791M	I:\oradata\SOFD70\ARGUS_INDEX_06.dbf
ESM_DATA_01	334M	531M	888M	I:\oradata\SOFD70\ESM_DATA_01.dbf
ESM_INDEX_01	346M	429M	574M	I:\oradata\SOFD70\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.

Note: The **Tablespace Creation** dialog 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.

Loading Factory Data

Before loading factory data verify that:

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

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: SOFD70

Argus Schema Owner: ARGUS_APP

Argus Schema Password: *****

DBA Username: SYSTEM

Password: ***

Log Directory: C:\Program Files\Oracle\Argus\DBInstaller

Select Log Directory

Proceed

Status

Enabling Oracle Text Complete.

Log File: C:\Program Files\Oracle\Argus\DBInstaller\OracleTextLog.txt

View

Close

- 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:
 - Click No.
3. When the system displays the **Disable Oracle Text** dialog box:

- 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.
 - 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.
 - Reenter the password in the Reenter Password field.
 - Click OK.
5. When the system redisplay 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 redisplay the MedDRA Dictionary Loader dialog box:, locate the Dictionary to Load section and do the following:

- 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** checkbox 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

Load to New Tables

MedDRA User: MEDDRA121_J

MedDRA Role: MEDDRA121_J_ROLE

Dictionary to Load

MedDRA Version: 12.1J

Dictionary Files: C:\Dict\MedDRA_12.1J\ASCI\MDRA_...

Primary SO Non-Primary SO MedDRA-Brows

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 checkbox 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:

- 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 checkboxes.
- 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 redisplay 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 redisplay 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** checkbox 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, please 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.

- In the New WHO-Drug Role dialog box, enter the New Role name and click OK.
5. When the system redisplay 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**.

The screenshot shows the 'WHO-Drug Dictionary Loader' dialog box. It is configured with the following settings:

- 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: whodruguser, Who-Drug Role: whodrugrole
- Dictionary to Load:** Dict Version: 2009-SEP, Dictionary Files: C:\Dict\WHO_2009_SEP\B2

Buttons include 'View Log file', 'Load', 'Close', 'Create User', and 'Create Role'. The status bar at the bottom indicates 'Ready...'.

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 the Dictionary Load dialog 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 redisplay 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.

Schema Validation

Database Connection: Validate DLP Schema

Users and Roles

Argus Schema Owner:

Argus Role Name:

Argus Login User:

ESM Schema Owner:

ESM Role Name:

ESM Login User:

VPD Admin Schema Owner:

DLP

DLP Database Name:

DLP Schema Owner:

DLP Schema Password:

Validation CTL File

Validation CTL Folder and File:

Validation Log Files

Select Log Files Folder:

Schema Difference Log File:

CTL Loader Log File:

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.

Schema Validation

Database Connection: Validate DLP Schema

Users and Roles

Argus Schema Owner:

Argus Role Name:

Argus Login User:

ESM Schema Owner:

ESM Role Name:

ESM Login User:

VPD Admin Schema Owner:

DLP

DLP Database Name:

DLP Schema Owner:

DLP Schema Password:

Validation CTL File

Validation CTL Folder and File:

Validation Log Files

Select Log Files Folder:

Schema Difference Log File:

CTL Loader Log File:

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. Please 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.

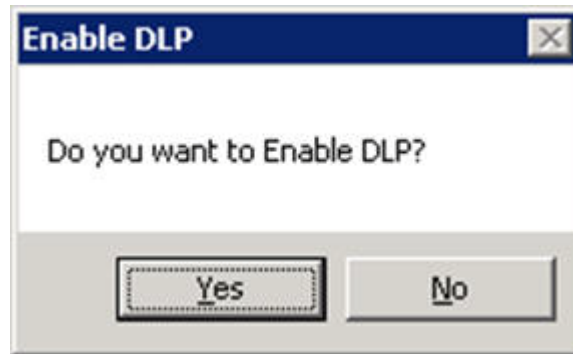
Enabling DLP

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

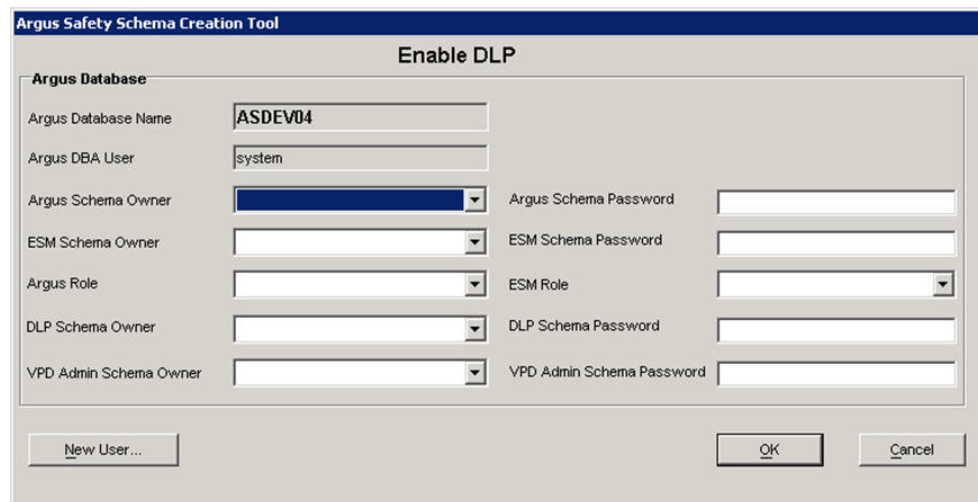
- Verify that the Schema Creation Tool is installed.
- Make sure an Oracle Argus database instance is available.
- Verify that either a DBA-privileged or a SYSTEM user account has been created.
- Verify that the database contains extra hard disk space to support DLP. It is advised that you should have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



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

A screenshot of the "Argus Safety Schema Creation Tool" dialog box, titled "Enable DLP". The dialog box has a blue title bar. Below the title bar, there is a section labeled "Argus Database" containing several fields and dropdown menus. The fields are: "Argus Database Name" (text box with "ASDEV04"), "Argus DBA User" (text box with "system"), "Argus Schema Owner" (dropdown menu), "ESM Schema Owner" (dropdown menu), "Argus Role" (dropdown menu), "DLP Schema Owner" (dropdown menu), and "VPD Admin Schema Owner" (dropdown menu). The corresponding password fields are: "Argus Schema Password", "ESM Schema Password", "DLP Schema Password", and "VPD Admin Schema Password". There is also an "ESM Role" dropdown menu. At the bottom left, there is a "New User..." button. At the bottom right, there are "OK" and "Cancel" buttons.

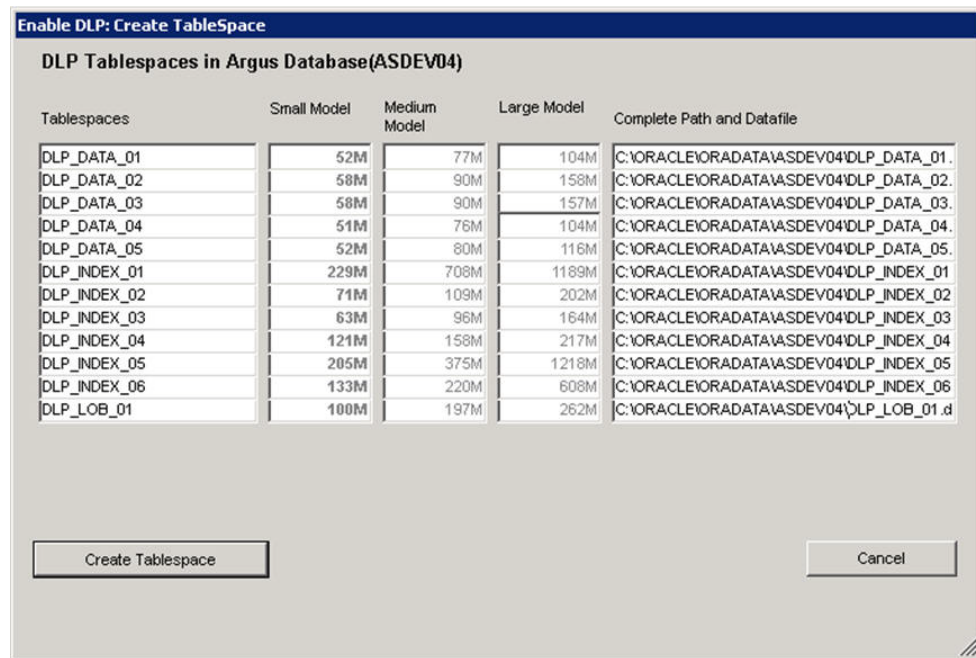
Click New User to create the DLP Schema Owner in the New User Information dialog box.

The screenshot shows a dialog box titled "Argus Safety Schema Creation Tool". It contains the following fields and values:

- Database: ASDEV04
- New User Name: dlp_schema
- New User Password: *****
- Re-enter Password: *****
- Default Tablespace: USERS
- Temporary Tablespace: TEMP

Buttons for "OK" and "Cancel" are located at the bottom of the dialog.

- 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 redisplay 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:



Note: The **Tablespace Creation** dialog 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 tablespaces 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 Enable/Disable DLP dialog box:
 - Click No.
3. When the system displays the Disable DLP dialog box:

- Enter the required information and click OK.
4. When the system displays the expanded Disable DLP dialog box:
 - Click OK to close the dialog box.
 - Click Proceed to start processing.
 5. When the system displays the following message, click OK and then click Proceed in the Disable DLP expanded dialog box.

- Click OK to close the dialog box.
 - Click Proceed to start processing.
6. 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.
 7. When the Disable DLP operation is complete:
 - Click Exit.
 8. DLP has been disabled.

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.

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 7.0.3.

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) 7.0.3 software to upgrade the Argus Safety database from AS 7.0.1.5 or AS 7.0.1 to AS 7.0.2, using the Database zip file.

AS 7.0.1.5 to AS 7.0.2, using the database zip file in the AS 7.0.3 software:

Extract 'Database_released_code_702.zip' in 'Previous Database Upgrades' folder of AS 7.0.3 software.

Use 'Database_released_code_702_from_7015' folder code to upgrade the database from AS 7.0.1.5 to AS 7.0.2.

AS 7.0.1 to AS 7.0.2, using the database zip file in the AS 7.0.3 software:

Extract 'Database_released_code_702.zip' in 'Previous Database Upgrades' folder of AS 7.0.3 software.

Use 'Database_released_code_702_from_701' folder code to upgrade the database from AS 7.0.1 to AS 7.0.2.

Please refer to the Argus Safety 7.0.2 Installation Guide for upgrade instructions.

Database Upgrade Procedure (with or without DLP) from AS 7.0.2 to AS 7.0.3

Note: The Oracle Database Server version should be upgraded to 11.2.0.3 prior to upgrading the database from 7.0.2 to 7.0.3.

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 ensure 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:

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.

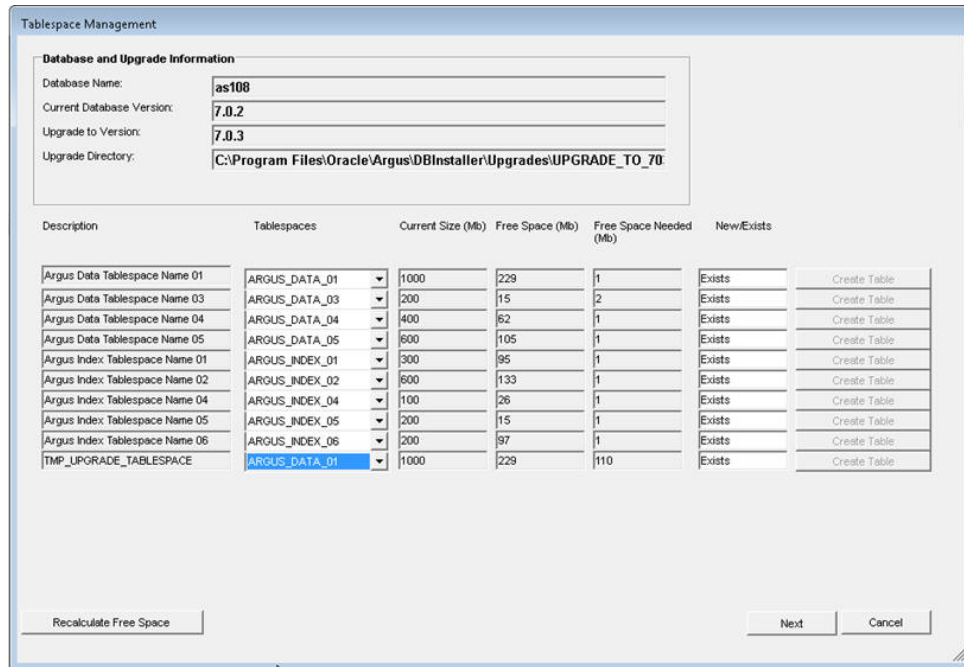
Note: The three optional functions SF_CASE_SERIOUSNESS, SF_CASE_LISTEDNESS, and SF_CASE_CAUSALITY have had their signatures changed. The original functions will be spooled to the log file at .\DBInstaller\Upgrades\UPGRADE_TO_703\UPG_SF_FUNCTIONS_SOURCE.LOG. If custom functions are in use, it will be necessary to re-apply them after the upgrade is complete to conform to the new signatures.

- Enter the Argus Safety Schema Owner password.

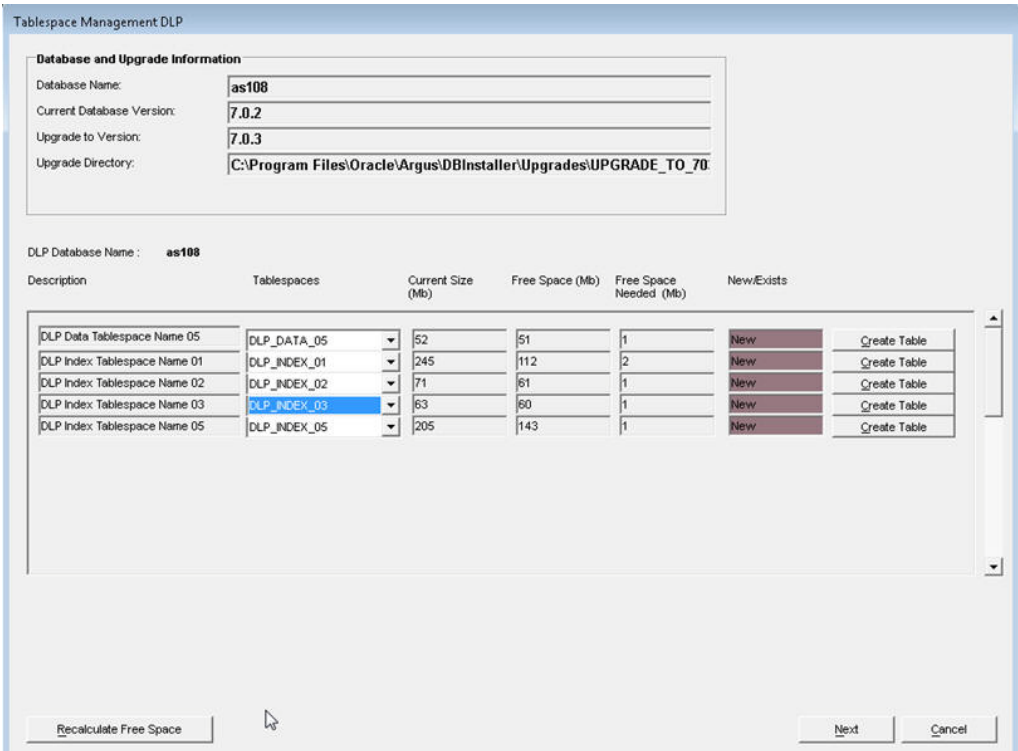
- Enter the ESM Schema Owner password.
- Click Next.

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

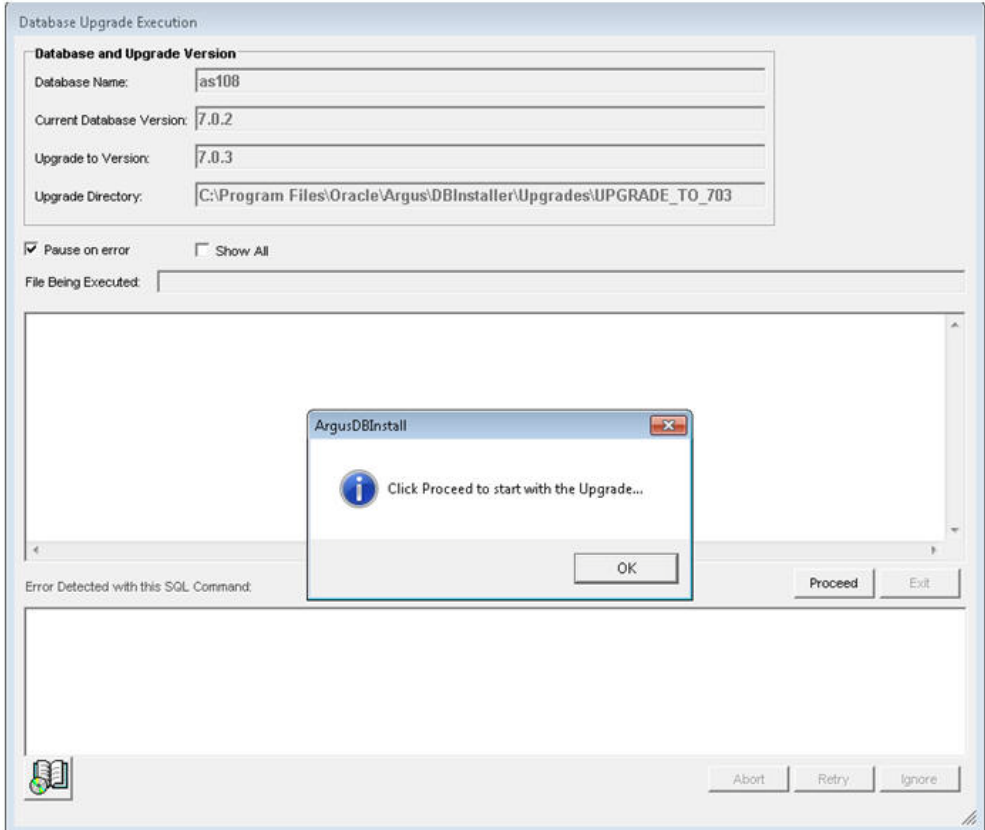
6. When the system loads the Tablespace Management window for the Argus database:



- 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.



- Enter the appropriate path of the tablespace.
8. When the system prompts for confirmation:



- Click OK and then click Proceed on the main screen.
- 9. When the upgrade is complete, the system opens the following window:
 - 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.

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 7.0.3 on a computer where Oracle 11.2.0.3 is installed.
- The source databases should be schema validated at Argus 7.0.3.
- 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 7.0.3 application. Make sure that Oracle Client version is 11.2.0.3.
- The Target databases should be Schema Validated at Argus 7.0.3.
- 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 please 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. Please 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. Please 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 Target 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 ensure 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 7.0.3 Schema Creation tool.
6. Import into Target database by running C:\CONFIG_EXP_IMP_70\ Data_ImportConfigOnly_11g.bat and follow the prompts
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.

Installing Argus Safety Web

This chapter includes the following sections:

- [Installing Argus Safety Web](#)
- [Adding the Argus Site as a Trusted Site](#)
- [Configuring the IIS Manager for Windows 2008](#)
- [Connecting to a Domain Account on Windows 2008](#)
- [Enabling SSL Support for Windows 2008](#)
- [Configuring Load Balancer in Argus Web](#)
- [Installing Argus Report Server](#)
- [Securing Sensitive Configuration and Operational Data](#)
- [Configuring Identity in the IIS Application Pools](#)
- [Resetting IIS](#)

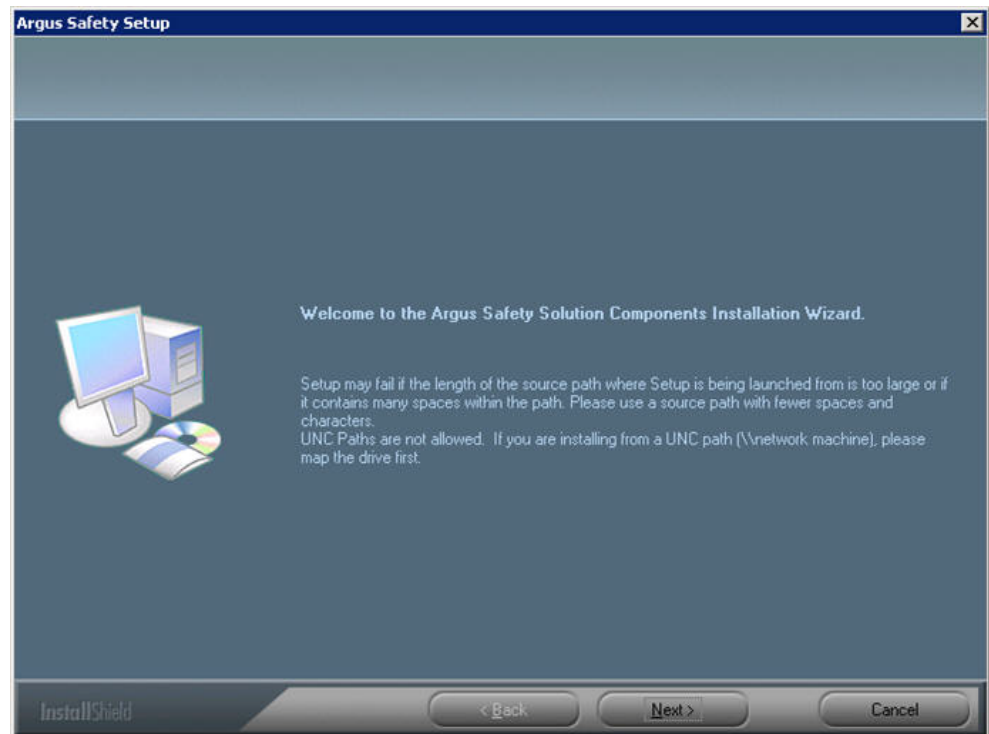
Installing Argus Safety Web

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

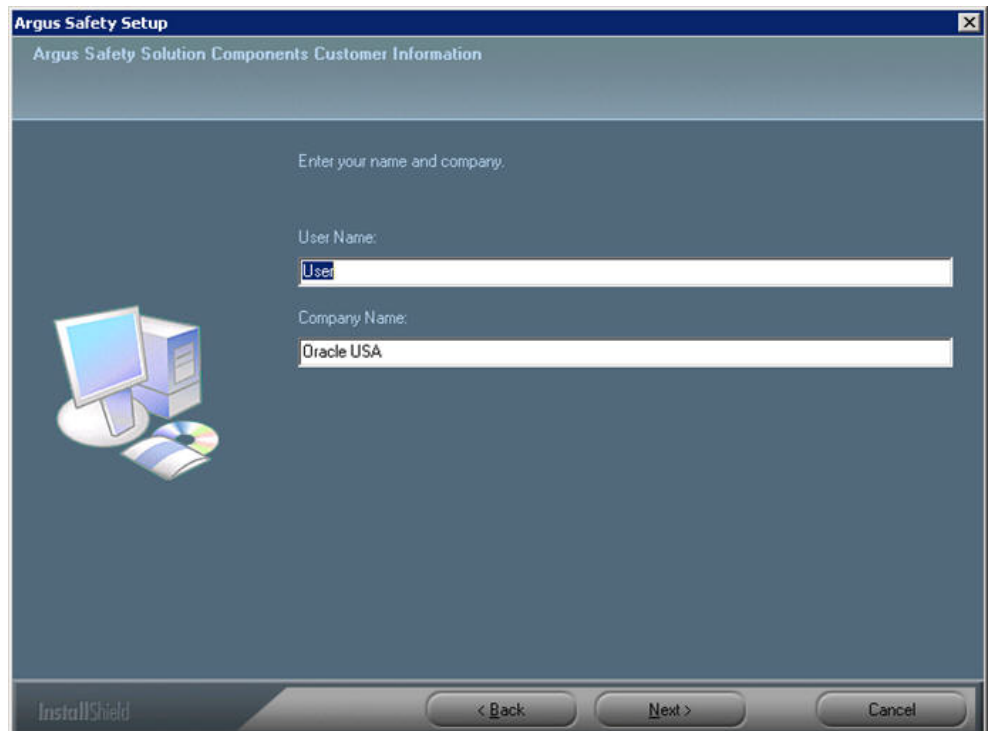
- During the installation, the information in this document may be different from what you see on your monitor if additional modules were selected during the Argus Safety Web Installation.
- A domain account with Local Administrator privileges to the Web server is required after the Argus Safety Web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

Use the following procedure to install Argus Safety Web:

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

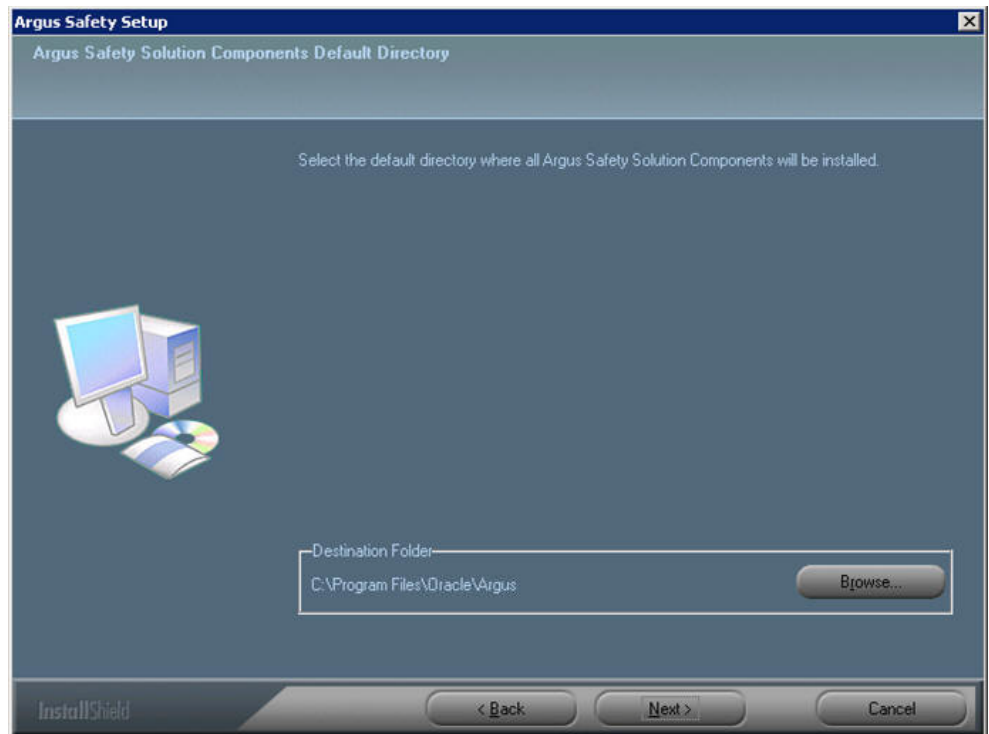


3. When the system displays the Customer Information screen:

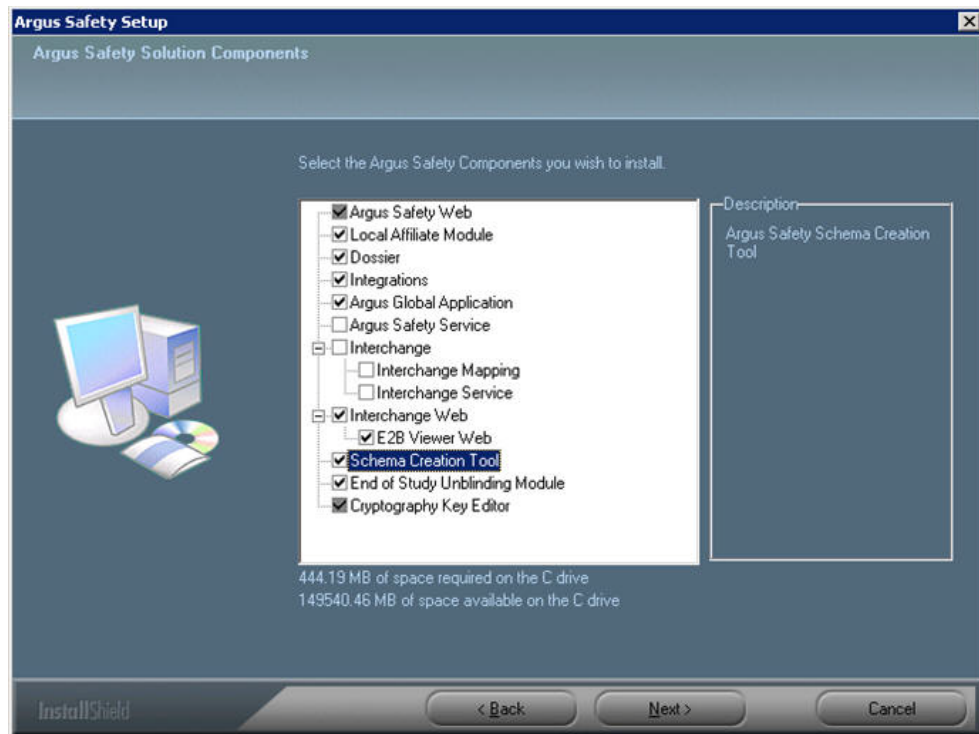


4. Enter the user name in the User Name field.
5. Enter the company name in the Company Name field.
6. Click Next >.

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.



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



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

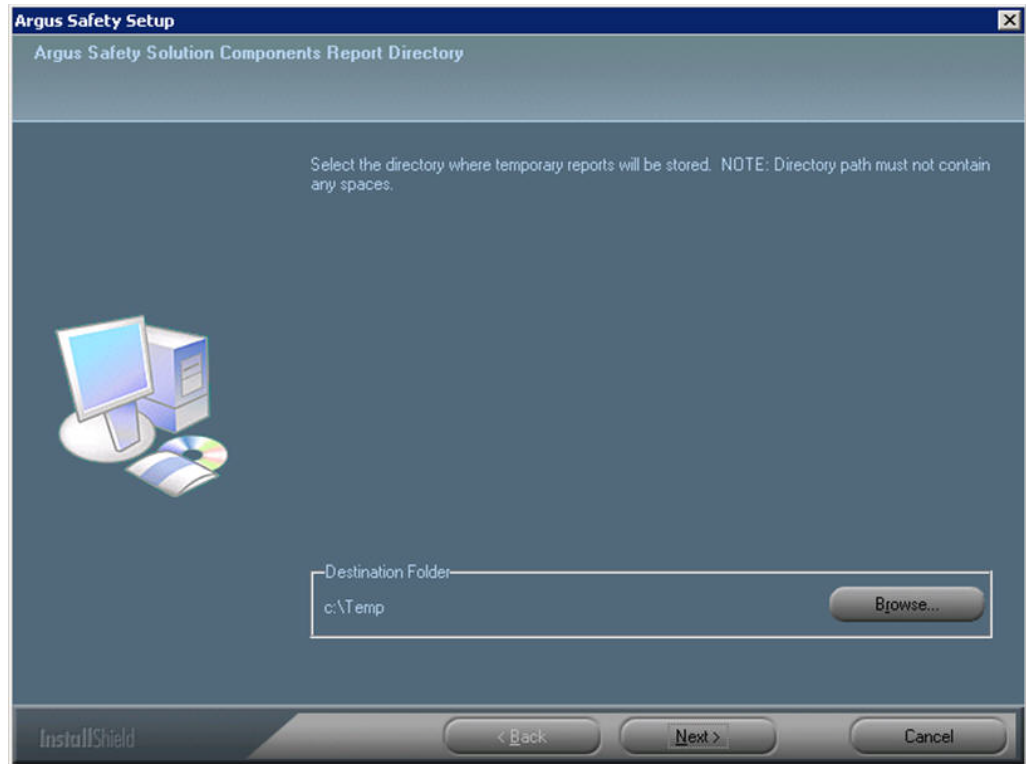
On selecting this option, global modules get installed on the same web server as Argus Safety Web and are accessible as a separate URL from the same web server. Global modules are components of Global Application having the same functionality as Portlets in the Global Homepage for Web Center.

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

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

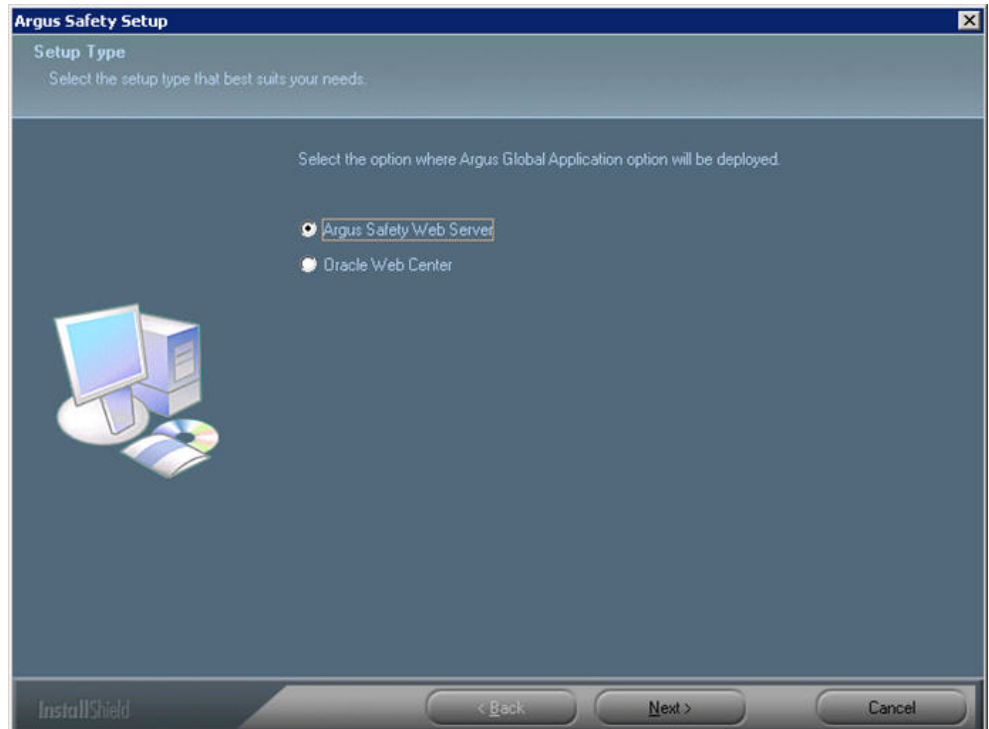
The Argus Global Application for the Argus Safety Web option is enabled only if Argus Safety Web is also selected.

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).

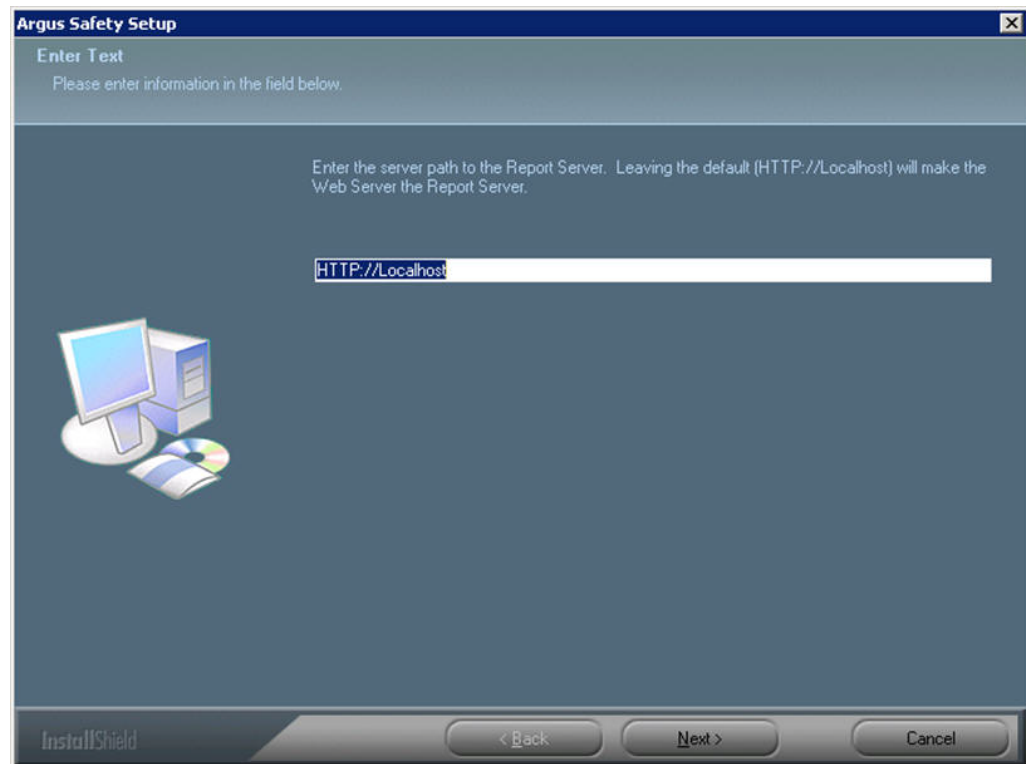


Note: It is recommended to install the Cryptography tool on the Web Server.

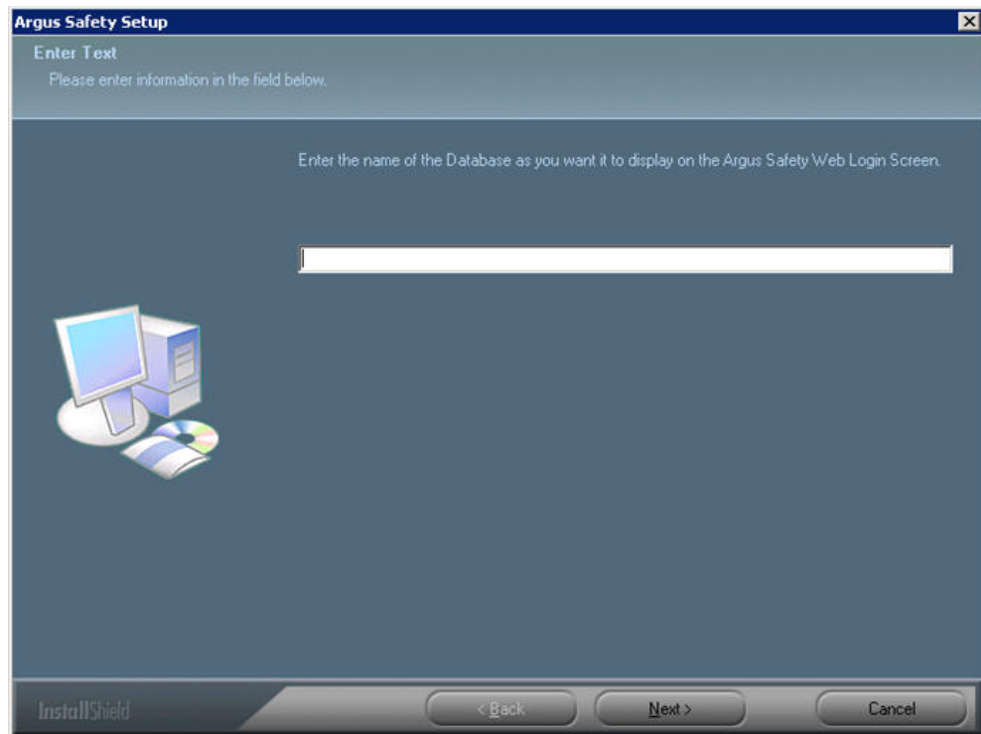
11. Click Next. The following screen is displayed:



12. Select the applicable Setup Type from the listed radio buttons, where the Argus Global Application will be deployed and click **Next >**.
13. Select Report Server Path if Report Server is configured on a separate Box. Leaving the default will configure the Web Server as the Report Server.

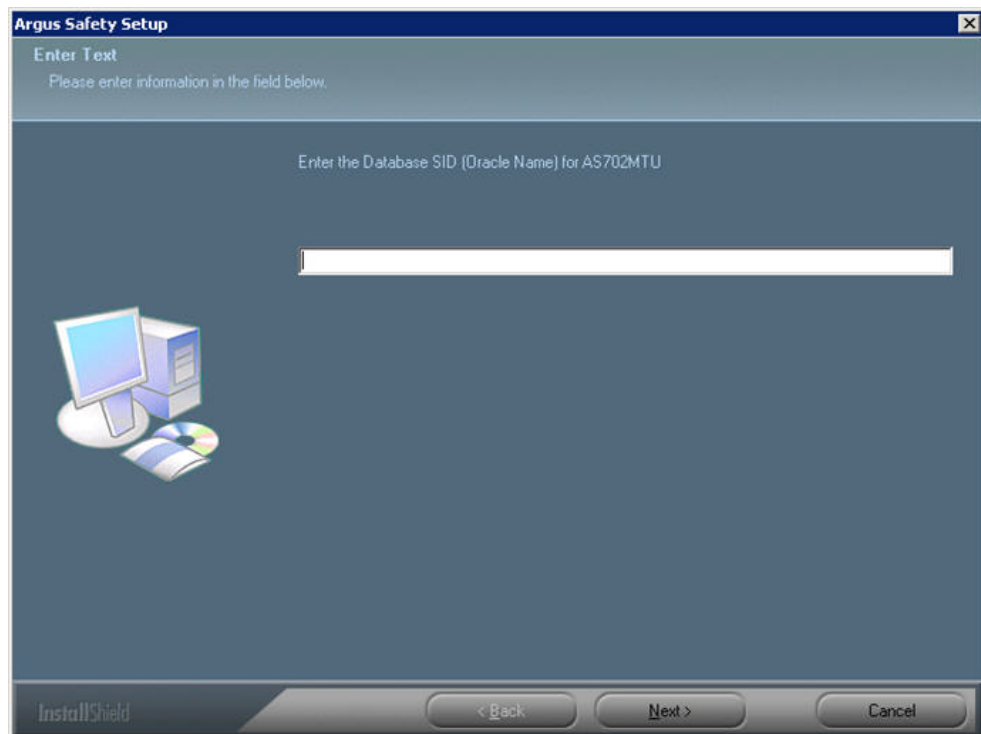


14. When the system asks whether you want to configure a database for Argus, click **Yes** to configure a database.
15. When prompted to enter a database name, enter the database name as you want it to appear on the Argus Login page.



16. Click Next > to continue.

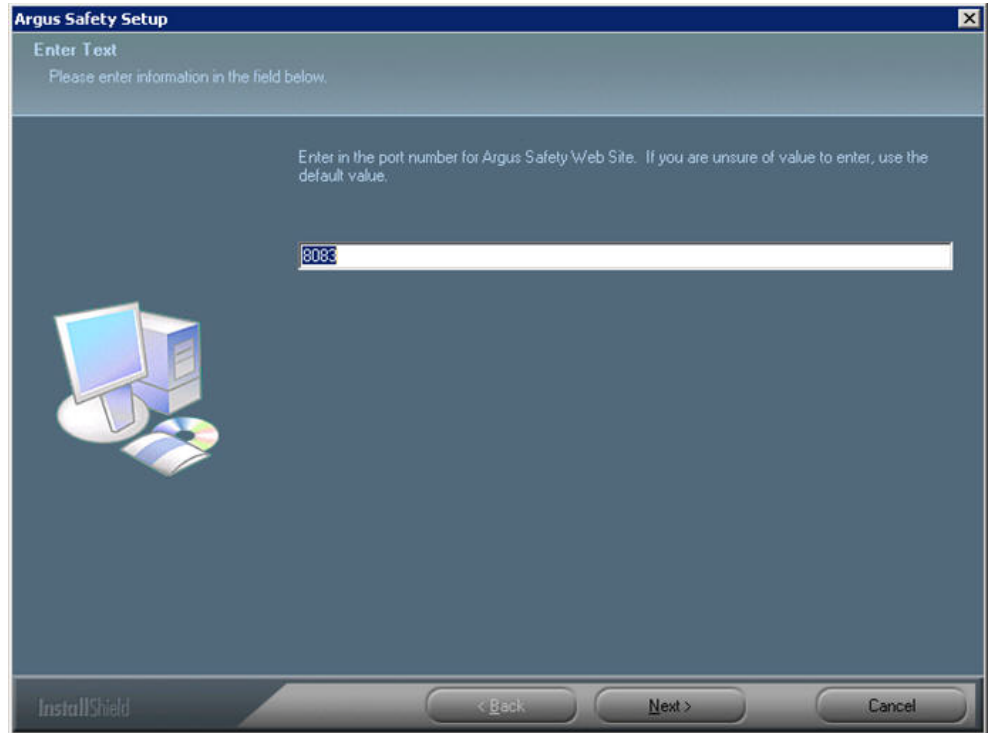
17. When prompted to enter the database SID: Enter the database SID.



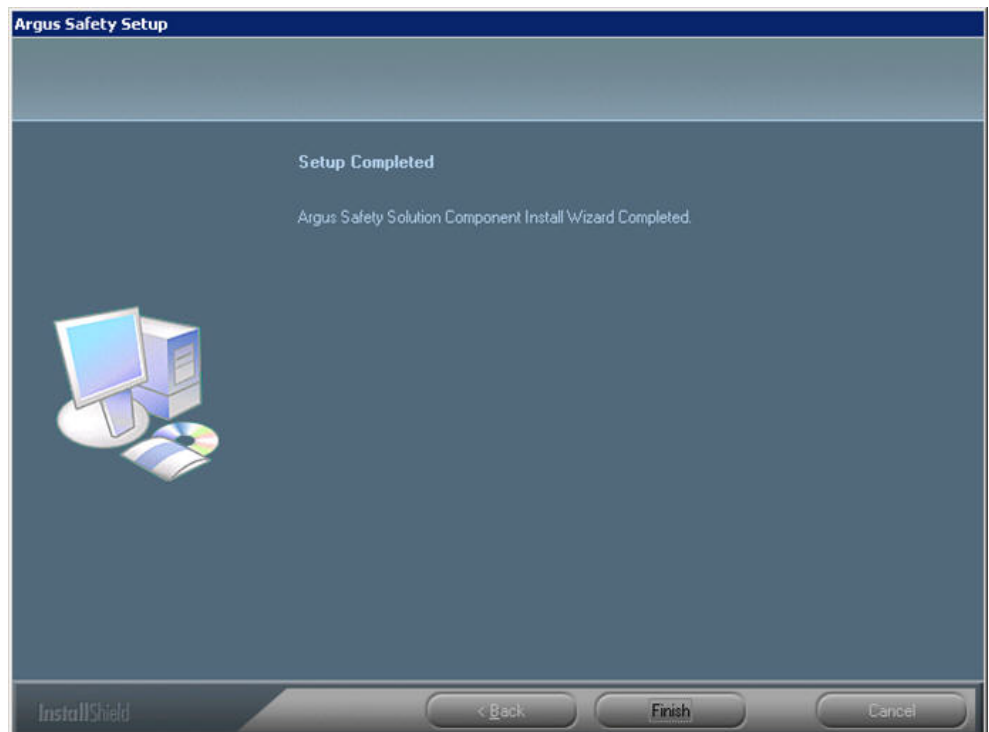
18. Click Next > to continue.

19. When the system asks if you would like to configure database settings for Argus: Click **Yes** to add an additional database to the Argus Login page.

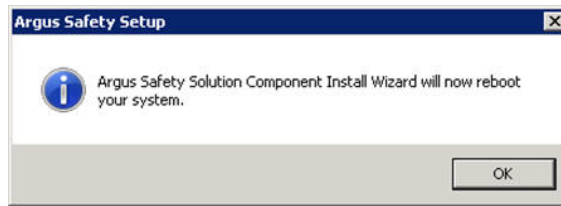
20. When the system prompts you to enter a port number, enter the Port for the Argus Web site (default is 8083).



21. Click Next > to continue.
22. The installer installs the Web site and its related components and shows the progress of the installation.
23. When the system displays the Setup Completed screen, click Finish.



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



Note: After installing Argus Safety Web, refer to the section [The Argus Safety 7.0.3 Application Servers](#) to set up the Argus Cryptography key.

Adding the Argus Site as a Trusted Site

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

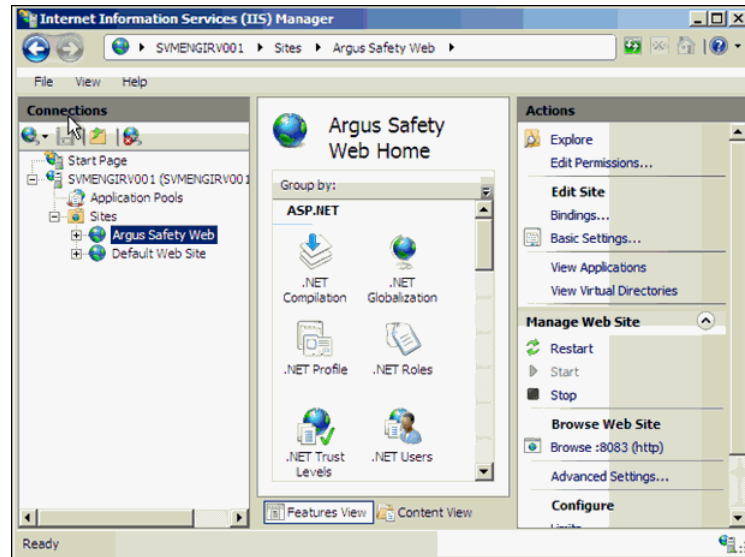
1. Open **Internet Explorer**.
2. Select **Tools => Internet Options**.
3. When the system displays the Internet Options dialog box.
4. When the system displays the Security tab: select **Local Intranet or Trusted Sites** and click **Sites**.
5. When the system displays the **Trusted Sites** dialog box.
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.

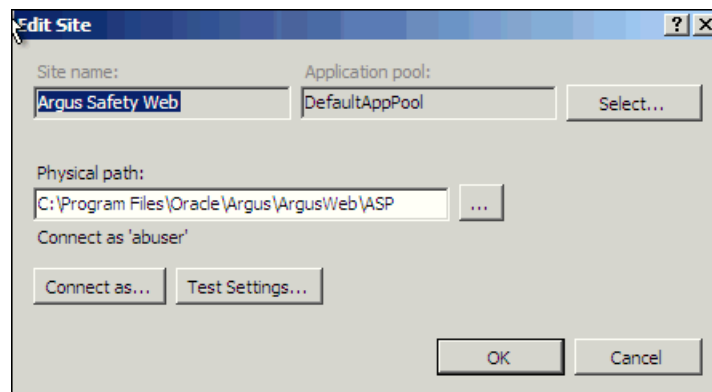
Configuring the IIS Manager for Windows 2008

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

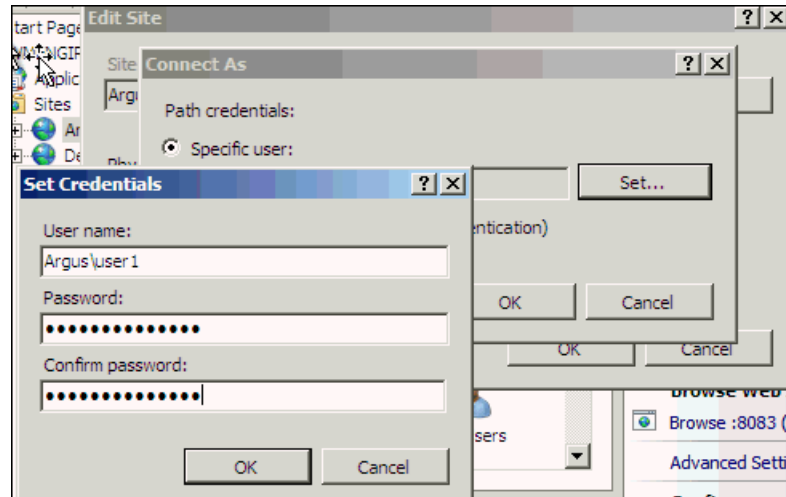
1. Select **Start => Administrative Tools => Internet Information Services (IIS) Manager**.
2. Expand the Connection Panel and open "Sites".
3. Select Argus Safety Web.



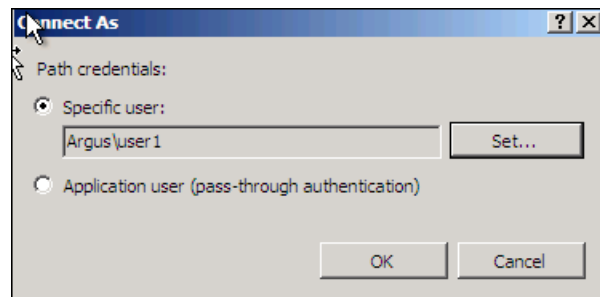
4. On the right panel, click on Basic Settings.



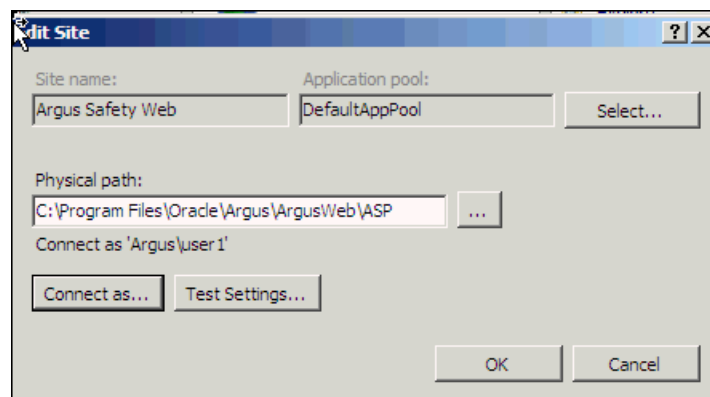
5. Click on Connect as...
6. Click on Specific User and click on Set.
7. Enter Domain user name and password and click OK.



8. Click OK.



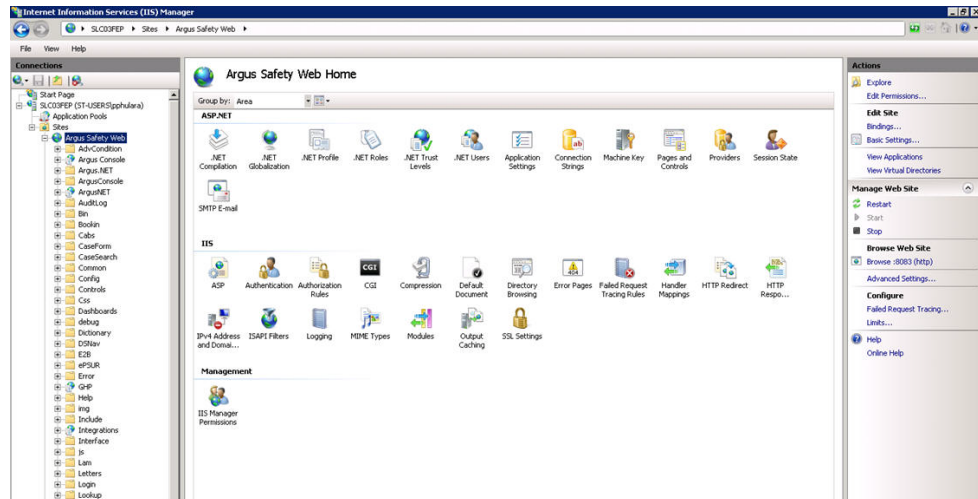
9. Click on Test Settings to verify the user credential is valid for the connection.



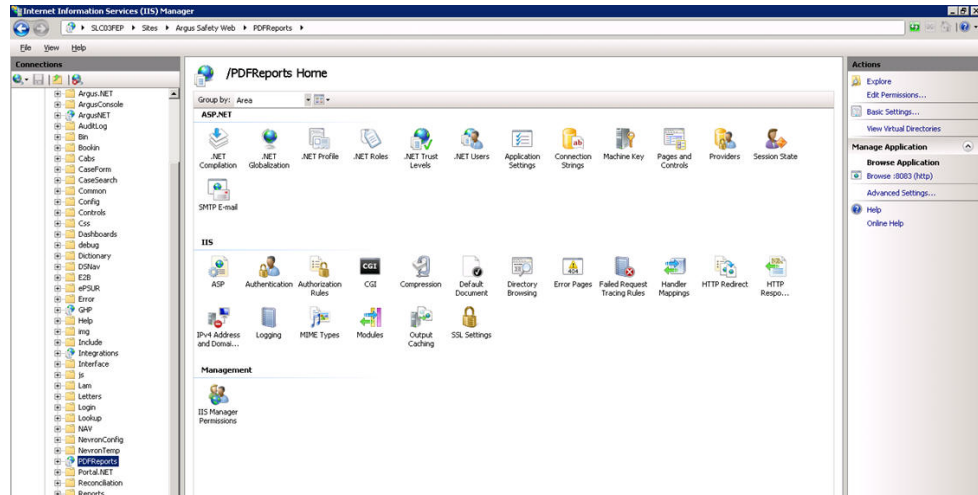
Connecting to a Domain Account on Windows 2008

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.

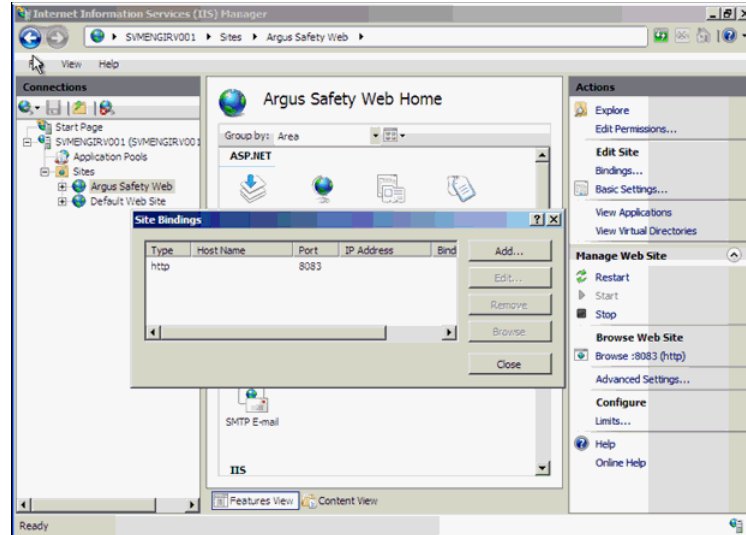
Note: You can click on Test Settings to verify the user authentication for the connection.

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

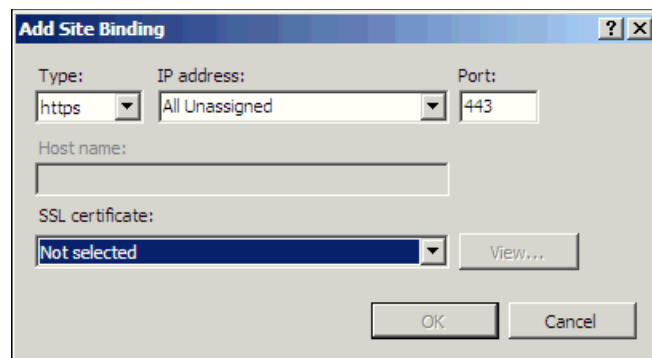
Enabling SSL Support for Windows 2008

Use the following procedure to enable SSL support for 2008:

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



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



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 ensure that the client machine has also got access to that share.

Installing Argus Report Server

Argus Report Server enables the Argus Web Server to offload or redirect the tasks for all reports such as Periodic, Expedited, E2B and System Reports to the Report Server. This enables the Web Server to effectively handle the actual end-user HTTP requests rather than spending system resources on report generation tasks.

Argus supports multiple Report Servers. However, these report servers cannot be put under a Load Balancer. Each web server configuration has to point to the report servers individually.

The Report Server installation and configuration is exactly same the Web Server configuration. The only difference is in the values of the ReportServer, ReportServerUser, and ReportServerPassword parameters in the Argus.ini file for the Web and Report Servers.

If you are using Report Server, the sample values of these three parameters on the Web / Report Server are displayed in the following table.

#	Parameter	Sample Value	Description
1	ReportServer	http://localhost	This parameter points to the Report Server URL for the Argus application.
2	ReportServerUser	reportuser	This is the username of an Argus user with user type as AG Service User configured in Argus database. This value must be unique for each report server.

#	Parameter	Sample Value	Description
3	ReportServerPassword	password	This is the password for the Report Server User in Argus database as described above.

Caution: Be aware of the following:

In the Argus.ini file on the Report Server, the ReportServer parameter must point to itself. For example, it can have a value such as `http://localhost`.

After installing the Report Server, you need to configure Argus.xml and Argus.ini. Instructions for doing so are available in [Chapter 12, Other Tasks](#).

Recommended Changes in IIS 7.5 on the Report Server

You need to use the Application Initialization module in IIS 7.5 to automatically start an IIS worker process without waiting for requests.

It is highly recommended to make the following changes in `C:\Windows\System32\inetsrv\config\applicationHost.config`:

```
<system.applicationHost>
```

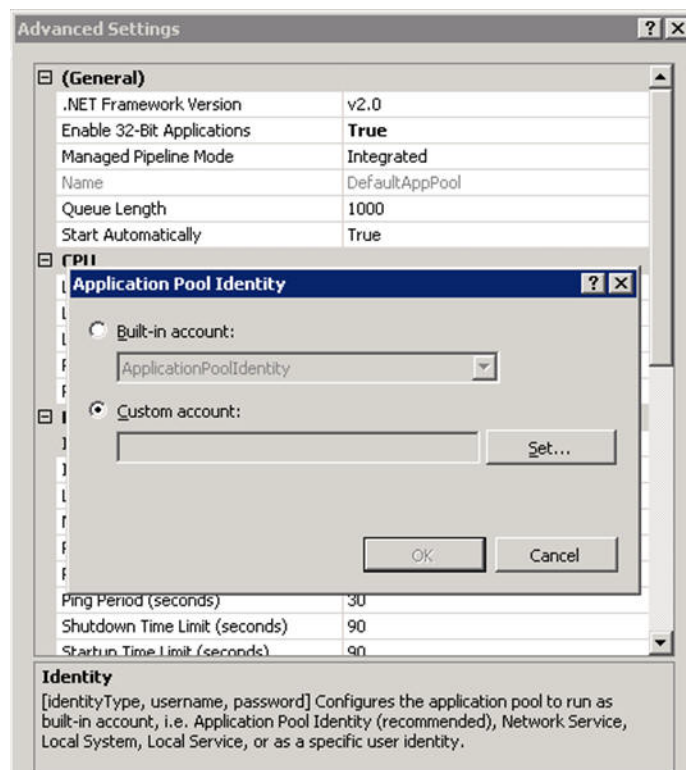
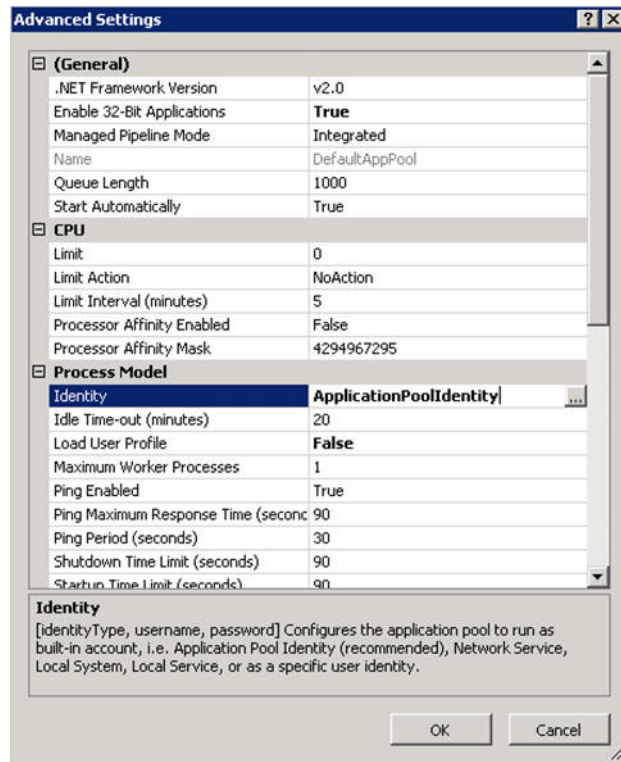
```
<applicationPools>
```

```
<add name="DefaultAppPool" enable32BitAppOnWin64="true" autoStart="true"
startMode="AlwaysRunning">
```

Note: Add the highlighted text (in **bold**) above in the `applicationhost.config` file. The other configurations can be made through the User Interface of IIS.

```
<processModel identityType="SpecificUser" userName="admin"
password="[enc:IISWASOnlyAesProvider:8CzE5P2agbC8fjbMLfitUX2bjn40PbikwgPC
rd4Dfx8=:enc]" />
```

To configure this process, execute the steps displayed in the following screens:



```
</add>
```

```
</applicationPools>
```

```
</system.applicationHost>
```

```
<application path="/" applicationPool="DefaultAppPool" preloadEnabled="true">
```

Note: Add the highlighted text (in **bold**) above in the applicationhost.config file. The other configurations can be made through the User Interface of IIS.

```
<virtualDirectory path="/" physicalPath="C:\Program Files
(x86)\Oracle\Argus\ArgusWeb\ASP" />

</application>
```

Securing Sensitive Configuration and Operational Data

The following security recommendations should be made to the following files and folders on the Safety Web and Report Server. 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 dictionaries

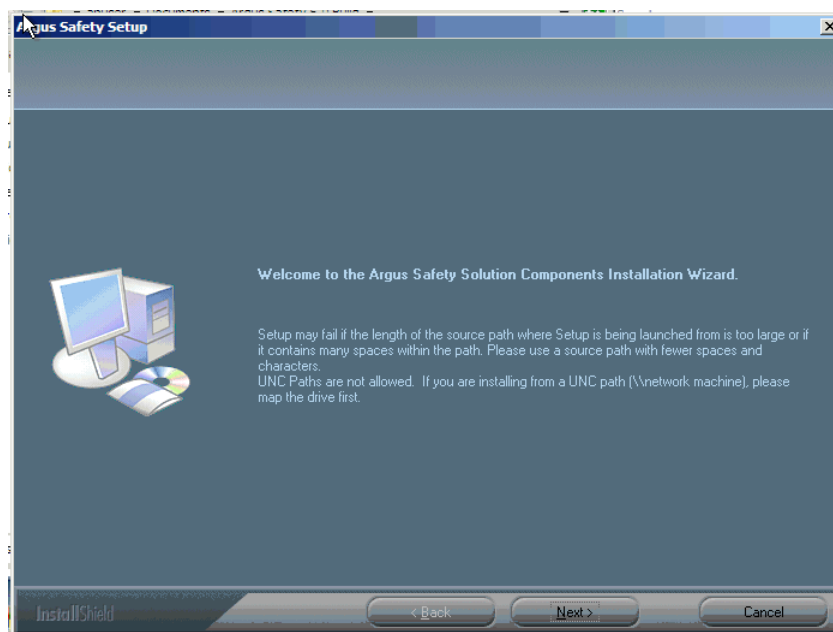
Installing Argus Safety Service

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

See [Section , "Setting Up easyPDF"](#) to continue installing Argus Safety Service.

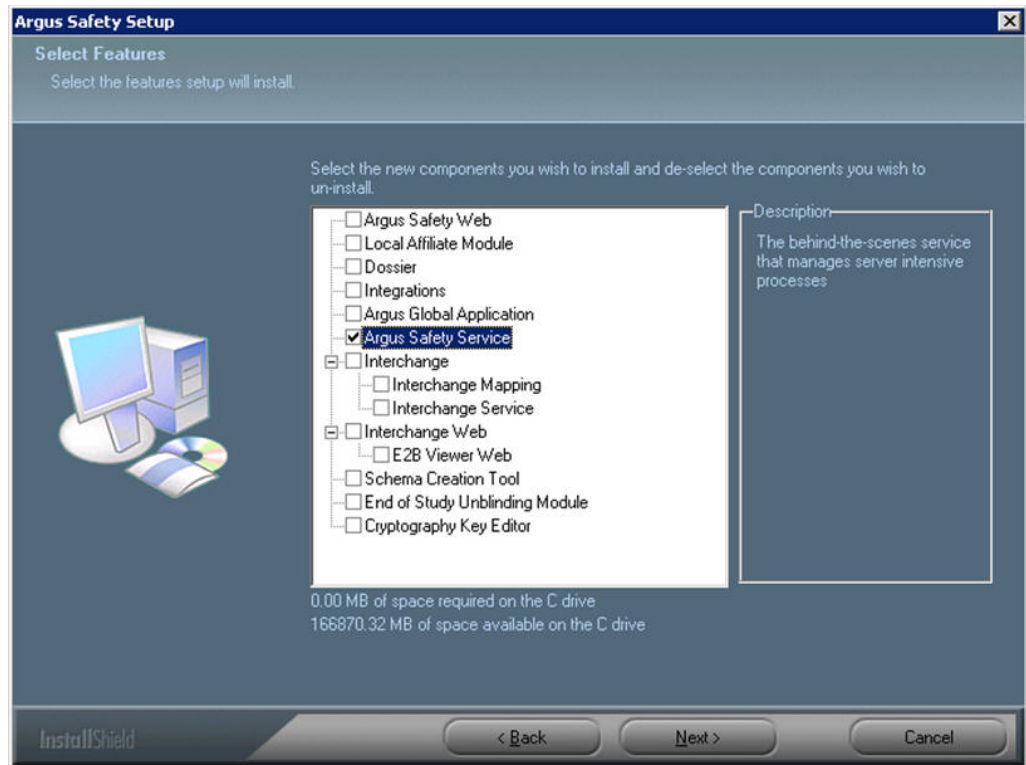
To install Argus Safety Service:

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

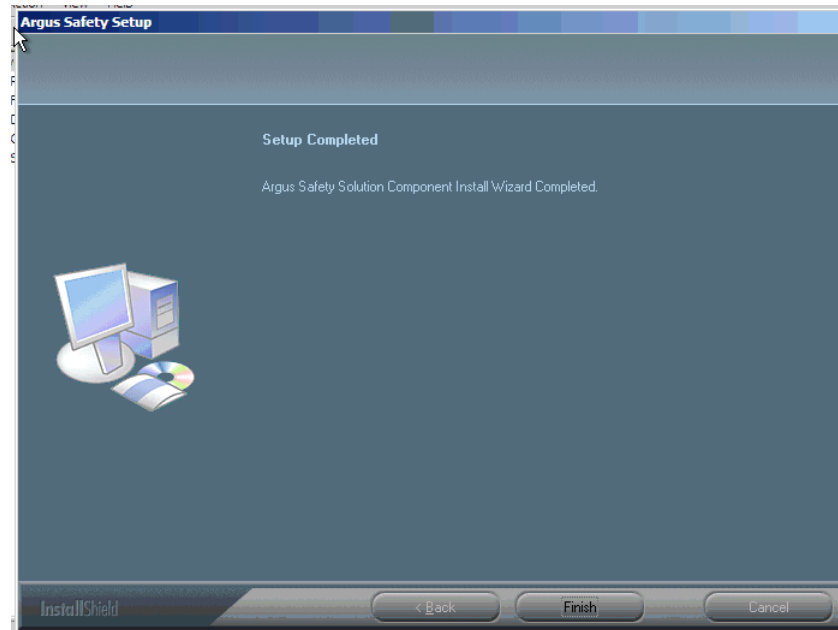


3. When the system displays the Customer Information dialog box:
4. Enter the User Name and Company Name.
5. Click **Next >**.
6. When the system opens the Default Directory dialog box, Click Browse to select the default installation directory where the Argus Safety Solution Components will be installed.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

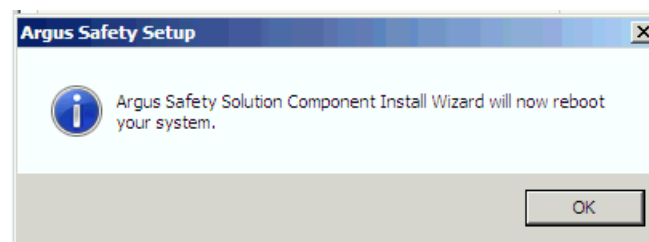
8. When the system opens the Argus Safety Components list:
9. Select **Argus Safety Service** from the list.



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



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



17. See [Chapter 12, "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 Argus Safety Service, refer to the section [The Argus Safety 7.0.3 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.

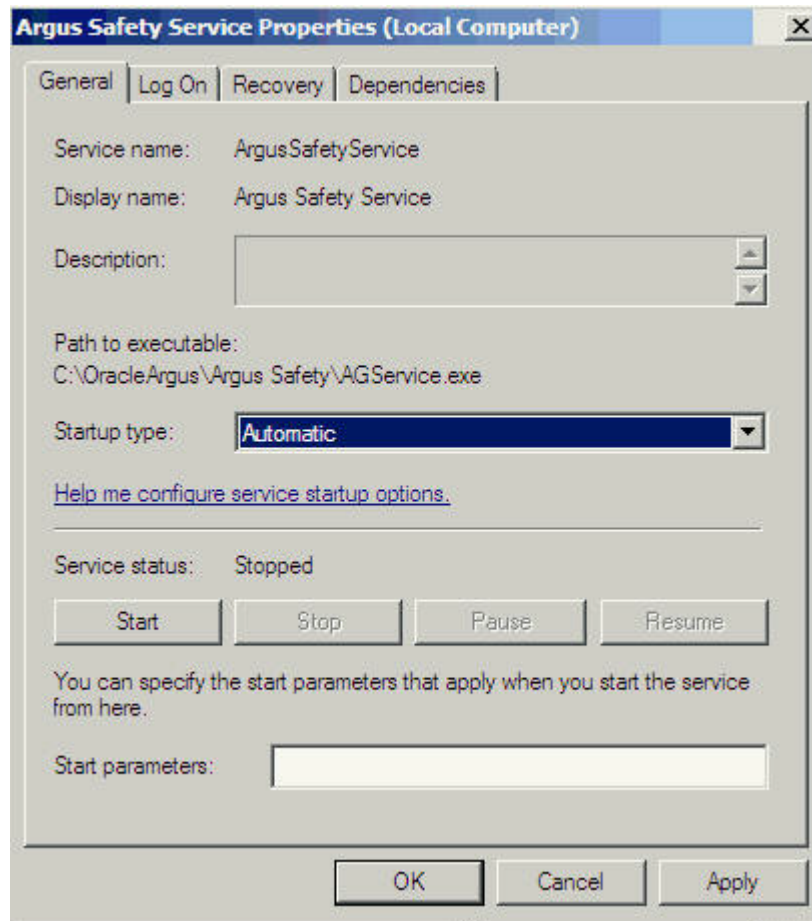
Starting Argus Safety Service

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

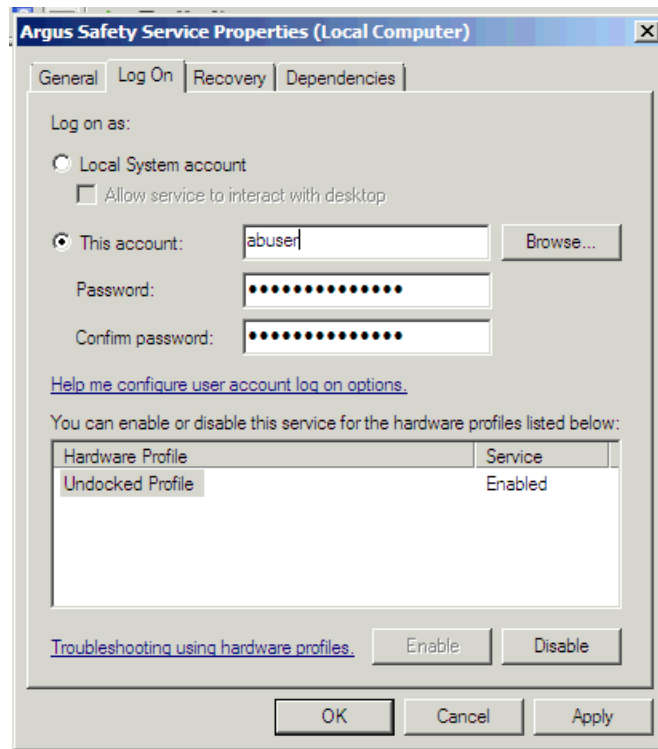
To start Argus Safety Service:

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.

- The following screen is displayed when the system opens the Argus Safety Service Properties dialog box:



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

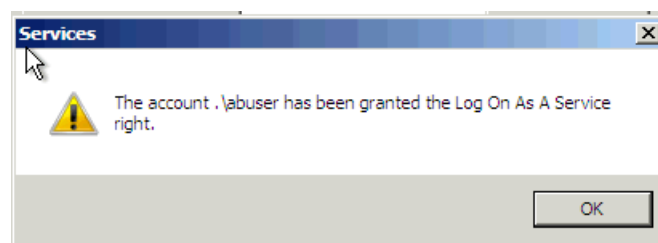


Note: Before starting Argus Safety Service, ensure that the service has been installed and at least one process has been configured. Refer to the Argus Safety Service Administrator's Guide for information on configuring Argus Safety Service Process.

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

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

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



13. When the system redisplay 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
 - 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
```

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. 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 GatewayInterchangeService for the local machine.
4. Double click to display the **GatewayInterchangeService Properties** dialog box.
5. When the system opens the GatewayInterchangeService 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>\build\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.iar</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.iar</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. Ensure 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.

Installing and Configuring Interchange

This chapter provides information about installing and configuring Interchange Service.

Note: Microsoft Visual Basic Power Packs 3.0 is required to be installed prior to installing Interchange Mapping.

It includes discussions of the following:

- [Installing Interchange Service](#)
- [Configuring Interchange Service](#)
- [Accessing EDI Gateway Shared Folders](#)
- [Configuring the Interchange Service.INI File](#)

Installing Interchange Service

Before installing Interchange Service, be aware of the following:

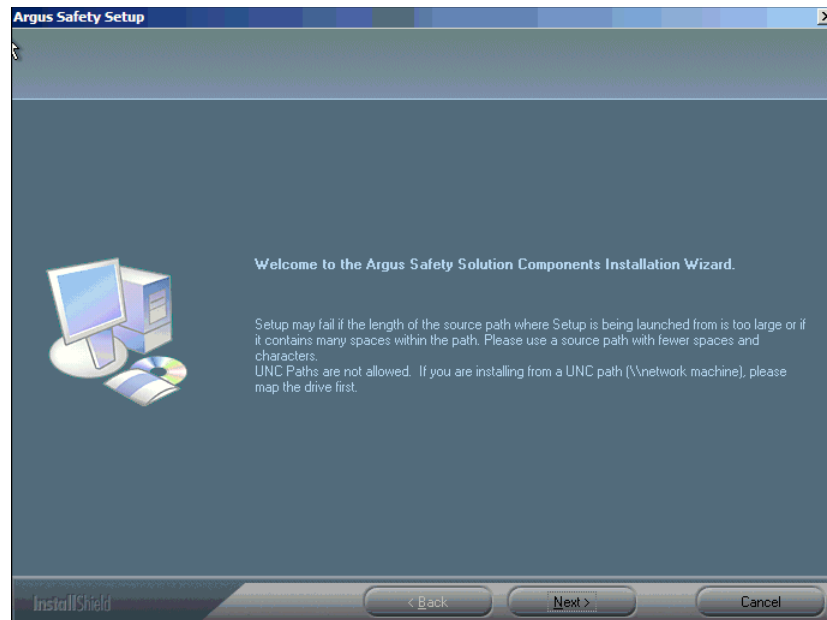
- Since Interchange Mapping has a user interface for configuring Interchange Service, it must be installed on the same system as Interchange Service. If they are not installed on the same system, you will be unable to access the user interface required to configure Interchange Service.
- You must also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

Use the following procedure to install Interchange Service.

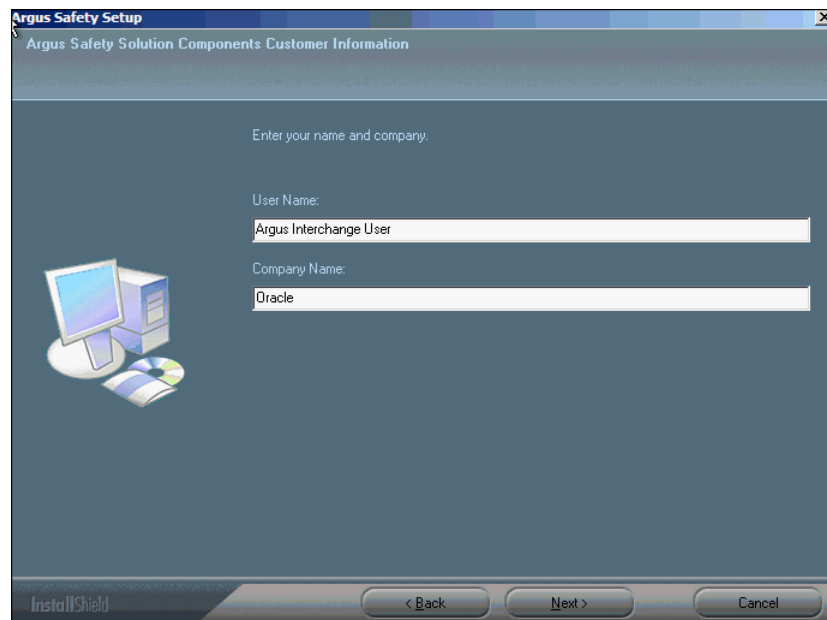
To install Interchange Service:

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

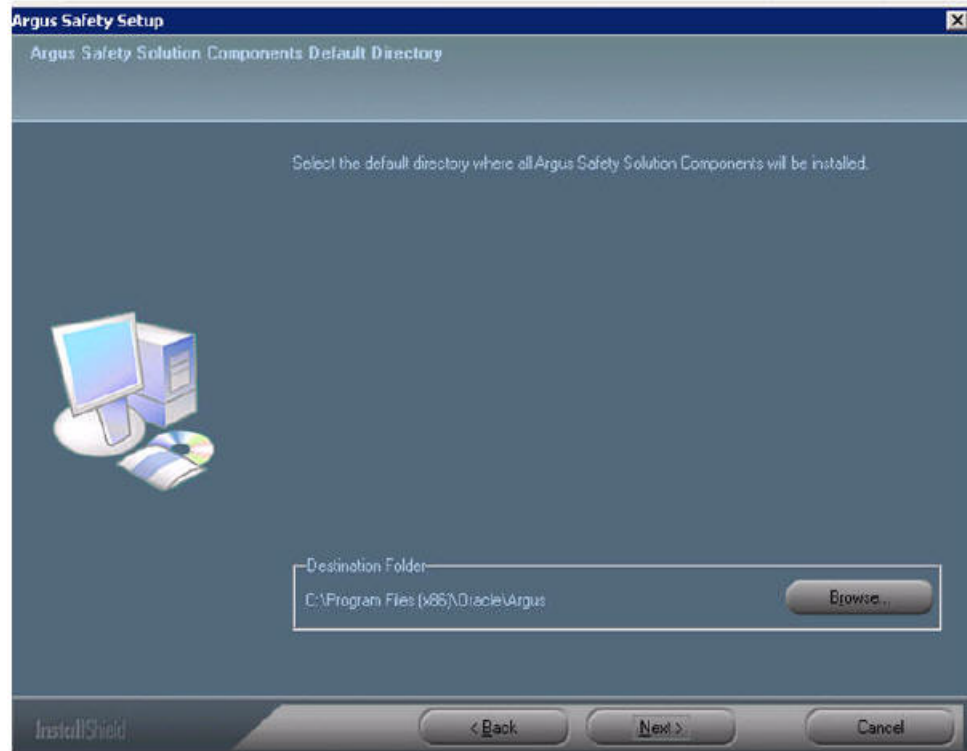
2. When the system displays the Argus Safety Solution Components Install Wizard dialog box, click **Next >** to continue.



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

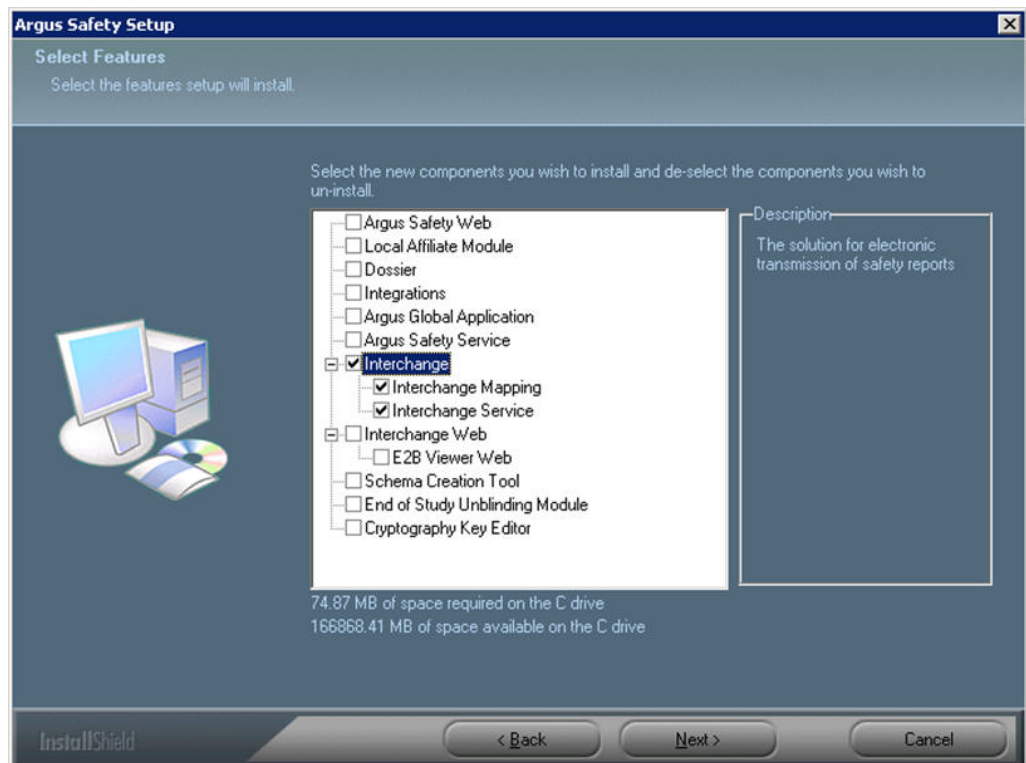


- Type the user name in the **User Name** field.
 - Type the company name in the **Company Name** field.
 - Click **Next >** to continue.
4. When the wizard opens the Default Directory dialog box:



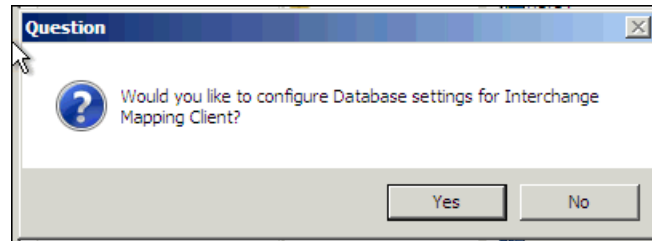
- Click **Browse** to default installation directory for the Argus Safety Solution components.

5. When the wizard opens the dialog box:

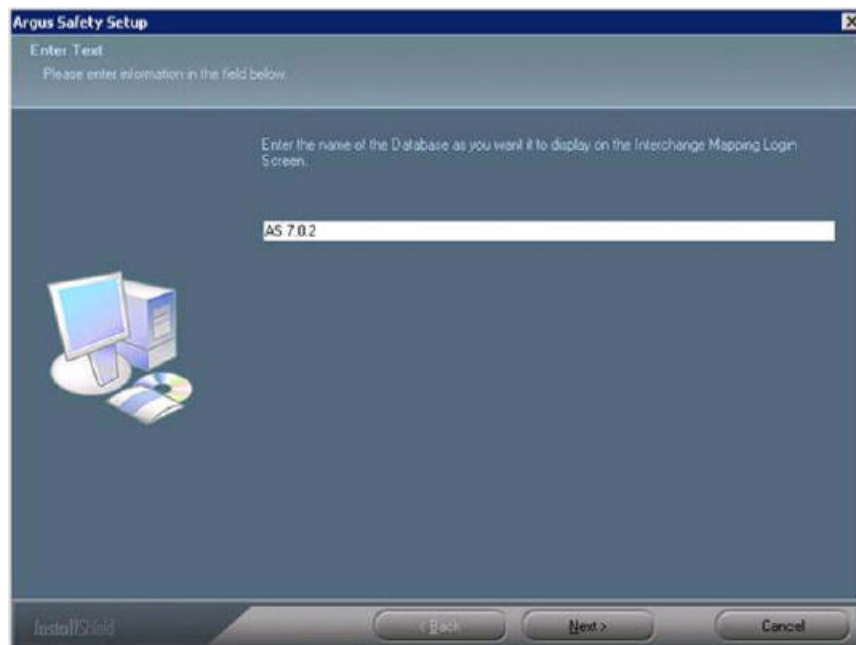


- Select **Interchange**.

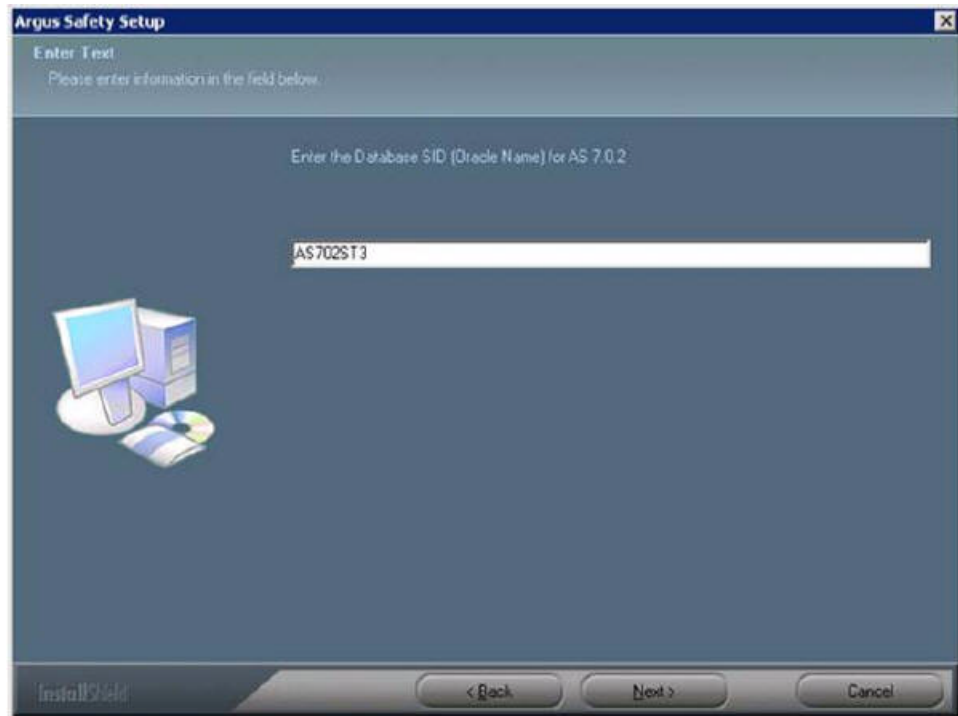
- Click **Next >** to continue.
Argus installs and shows the progress of the installation.
6. When the system asks whether you want to configure a database for Argus Interchange:



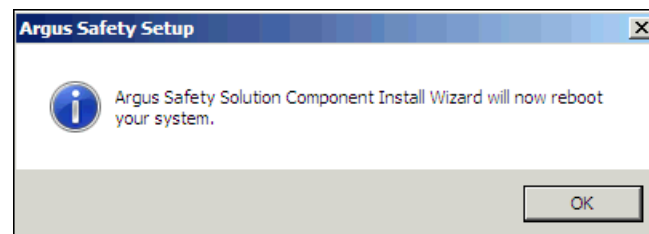
- Click **Yes** to configure a database for Argus Interchange.
7. When prompted to enter a database name:



- Enter the database name as you want it to appear in Argus Interchange.
 - Click **Next >** to continue.
8. When prompted to enter the database SID:



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



11. Click **OK** to reboot.

Note: After installing Interchange Service, refer to the section [The Argus Safety 7.0.3 Application Servers](#) to set up the Argus Cryptography key.

Configuring Interchange Service

Use the following procedure to configure Interchange Service:

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

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

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

Transmitting E2B Attachments

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

Accessing EDI Gateway Shared Folders

Use the following procedure to access EDI gateway shared folders:

1. Log on to the machine where Interchange Service is installed.
2. Browse to the data folder in the Axway Synchrony installation directory.

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

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

Configuring the Interchange Service.INI File

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

Use the following procedure to configure Interchange Service:

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

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

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

Performing Post-installation Checks

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

- [Post-Installation Tasks](#)
- [Verifying the Web Server Installation and IIS Configurations](#)
- [Configure and Verify the Dossier Installation](#)
- [Verify Files installed on Middle Tier Servers:](#)
- [Verifying the Documentum Installation](#)
- [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 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 and Report Server.
- A single domain user account <Domain User> is running Argus Web application on all web servers and report 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, open following files under the installation folder. The installation folder, typically is, C:\Program Files\Oracle\ArgusWeb\ASP\Argus.NET\bin

RelsysWindowsService.exe.config

1. Uncomment the following entries under the <RelsysConfigFilesSection>/<RelsysConfigFiles>
 - Relsys.InterfaceComponents.ProcessorsConfiguration
 - Relsys.CaseIntake.FolderConfiguration
2. Ensure 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 ="receptient@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 ="receptient@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 ="receptient@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 and the path is pointing to the `<PDFReportPath>` folder on the Report Server and that there is an ending `<\>` back slash at the end of the 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, that the path is pointing to the `<UploadedLetterspath>` folder on the Report Server, and that there is an ending `<\>` back slash at the end of the 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. Please 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:

- For Report Server Setup Only - Verify the following on each web server (Excluding Report Server)
 - Cache= <This should be the same shared path to the report server <PDFReportpath> Folder>. Verify that there is an ending <\> back slash at the end of the path.
 - Upload= <This should be the same shared path to the report server <UploadedLetterpath> Folder>. Verify that there is an ending <\> back slash at the end of the path.
 - ReportServer = <ReportServer> <This should have the URL for the Report Server, not Localhost> <If a report server is not being used, leave the default of "http://localhost">
 - ReportServerUser = <ReportServeruser> <Verify that this user is correct and configured in Argus>. This parameter value is case sensitive
- 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:

1. Argus Report Services is enabled.
2. Service is set to automatic on all Web servers if a report server is used.

Verifying the Web Server Installation and IIS Configurations

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

- [Verifying IIS 7 Configuration](#)
- [Configuring the Dossier Application](#)

Verifying IIS 7 Configuration

Use the following procedure to verify the IIS 7 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. Ensure there is no value "Cache Control" header.
6. Click the "Set Common Headers" option.
7. Ensure 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. Ensure that the web site 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. Ensure 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="GOLDDDEMO"
 - 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 ="receptient@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 ="receptient@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 ="receptient@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. Please 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 / Report 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 and Word 2010.

Validating the easyPDF Installation for Word 2007 and Word 2010

Use the following procedure verify that easyPDF has installed correctly.

1. Open Word 2007.
2. Select File=> Word Options. go to file Menu-> Word Option -> Add-ins. Observe that "BCL easyPDF 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.

Enabling IIS HTTP Compression

This chapter describes how to enable IIS HTTP Compression on a Windows 2008 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 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 enable HTTP Compression in IIS 7:

1. Open "Internet Information Services (IIS) manager" from Control Panel -> Administrator Tools.
2. Browse to the "Argus Safety Web" web site.
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. 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. Ensure "Cache Control" header with value of "no-cache" exists.
5. Click the "Set Common Headers" option.
6. Ensure 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. Ensure "Cache Control" header does not exist.
11. Click the "Set Common Headers" option.
12. Ensure 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.

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	<p>This field enables you to select the authentication type. There are three types of authentication:</p> <p>No Authentication</p> <p>In No Authentication, the Username and Password fields are disabled.</p> <p>Basic Authentication</p> <p>The user is required to enter the Username and Password fields. This is the default authentication.</p> <p>NTLM Authentication</p> <p>The authentication of the OS user logged into the system is automatically passed. The Username and Password fields are disabled in this authentication.</p>
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.

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	Please refer to the Hardware requirements for Argus Safety 7.0.3
Database Server	(Same requirements as Argus Safety 7.0.3 Database Server) A Tablespace with 500MB free space to create EOSU Schema Argus 7.0.3 schema (This is a prerequisite for the EOSU package to be installed.)
Client Machine	Windows XP Pro SP3 (English and Japanese) Windows 7 (English and Japanese) Oracle Client v11.2.0.3 Oracle ODAC 11.2.0.3 Microsoft .NET 3.5 Framework Visual C++ 2008 SP1 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, Please 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. Please 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 7.0.3 Application Servers](#) to set up the Argus Cryptography key.

This chapter provides information for performing other installation and configuration tasks. It includes discussions of the following:

- [Configuring the Argus.xml File](#)
- [Configuring the Argus.ini File](#)
- [Deploying a Portlet on Oracle WebLogic Server](#)
- [Pre-Deployment Configuration](#)
- [Configuring SSO in Oracle Access Manager 10g](#)
- [Configuring SSO in Oracle Access Manager 11g](#)
- [Installation and Configuration of Oracle Web Tier Suite](#)
- [Configuring the WebCenter Security Provider for Identity Assertion](#)
- [Installation Maintenance Tasks](#)
- [Web Client Tips](#)
- [Clearing Oracle Temp Files](#)
- [Configuring easyPDF](#)
- [Setting Printer Defaults](#)

Configuring the Argus.xml File

The Argus.xml file is generated during installation on Argus Web / Report Server, 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>	<p>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.</p> <p>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</p> <p><DBNAME id="TESTDB">Testing Database</DBNAME>.</p>

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 / Report Server 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/Report Server and some are specific to the Transactional (AG) Server

Parameters specific to the Web / Report Server are:

- ReportServer
- ReportServerUser
- ReportServerPassword
- 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 / report 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 / report servers, this is a shared path on the network. For use with Web/Report Server.

#	Section	Parameter	Sample Value	Description
3	Workstation	Upload	c:\ArgusReports\Upload edLetters\	This is the shared path for uploaded letters. In case of multiple web / report servers, this is a shared path on the network. For use with Web/Report Server.
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/Report 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\Docume ntation\	This is the base folder where all the files related to various modules of Argus are placed.
7	Workstation	PrintRunTime	10	This is used by the AG Service Print 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/Report 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	Workstation	ReportServer	http://<ReportServerPat h>:8083/	In case of Report Server, enter the path of the Report Server along with its Port Number. If the Report Server is the same as the Web Server, the value of this parameter should be http://localhost:8083/
12	PDFReports	TempFileDeleteInter val	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.

#	Section	Parameter	Sample Value	Description
13	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.
14	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.
15	Argus Server	Pool_Initial_Size	3	This refers to the DB Connection Pool Initial Size. For use with Web/Report Server.
16	Argus Server	Pool_Maximum_Size	120	This refers to the DB Connection Pool Maximum Size. For use with Web/Report Server.
17	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/Report Server.
18	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/Report Server.
19	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.

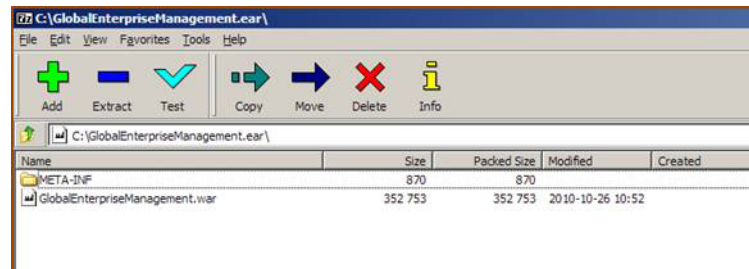
Follow the steps listed below to increase the IE Timeout Setting (and thereby run Reports successfully):

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.

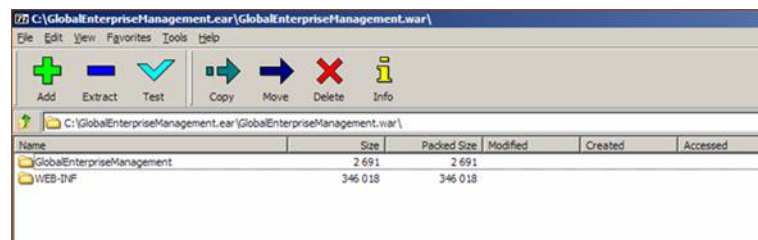
Deploying a Portlet on Oracle WebLogic Server

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.

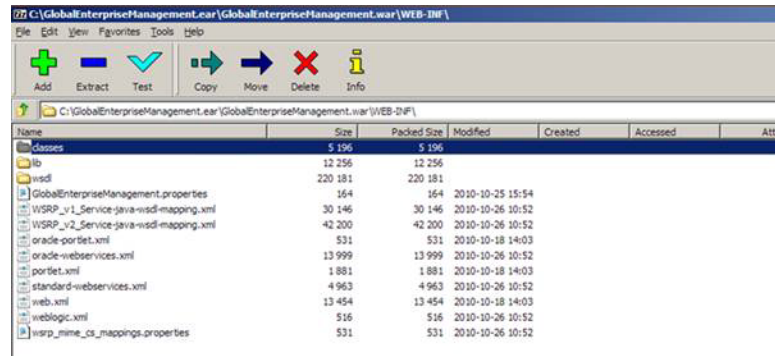
1. Open the .ear file using a Zip utility. The zip program will open with files as seen below.



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

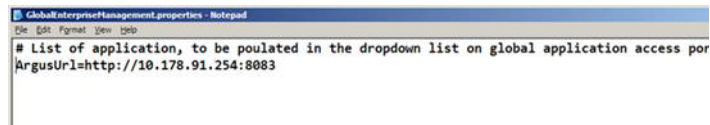


3. Double click the file **portletname.properties** where portletname is the name of the portlet ear file under modification.



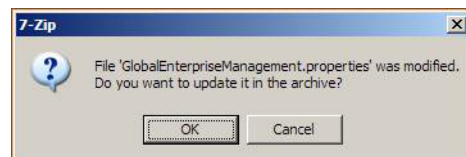
- In the editor find the key named “ArgusURL” and modify the URL value to the value of your Argus Web Server or Argus Web Load Balancer.

ArgusUrl=http://10.178.91.250:8083. For OAM integration, Oracle recommends that using the FQDN of the machine.

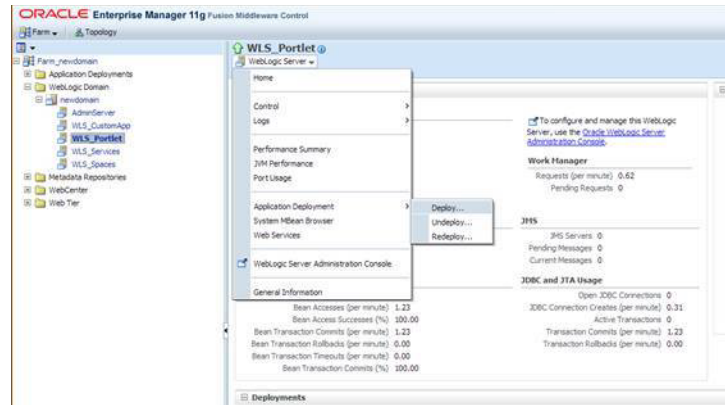


Note: Please make sure there is no space between the tokens “ArgusUrl”, “=” and the actual URL value.

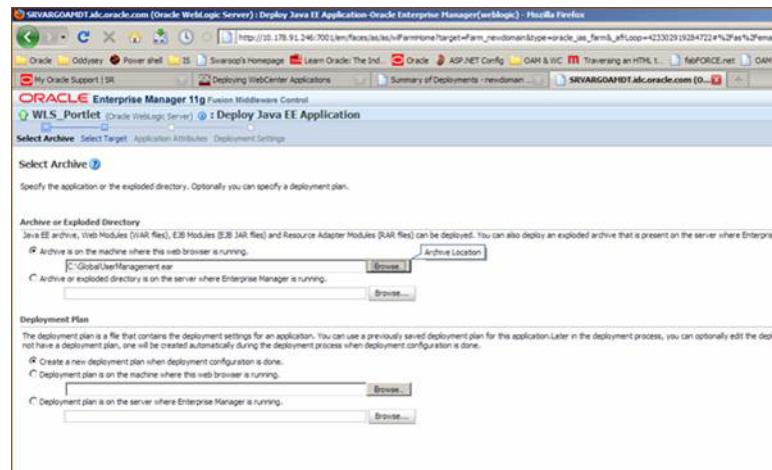
- Save the changes to the properties file and close it. Close the 7-zip manager window and press OK to save the changes in the archive. You are now ready to deploy the ear file.



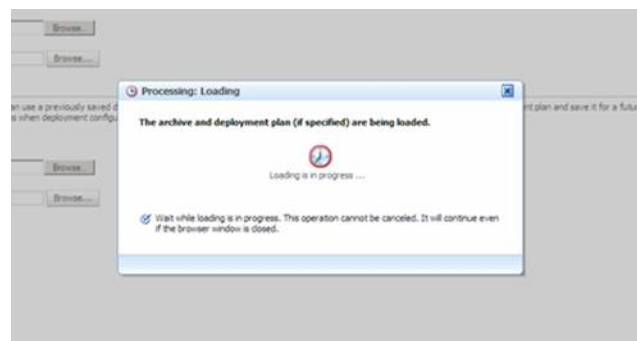
- Log in to the Oracle Enterprise Manager Admin Console and navigate to **WebLogic Domain>Your Domain>WLS_Portlet**. From the top left corner, navigate to **Weblogic Server >Application Deployment>Deploy**.



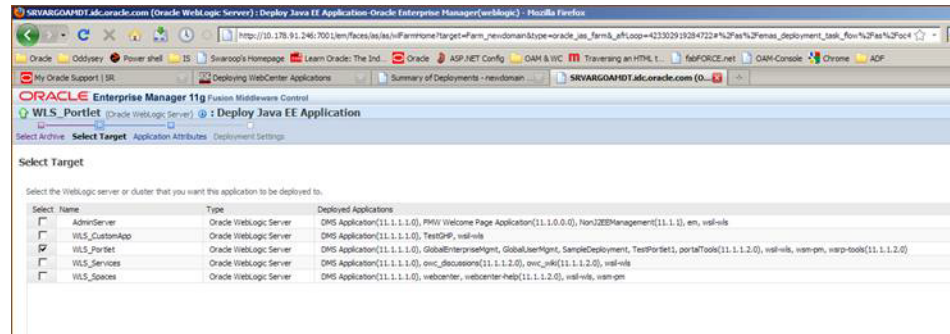
7. Select **Archive** is on the machine where this web browser is running and click **Browse**. Browse to the modified .ear file on your local machine.



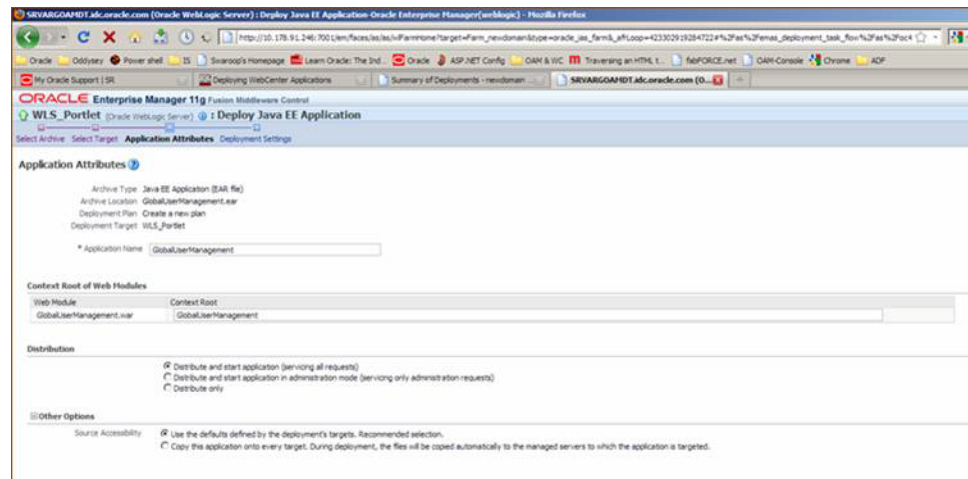
8. The Portlet will now get uploaded to the server.



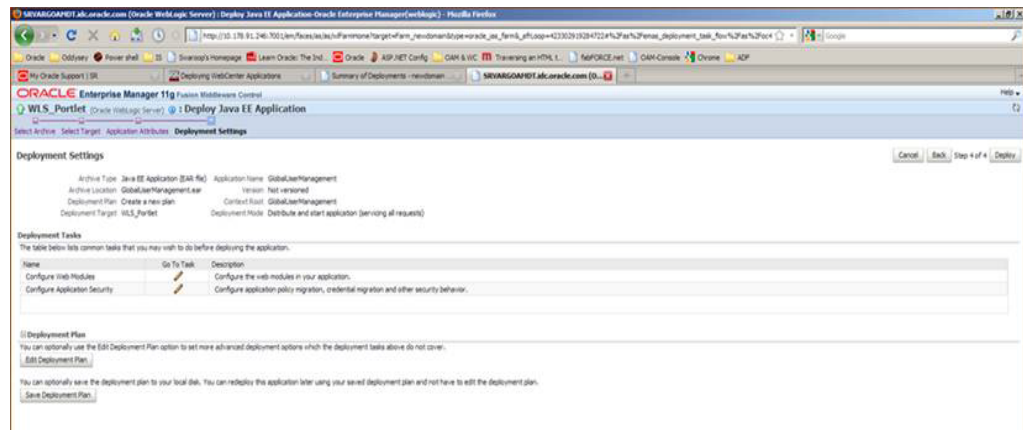
9. Once the Portlet is uploaded, by default **WLS_Portlet** will be selected. If not then select and click **Next**.



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



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



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.

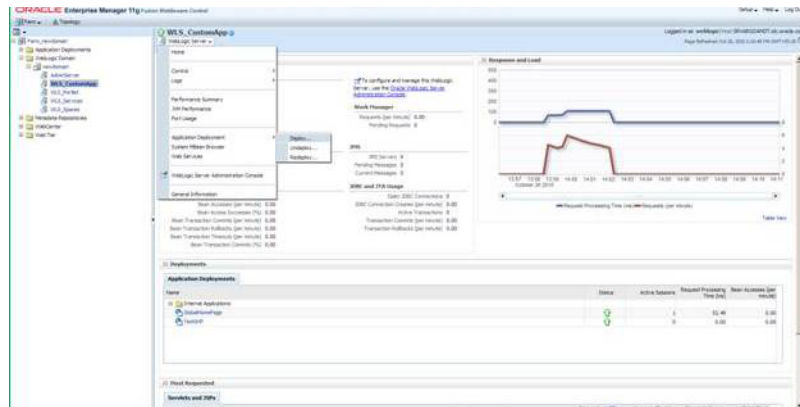
Deploy Company Logo

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.

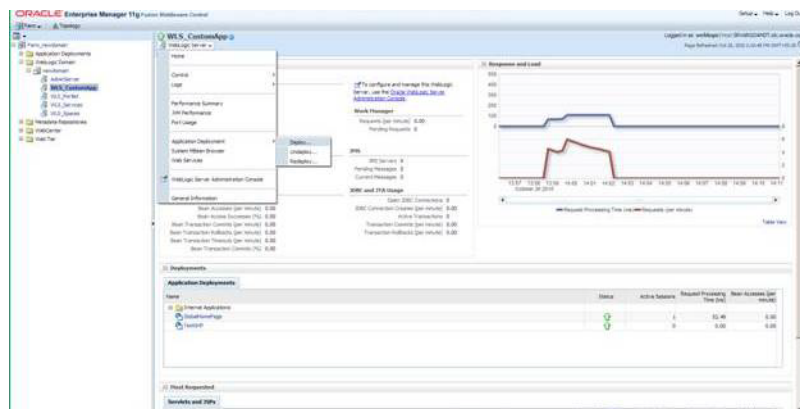
Pre-Deployment Configuration

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**.

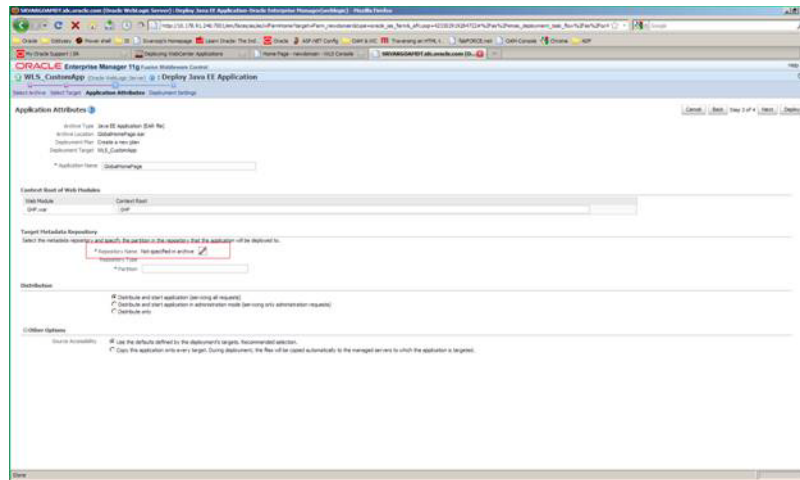


- Log in to the Enterprise Manager Admin console. In the left hand tree navigation, select **WebLogic Domain>Your Domain>WLS_CustomApp** in the left hand tree navigation. The WLS_CustomApp is the name of the server that we have created to deploy Global Home Page. Click the menu just below the name of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

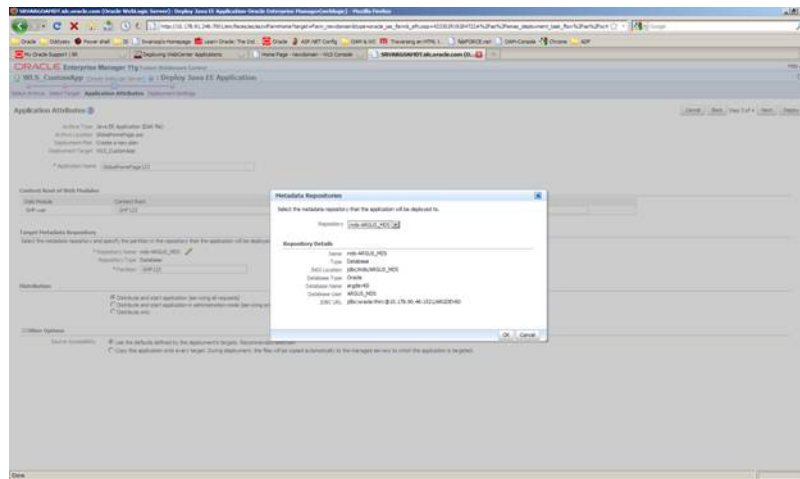


- The following screen appears. Browse for the application. ear file and click Next.

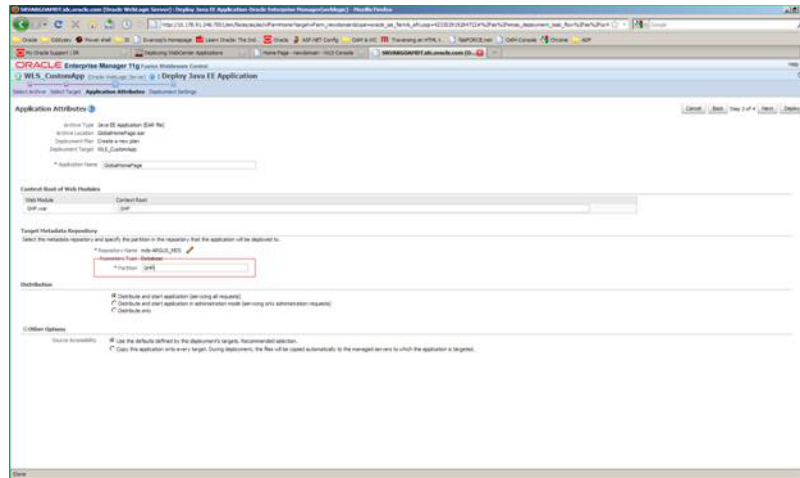
- Click the “pencil” icon in the **Target Metadata Repository** section.



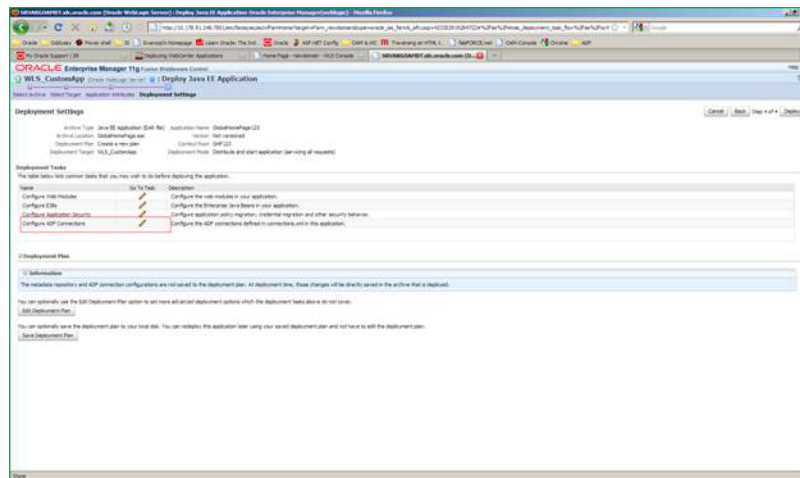
- A modal dialog appears that allows you to specify the metadata repository for this application. Choose a metadata repository and click OK.



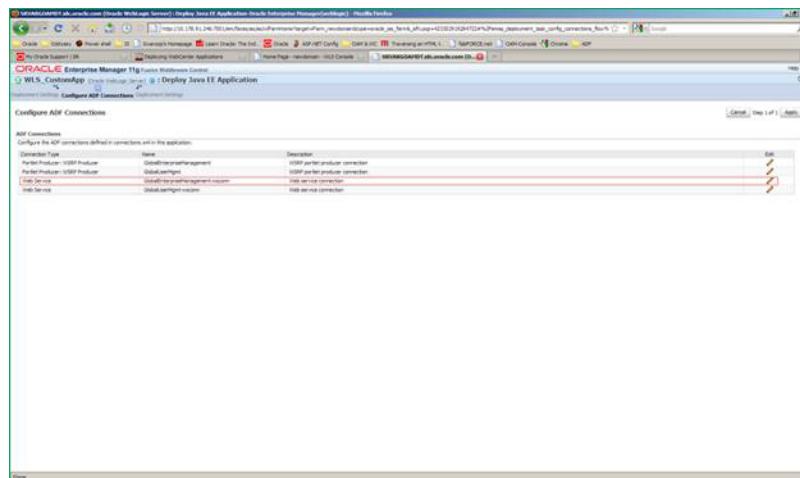
- Specify the “partition” value. You may choose any value but Oracle recommends using the application name itself as the partition value. Click Next.



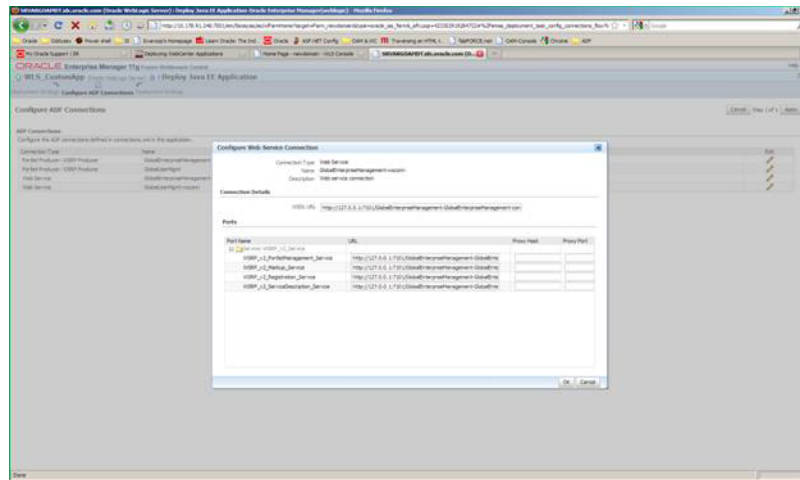
- In the "Configure ADF connections" section, click "pencil" icon, you will be redirected to the "Configure ADF connections" screen.



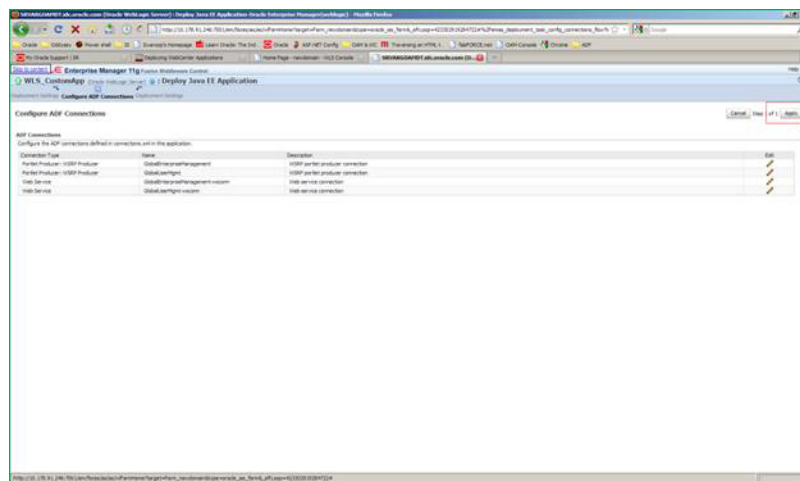
- In the Configure ADF connections screen, modify the web service connection. Click the "pencil" icon to edit the ADF connection settings.



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



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:

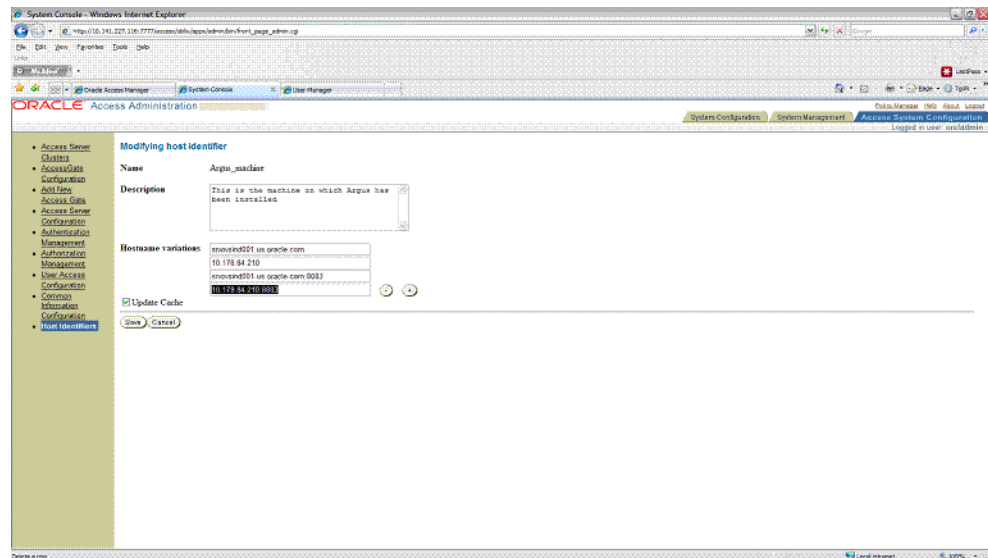
- The system should have an OAM installation (Identity server, Access server, WebPass, Policy Manager).

- 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.

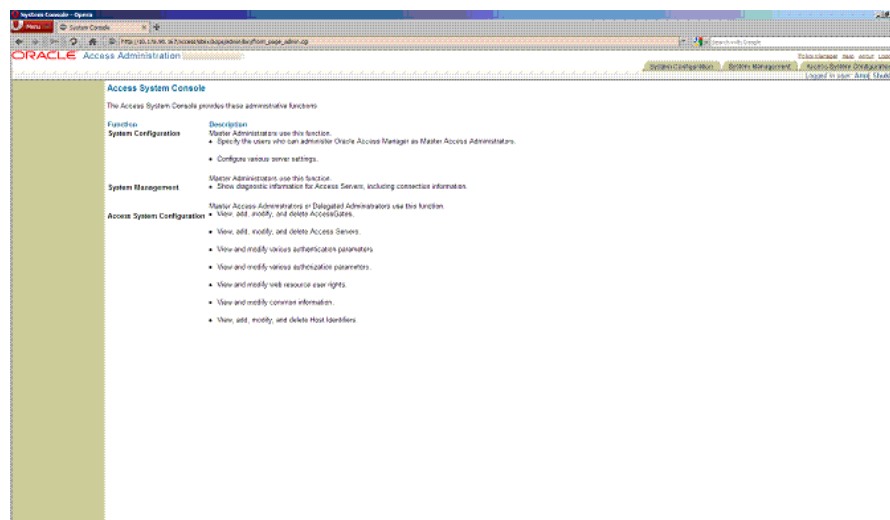
Perform the following steps to install SSO on the OAM:

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:

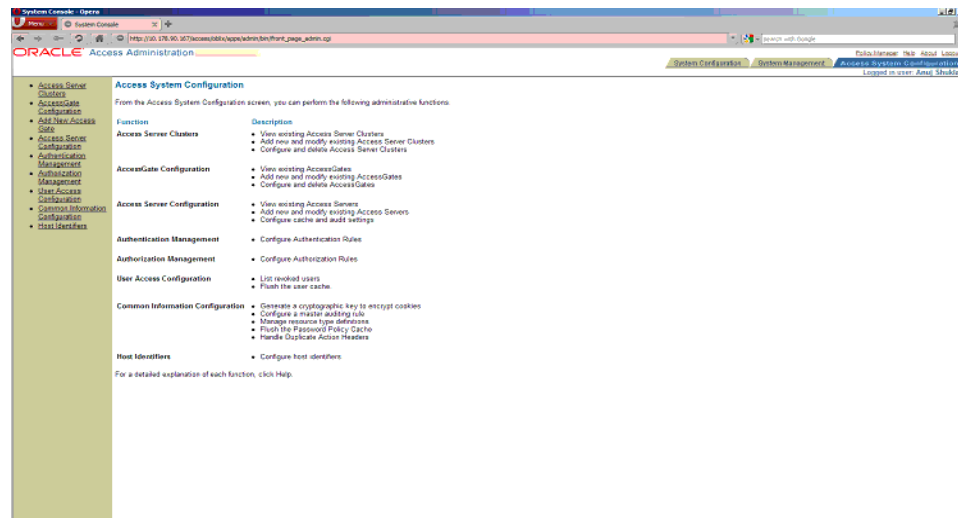
- srvovsind001.us.oracle.com
- srvovsind001.us.oracle.com:8083
- 10.178.84.210
- 10.178.84.210:8083



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



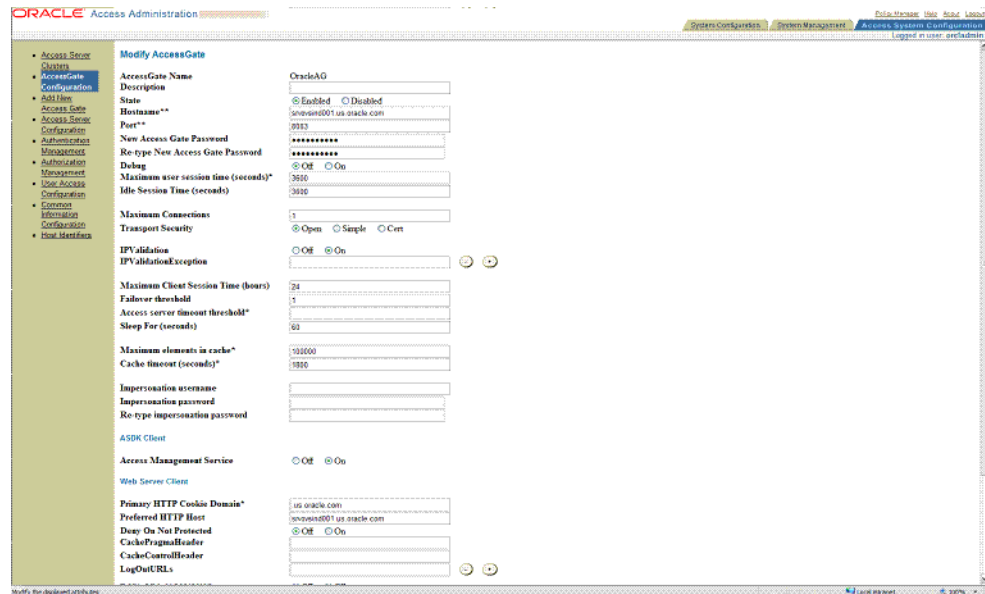
3. Click Add New Access Gate link on left panel.



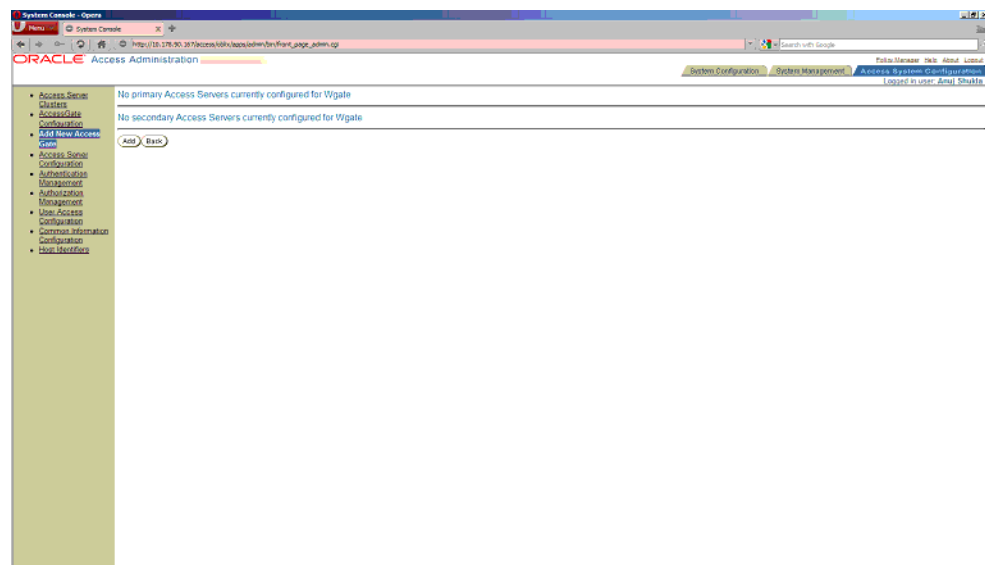
4. Provide details like access gate name, port, and password. Also, enter the following details:

- **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.oracle.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.

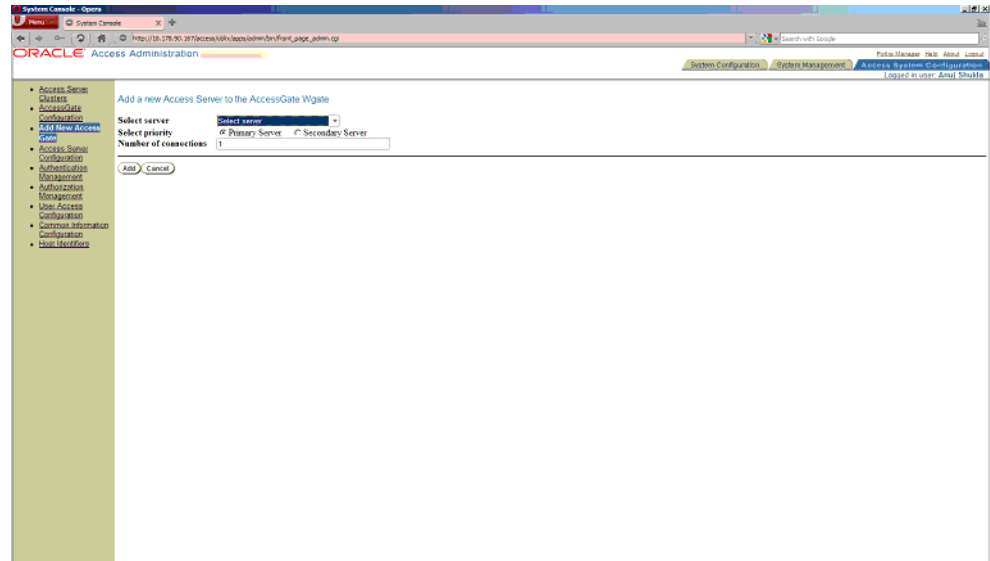


5. You will see the message "Please associate an Access Server or Access Server Cluster with this AccessGate."
6. Click **List Access Servers**. The following screen appears:



7. Click **Add**. Select an access server from the dropdown and click add to associate webpage 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.

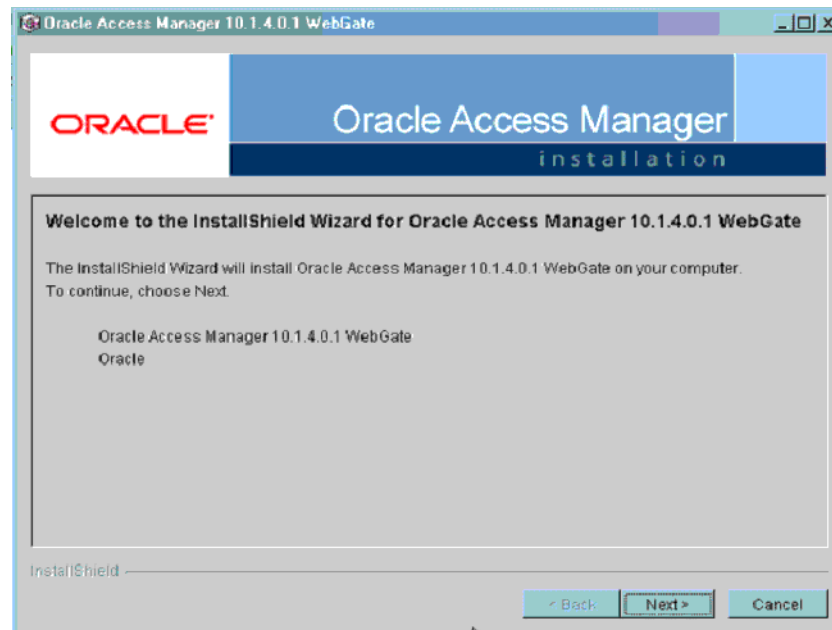


8. Navigate to the Argus Web Server Machine, that is the machine where you have installed Argus. Run the installer for Webgate.

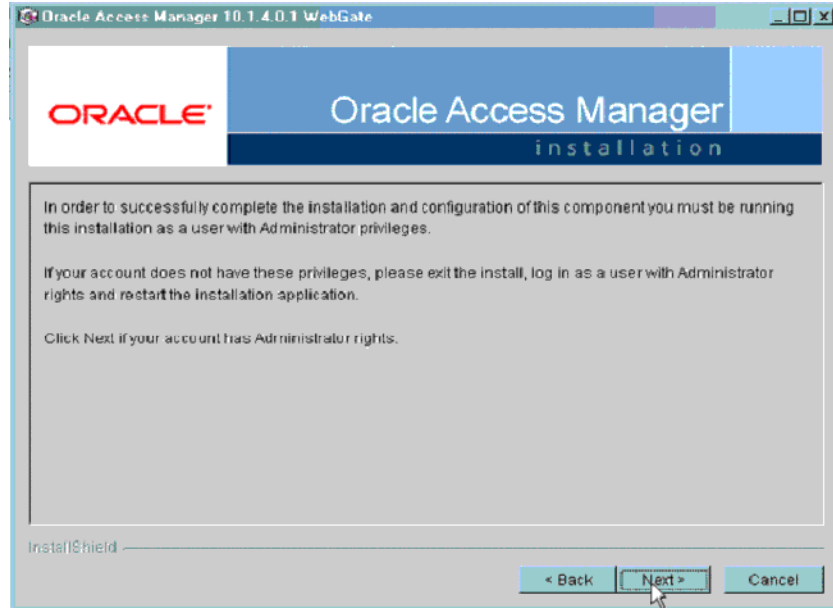
Installing WebGate

Following is the procedure to install WebGate:

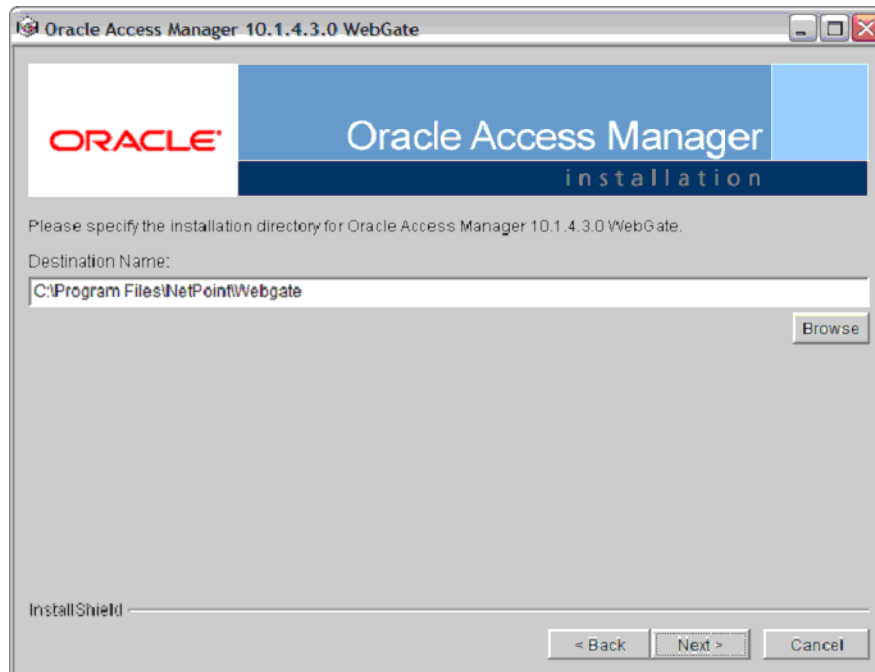
1. Run the file Oracle_Access_Manager10_1_4_3_0_Win32_ISAPI_WebGate.exe. The following screen appears. Click **Next**.



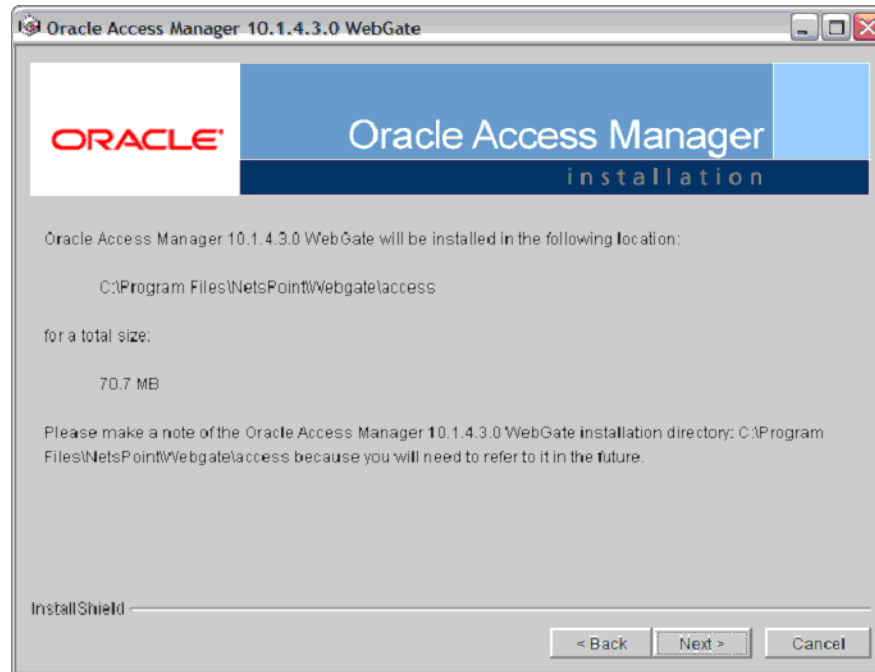
2. You must have administrative privileges to run the installation. If you are logged in as a different user, you must exit the installation, log in as the Administrator and then restart the installation. When the following screen appears, click **Next**.



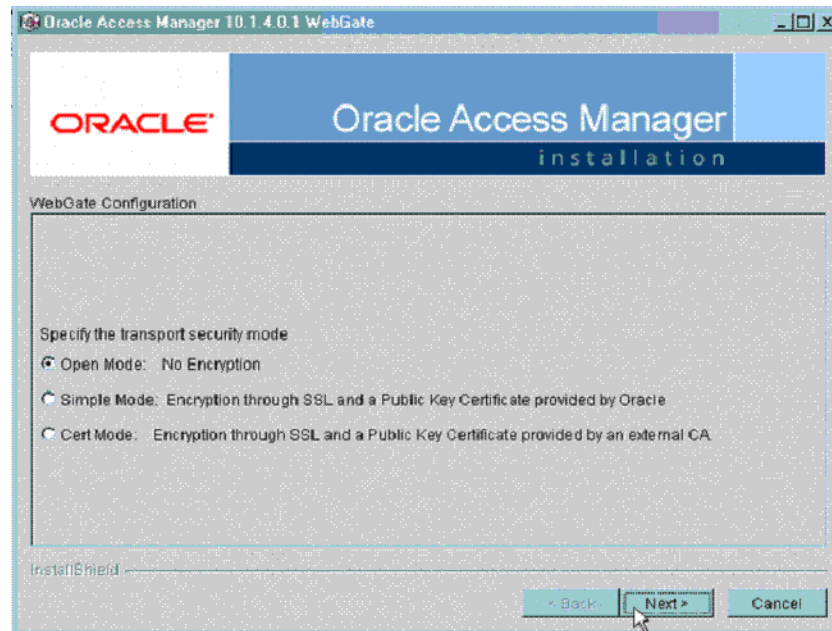
3. In the **Destination Name**, set the installation directory and click **Next**.



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**.



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



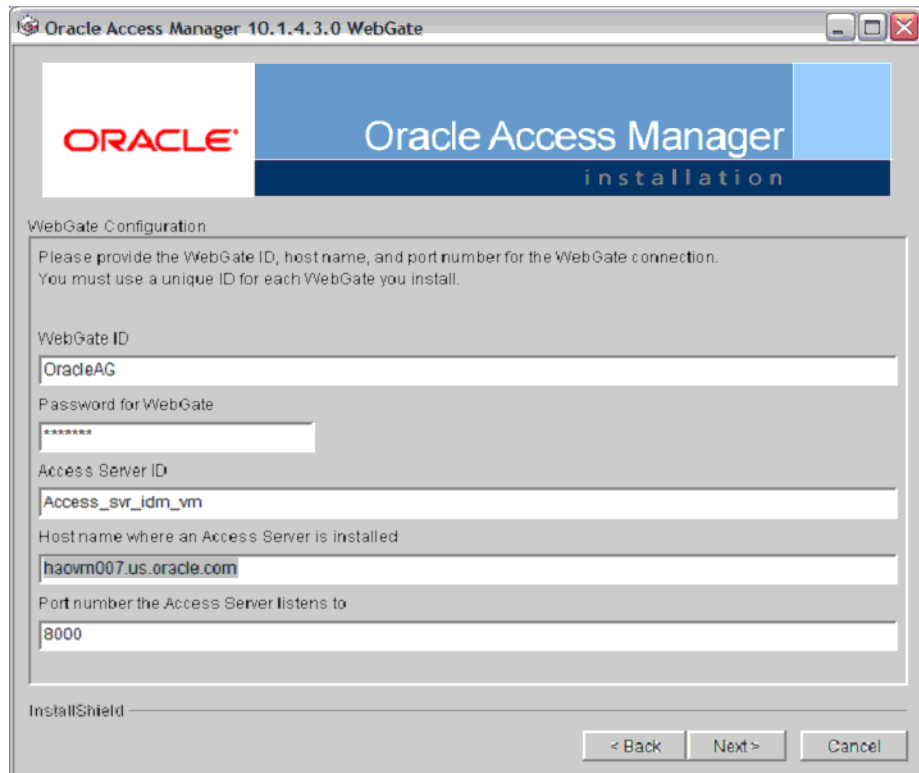
6. Provide the following details and click **Next**.

Table 12-1 Values for WebGate configuration

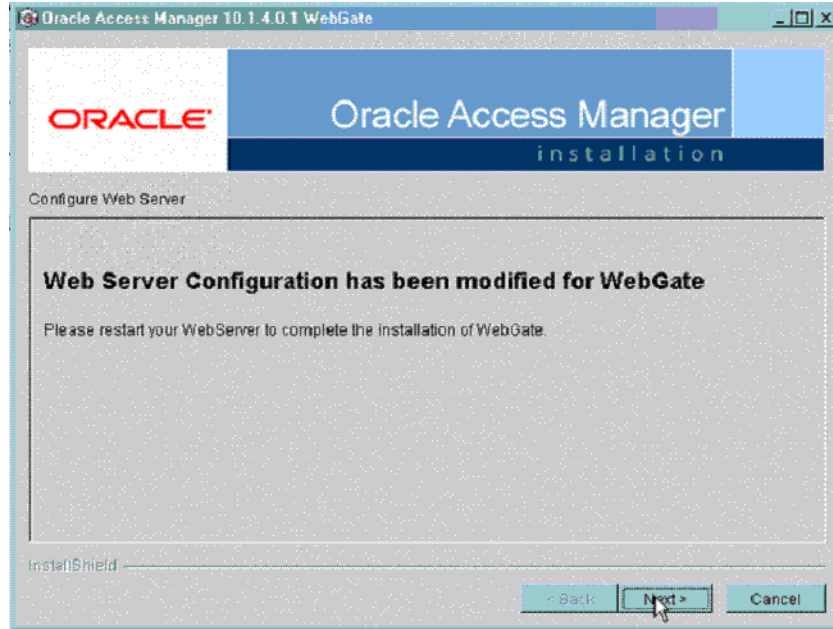
Parameter	Description
WebGate ID	Name of the webgate.
Password	Password for the webgate.

Table 12-1 (Cont.) Values for WebGate configuration

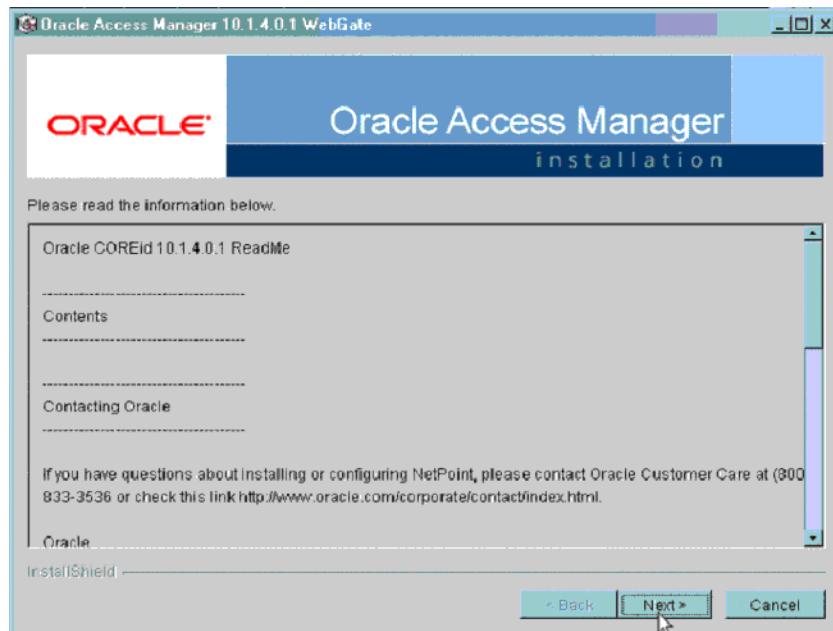
Parameter	Description
Access Server ID	Name of the access server that is configured in access server console.
Host name	FQDN of the machine where the access server is installed.
Port number	Port of the access server



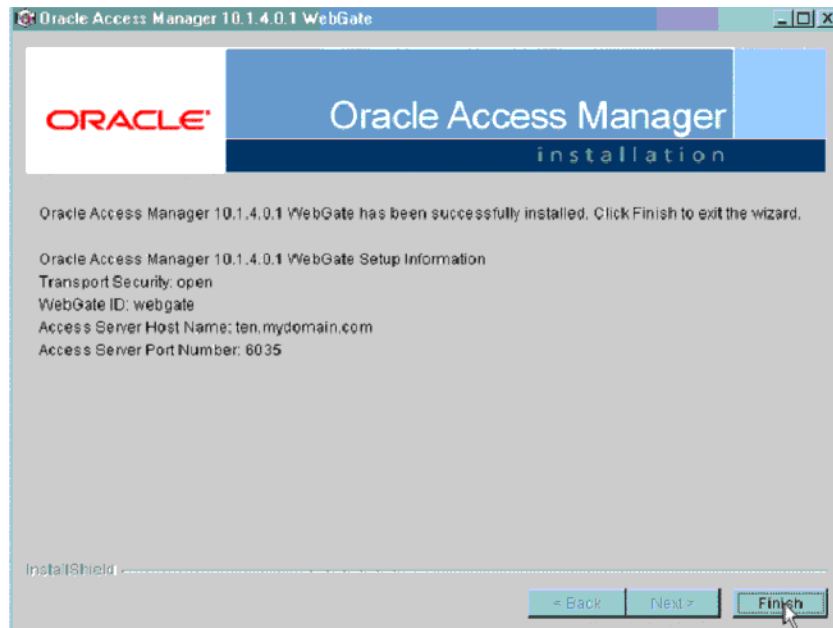
7. The following screen appears:



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



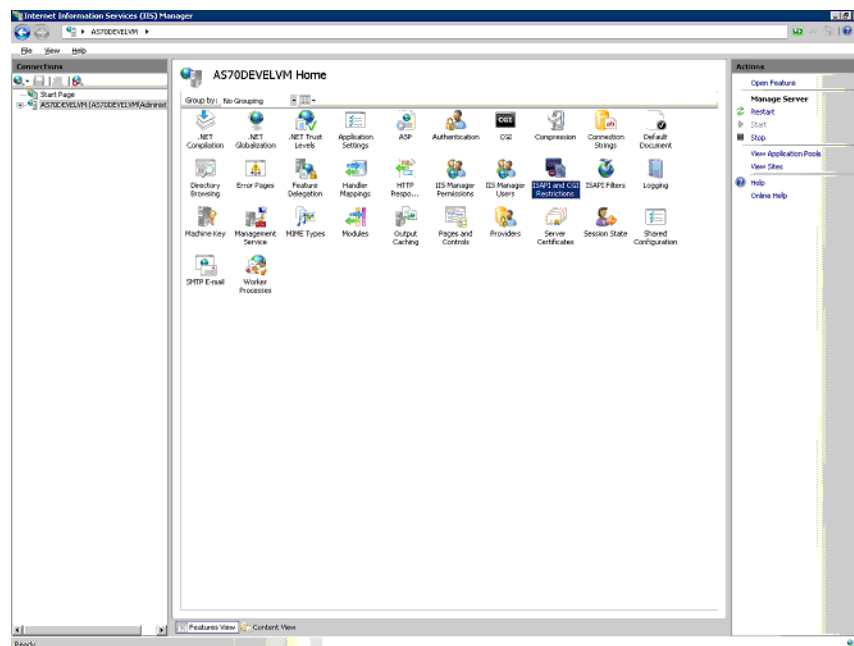
9. You can review the WebGate for IIS configuration settings and click **Finish**.



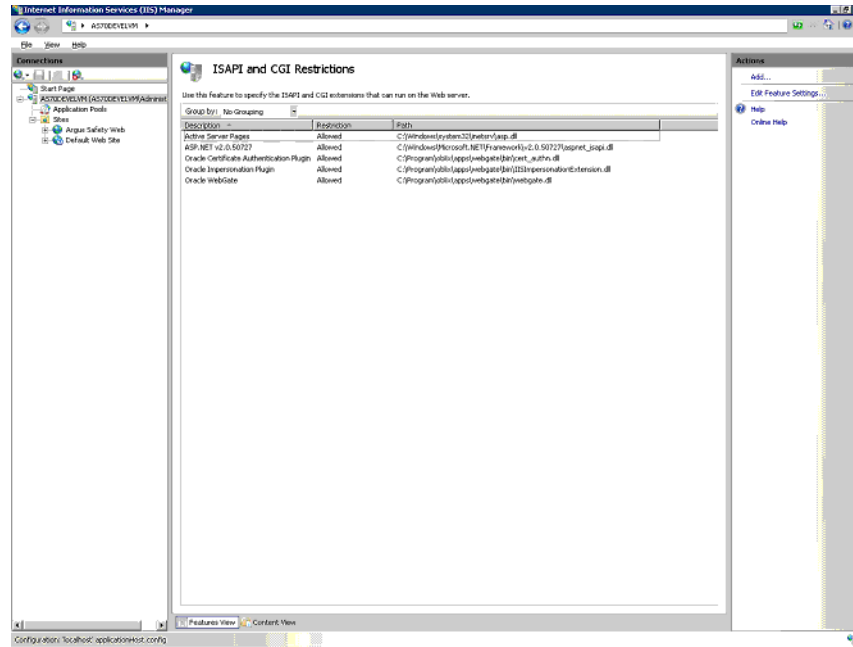
Configuring WebGate on Windows Server 2008

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

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:

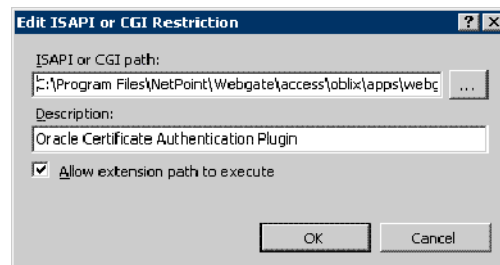


- You have to correct the path for the following DLLs to reflect the path where you have installed the WebGate. To do this, double click the DLL entry and you will see the **Edit ISAPI or CGI Restrictions** dialog box as shown below. In this dialog box, enter the path given in the following table and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

Table 12–2 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
Oracle Impersonation Plugin	C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\II_SImpersonationExtension.dll
Oracle WebGate	C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\webgate.dll

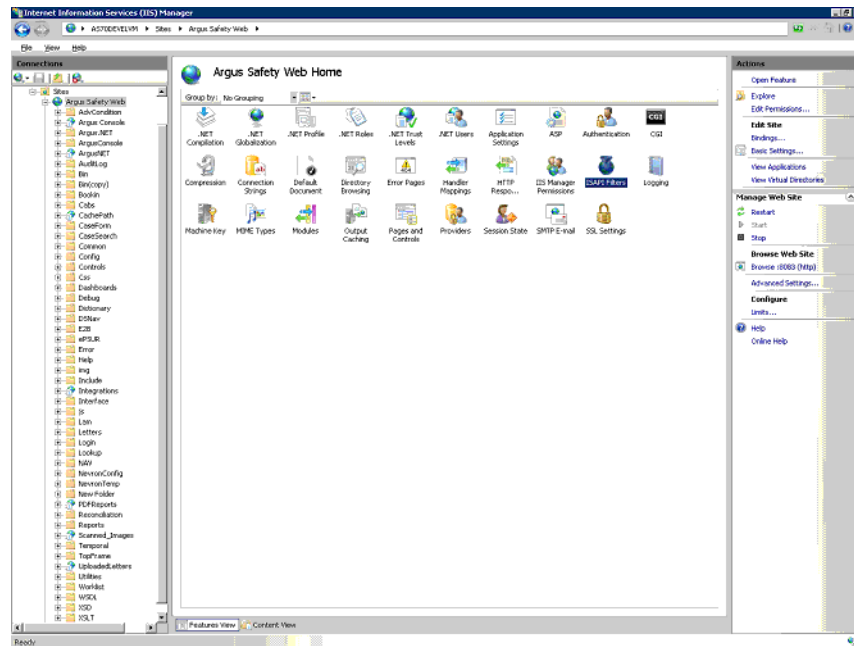
Note: For Windows 2008 R2, the DLLs must be manually added by clicking on the Add link in the right-most pane.



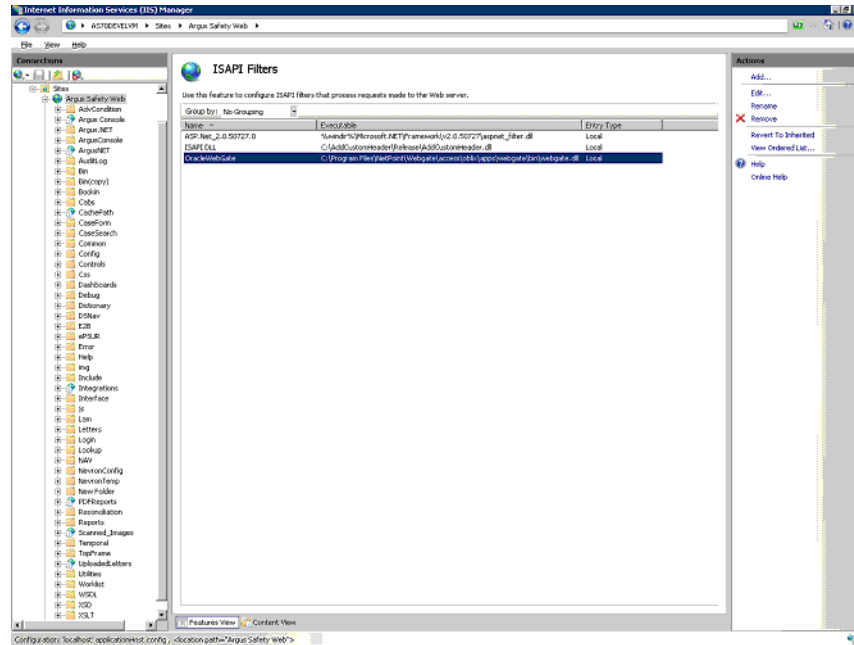
- Click **Edit Feature Settings** in the **Actions** panel in the right. The following dialog box appears:



- Check both the boxes and click **OK**.
- Click **Argus Safety Web** node, which will open the home page for the application as shown below.

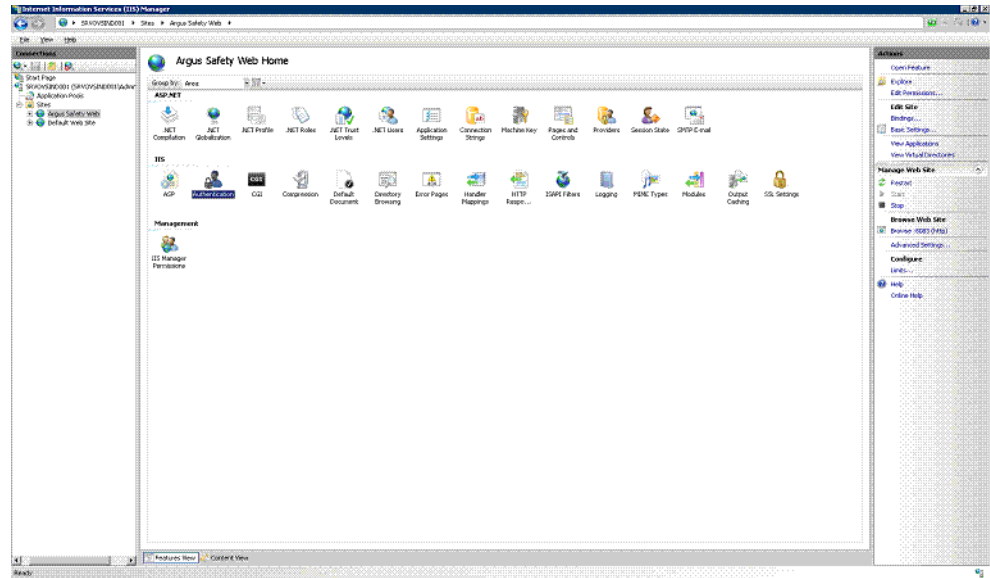


- Click **ISAPI Filters** and the following screen appears:



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:
 1. Navigate to Windows\System32\inetsrv\config and open the applicationHost.config file.
 2. Search for the `<hiddenSegments>` module.
 3. Remove the entry `<add segment="bin"/>` if it is present.
 4. 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:

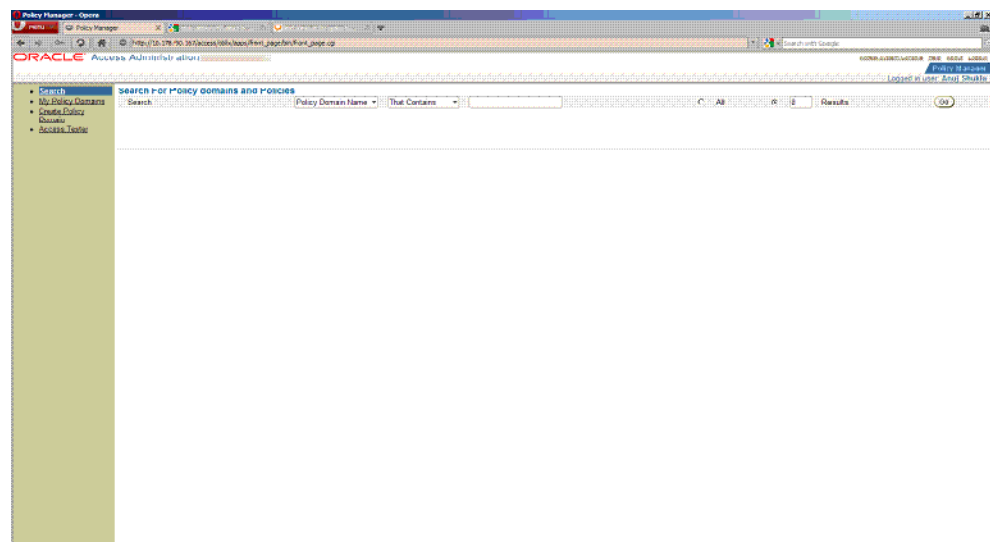


Right click on **Windows Authentication** and check if it is enabled. If yes, then disable it. This completes the WebGate installation on Windows Server 2008.

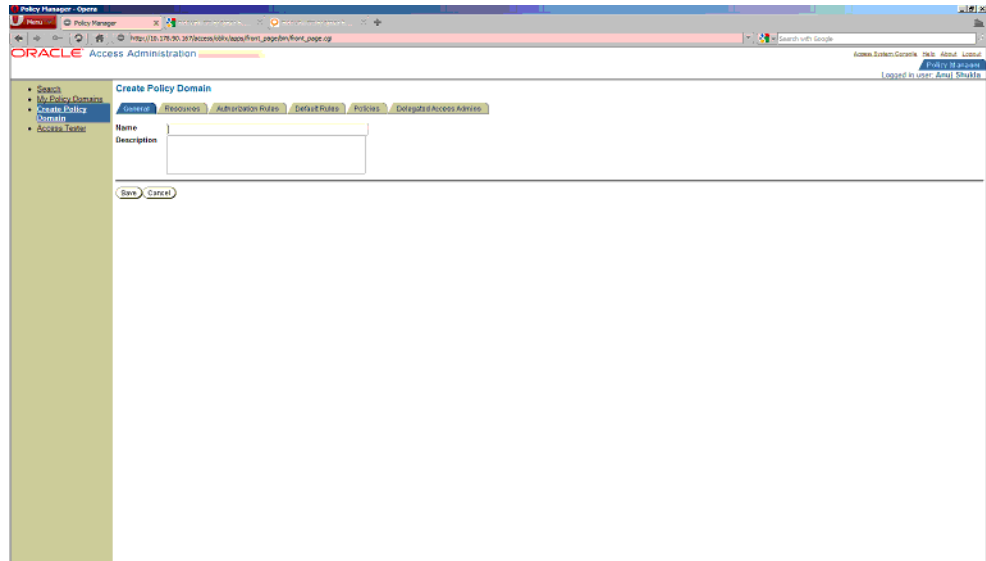
Protecting Files in the Argus Directory

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

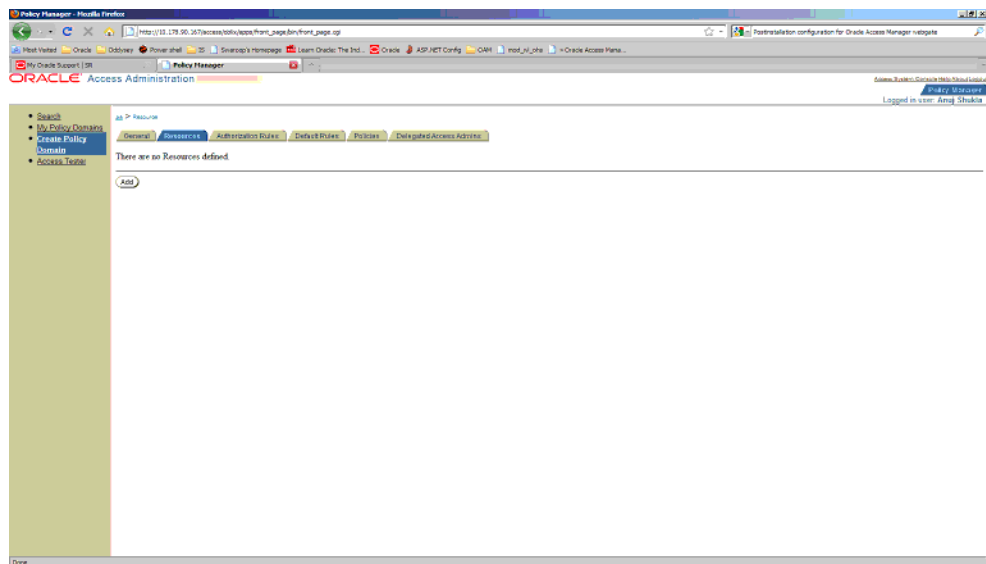
1. Navigate to the policy manager console and click **Create Policy Domain**.



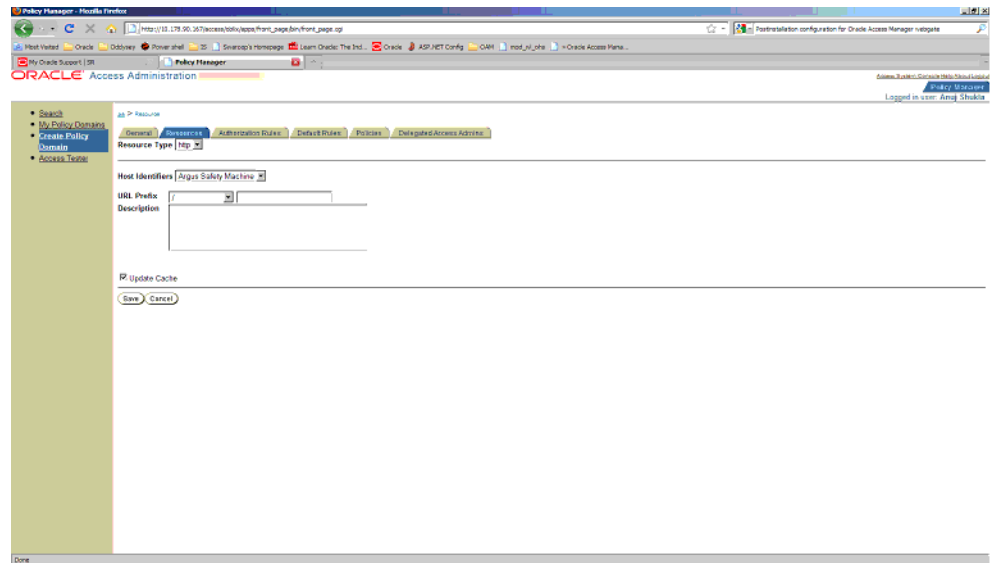
2. Under the **General** tab provide a name and description and click **Save**.



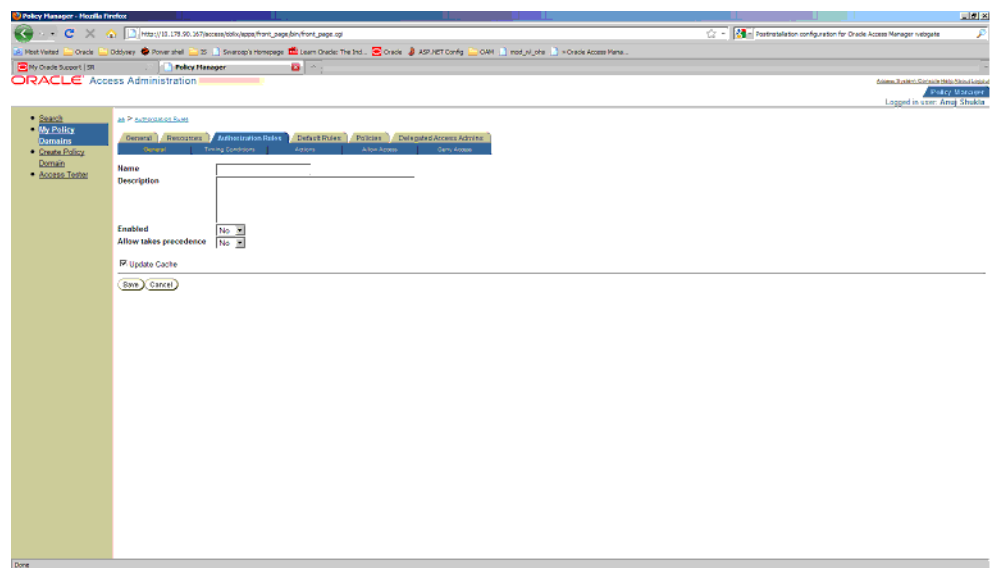
3. Click the **Resource** tab and then click **Add**.



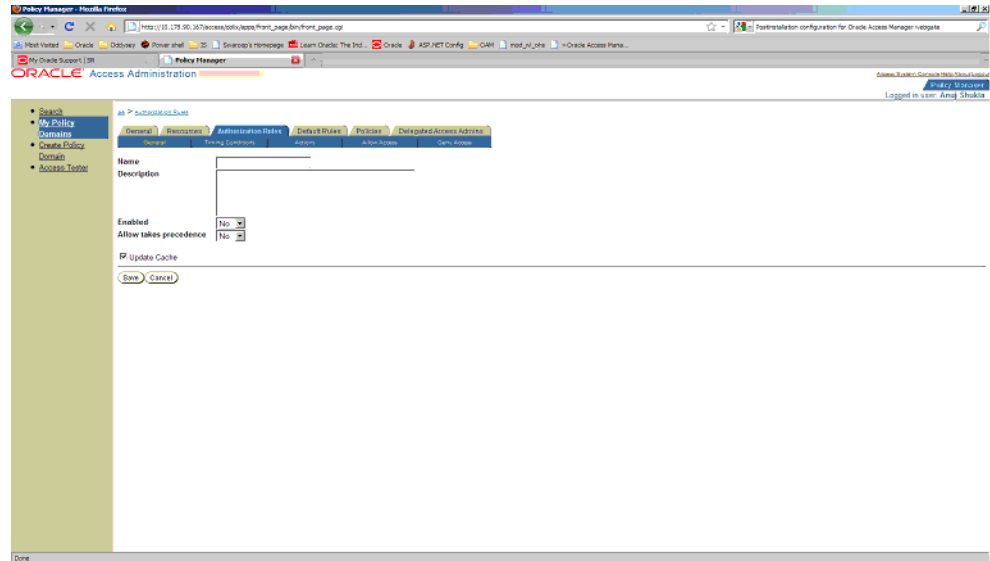
4. Select **Host Identifier** from the dropdown list and select **URL Prefix** as / and provide a description. Click **Save**.



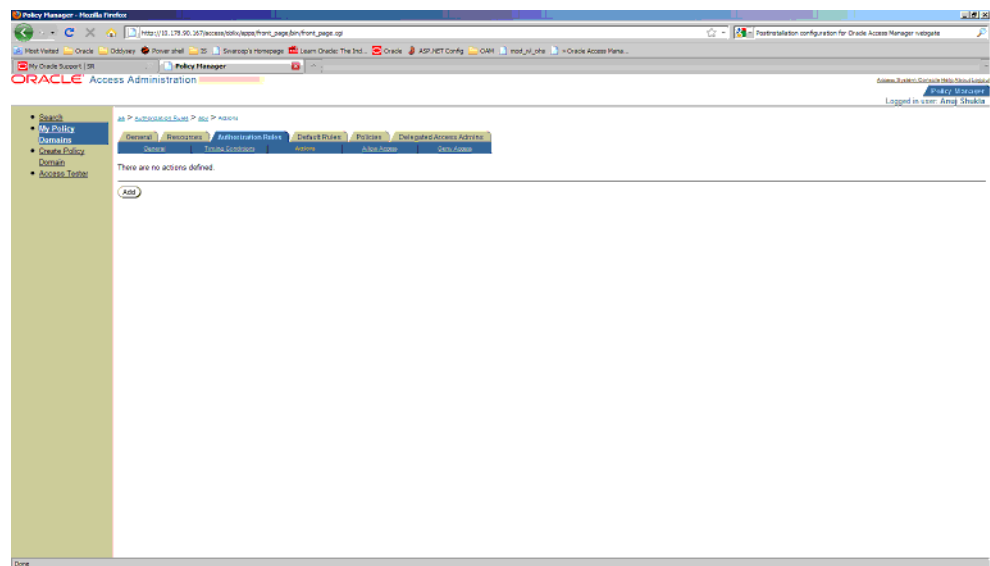
5. Click the **Authorization Rules** tab and select the **General** sub tab.



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 dropdown list.
 - **Allow takes precedence** - Select **Yes** from the dropdown list.



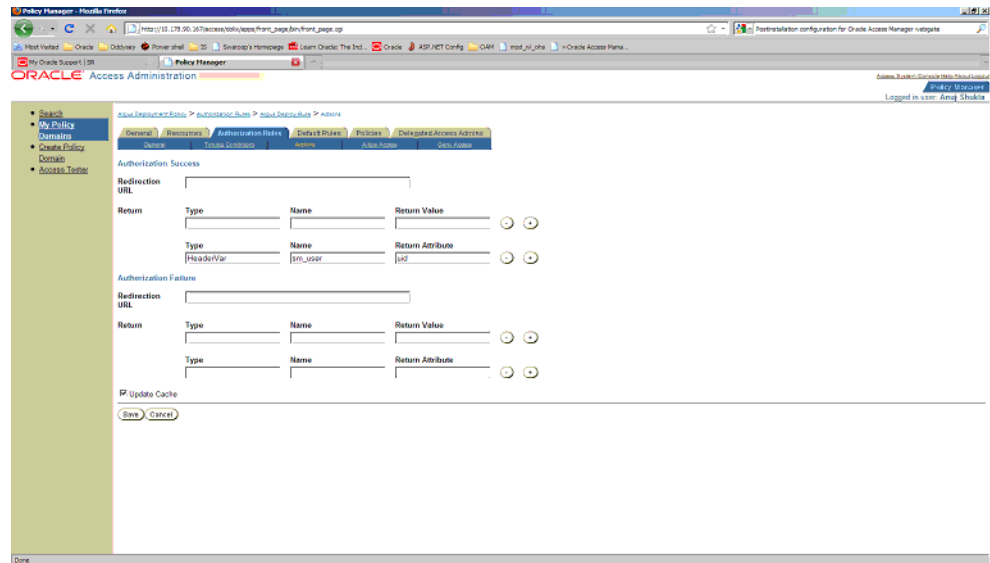
7. Now click the **Actions** sub tab. Click **Add**.



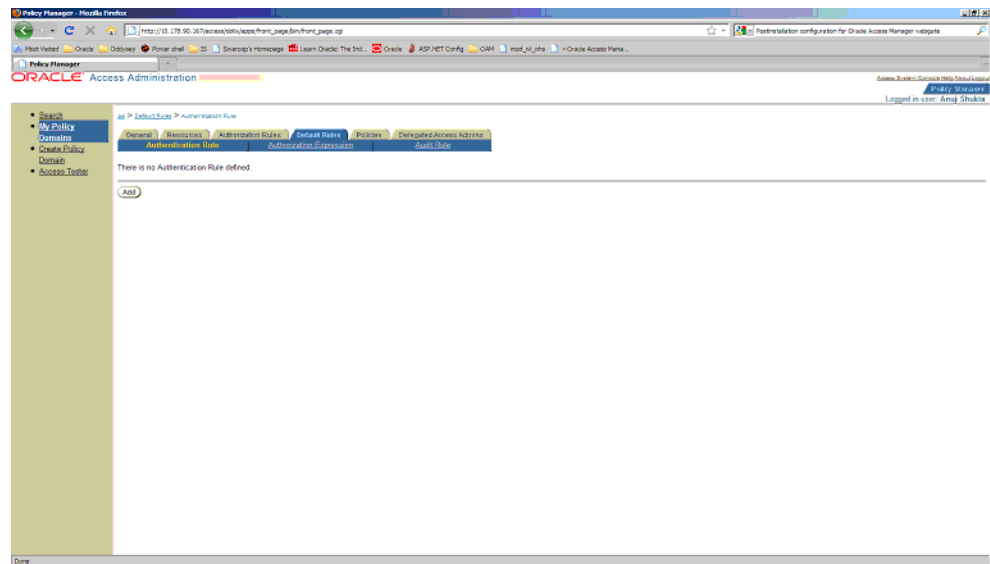
8. In the **Authorization Success** section under **Return**, enter the following values and click **Save**:

Table 12–3 Values for Return field

Field name	Value
Type	HeaderVar
Name	SM_USER
Return Attribute	uid

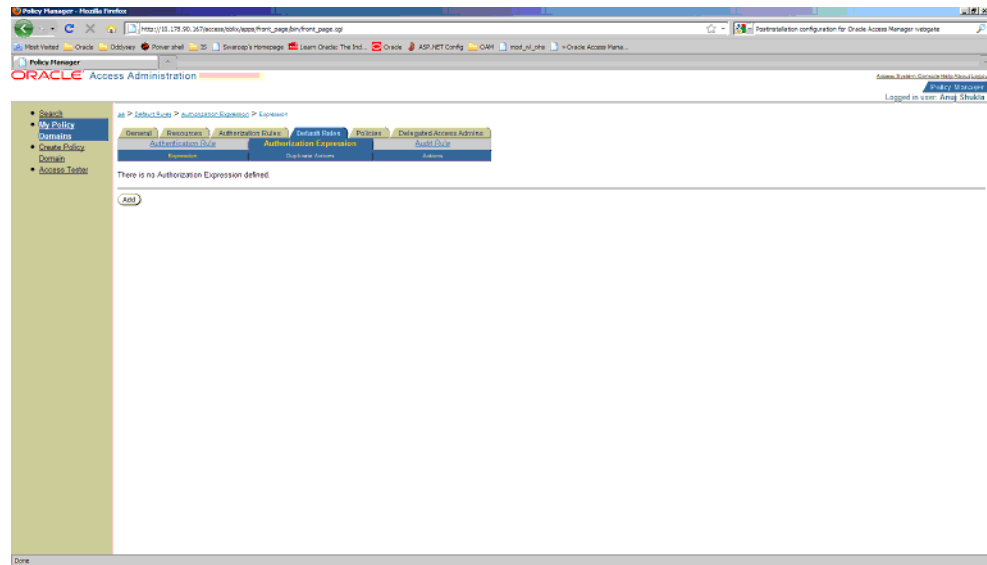


9. Navigate to **Default Rules > Authentication Rule**. Click **Add**.



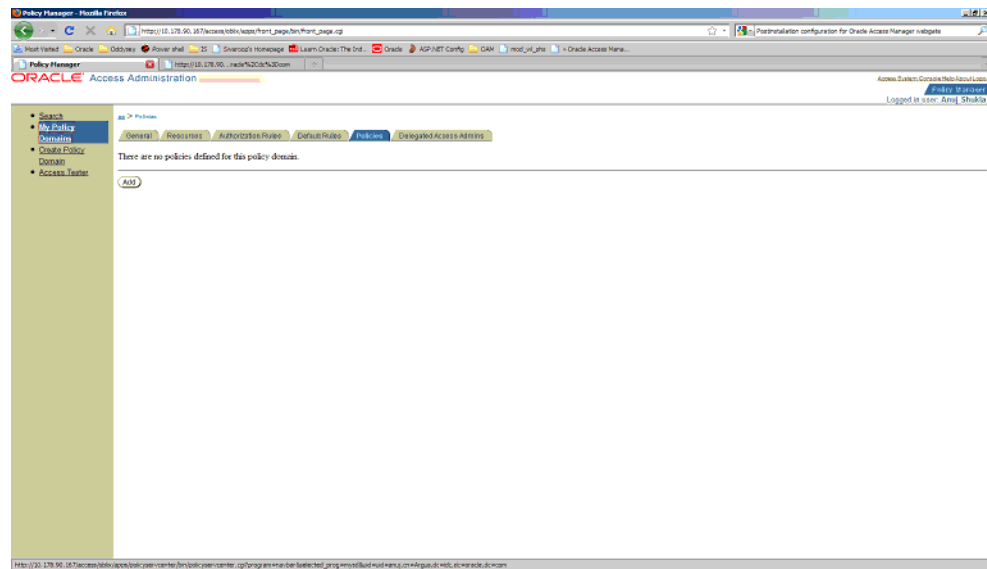
10. Enter details for Name and description and select Authentication Scheme as **Oracle Access and Identity Basic Over LDAP**. Click **Save**.

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



12. Select **Authorization Rule** from the dropdown. Click **Add** and then click **Save**.

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



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:

The screenshot shows the Oracle Access Administration console with the following configuration details:

- Policy Name:** Argus_Policy
- Description:** This is an Argus Policy
- Enabled:** Yes
- Resource:**
 - Resource Type: Http
 - Host Identifiers: Argus_machine
 - URI Prefix: /
- Authorization Rules:**
 - Name: Auth_rule
 - Description: (empty)
 - Enabled: Yes
 - Allow takes precedence: Yes
 - On Success:
 - HTTP Header Variable:
 - Type: HeaderVar
 - Name: SM_USER
 - Return Attribute: uid
 - HTTP Header Variable: Allow Access
 - Role: Any one
- Default Rules:**
 - Authentication Rule:
 - Authentication Scheme: Auth_RULE_OverLDAP
 - 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: (empty)
 - 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: [ecchshen](#)
 - Grant Rights: (empty)
 - There are no Delegated Access Admins with this right.
 - Basic Rights: (empty)
 - 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:



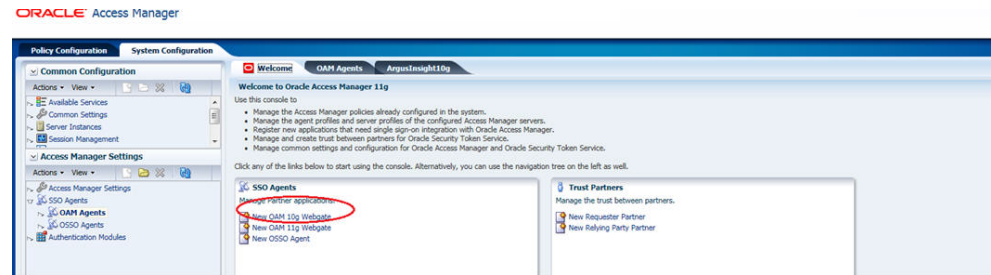
Configuring SSO in Oracle Access Manager 11g

This section describes how to configure SSO in the Oracle Access Manager (OAM) 11g. Following are the pre-requisites to this task:

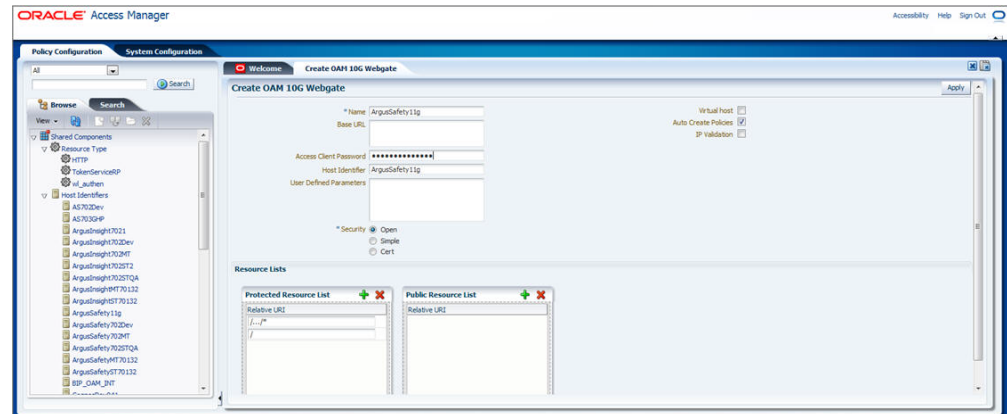
- The system should have an OAM installation (Identity server, Access server, WebPass, Policy Manager).
- User profiles should exist in the LDAP server as well as in Argus with the same credentials.
- LDAP should be configured in the Argus Console.
- The LDAP flag should be set to ON for the users in Argus.

Perform the following steps to install SSO on the OAM:

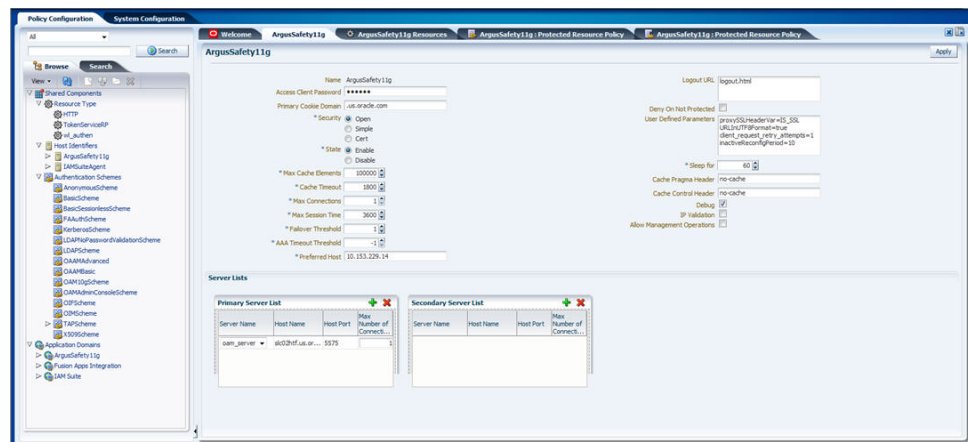
1. Navigate to the **System Configuration** tab of OAM and select the **New OAM 10g Webgate** link.



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**.



3. The following screen is displayed:



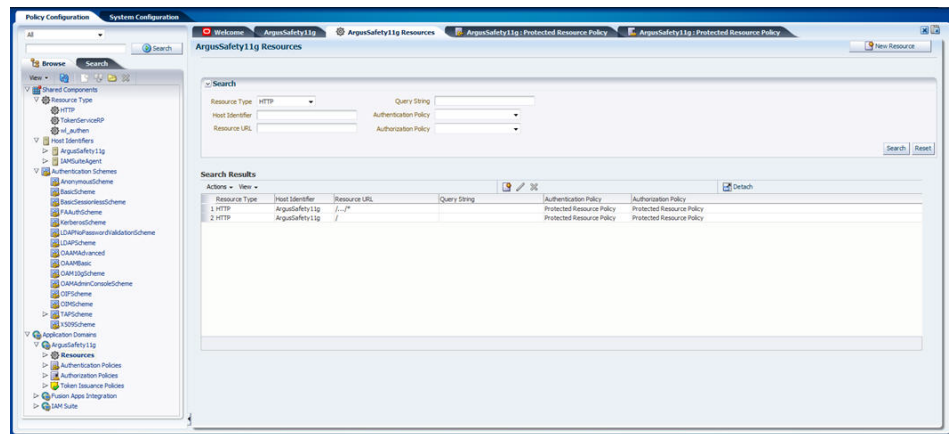
Note: Refresh the Host Identifier list to view the newly created Webgate within the Policy Configuration tab.

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.oracle.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.

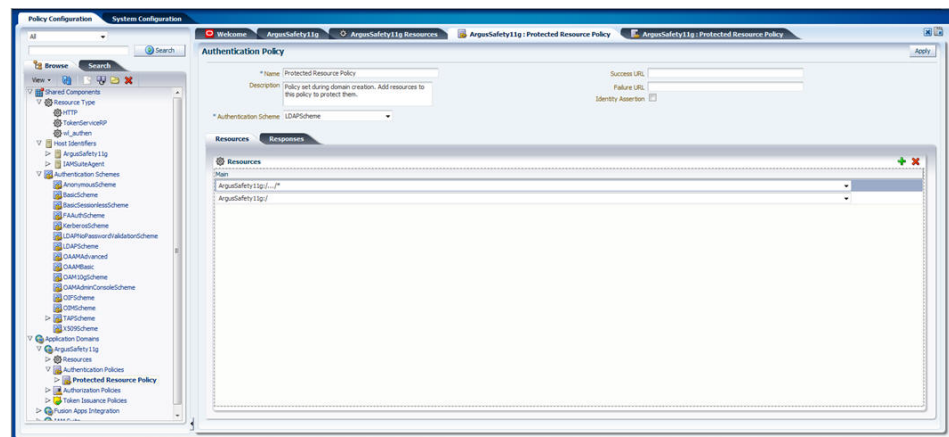
Double-click on **Resources**. On the **Resources** screen, click the **Create** icon (displayed in the Search Results section, with the + symbol in red).

Create the resource type with the correct host identifier, as displayed in the following screen:

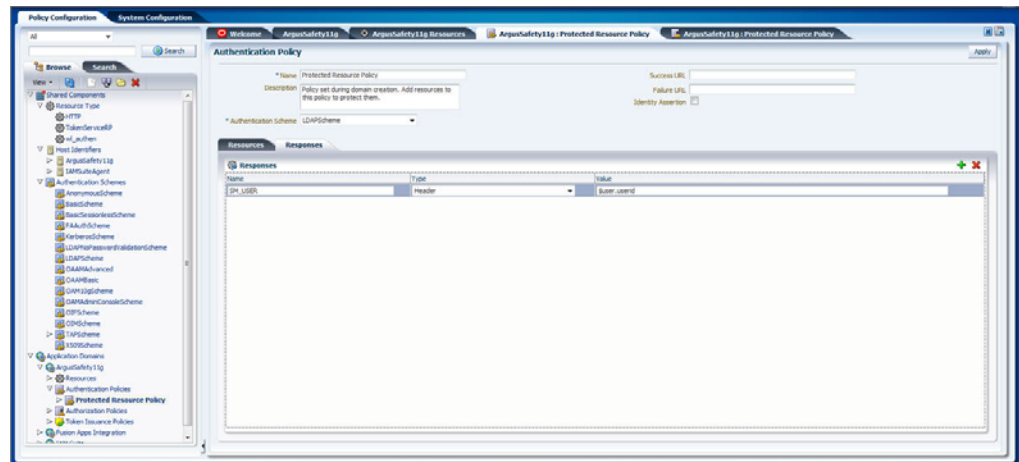


5. Expand the **Authentication Policies** under the newly created Webgate.

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

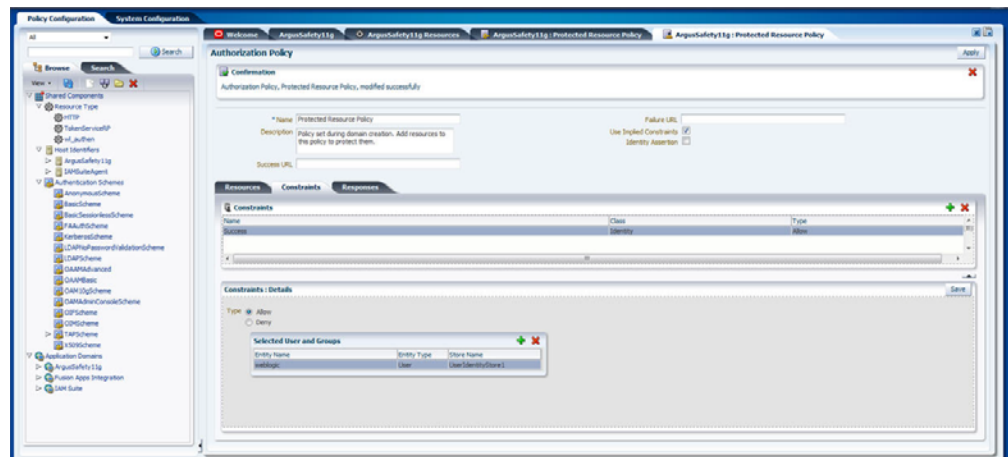


6. Navigate to the **Responses** tab and click the + button to add the **Name**, **Type**, and **Value** for the responses, as shown in the following screen:



- 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:



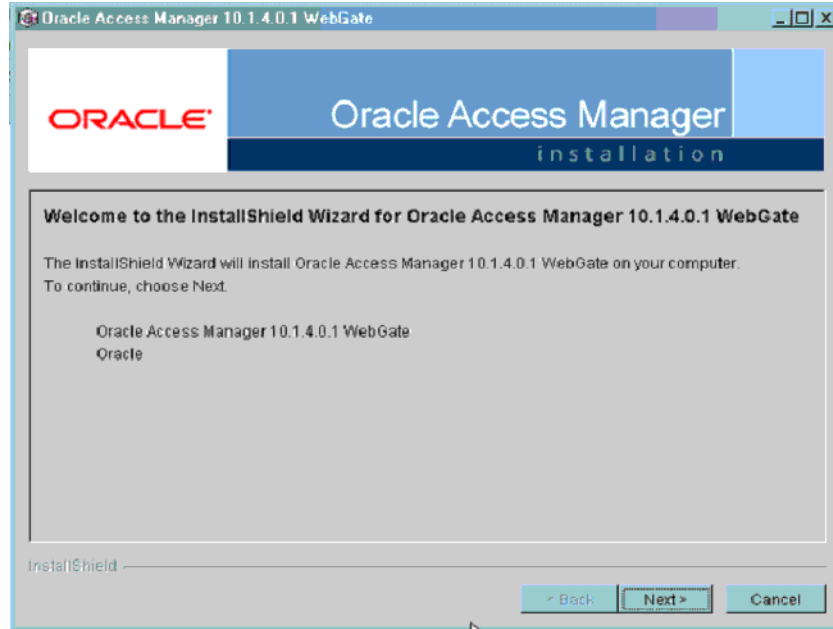
Note: All the names under the Constraints tab with **Type** as **Allow** can access the Argus Safety Server where Webgate has been installed. Select the **Type** as **Deny** if a user should be denied access to the Argus Safety Server where Webgate has been installed.

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.

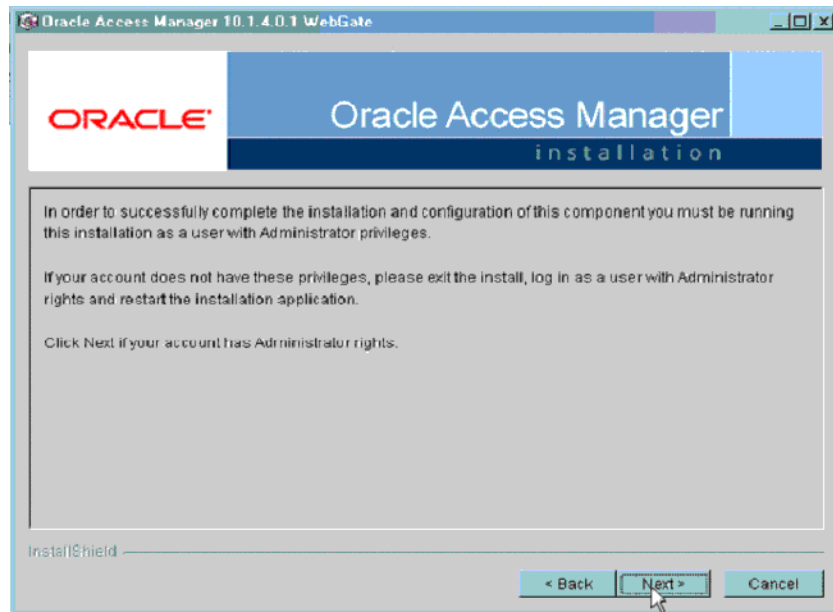
Installing WebGate

Following is the procedure to install WebGate:

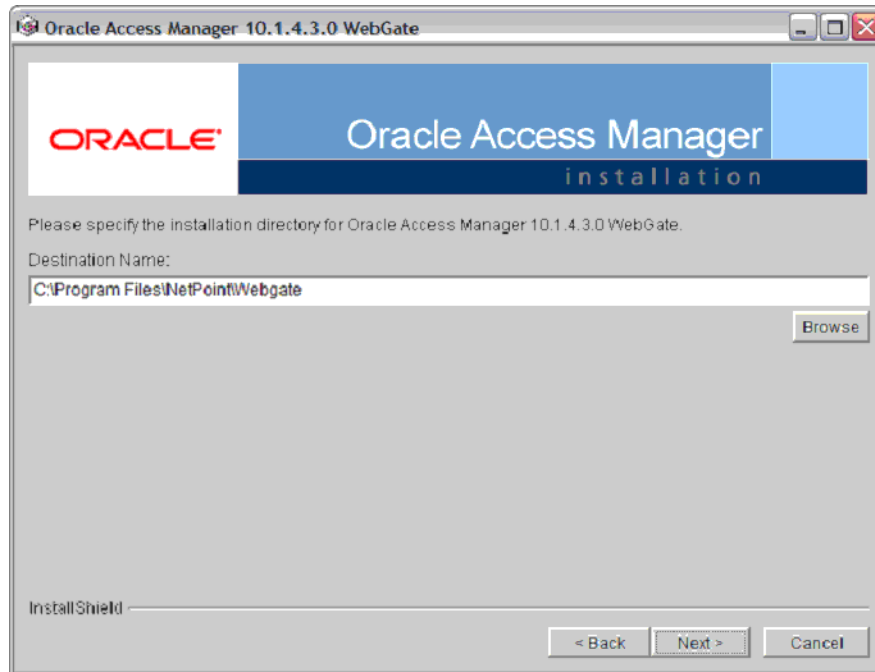
- Run the file `Oracle_Access_Manager10_1_4_3_0_Win32_ISAPI_WebGate.exe`. The following screen appears. Click **Next**.



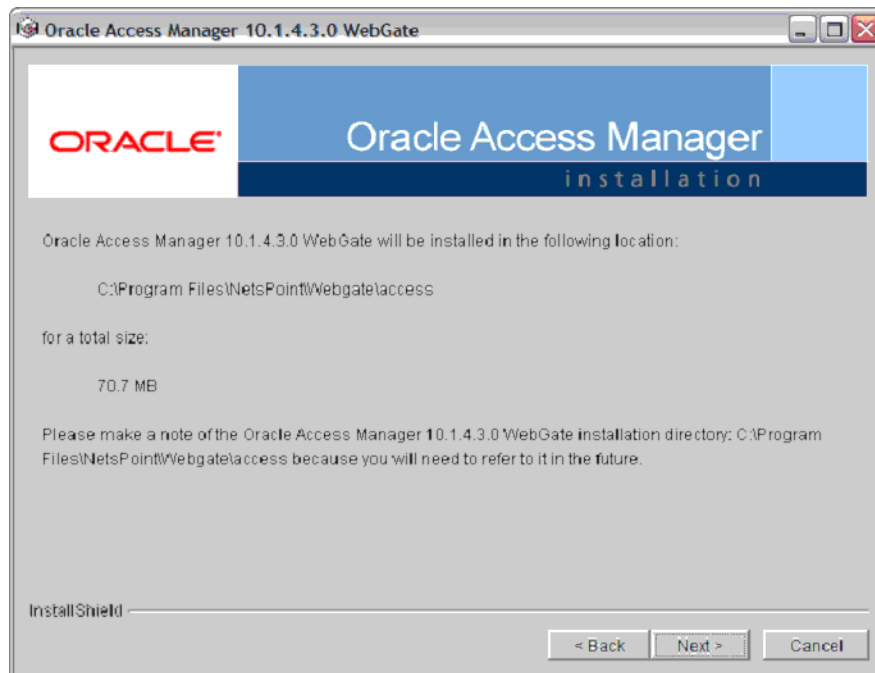
2. You must have administrative privileges to run the installation. If you are logged in as a different user, you must exit the installation, log in as the Administrator and then restart the installation. When the following screen appears, click **Next**.



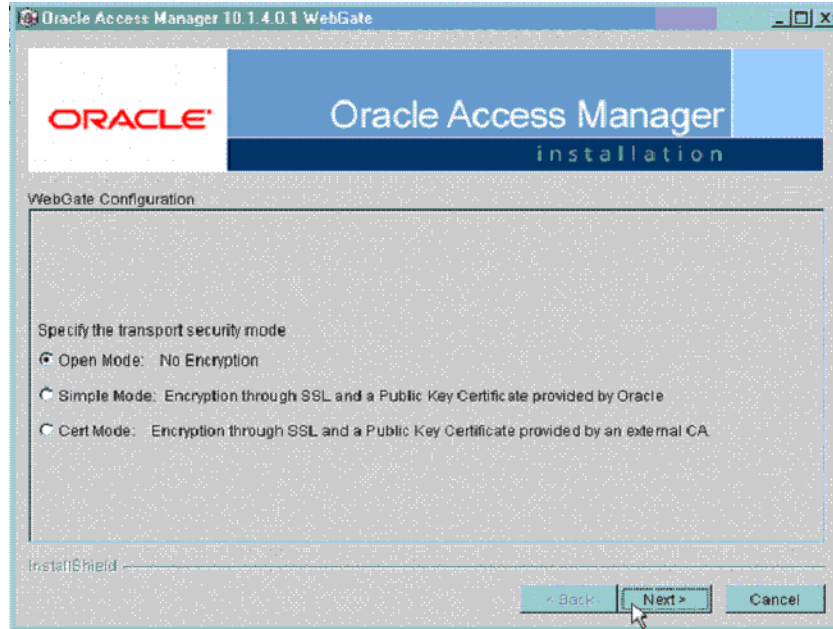
3. In the **Destination Name**, set the installation directory and click **Next**.



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**.



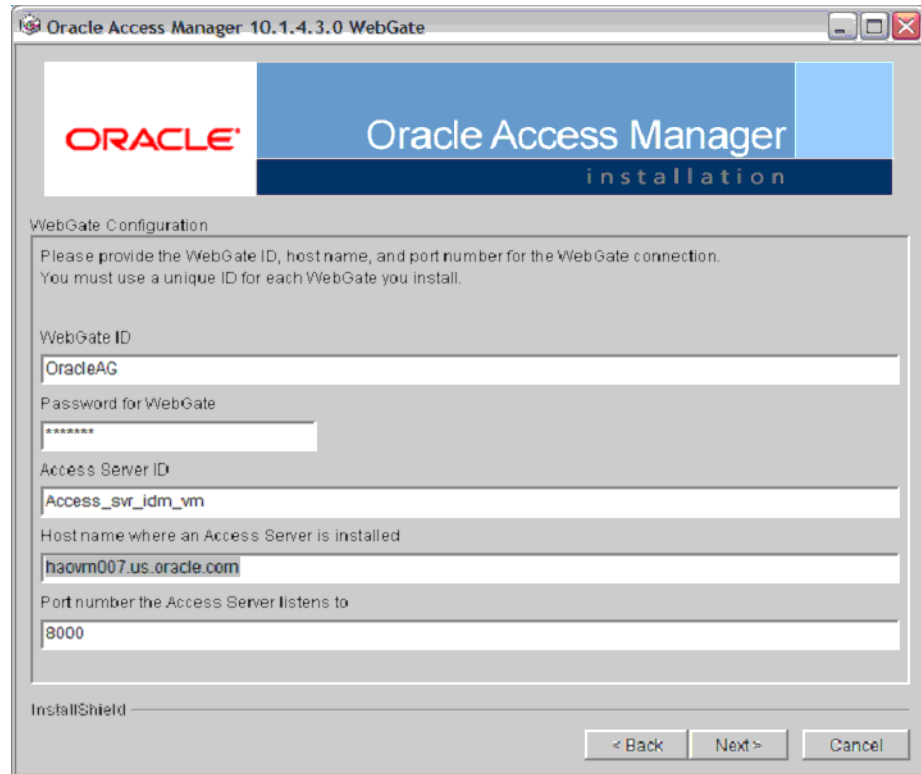
5. The installer begins copying the WebGate files for IIS. Now select **Open Mode: No encryption** for the transport security mode and click **Next**.



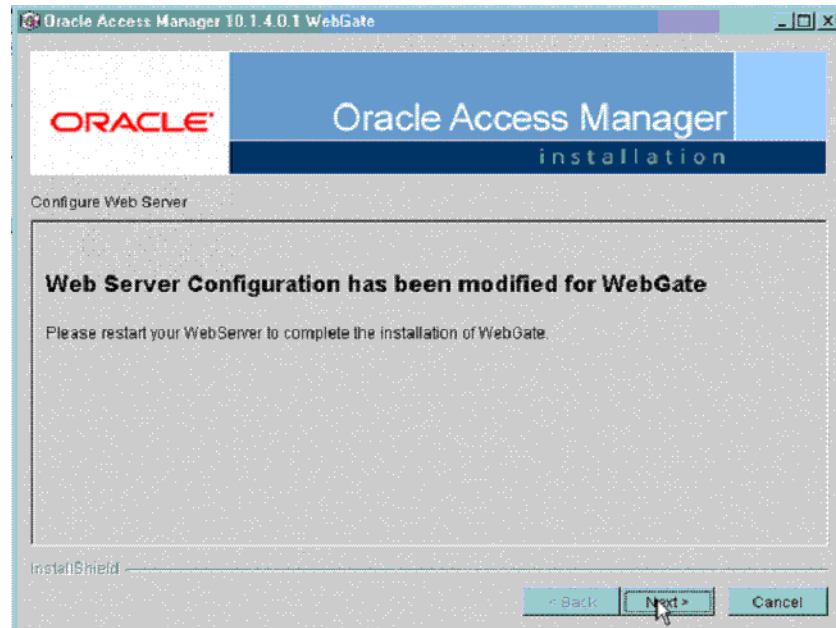
6. Provide the following details and click **Next**.

Table 12–4 Values for WebGate configuration

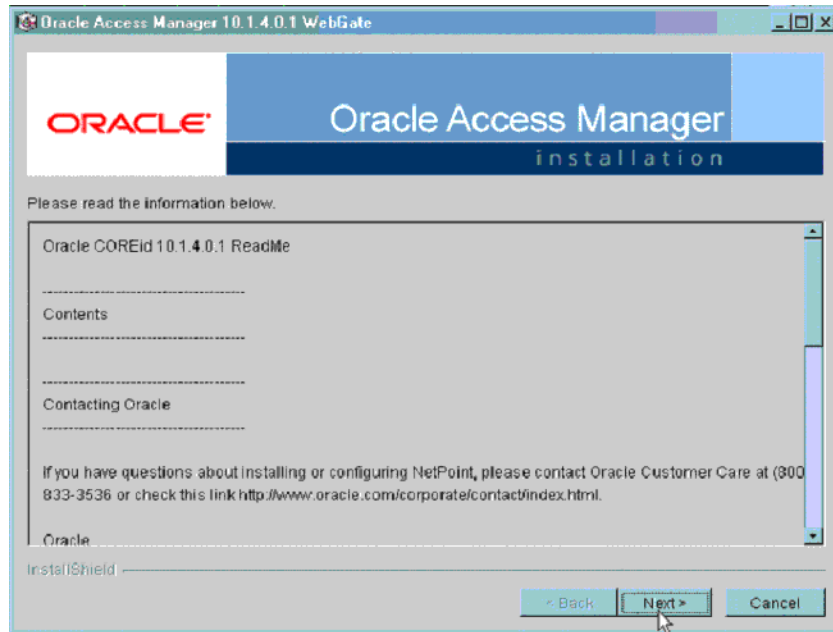
Parameter	Description
WebGate ID	Name of the webgate.
Password	Password for the webgate.
Access Server ID	Name of the access server that is configured in access server console.
Host name	FQDN of the machine where the access server is installed.
Port number	Port of the access server



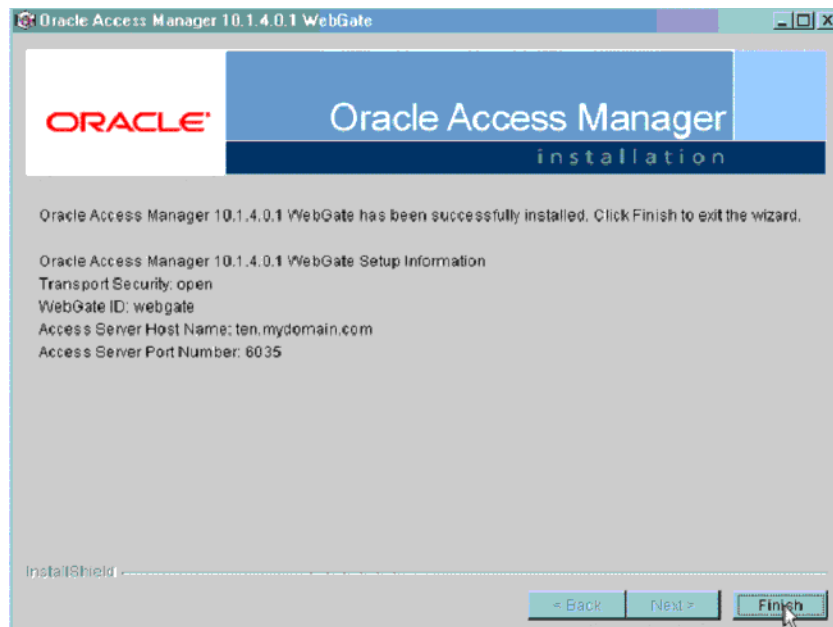
7. The following screen appears:



8. Review the Readme page and click Next.



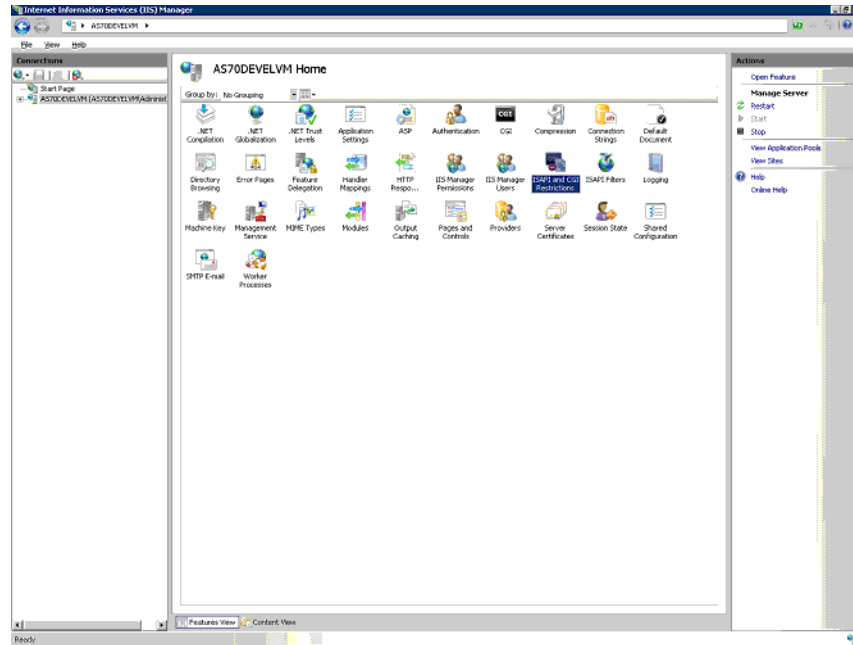
9. You can review the WebGate for IIS configuration settings and click **Finish**.



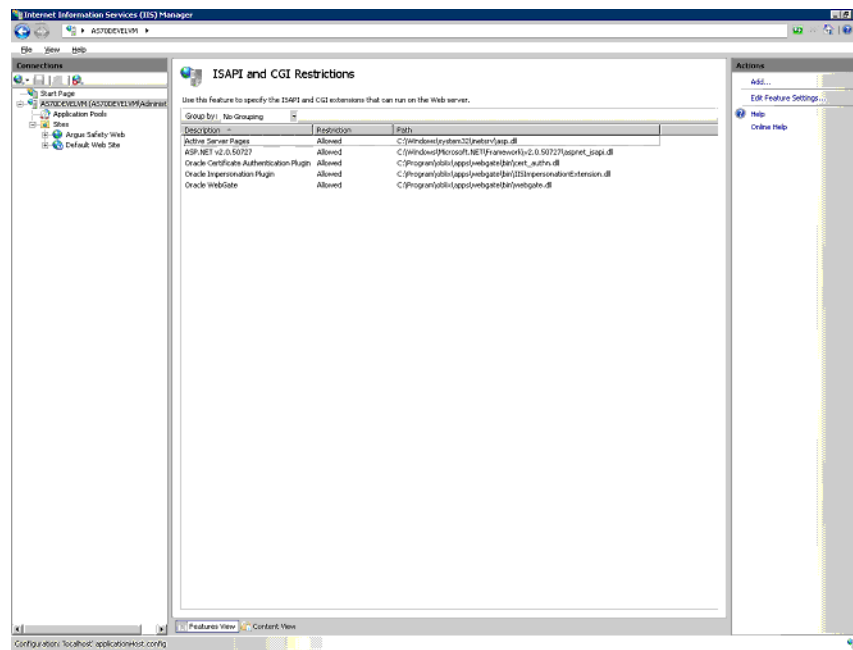
Configuring WebGate on Windows Server 2008

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

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:

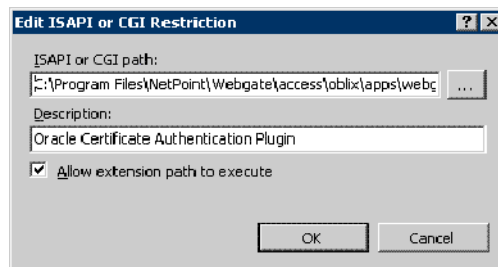


3. You have to correct the path for the following DLLs to reflect the path where you have installed the WebGate. To do this, double click the DLL entry and you will see the **Edit ISAPI or CGI Restrictions** dialog box as shown below. In this dialog box, enter the path given in the following table and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

Table 12–5 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
Oracle Impersonation Plugin	C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\II_SImpersonationExtension.dll
Oracle WebGate	C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\webgate.dll

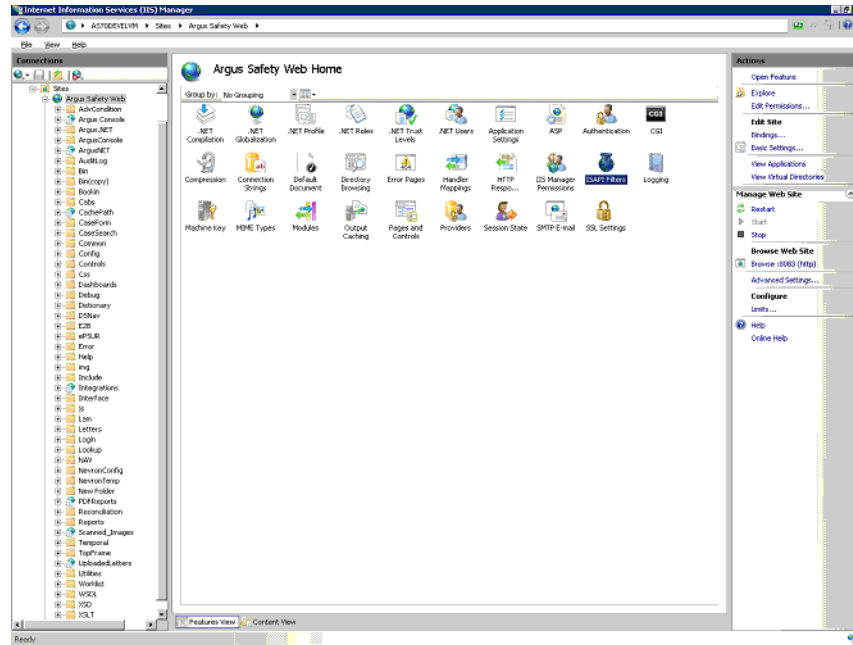
Note: For Windows 2008 R2, the DLLs must be manually added by clicking on the Add link in the right-most pane.



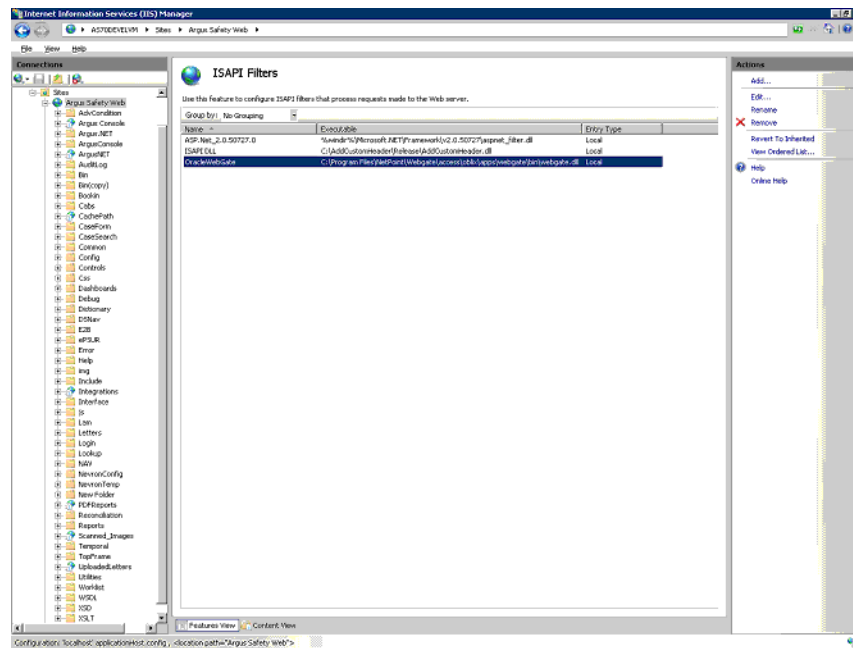
- Click **Edit Feature Settings** in the **Actions** panel in the right. The following dialog box appears:



- Check both the boxes and click **OK**.
- 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:



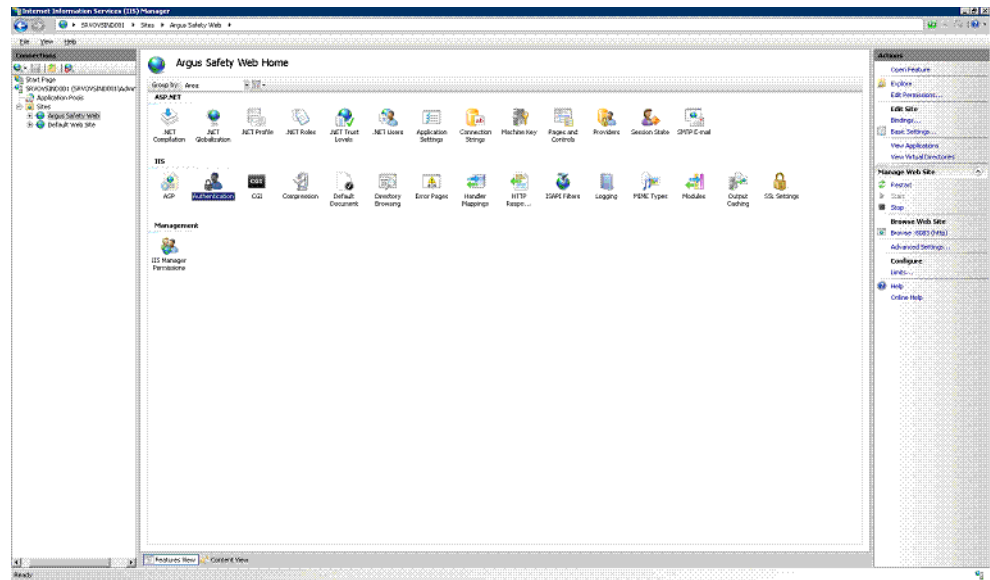
8. Double click **OracleWebGate** and enter the path to where you have installed WebGate. The default path is C:\Program Files\NetPoint\Webgate\access\oblix\apps\webgate\bin\webgate.dll

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:

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

2. Search for the <hiddenSegments> module.
 3. Remove the entry <add segment="bin"/> if it is present.
 4. 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:

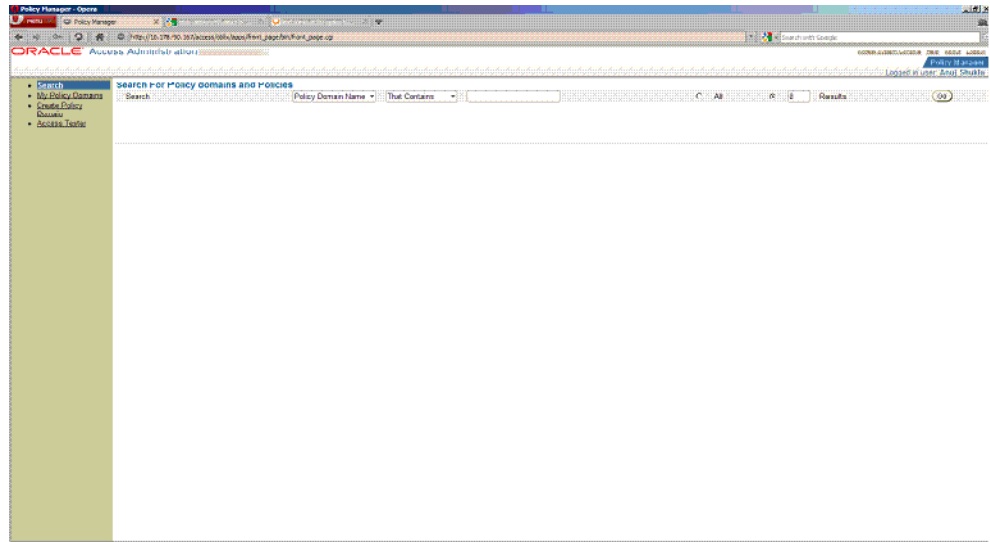


Right click on **Windows Authentication** and check if it is enabled. If yes, then disable it. This completes the WebGate installation on Windows Server 2008.

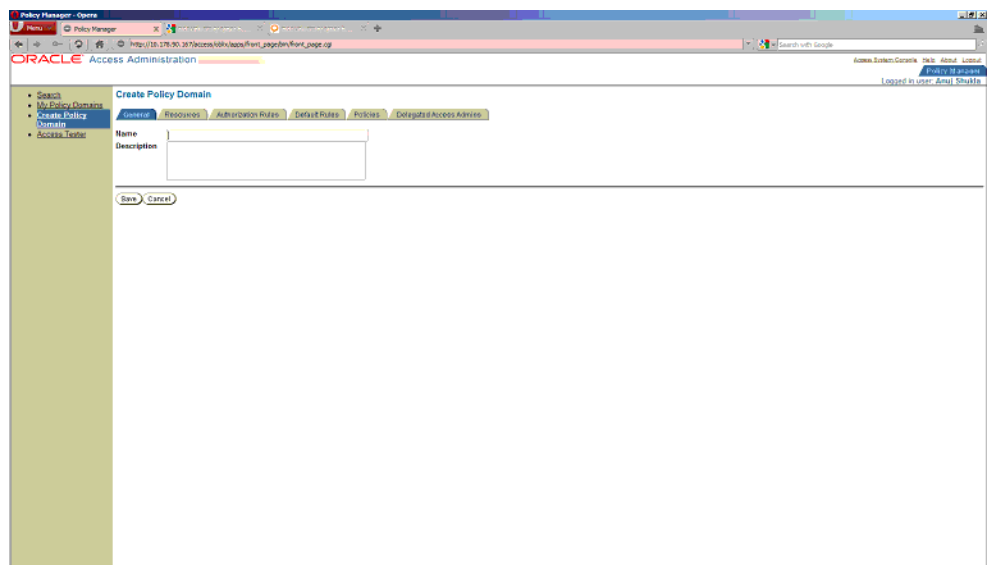
Protecting Files in the Argus Directory

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

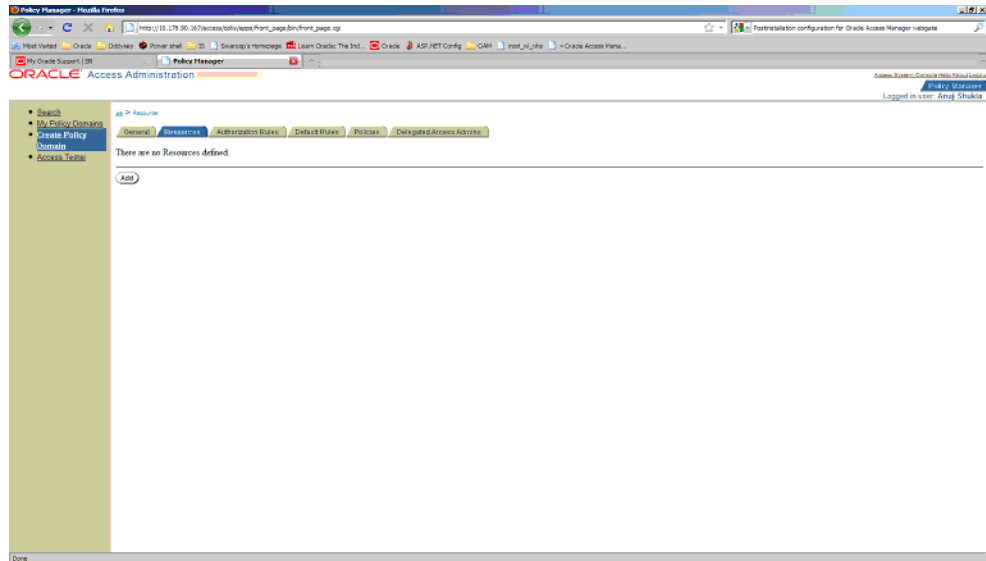
1. Navigate to the policy manager console and click **Create Policy Domain**.



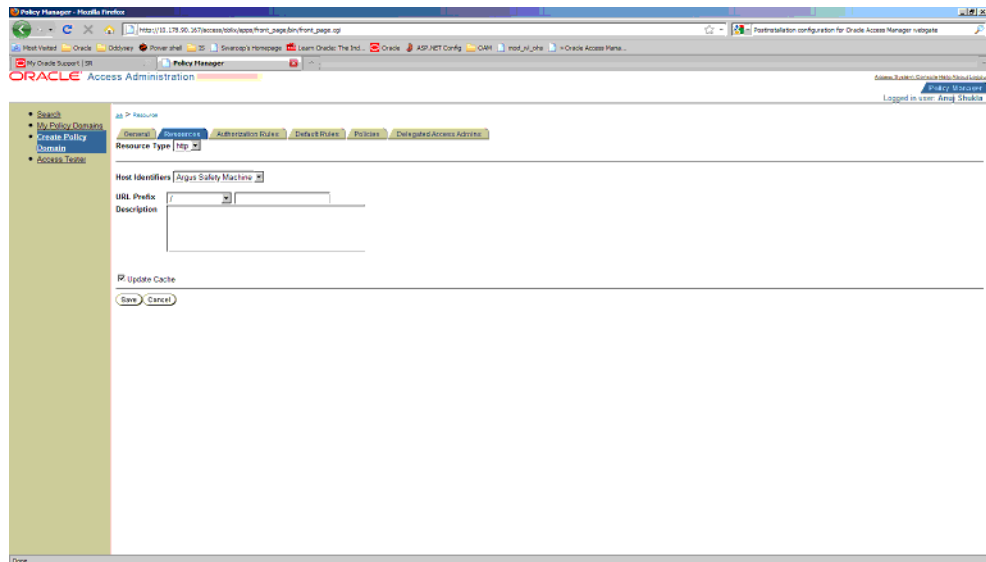
2. Under the **General** tab provide a name and description and click **Save**.



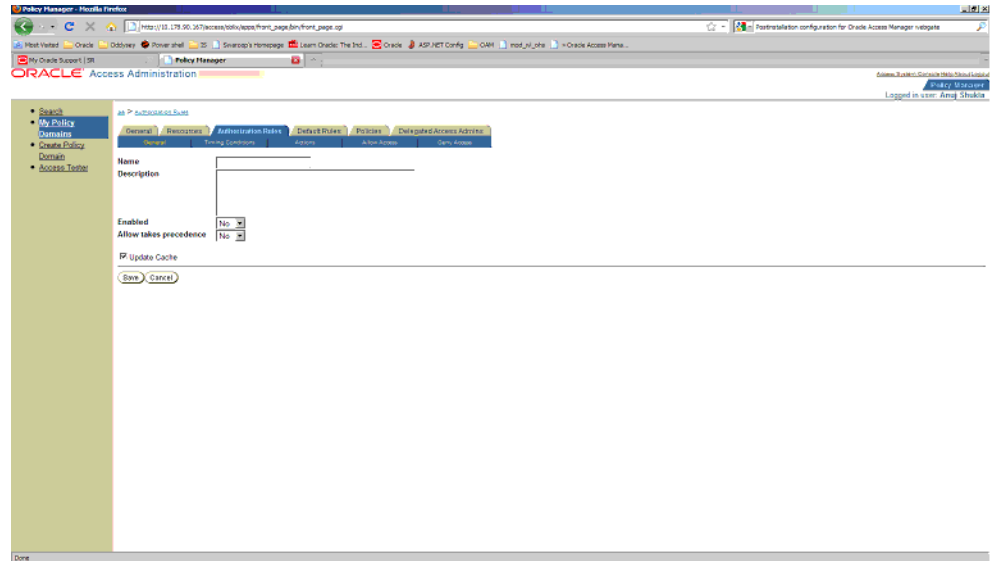
3. Click the **Resource** tab and then click **Add**.



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

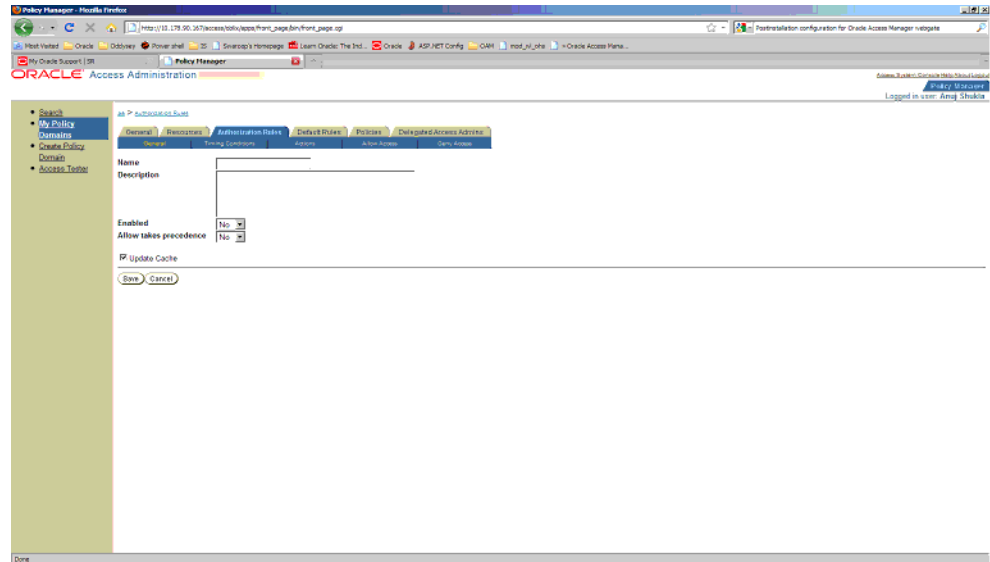


5. Click the **Authorization Rules** tab and select the **General** sub tab.

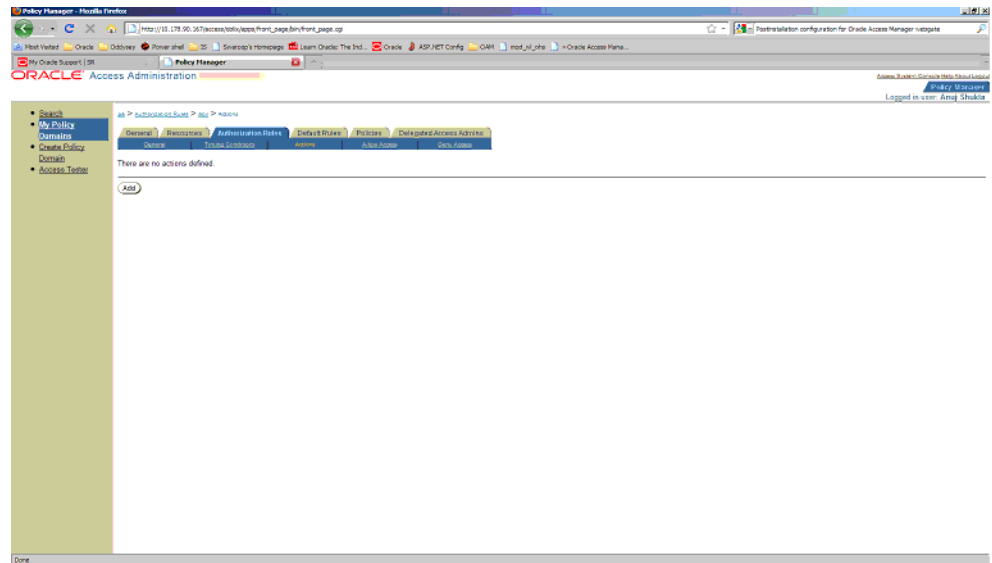


6. Enter the following details in this tab and click **Save**:

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



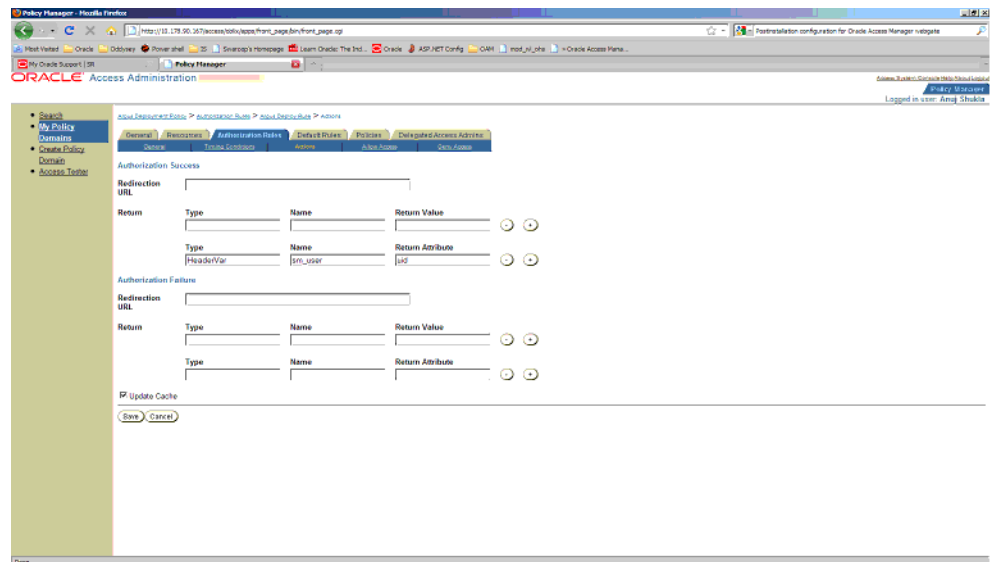
7. Now click the **Actions** sub tab. Click **Add**.



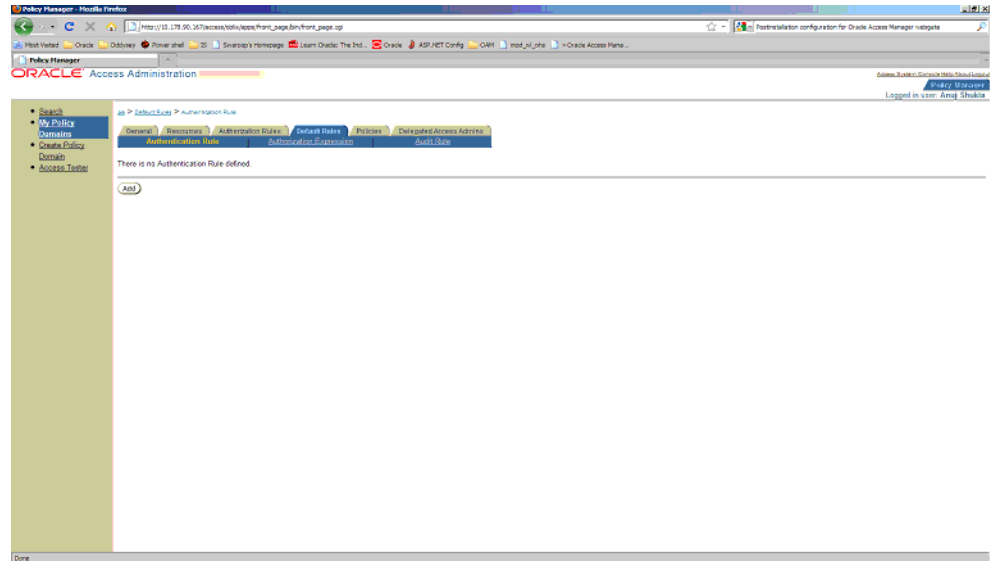
- In the **Authorization Success** section under **Return**, enter the following values and click **Save**:

Table 12–6 Values for Return field

Field name	Value
Type	HeaderVar
Name	SM_USER
Return Attribute	uid

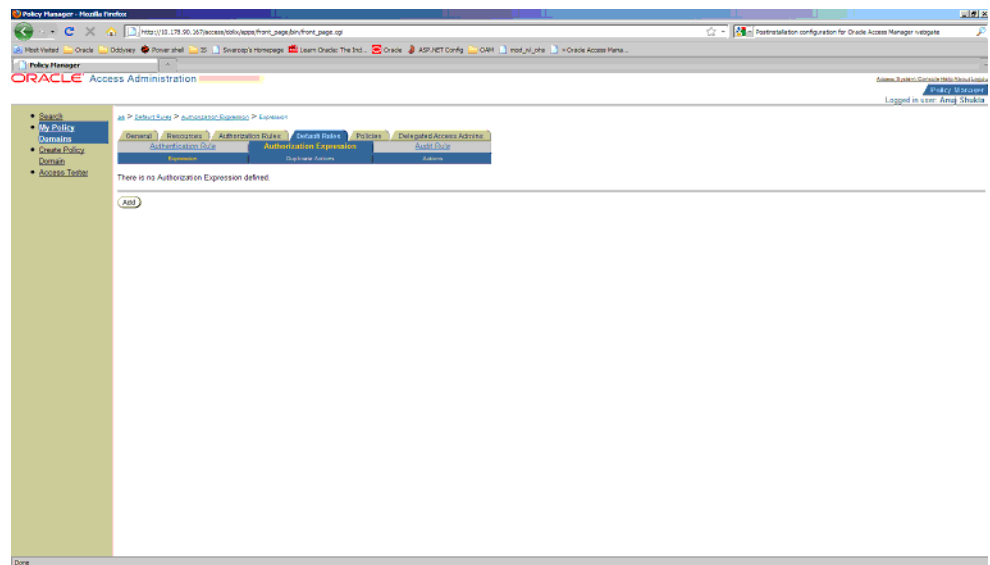


- Navigate to **Default Rules > Authentication Rule**. Click **Add**.



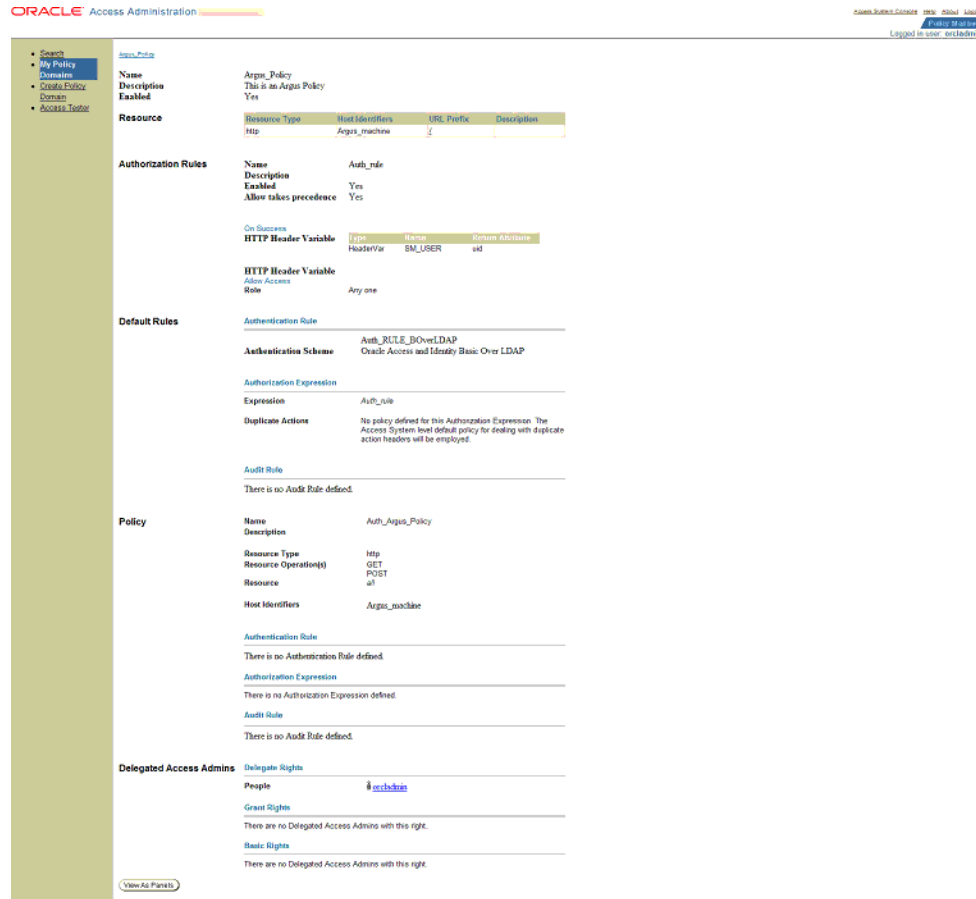
10. Enter details for Name and description and select Authentication Scheme as **Oracle Access and Identity Basic Over LDAP**. Click **Save**.

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



12. Select **Authorization Rule** from the dropdown. Click **Add** and then click **Save**.

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



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



Installation and Configuration of Oracle Web Tier Suite

The Oracle Web Tier Suite consists of following products:

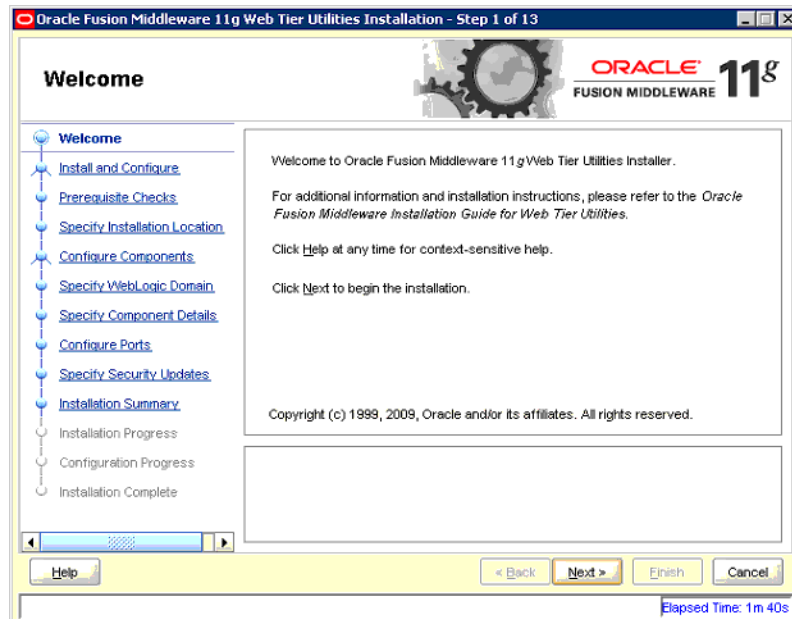
- Oracle Process Manager Notification (OPMN)
- Oracle HTTP Server (OHS)

- Oracle Web Cache

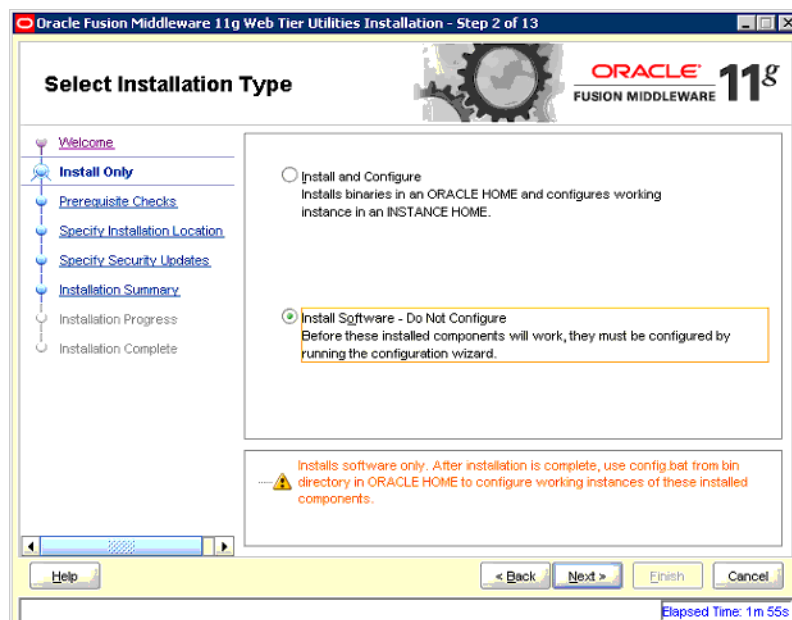
Installing Oracle Web Tier

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.

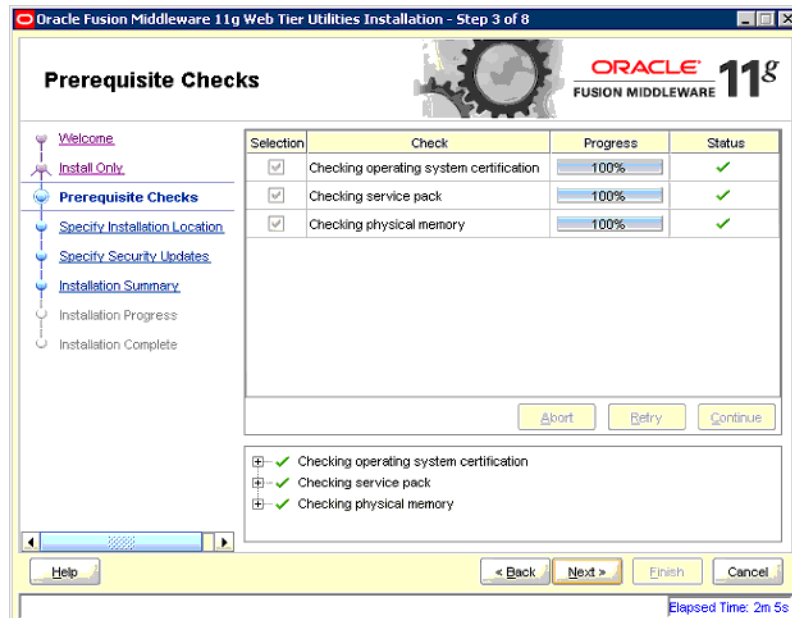
1. Navigate to folder \ofm_webtier_win_11.1.1.2.0_32_disk1_1of1\Disk1 and double click setup.exe to start the installer. The installer will begin after a check has been made for installer requirements.
2. Click **Next** to continue.



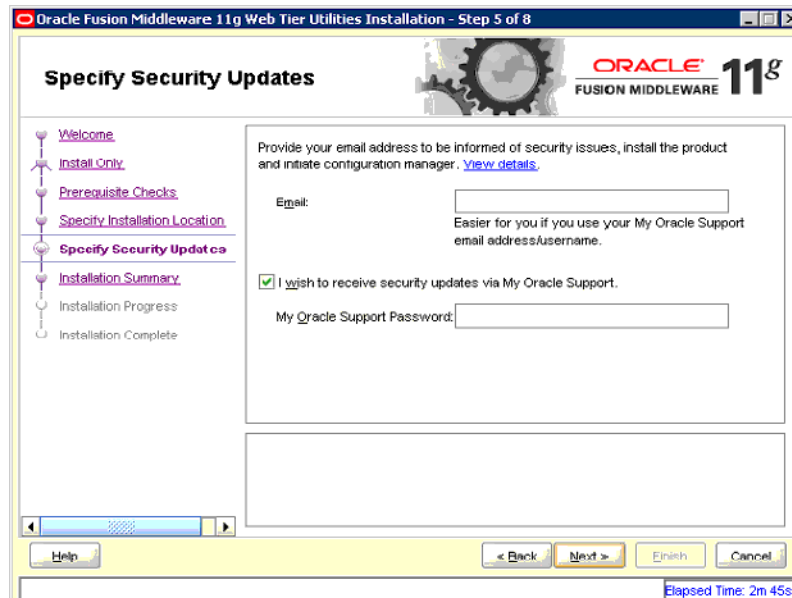
3. Select **Install Software - Do Not Configure** and click **Next**.



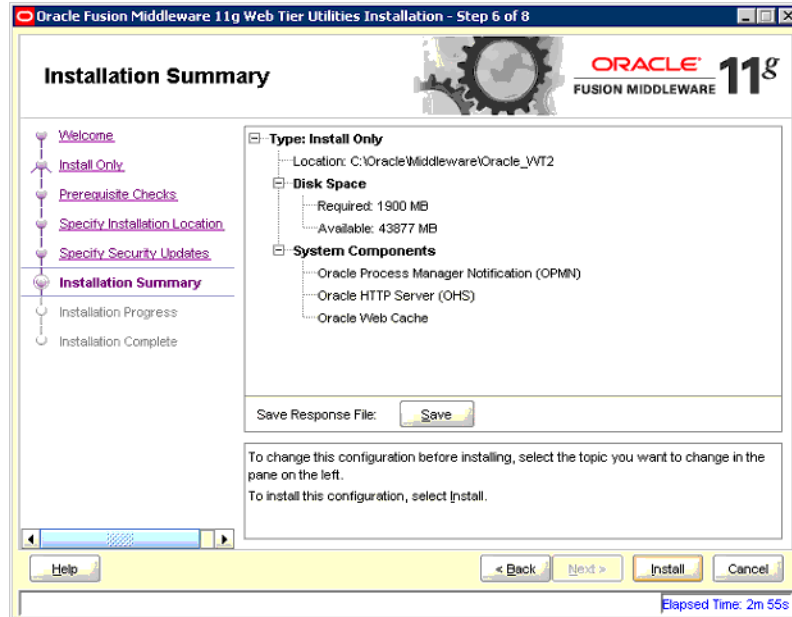
- In the next screen, the installer performs Prerequisite Checks. Click **Next** to continue.



- 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**.



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



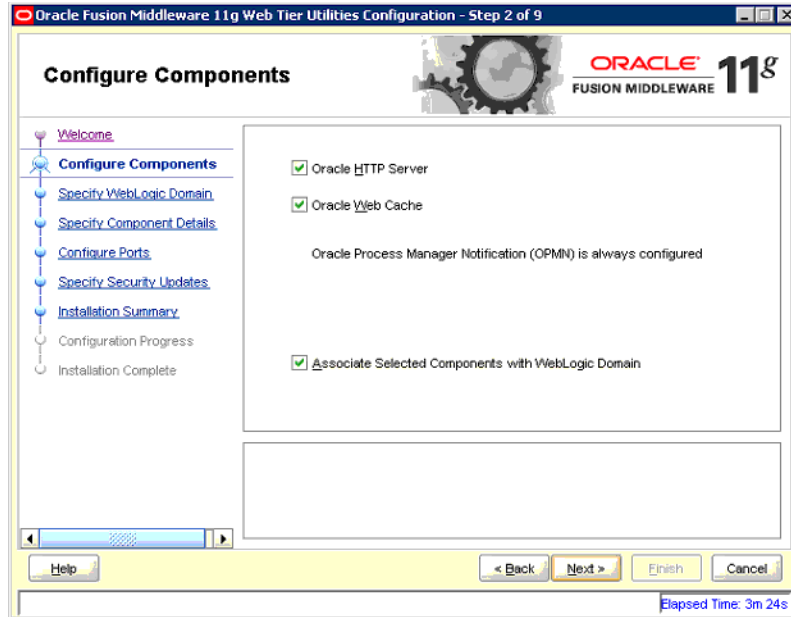
Configuring Oracle Web Tier

The following section describes the procedure to configure the Oracle Web Tier (OHS).

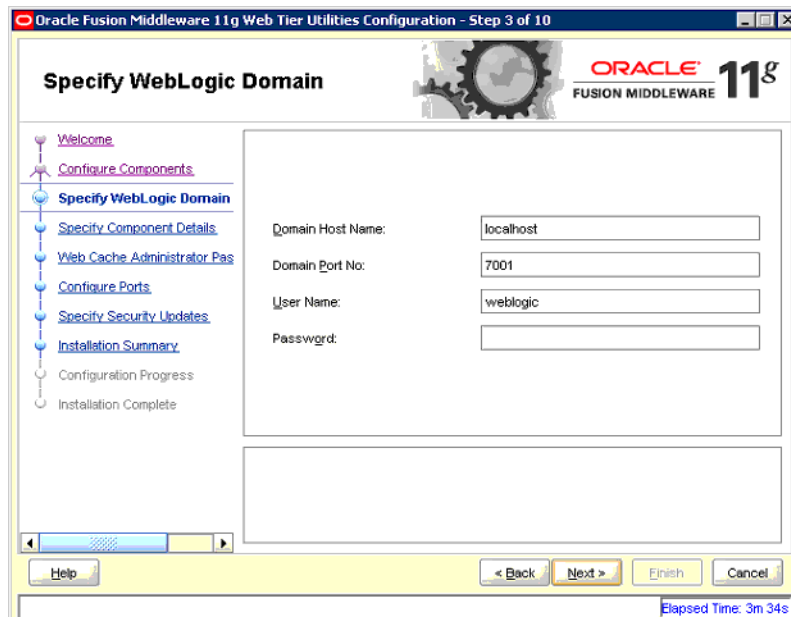
1. Navigate to the folder Oracle_Middleware_Home\Webtier_Instance\bin. For example, C:\OracleNew\Middleware\Oracle_WT1\bin. Here Oracle_WT1 is the name of the webtier instance created during installation. In the folder, run config.bat to start the configuration wizard.



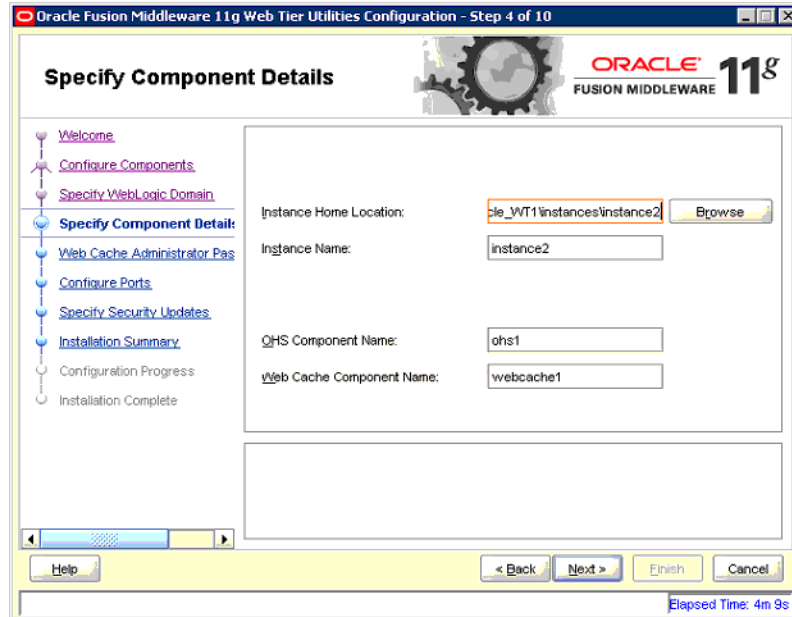
2. In the next screen, click **Next**.



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



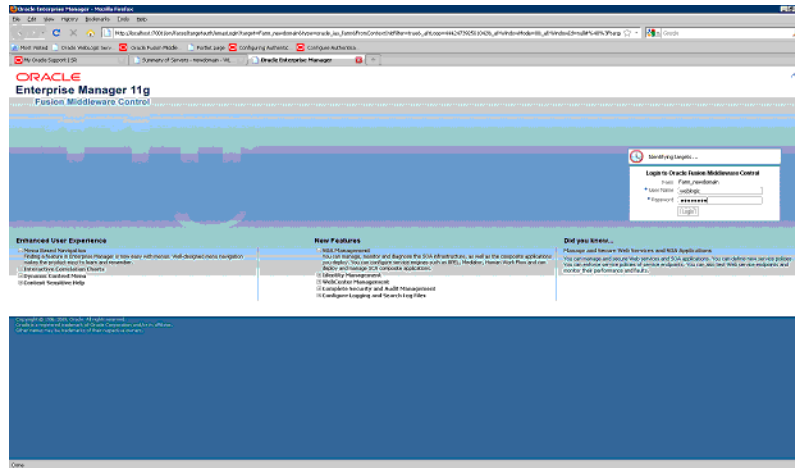
4. In the next screen, click Next.



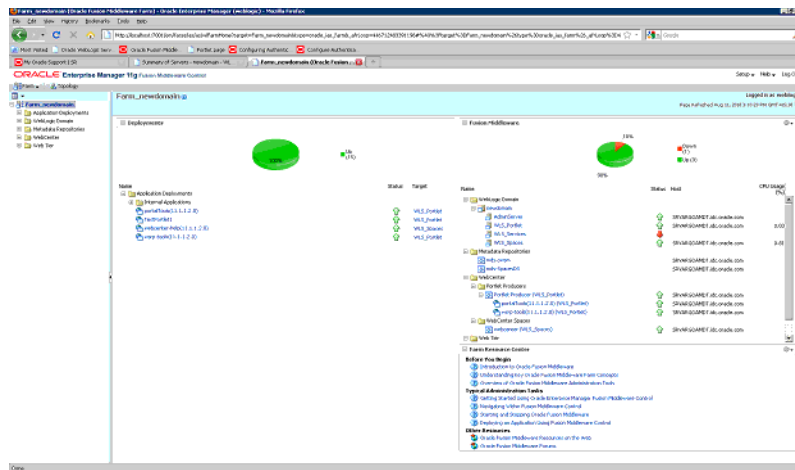
5. Enter a password for Web Cache and click Next.



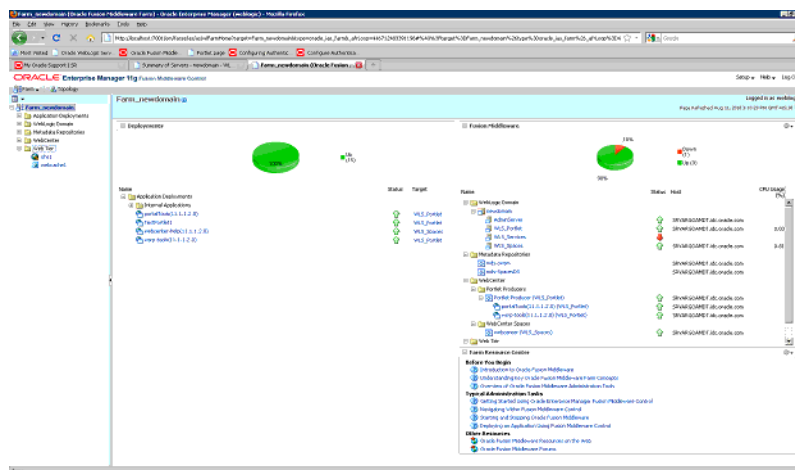
6. Select auto configuration port in the Configure Ports screen. Click Next.
7. Skip security updates for now and then click Next to continue configuring the Web Tier.
8. After the configuration, navigate to <http://localhost:7001/em>. This will open the Enterprise Management console for Fusion Middleware as shown below. Log in using the same credentials as that of the WebLogic server.



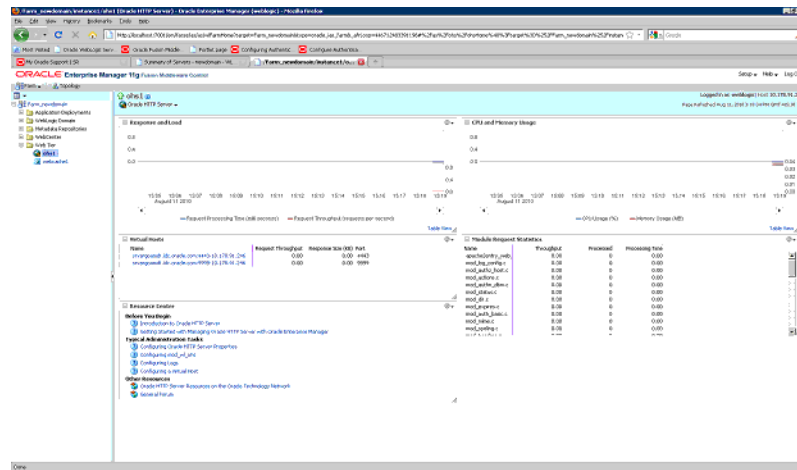
9. Click the Web Tier node on the left.



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



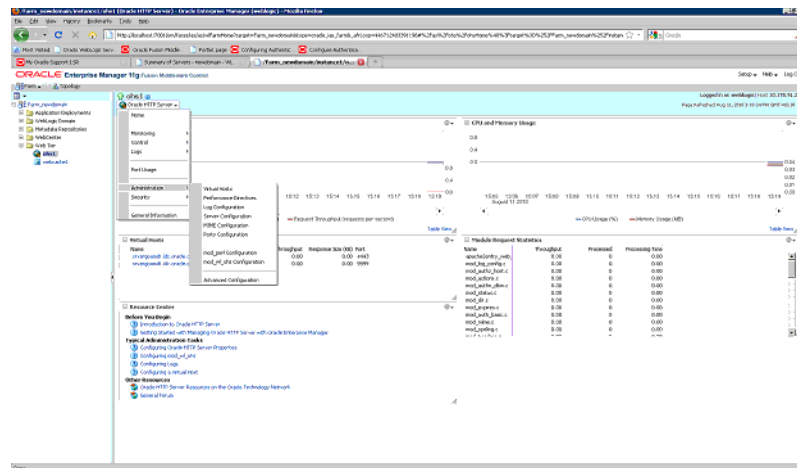
11. You will see all the details related to Oracle Http server on this console.



Oracle 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:

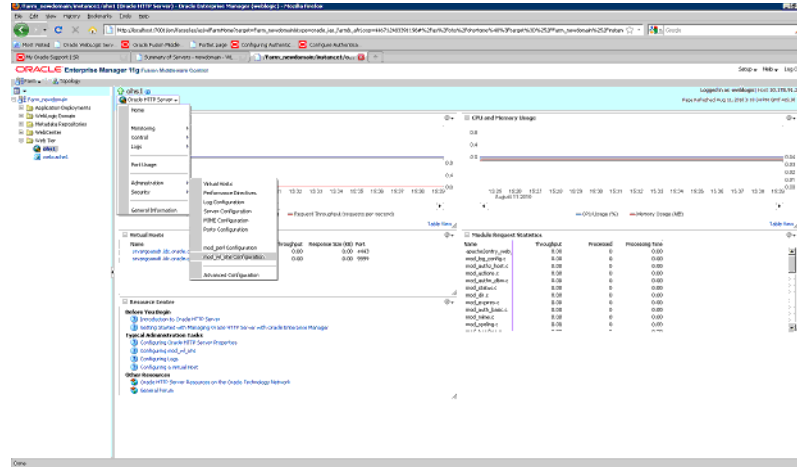
- Control => Start Up - You can start an OHS instance using this option.
- Control => Shut Down - You can stop and OHS instance using this option.
- Control => Restart - You can restart an OHS instance using this option.
- Logs => View Log Messages - You can view logs of the OHS instance using this option.

Configuring Oracle Http Server as Reverse Proxy Server for WebLogic

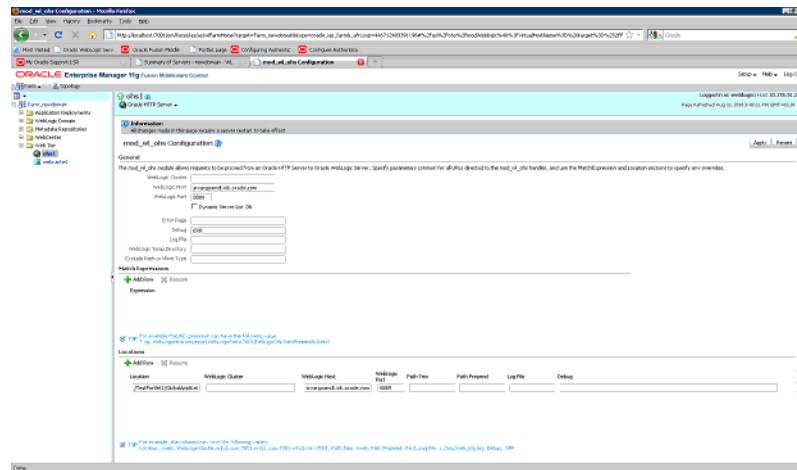
This section describes the procedure to configure the Oracle Http Server to act as a reverse proxy server for the WebLogic Server. Prior to following this procedure, ensure

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:

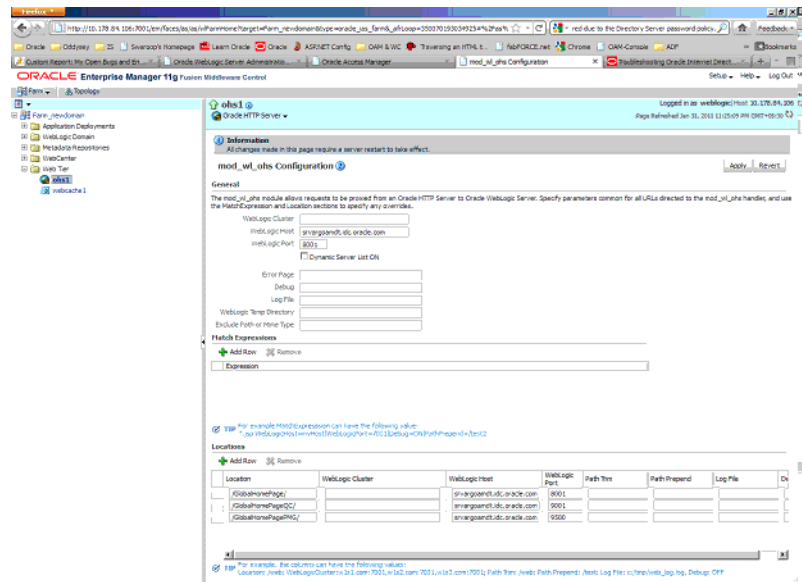
- **Weblogic host:** FQDN of the machine where weblogic server and other managed servers are running.
- **Weblogic port:** Port of the WebLogic server.
- **Debug:** Give ERR.
- **Log File:** You can provide a log file here.

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://srvargoamdt.idc.oracle.com:8001/GlobalHomePage/faces/GlobalHome`, then `srvargoamdt.idc.oracle.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://srvargoamdt.idc.oracle.com:7777/GlobalHomePage/faces/GlobalHome`. Here `srvargoamdt.idc.oracle.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.



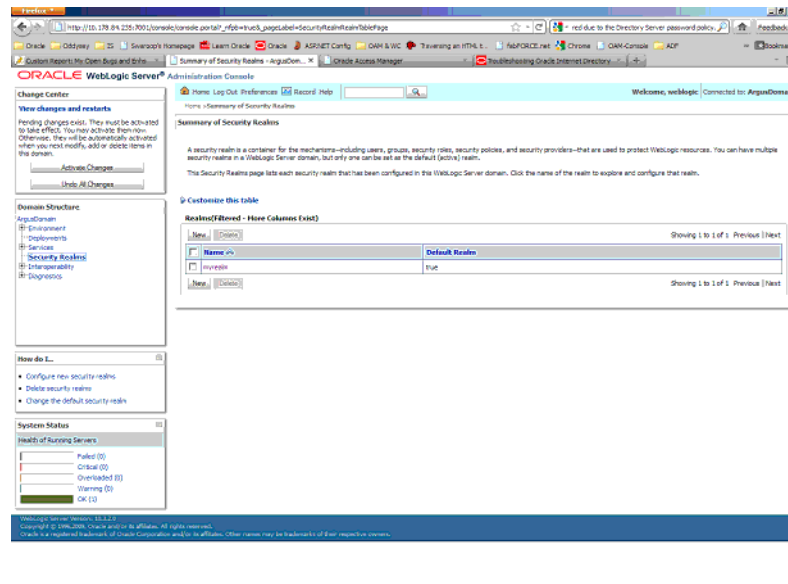
Configuring the WebCenter Security Provider for Identity Assertion

This section describes how to set the security provider of Web Logic Server to use Oracle Internet Directory which is the OAM identity store.

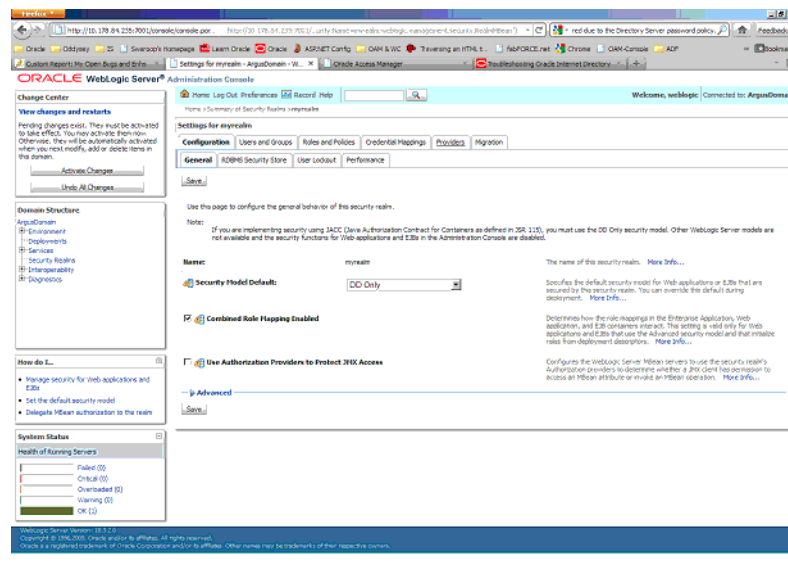
Configuring the Oracle Internet Directory Authenticator

This section describes the procedure to configure the Oracle Internet Directory Authenticator.

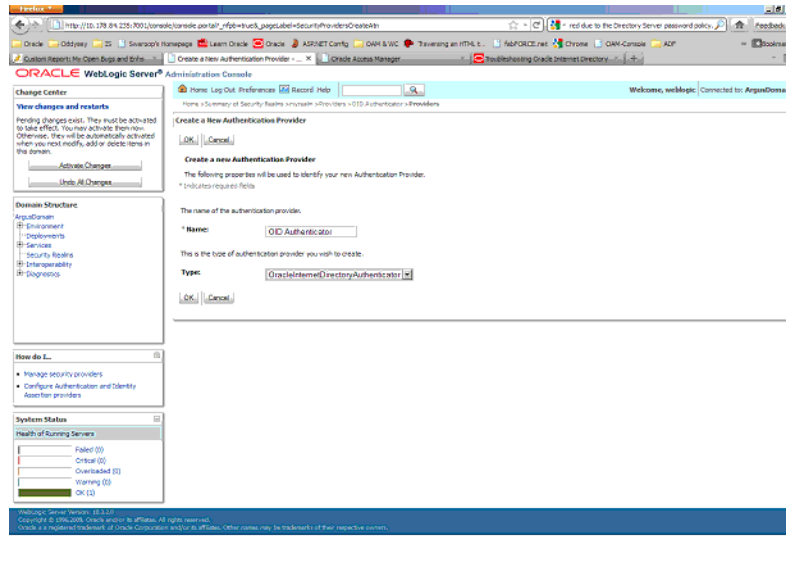
1. Log in to the WLS Administration Console. From the **Domain Structure** pane, click **Security Realms**. Then click **myrealm**.



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



3. Enter Name as OID Authenticator and select type from the dropdown as OracleInternetDirectoryAuthenticator. Click OK.

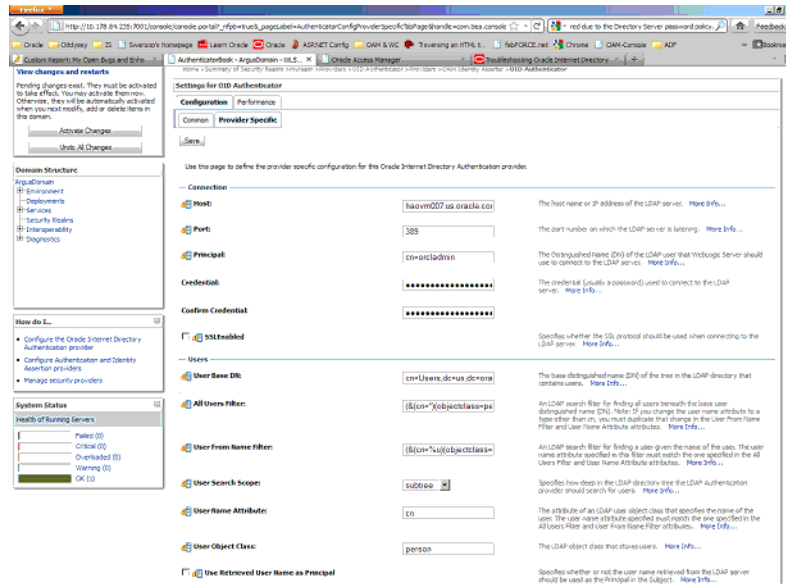


4. Go back to the Providers tab and click **OID Authenticator**, which appears as link.
5. In the **Common** sub tab modify the **Control Flag** field to **Sufficient** and click **Save**.
6. Click the **Providers Specific** tab and provide values for the fields described in the table below:

Table 12–7 Values for the Providers Specific tab

Parameter Name	Description	Sample Value
Host	LDAP Hostname	infra.vm.oracle.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
All Users Filter	Set as (&(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

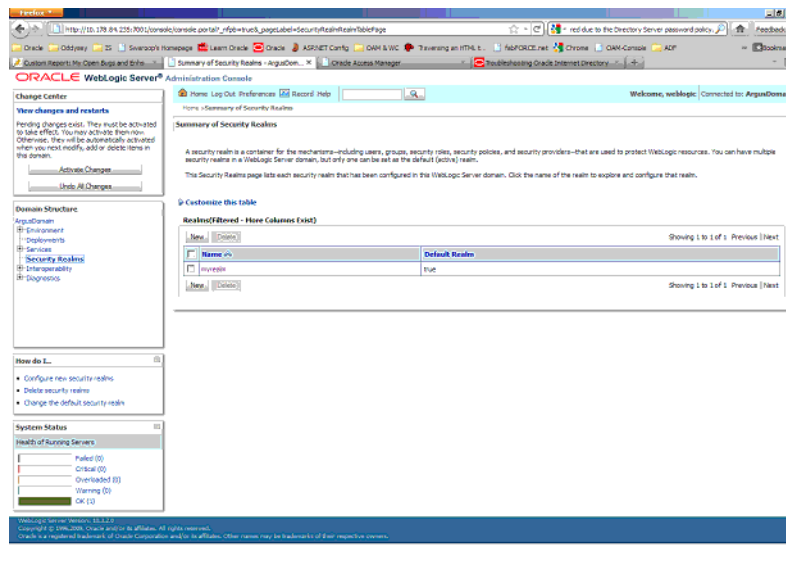
Retain the default values for the remaining attributes. Click **Save**.



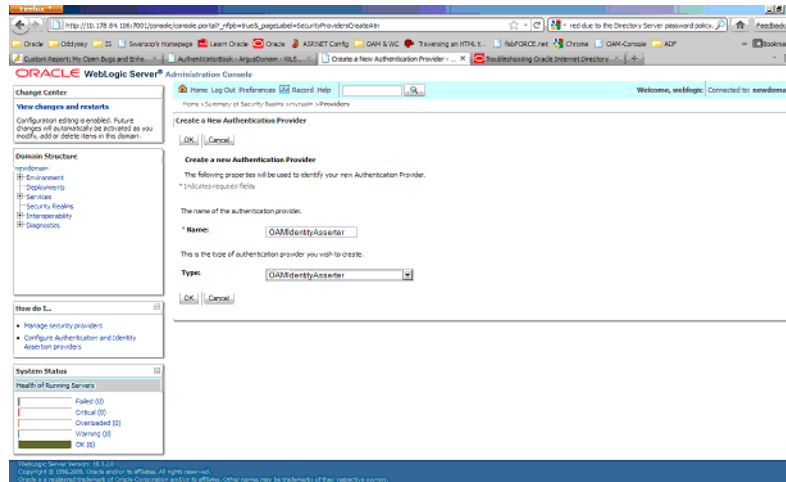
Configuring the OAM Identity Asserter

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.



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

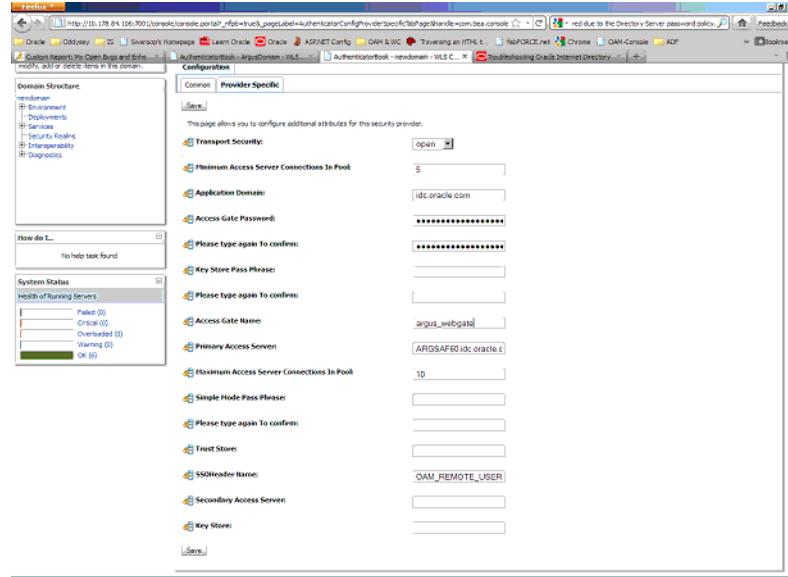


4. Click **OK** to save the details. Now click the newly added OAMIdentityAsserter, which appears as link to view its details.
5. In the Common sub tab select **control flag** as **REQUIRED** and click **Save**.
6. Navigate to the Providers sub tab and provide the details in the table below:

Table 12–8 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	argsaf60.us.oracle.com:6021
Access Gate Name	Copy the Access Gate name from the AG created from Step 3.	idc.oracle.com_AG
Access Gate Password	Type the Access Gate Password configured in access system console	

Retain the default values for the remaining attributes.



Configuring the Default Authenticator and Setting the Order of Providers

This section describes how to configure the default authenticator and set the order 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 checkbox for one or more components to install.
 - Select **Next >** to continue.

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

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

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 **checkbox** 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 Resizing checkbox.
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. Please refer to the section [Section , "Enabling SSL Support for Windows 2008"](#) 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. Please 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, please 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 Report 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.
- Please 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 6 Loader and double-click.
 - When the BCL easyPDF SDK 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 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 and Report 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, report server, integration server, transaction server, and so on). The directory structure of the file, however, remains constant. Refer to the following list of commonly modified configuration files:

- .\ArgusWeb\ASP\Argus.NET\bin\Intake.config
- .\ArgusWeb\ASP\Argus.NET\bin\RelsysWindowsService.exe.config
- .\ArgusWeb\ASP\Argus.NET\bin\Service.config
- .\ArgusWeb\ASP\Argus.NET\web.config
- .\ArgusWeb\ASP\ArgusConsole\web.config
- .\ArgusWeb\ASP\Integrations\Service.config
- .\ArgusWeb\ASP\Integrations\Web.config

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

Argus Integrations

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

- [Installing Argus Integrations](#)
- [Resetting IIS](#)
- [Overview: Argus Web Service Interface](#)
- [Basic Configuration Overview](#)
- [Safety Message Overview](#)
- [MedDRA Interface](#)
- [Product License Study Interface](#)
- [WHO Drug Coding Interface](#)
- [Lot Number Interface](#)
- [Worklist Intake](#)
- [Literature Intake](#)
- [Extended E2B Interface](#)

Installing Argus Integrations

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

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

Use the following procedure to install Argus Safety Integrations:

1. When the system displays the Argus Safety screen:
 - Click **Argus Safety** to start the installation.
2. When the system displays the Argus Safety Setup screen:
 - Click **Next >**.
3. When the system displays the Customer Information screen:
 - Enter the user name in the **User Name** field.

- Enter the company name in the **Company Name** field.
- Click **Next >**.
4. When the system displays the Default Directory screen, click Browse to select the default installation directory where the Argus Safety Solution Components will be installed.
 - Click **Next** to display the Argus Safety Components list and select the default installation directory where the Argus Safety Solution Components will be installed.
5. When the system displays the component list:
 - Select the modules to install.
 - Click **Next >**.
6. When the system displays the Argus Safety Solution Components Report Directory screen:
 - Click **Browse**, select the folder to store the temporary reports in, and click **OK**.
 - Click **Next >** to continue.

Argus installs and shows the progress of the installation.
7. When the system prompts you to enter a port number:
 - Enter the Port for the Argus Web site (default is 8083, and can be changed to port 80 at any time).
 - Click **Next >** to continue.

The installer installs the Web site 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 7.0.3 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 7.0.3 release supports 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, please 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:\Program 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_IReSysService_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/IRelsysService/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>
```

```

    </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/IRelsysService
      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/IRelsysService
      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/IRelsysService
      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	<p>An enumeration supporting the following values (currently only one):</p> <p>Auto</p> <p>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.</p>
Source	<p>An enumerated value that specifies additional information that may be required for coding based on origination as follows:</p> <ul style="list-style-type: none"> ■ Reaction 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	<p>Case Form Events Tab Event Tab Description to be Coded</p> <p>Case Form Events Tab Death Information Cause of Death and Autopsy Results Description as Reported</p>
Diagnosis	Argus Case Form Analysis Tab Analysis Tab Company Diagnosis Syndrome
Term(v 1.0)	<p>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.</p> <p>Reported</p> <p>Coded</p>
Term(v 1.1)	<p>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.</p> <p>Reported</p> <p>Coded</p> <p>Lang</p>

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 checkbox 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. Please 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>
```

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

- **Web.Config**

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

Sample endpoint configuration with binding configuration:

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

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/IRelsysService
      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>

```

```

    </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/IRelsysService/
      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: <ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ LOT Number ▪ Expiration Date ▪ Custom <p>Provides a mechanism</p> <p>Name: Attribute value is used to identify Case Form field that is to be populated with data in the node</p> <p>Metadata: Attribute value is used as labels in the LOT Number selection selection dialog displaying the data</p>

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.XSLTFactory" InterfaceType="Outbound"
RequestType="Response" MessageType="RelsysMessage" Enabled="true"
TransformID="LOT_NUMBER"
Metadata="InputValidationXSD=/Integrations/XSD/v1.0/Lot_Response.xsd;" />
```

- Lot Number Web Service XSLT

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

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

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

```
<?xml version="1.0" encoding="utf-8"?>
<tnc:SAFETY_MESSAGE xmlns:tnc="http://www.oracle.com/Argus/Base/v1.0"
xmlns:tnsa="http://www.oracle.com/Argus/CodeListCommon/v1.0"
xmlns:tnsb="http://www.oracle.com/Argus/ProductFamilyEntity/v1.0"
xmlns:tncs="http://www.oracle.com/Argus/Case_Intake/v1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" tnc:Type="Request">
<tnc:CASE_INTAKE>
<tnc:CASES>
<tnc:CASE>
<tnc:CASE_TYPE>Sponsored Trial</tnc:CASE_TYPE>
<tnc:COUNTRY_OF_INCIDENCE>US</tnc:COUNTRY_OF_INCIDENCE>
<tnc:EVENT_PT>Pyrexia</tnc:EVENT_PT>
<tnc:EVENT_VERBATIM>Fever</tnc:EVENT_VERBATIM>
<tnc:FLTH>LT</tnc:FLTH>
<tnc:GENERIC_NAME>Cure All</tnc:GENERIC_NAME>
<tnc:INITIAL_DATE>2001-06-07</tnc:INITIAL_DATE>
<tnc:PRIORITY>1</tnc:PRIORITY>
<tnc:PRODUCT_NAME>Cure All</tnc:PRODUCT_NAME>
<tnc:REPORTER_TYPE>Health Care Professional</tnc:REPORTER_TYPE>
<tnc:SITE>United States</tnc:SITE>
<tnc:STUDY_ID>Test Study</tnc:STUDY_ID>
<tnc:SUR>Yes</tnc:SUR>
<tnc:ATTACHMENTS>
<tnc:ATTACHMENT>
<tnc:FILENAME>Case12345.pdf</tnc:FILENAME>
<tnc:DOCID>001219988776655</tnc:DOCID>
<tnc:CLASSIFICATION></tnc:CLASSIFICATION>
<tnc:ATTACHMENT_DESC>Contains case data for 12345</tnc:ATTACHMENT_DESC>
</tnc:ATTACHMENT>
</tnc:ATTACHMENTS >
```

```

</tnsc:CASE>
</tnsc:CASES>
</tnsc:CASE_INTAKE>
<tns:EXTENSION>
<tns:CUSTOM tns:Name="ABC" tns:Metadata="DEF">GHI</tns:CUSTOM>
</tns:EXTENSION>
</tnsc:SAFETY_MESSAGE>

```

Response

```

<?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" tns:Type="Response">
<tnse:CASE_INTAKE>
<tnse:CASES>
<tnse:CASE>
<tnse:INTAKE_DATE>09-SEP-2009 09:09:09</tnse:INTAKE_DATE>
<tnse:CASE_NUMBER>2009JP000001</tnse:CASE_NUMBER>
<tnse:CASE_ID>10002901</tnse:CASE_ID>
<tnse:CASE_PRODUCT>Cure All</tnse:CASE_PRODUCT>
<tnse:DATE_TIME>18-SEP-2009 18:18:18</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>
<tns:EXTENSION>
<tns:CUSTOM tns:Name="ABC" tns:Metadata="DEF">GHI</tns:CUSTOM>
</tns: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 on 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 checkbox 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?, patientgpmedicalrecordnum?, patientspecialistrecordnum?,
patienthospitalrecordnum?, patientinvestigationnum?, 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:

```

EMEAEXT-ICSR-V2.1.dtd
<!-- 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;

```

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 7.0.3

Whether you are upgrading to Argus Safety 7.0.3 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 7.0.3 Database

Prior to creating a 7.0.3 database or upgrading to a 7.0.3 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 7.0.3 Application Servers

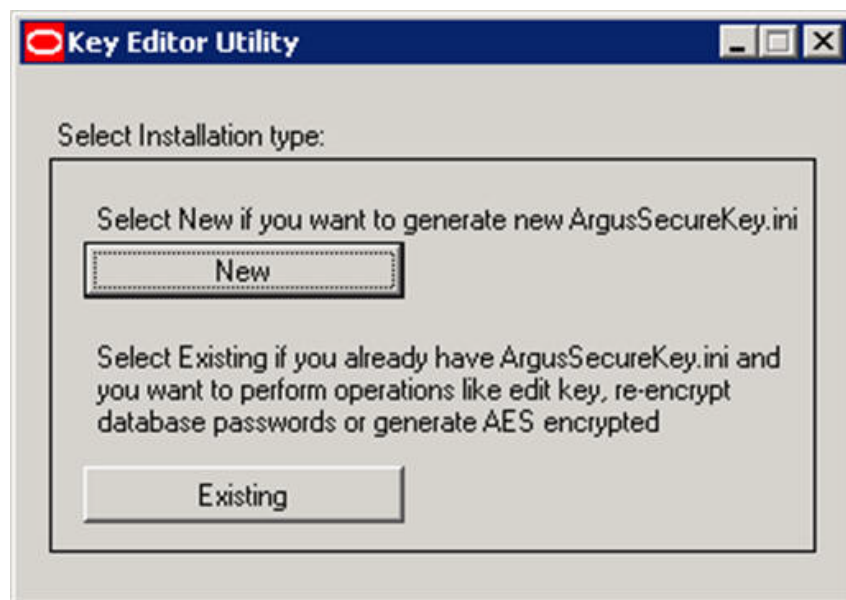
After the application servers have been installed with 7.0.3, copy the ArgusSecureKey.ini file from the .\Windows folder of the system which was used to create or upgrade the database to the .\Windows folder of each installed application server.

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:

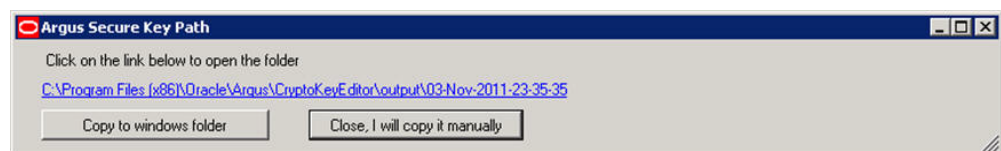
1. Launch the **Cryptography Key Editor**. The **Key Editor Utility** screen appears.



2. Click **New**.
3. The following screen appears.



4. 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.
5. In the **Enter ARGUSUSER password** field, enter the password for the database user called ARGUSUSER.
6. Confirm the password in the **Confirm password** field.
7. Click **OK**. The ArgusSecureKey.ini file gets created in the <Installation folder> \ CryptoKeyEditor\output\<DateTimeStamp>\.
8. The **Argus Secure Key Path** dialog is displayed.



9. Click the link in the **Argus Secure Key Path** dialog to open the folder in Windows Explorer.
10. Click **Close, I will copy it manually** to close the dialog and copy the file manually from the window that gets opened by clicking on the link mentioned above (in step 9).
11. 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](#)

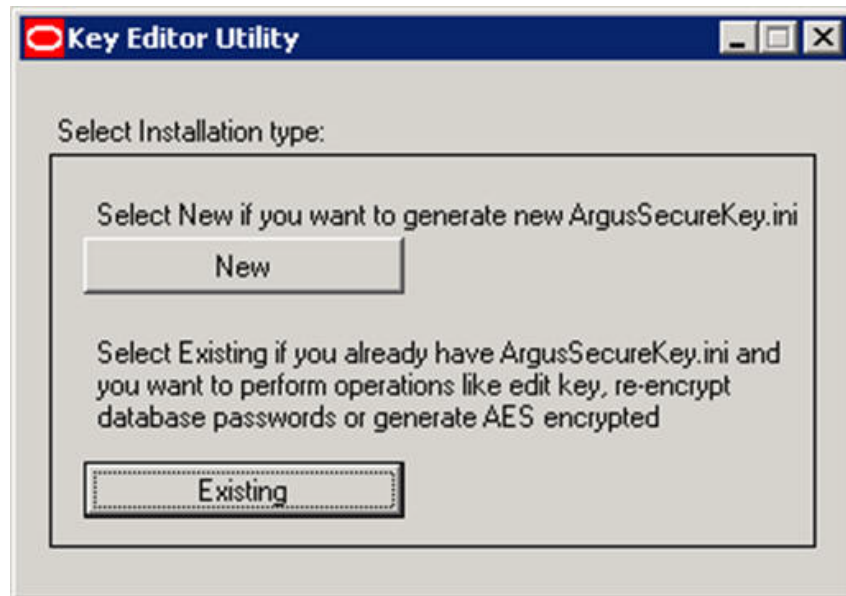
- [Generating Encrypted String from Clear Text on Configured User Cryptography Key](#)
- [Resetting the Environment if ArgusSecureKey.ini is Lost](#)

Resetting the ARGUSUSER Password

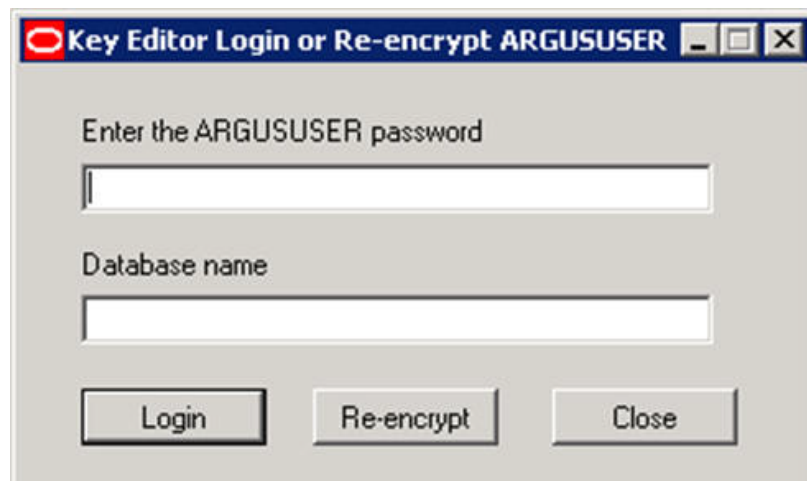
If the password for the database user "ARGUSUSER" has changed, you will need to reset the password in the ArgusSecureKey.ini file on all the servers.

Execute the following steps to reset the ARGUSUSER password:

1. Launch the **Cryptography Key Editor**. The **Key Editor Utility** screen appears.



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 **Re-encrypt**. The following dialog appears.



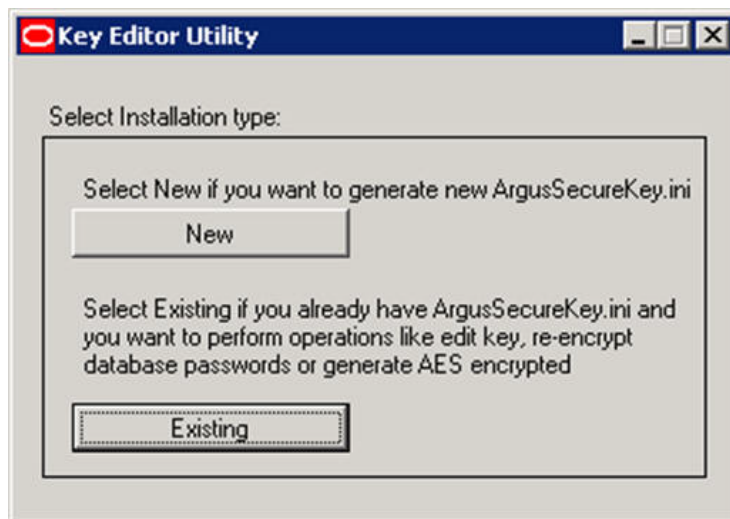
6. Click **Yes**.
7. Copy the updated ArgusSecureKey.ini File from the .\Windows folder to all the .\Windows folder of all the application servers.
8. Verify that you can login to the Argus Safety application.

Editing Keys

An administrator might want to change a key due to various reasons like a policy to change key every few days, network compromise, etc.

Execute the following steps to edit the cryptography keys:

1. Launch the **Cryptography Key Editor**. The **Key Editor Utility** screen appears.

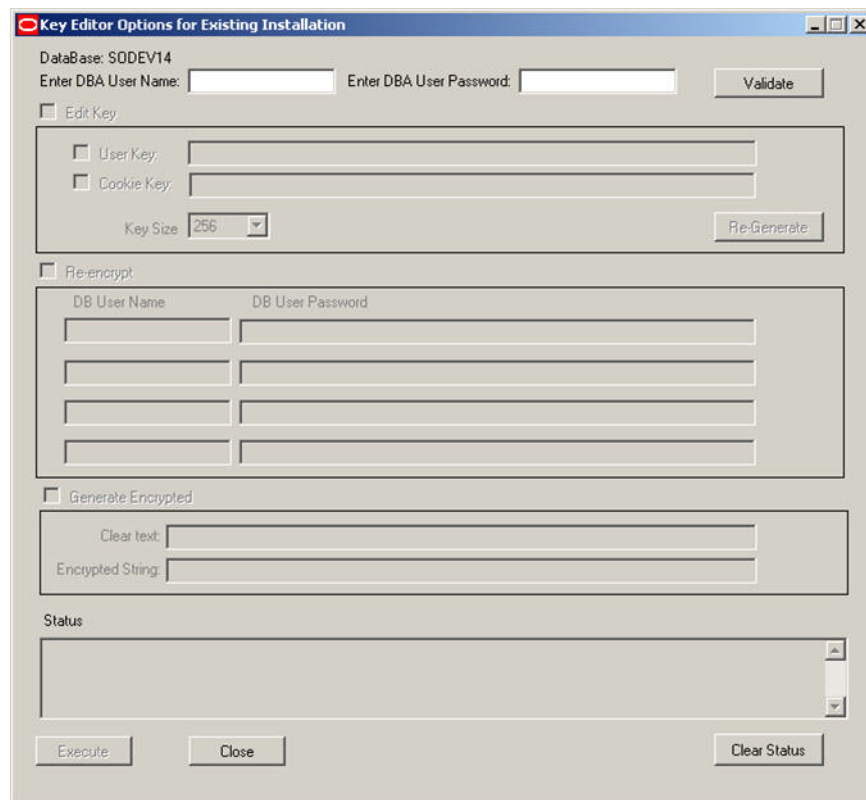


2. Click **Existing**. The **Key Editor Login or Re-encrypt ARGUSUSER** screen appears.



The dialog box has a title bar that reads "Key Editor Login or Re-encrypt ARGUSUSER". It contains two text input fields: "Enter the ARGUSUSER password" and "Database name". Below these fields are three buttons: "Login", "Re-encrypt", and "Close".

3. In the **Enter the ARGUSUSER password** field, enter the password for the database user called ARGUSUSER.
4. Enter the name of the database in the **Database name** field.
5. Click **Login**. The following **Key Editor Options for Existing Installation** screen appears.



The dialog box has a title bar that reads "Key Editor Options for Existing Installation". It displays "DataBase: SODEV14". It contains several sections:

- DB User Information:** "Enter DBA User Name:" and "Enter DBA User Password:" fields with a "Validate" button.
- Edit Key:** A checkbox labeled "Edit Key". If checked, it enables "User Key:" and "Cookie Key:" fields, a "Key Size" dropdown menu (set to 256), and a "Re-Generate" button.
- Re-encrypt:** A checkbox labeled "Re-encrypt". If checked, it enables a table with two columns: "DB User Name" and "DB User Password", containing four rows of empty text boxes.
- Generate Encrypted:** A checkbox labeled "Generate Encrypted". If checked, it enables "Clear text:" and "Encrypted String:" fields.
- Status:** A large text area for displaying status messages.

 At the bottom are "Execute", "Close", and "Clear Status" buttons.

6. Enter the DBA User Name and User Password.
7. Click **Validate**.
8. Check the **Edit Key** checkbox. This enables the child checkboxes of **User Key** and **Cookie Key**.

Key Editor Options for Existing Installation

DataBase: SODEV14
 Enter DBA User Name: ARGUS_APP Enter DBA User Password: ***** Validate

Edit Key

User Key: 482BF0BF9B8512CC71971F0F18912038941BC5FABEE8D54B8DD485EE3439AF490C5AE
 Cookie Key: 3158B082CB1CDEEB20B577CB869030B5423DB417DA4E3B442E679650C9E591D668D6

Key Size: 256 Re-Generate

Re-encrypt

DB User Name	DB User Password
ARGUS_LOGIN	
ARGUS_LOGIN_I	
ARGUS_LOGIN_IPS	
DLP_OWNER	

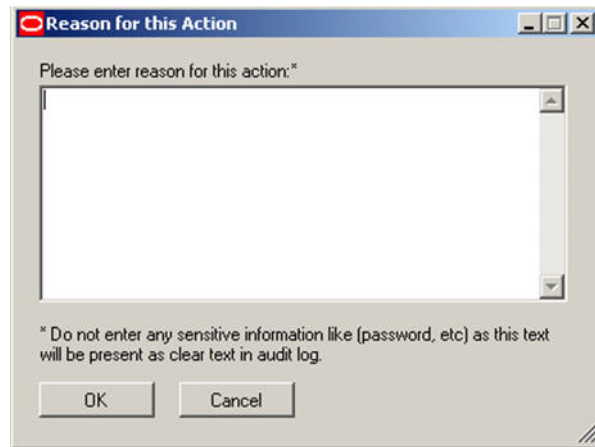
Generate Encrypted

Clear text:
 Encrypted String:

Status

Execute Close Clear Status

9. The User Key is used for all the encrypted strings which are persisted in the database or file server.
10. The Cookie Key is only used to encrypt and decrypt the key.
11. The user has the option to change either one or both keys.
12. Select the checkboxes in front of the key that you want to change.
13. 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.
14. Click **Re-Generate**. This will change the value of the checked items and the new value will be visible in the textbox.
15. Click **Execute**. The **Reason for this Action** dialog is displayed, prompting the user to add a reason for his action.



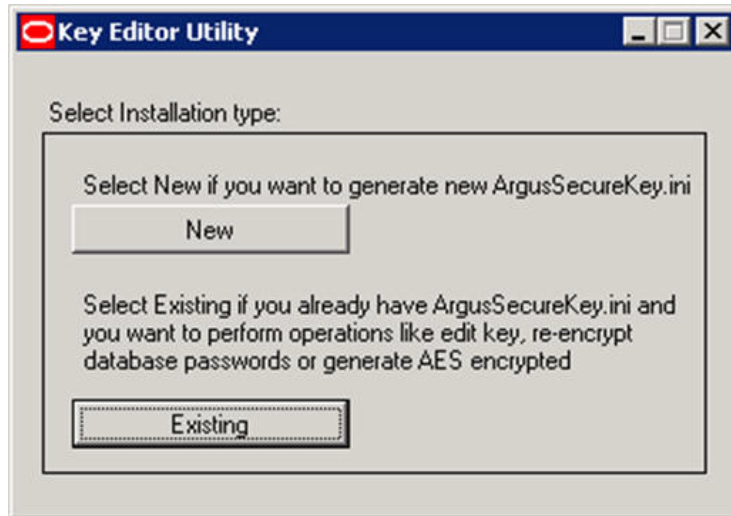
16. The text entered here is visible in the Audit Log in the Argus Safety application.
17. Click **OK**.
18. Check the status box to verify if the operation has been successful.
19. If the operation is successful and the Cryptography key is checked, then the changed key is now stored in the ArgusSecureKey.ini. 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.
20. 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:
 21. Items to be changed from the User Interface:
 22. Argus Services: Open Argus Safety Service Configuration: Open all the processes and enter password again
 23. Cyclone: Open ESM Mapping utility and reenter Cyclone password
 24. ESM Common User: Open ESM Mapping utility and reenter ESM Common user password
 25. Re-enter the DBPassword in the configuration files, as explained in the following sections:
 26. Point 2 of the [RelsysWindowsService.exe.config](#) sub-section
 27. Point 5 of the [Configuring the Dossier Application](#) section
 28. 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.



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 following **Key Editor Options for Existing Installation** screen appears.

Key Editor Options for Existing Installation

DataBase: S0DEV14
Enter DBA User Name: Enter DBA User Password:

Edit Key

User Key:
 Cookie Key:

Key Size: 256

Re-encrypt

DB User Name	DB User Password
<input type="text"/>	<input type="password"/>
<input type="text"/>	<input type="password"/>
<input type="text"/>	<input type="password"/>
<input type="text"/>	<input type="password"/>

Generate Encrypted

Clear text:
Encrypted String:

Status

6. Enter the DBA User Name and User Password.
7. Click **Validate**.
8. Check the **Re-encrypt** checkbox.
9. Enter the passwords for the common users.

10. Click **Execute**. The **Reason for this Action** dialog is displayed, prompting the user to add a reason for his action.

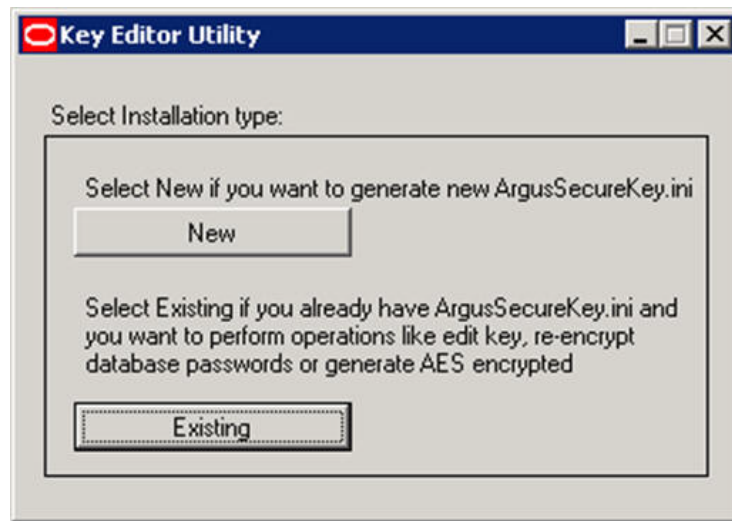
11. The text entered here is visible in the Audit Log in the Argus Safety application.
12. Click **OK**.
13. Check the status box to verify if the operation has been successful.

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.



2. Click **Existing**. The **Key Edit Login** 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 following **Key Editor Options for Existing Installation** screen appears.

Key Editor Options for Existing Installation

DataBase: S0DEV14
Enter DBA User Name: Enter DBA User Password:

Edit Key

User Key:
 Cookie Key:

Key Size: 256

Re-encrypt

DB User Name	DB User Password
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Generate Encrypted

Clear text:
Encrypted String:

Status

6. Enter the DBA User Name and User Password.
7. Click **Validate**.
8. Check the **Generate Encrypted** checkbox.
9. Enter the password in the **Clear text** field.

10. Click **Execute**. The **Reason for this Action** dialog is displayed, prompting the user to add a reason for his action.

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

Third Party Attributions

This Appendix provides information about third party software.

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.

Axway Synchrony Gateway

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

Important: Oracle does not ship the Axway Synchrony Gateway licenses along with these products. You must purchase the Axway Synchrony Gateway license directly from Axway 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.

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.

Captaris RightFax

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

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