Oracle® Argus Safety

Installation Guide

Release 8.1.1

E80573-02

October 2017

Oracle Argus Safety Installation Guide, Release 8.1.1

E80573-02

Contents

3 Install and Configure Argus Safety Web

4 Enable IIS HTTP Compression

5 Install and Start Argus Safety Service

6 Install and Configure Interchange

7 Configure E-mail

Part III Install or Upgrade Argus Safety Database Tier

11 Install Argus Safety Database

12 Upgrade Argus Safety Database

16 Install and Configure Oracle B2B

17 Configure OBIEE or BI Publisher

18 Install Argus Unblinding

19 Install and Configure Argus Integrations

21 Argus Password Management - Cryptography Tool

A Configure BI Publisher Security Model

Preface

You can use this guide to:

- Install Oracle Argus Safety 8.1.1
- Upgrade from Argus Safety 8.x.x release to Oracle Argus Safety 8.1.1

Where to Find More Information

Oracle Help Center

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

My Oracle Support

The latest release notes, patches and white papers are on My Oracle Support (MOS) at `https://support.oracle.com`.

For help with using MOS, see `https://docs.oracle.com/cd/E74665_01/MOSHP/toc.htm`.

Documentation Accessibility

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

Access to Oracle Support

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

Revision History

Version, Date	Description
1.0, September 2017	Original document for the release.

Version, Date	Description
2.0, October 2017	While upgrading Argus Safety Database, in certain cases, the upgrade tool was not populating User Roles correctly. With this revision, the instructions for the upgrade process are updated. See Section 12.2, "Argus Safety Database Upgrade."

Part I

Prepare to Install Argus Safety

Argus Safety is a configurable system and, based on user needs, you (administrators) may install all or some of the components.

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

1

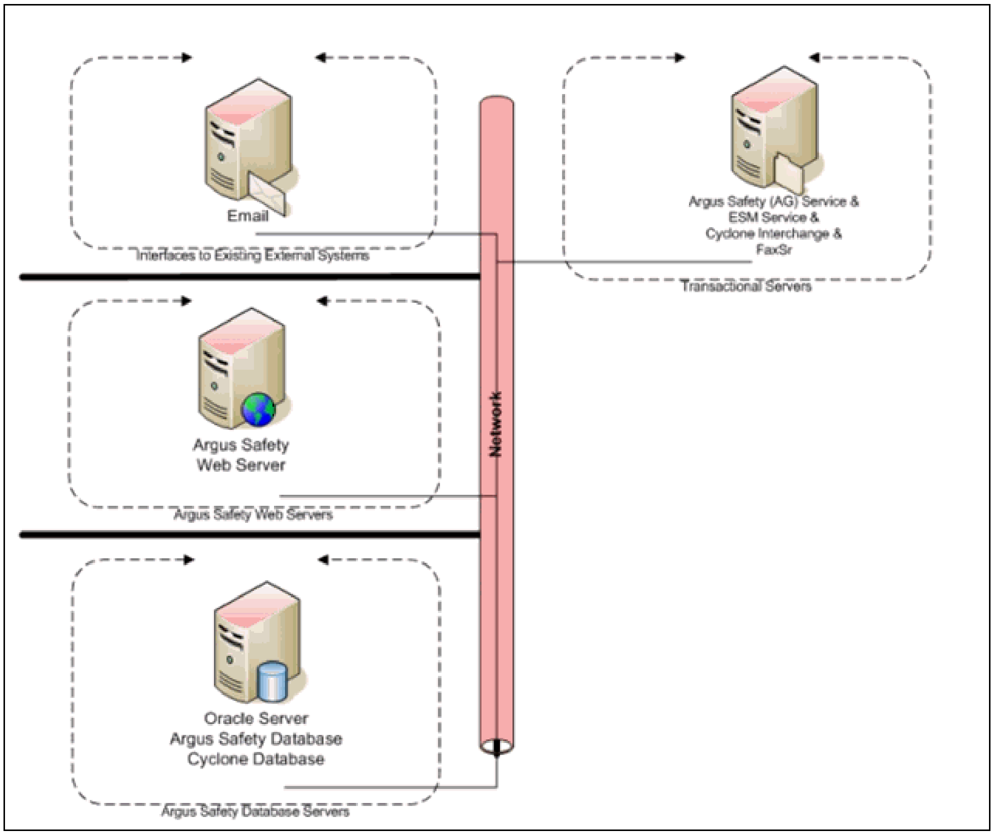
System Requirements

1.1 Argus Safety Recommended Hardware Topology

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

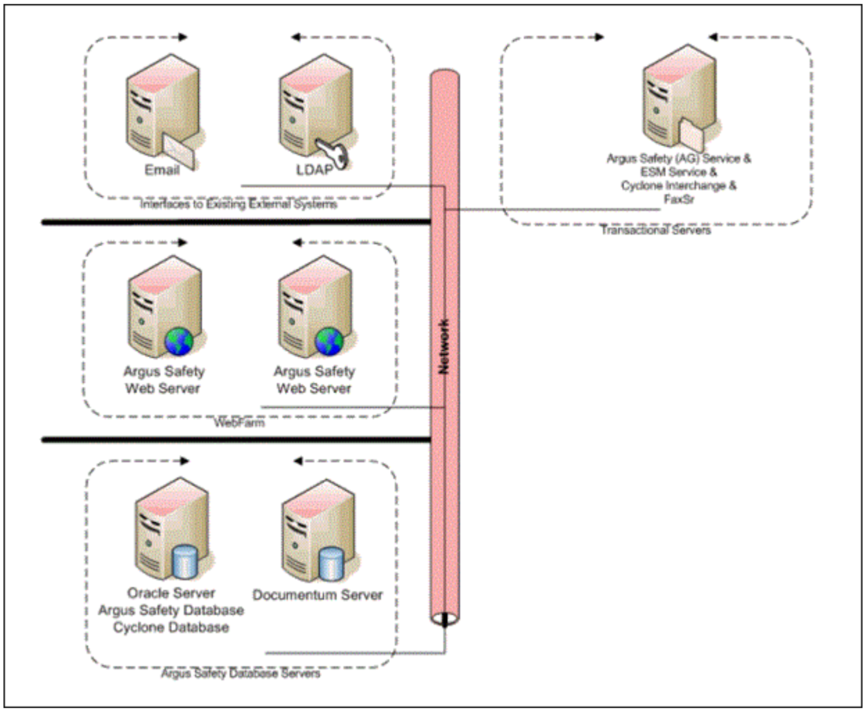
1.1.1 Small Company

(1 to 50 concurrent users, fewer than 200 new cases reported each month)



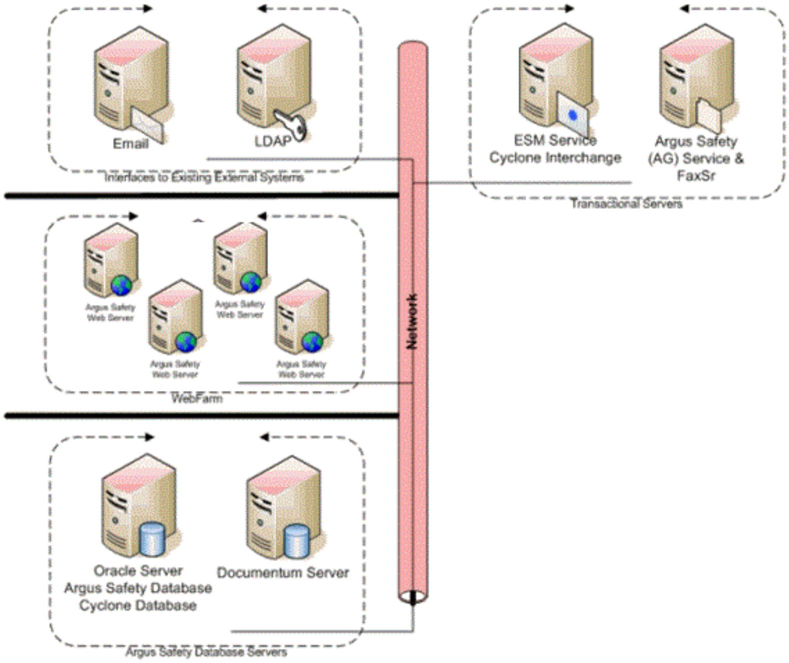
1.1.2 Mid-sized Company

(51 to 100 concurrent users, 300 to 600 new cases reported each month)



1.1.3 Large Company

(Over 100 concurrent users, 1000 to 5000 new cases reported each month)



1.1.4 Hardware Requirements for Argus Safety

- **Argus Safety Database Server**

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

- **Argus Safety Web Server, Transaction Server, and Interchange Server**

Hardware Requirements	Small	Mid-Sized	Large
RAM	4 GB	4 GB	4 GB
CPU or Processor	1 Dual Core CPU x 3 GHz	2 Dual Core CPUs x 3 GHz	2 Dual Core CPUs x 3 GHz
Virtualization	Physical Server or Oracle Virtual Machine (OVM 3.2.10, 64-bit)	Physical Server or Oracle Virtual Machine (OVM 3.2.10, 64-bit)	Physical Server or Oracle Virtual Machine (OVM 3.2.10, 64-bit)
Minimum Resolution	1280 x 1024	1280 x 1024	1280 x 1024

- **Argus Safety Web Client**
  - RAM: 2 GB
  - Pentium IV x 3 GHz
  - Minimum Resolution: 1280 x 1024
- **Argus End of Study Unblinding Tool**
  - RAM: 4 GB
  - 1 Dual Core CPU x 3 GHz
  - Minimum Resolution: 1280 x 1024

1.2 Software Requirements for Argus Safety

1.2.1 Argus Safety Database Server

Components	Software Required
Operating System	As certified by the Oracle Database version.
Oracle Database	Oracle 12.1.0.2 (supports both Standard Edition 2 (SE2) or Enterprise Edition over the CDB/PDB or traditional Non-CDB database format.)
Other Oracle Database Components (Optional)	■ Oracle Advanced Security Transparent Data Encryption (TDE)* ■ Oracle Advanced Security Network Encryption ■ Oracle XML Developer's Kit (XDK) (Required only for PMDA R3 Paper Reports) ■ Tablespace with 500MB free space to create Argus Unblinding Schema in Argus Safety Schema.

*** Note:** Oracle Database TDE feature is part of the Oracle Advanced Security option available for Oracle Database Enterprise Edition 12c (https://docs.oracle.com/database/121/ASOAG, or

http://www.oracle.com/technetwork/database/options/advanced-security/overview/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.

1.2.2 Argus Safety Web Server

Note:

- Generate New Cryptography Key, and place the updated ArgusSecureKey.ini file under the .\Windows folder of the server.
- Report Server is not required for the Argus Safety installation. Existing customers can Convert Argus Safety Report Server to Argus Web Server.

Components	Software Required
Operating System	■ Microsoft Windows 2012 Standard ■ Microsoft Windows 2012 R2 Standard
Oracle Client	■ Oracle 12c Release 1 Client 12.1.0.2 (32-bit only) ■ Oracle Call Interface ■ ODAC ■ MTS ■ ODP.NET

Components	Software Required
Other Software (Required)	■ Microsoft Visual C++ 2005 SP1 Redistributable Package MFC Security Update (32-bit) ■ Microsoft Visual C++ 2012 Runtime ■ Microsoft .NET 3.5 SP1 Framework ■ Documentum DFC 7.2 or 6.7 SP2 (64-bit)
Other Software (Optional)	Documentum DFC 7.2 or 6.7 SP2 (64-bit)
Oracle WebCenter (Deprecated)	Argus Safety no longer supports Oracle WebCenter. While upgrading, if this component appears, uncheck it.

1.2.3 Argus Safety Transaction Server

> **Recommendation:** Do not run Argus Safety Service or ESM Service on the Web Server, because the agproc.exe and argusvr2.exe services might conflict with each other when running together.

Components	Software Required
Operating System	■ Microsoft Windows 2012 Standard ■ Microsoft Windows 2012 R2 Standard
Oracle Client	■ Oracle 12c Release 1 Client 12.1.0.2 (32-bit only) ■ Oracle Call Interface ■ ODAC ■ MTS ■ ODP.NET
Other Software (Required)	■ Java JDK 1.8 ■ Microsoft Visual C++ 2005 SP1 Redistributable Package MFC Security Update (32-bit) ■ Microsoft Visual C++ 2012 Runtime ■ Microsoft .NET 3.5 SP1 Framework
Other Software (Optional)	■ Documentum DFC 7.2 or 6.7 SP2 (64-bit) ■ RightFax 10.6 -Required files only

1.2.4 Argus Interchange Server (Optional)

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

Components	Software Required
Operating System	■ Microsoft Windows 2012 Standard ■ Microsoft Windows 2012 R2 Standard

Components	Software Required
Oracle Client	■ Oracle 12c Release 1 Client 12.1.0.2 (32-bit only) ■ Oracle Call Interface ■ ODAC ■ MTS ■ ODP.NET
Other Software (Required)	■ Microsoft Visual C++ 2005 SP1 Redistributable Package MFC Security Update (32-bit) ■ Microsoft Visual C++ 2012 Runtime ■ Microsoft .NET 3.5 SP1 Framework
Other Software (Optional)	Documentum DFC 7.2 or 6.7 SP2 (64-bit)

1.2.5 Argus Safety Web Client

Components	Software Required
Operating System	■ Microsoft Windows 7 (32 or 64-bit) ■ Microsoft Windows 8.1 (32 or 64-bit) ■ Microsoft Windows 10 (32 or 64-bit)*
Browser	Microsoft Internet Explorer, Version 11.0 (32 or 64-bit) - Compatibility View only
Oracle Client	■ Oracle 12c Release 1 Client 12.1.0.2 (32-bit only) ■ Oracle Call Interface ■ ODAC ■ MTS ■ ODP.NET
Other Software (Required)	Adobe Acrobat Reader DC/XI with East Asian Fonts
Other Software (Optional)	■ Microsoft Office (32 or 64-bit) ■ Oracle BI Publisher 12.2.1

*** To apply Oracle Client Patch required for the Schema Creation Tool**

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

Apply the following workaround after successfully installing this patch:

1. Set oracle_home to your client home location

   For example:

   SET ORACLE_HOME=C:\app\client32\product\12.1.0\client_1

   Go to %oracle_home%\bin\ of the client

   Copy file "oranfsodm12.dll" present in "\p19720843_121020_WINNT\19720843\files\bin\" and paste it under %oracle_home%\bin

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

1.2.6 Argus Unblinding, Schema Creation Tool and Interchange Mapping Tool

Components	Software Required
Operating System	- Microsoft Windows 2012 Standard - Microsoft Windows 2012 R2 Standard
Operating System—Windows Client Machine	- Microsoft Windows 7 (32 or 64-bit) - Microsoft Windows 8.1 (32 or 64-bit) - Microsoft Windows 10 (32 or 64-bit)* * To apply Oracle Client Patch required for the Schema Creation Tool, click the link.
Browser	Microsoft Internet Explorer, Version 11.0 (32 or 64-bit) - Compatibility View only
Oracle Client	- Oracle 12c Release 1 Client 12.1.0.2 (32-bit only) - Oracle Call Interface - ODAC - MTS - ODP.NET
Other Software (Required)	- Microsoft Visual C++ 2005 SP1 Redistributable Package MFC Security Update (32-bit) - Microsoft Visual C++ 2012 Runtime - Microsoft Visual Basic Power Packs 10.0—Required for Interchange Mapping Tool - Microsoft .NET 3.5 SP1 Framework - Adobe Acrobat Reader DC/XI

1.2.7 Argus Safety OBIEE or BI Publisher Server

The OBIEE or BI Publisher Server installation is optional, and required only if Argus Safety Flexible Aggregate Reporting (FAR) is enabled or Japanese PMDA R3 Paper Forms need to be generated.

Argus 8.1.1 supports OBIEE or BI Publisher 12.2.1.

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

1.2.8 Generic—Other Supported Features (Optional)

If you are using...	You must install...
Single Sign-On	Oracle Identity Manager (OIM) 11.1.2.2 - WebGate 10.1.4.3 (32-bit only) integration with Oracle Identity Manager.
Built-in Reports to run the PMDA E2B R3 Paper Reports or Flexible Aggregate Reporting	- Oracle Business Intelligence Enterprise Edition (OBIEE) 12.2.1.0 with Patch 21918899 (fonts only) - Oracle BI Publisher 12.2.1.0 with Patch 21918899 (fonts only) (for Argus SE only) - BI Publisher Desktop tool on the client machine to customize the reports.
LDAP for authentication support	LDAP/LDAPS Protocol Version 3.0

If you are using...	You must install...
E-mail capabilities within Argus	SMTP Protocol. The following Argus Safety components support SMTPS: ■ Argus Safety—Supports SMTPS and TLS 1.2 (Forced). Both Implicit and Explicit modes. ■ AxWay 5.12 SP8+—Supports SMTPS and TLS 1.2. Implicit mode only. ■ OBIEE/BIP—Supports SMTPS and TLS 1.2, and must have JDK 1.8 for SMTPS. Both Implicit and Explicit modes. Note that B2B does not supports SMTPS.
Documentum for Storage	Documentum DFC, Version 6.7 SP2 (64-bit), or 7.2
Faxing capabilities for Expedited Reports	RightFax 10.5 or 10.6
E2B Reporting for exchange	■ Oracle B2B - 12.2.1—Certified with both AS1 and AS2 protocols for E2B exchanges between regulatory authorities and pharmaceutical companies. ■ Axway Interchange 5.12 SP8 (64-bit)

2 Install Oracle Database

Install Oracle Database on the Database Server.

2.1 Get the Oracle Database 12.1.0.2 Installation Guide

Open or download the installation guide for your operating system:

- http://docs.oracle.com/database/121/nav/portal_11.htm

2.2 Download and Extract the Oracle Database 12.1.0.2 Software

Refer to the *Oracle Database Installation Guide* for instructions.

As a part of the Oracle Database, Argus Safety requires:

- Oracle Database Enterprise or Standard Edition
- Oracle Database Client
- Oracle Identity Manager (OIM) with WebGate

2.3 Install Oracle Database 12.1.0.2

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

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

For an explanation of which options require an additional license, see the Database Licensing Information User Manual at

http://docs.oracle.com/database/121/DBLIC/toc.htm

2.3.1 Database Software Options

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

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

2.3.2 Database Configuration Options

- Oracle Automatic Storage Management (Recommended)—To provide an alternative to conventional volume managers, file systems, and raw devices.
- Character Set: Select AL32UTF8.
- Automatic Memory Management (Recommended)—To manage instance memory to allow the Oracle Database instance to automatically manage and tune it for you.
- Oracle Text (Required)—Included automatically if you install the database during server installation.
- Oracle Database Examples (Required)
- Oracle JVM (Required)
- Oracle XML DB (Required)—Included automatically if you use the Oracle Database Configuration Assistant to create the database. http://docs.oracle.com/database/121/ADXDB/appaman.htm#ADXDB2700

2.4 Set Up Database Parameters

2.4.1 Argus Safety Database Instance Parameters (Recommended)

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

#	Database Parameters	Small (under 30,000 cases reported per month)	Mid-Sized (30,000 to 200,000 cases reported per month)	Large (200,000 to 1,000,000 cases reported per month)	Very Large (over 1,000,000 cases reported per month)
1	MEMORY_ TARGET	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

#	Database Parameters	Small (under 30,000 cases reported per month)	Mid-Sized (30,000 to 200,000 cases reported per month)	Large (200,000 to 1,000,000 cases reported per month)	Very Large (over 1,000,000 cases reported per month)
10	DB_BLOCK_ SIZE (bytes)	8192	8192	8192	8192
11	PGA_ AGGREGATE_ TARGET	500 MB	500 MB	1 GB	2 GB

2.4.2 Additional Database Setup Information

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

2.5 GMT Offset Calculation

The system uses the time zone of the DB server to do GMT calculations. This time zone is initially loaded during the Argus database installation.

To set up the time zone:

1. Go to Argus Console > System Configuration > Database.
2. From the **Database Server OS Timezone** drop-down list, select a time zone.
3. Alternatively, update the DATABASE_TIMEZONE key in CMN_PROFILE table.

Make sure:

- Argus is using function gss_util.gmt_offset to derive the GMT OFFSET which impacts the calculation of GMT date and time.
- 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.

Part II

Set Up Argus Safety Middle and Client Tiers

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

Prerequisites:

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

3

Install and Configure Argus Safety Web

Before installing the Argus Safety Web:

- Make sure that the regional settings are US settings.
- Install East Asian languages.

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

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

This is usually accomplished by running aspnet_regiis.exe -i from the.NET V2.0.50727 folder.

Manually modify Machine.config

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

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

```
</system.serviceModel>
<system.transactions>
        <machineSettings maxTimeout="01:00:00" />
     </system.transactions>
</configuration>
```

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

3.1 Install Argus Safety Web

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 click **setup.exe**.
4. In the Argus Safety Setup screen, click **Next >**.
5. Enter the User Name and Company Name, and click **Next >**.
6. In the Default Directory screen, to select the default installation directory where the Argus Safety Solution Components will be installed, click **Browse**.

Note: If Terminal Services are enabled, to install Argus Safety Solution components:

1. Go to Control Panel > Add or Remove Programs > Add New Program.
2. Open the setup.exe in your local directory.

7. To display the Argus Safety Components list, click **Next**, and select the default installation directory.
8. From the component list, select **Argus Global Application**.
   - For the multi-tenancy feature, in the Installer Modules selection screen, select the **Argus Global Application for Argus Safety Web** option.
   - The global modules are installed on the same Web Server as Argus Safety Web and are accessible as a separate URL from the same Web Server.
   - After installing the IIS Global Homepage, make sure that you can access the following URL:

     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.
9. Select the modules to install, and click **Next**.

   The Argus Safety Solution Components Report Directory appears.
10. Select the directory where temporary reports will be stored.

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

Recommendation: Install the Cryptography tool on the Web Server.

11. To configure a database, click **Yes** when prompted.
12. Enter a database name, and click **Next >**.

    This database name will appear on the Argus Login page.
13. Enter the database SID, and click **Next >**.
14. To add an additional database to the Argus Login page, click **Yes** when prompted to configure database settings.
15. Enter the Port for the Argus Safety website (default is 8083), and click **Next >**.

    The website and its related components are installed, and the progress of the installation appears.
16. In the Setup Completed screen, click **Finish**.
17. Click **OK** to reboot the system.
18. Set up the Argus Cryptography key by following the instructions in the Section 21.1.3, "Argus Safety 8.1.1 Application Servers".

3.2 Configure the IIS Manager for Windows 2012

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

1. Select Start > Administrative Tools > Internet Information Services (IIS) Manager.
2. Expand the Connection Panel, and open **Sites**.
3. Select Argus Safety Web.
4. On the right panel, click **Basic Settings**.
5. Click **Connect as…**
6. Click **Specific User**, and click **Set**.
7. Enter Domain user name and password, and click **OK**.
8. Click **OK**.
9. To verify the user credential is valid for the connection, click **Test Settings**.

3.3 Connect to a Domain Account on Windows 2012

If multiple Web Servers are configured for Argus Safety in a load-balanced environment, the reports folder must be on a shared path on the network.

1. From the left panel, open Argus Safety Web folder.
2. From the left panel, click **PDFReports**.
3. From the right panel, click **Basic Settings**.
4. Change the Physical Path to a shared folder in the Domain.
5. Click on **Connect as…** and select **Specific User.**
6. Enter the Domain User ID and Password, and click **OK**.
7. To verify the user authentication for the connection, click **Test Settings**.
8. Repeat the above-mentioned steps for:
    - UploadedLetters
    - Integrations
    - GHP
    - ArgusNet
    - Argus Console
    - Scanned_Images

3.4 Enable SSL Support for Windows 2012

1. Obtain and install the SSL certificate.
2. Click Argus Safety Web > Bindings.
3. Click on **Add**, and change Type to HTTPS.
4. Select SSL Certificate, and click **OK**.

3.5 Configure Load Balancer in Argus Web

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

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

3.5.1 Set Up Argus Web Load Balancer IP Address

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

1. Login to Argus Console.
2. From System Configuration Menu, select System Management.
3. Click the Network Settings Folder.
4. Enter the Load Balancer IP Address, and click **Save**.

3.5.2 Set Up Load Balanced Folders

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

- pdfreports
- uploadedletters
- scannedimages

3.5.3 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.
>
> Besides, you must also make sure that the client machine has access to that share.

3.6 Secure Sensitive Configuration and Operational Data

To make sure that only the IIS user with Administrator rights can access the following files and folders, set the minimum permission as **Full Control** for the user under which IIS is running.

- Windows Directory File—Argus.ini
- Shared Folders:

- MessageCache
- PDFReports
- Scanned_Images
- UploadedLetters

3.7 Configure Identity in the IIS Application Pools

1. Select **Start > Administrative Tools > Internet Information Services (IIS) Manager.**
2. Select **Application Pools**.
3. Right-click the **Argus Console Pool**, and select **Advanced** settings.
4. In the identity field, enter user ID and password.
5. Reset IIS.

   > **Note:** Make sure to reset IIS after modifying the areas listed in the Reset IIS section.

6. Repeat the same configuration for **Argus NET Pool**.

   > **Note:** This configuration will prevent any error when filtering data on the Worklist Portal screen.

3.8 Reset IIS

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

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

4 Enable IIS HTTP Compression

Enable IIS HTTP Compression on a Windows 2012 Server when the pipeline between the Web Server and the IIS Client have low bandwidth or have high amounts of data usage.

4.1 IIS Web Page Compression

4.1.1 HTTP Compression

By default, HTTP compression is disabled in Windows 2012 but can be enabled as necessary. Enable the compression, when:

- 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).

4.1.2 Known Effects of Enabling Compression

Enabling IIS Compression increases CPU usage on the Web Server.

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, and HTM are compressed only once, and then stored in a cache on the Web Server for later requests.

The Web Servers should be monitored frequently to prevent occurrence of a CPU bottleneck, which would decrease performance rather than increasing it.

4.1.3 Enable HTTP Compression

1. Go to Control Panel > Administrator Tools > Internet Information Services (IIS) manager.
2. Browse to the **Argus Safety Web** website.
3. In the Features View, double-click **Compression**.
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.

4.2 IIS Caching Settings

4.2.1 IIS Caching

IIS Caching is supported in Windows 2012.

To prevent the web server from having to re-serve certain files to the IE Client when the file has not changed, use IIS Caching. For example, files like Images do not change on a day-to-day basis, and 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.

To make sure that IIS Caching functions properly:

- Set up the IIS
- Set up the local IE client settings correctly

4.2.2 Known Effects of Enabling Caching

Currently, there are no known effects of enabling caching on the Web Server.

However, enabling cache should only be used on files and folders where the files are not dynamic or do not change daily. Certain files, such as .ASP and .ASPX files, should never be cached.

4.2.3 Enable Caching

1. Go to Control Panel > Administrator Tools > Internet Information Services (IIS) manager.
2. Browse to the **Argus Safety Web** website.
3. Double-click the **HTTP Response Headers**.

   Make sure that **Cache Control** header with value of **no-cache** exists.
4. Click **Set Common Headers**.

   Make sure that **Expire Web Content** is checked, and the option **Immediately** is selected.
5. Apply the changes.
6. Click the **PDFReports** folder.
7. Double-click the **HTTP Response Headers**.

   Make sure that **Cache Control** header does not exist.
8. Click **Set Common Headers**.

   Make sure that **Expire Web Content** is unchecked.
9. Repeat the same steps for **UploadedLetters** (Steps 6-10).

10. Make sure that on the **Set Common Headers**, the **After** option is checked, 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

4.3 Local Internet Explorer (IE) Client Caching Settings

4.3.1 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.

4.3.2 IE Client Caching—Tab Options

Option	Description
Every Time I visit the Web Page	No file is cached. 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.
Every Time I Start Internet Explorer	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	Allows 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 multiple times, 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 option should be used for best performance.
Never	IE will always cache every file which can cause problem with sites that have dynamic data, and should not be used. Besides, if a file has been updated on the server due to an upgrade, the new file will not be sent to the client.

4.3.3 Enable IE Caching

1. In Internet Explorer, select **Tools > Internet Options**.
2. Select the General Tab, locate the Browsing history section, and click **Settings**.
3. In the Temporary Internet Files and History Settings dialog box, select **Automatically**, and click **OK**.
4. Close the Internet Explorer browser, and restart it to begin caching.

5

Install and Start Argus Safety Service

5.1 Install Argus Safety Service

1. Install East Asian languages.
2. Log on as the Administrator on the system where Argus Safety is being installed.
3. Copy the installation package to the local directory of the target machine.
4. Open the Argus Safety folder, and click **setup.exe**.
5. In the Argus Safety Setup screen, click **Next >**.
6. In the Argus Safety Solutions Components Installation Wizard, click **Next >**.
7. In the Customer Information dialog box, enter the User Name and Company Name, and click Next >.
8. In the Default Directory screen, to select the default installation directory where the Argus Safety Solution Components will be installed, click **Browse**.
9. To open the Argus Safety Components list, click **Next**.

> **Note:** If Terminal Services are enabled, to install Argus Safety Solution components:
>
> 1. Go to Control Panel > Add or Remove Programs > Add New Program.
> 2. Open the setup.exe in your local directory.

10. From the Argus Safety Components list, select **Argus Safety Service**, and click **Next >**.
11. In the Argus Safety Setup dialog box, click **Browse**, select the folder to store the temporary reports in, and click **OK**.
12. Click **Next >**.

    Argus Safety Service is installed and the progress of the installation appears.
13. In the Setup Completed dialog box, click **Finish**.
14. In the Argus Safety Setup dialog box, click **OK** to reboot the system.
15. See Chapter 10, "Other Tasks" for information about tasks that must be completed after Argus Safety service has been installed.

16. Follow the instructions in Section 10.6, "Set Up easyPDF".
17. To set up the Argus Cryptography Key, refer to Section 21.1.3, "Argus Safety 8.1.1 Application Servers".
18. To configure Argus Safety Service user passwords, refer to Section 21.2.4, "Generate Encrypted String".

5.2 Start Argus Safety Service

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

To start Argus Safety Service:

1. Select Start > Control Panel > Administrative Tools.
2. Double-click the Component Services shortcut.
3. In the list of services, locate Argus Safety Service, and select **Properties**.
4. In the Argus Safety Service Properties > General tab, from the **Startup type** drop-down list, select **Automatic**.
5. Click the **Log On** tab, enter the parameters, and click **OK**.

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

6. In Services dialog box, click **OK**.
7. Click **Start**.
8. Click **OK**.
9. View the log file from <target directory>\Oracle\Log.

5.3 Set Up RightFax

> **Note:** To communicate with RightFax Server, configure Argus Safety Service, where:
>
> - <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 the following files on the Right Fax Server:
   - RFLanguage.dll (from the English Folder)
   - rfcomapi.dll (register)
   - RFI32RPC.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:

   - **Rfcomapi.dll**

     a. From the command prompt, browse to the <ARGUSSAFETY>\Argus Safety folder.

     b. Enter *%WINDIR%\System32\Regsvr32 rfcomapi.dll*

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

     %WINDIR%\SysWOW64\Regsvr32 rfcomapi.dll

     ---

     c. In the Registration dialog box, click **OK**.

   - **RightFax.dll**

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

     a. From the command prompt, browse to the <ARGUSSAFETY>\Argus Safety folder.

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

     c. In the Registration dialog box, click **OK**.

6

Install and Configure Interchange

To configure Interchange Services through Interchange Mapping user interface, both must be installed on the same system.

6.1 Prerequisites

1. Install Microsoft Visual Basic Power Packs 10.0
2. Install East Asian languages
3. Obtain a domain account with local administrator privileges.
4. Uninstall the existing Interchange Services.
5. 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.

6.2 Install Interchange Service

1. To start the Argus Safety Setup installation wizard, double-click **setup.exe**.
2. Click **Next >**.

   The Customer Information dialog box appears.
3. Enter the parameters, and click **Next >**.

   The Default Directory dialog box appears.
4. Click **Browse** to default installation directory for the Argus Safety Solution components.
5. From the list of available features, select **Interchange**, and click **Next**.
6. Click **Yes** to configure a database for Argus Interchange.
7. Enter the database name as you want it to appear in Argus Interchange, and click **Next >**.
8. Enter the database SID, and click **Next >**.
9. To add an additional database to the Argus Interchange, click **Yes**.
10. Click **OK** to reboot.
11. To set up the Argus Cryptography Key, refer to Section 21.1.3, "Argus Safety 8.1.1 Application Servers".

6.3 Configure Interchange Service

1. Select Start > Control Panel > Administrative Tools.
2. Open Component Services.
3. In the services list, locate Argus Interchange Service, from the drop-down menu, right-click and select **Properties**.
4. In the Electronic Submission Manager Properties dialog box, from the **Startup type** drop-down list, select **Automatic**, and click **Log On** tab
5. In the Log On tab:
   a. In the Logon as Option, select **This Account**.
   b. From the Company domain list, select the user account.

      This account must have local admin privileges and access to all site printers.
   c. Enter and confirm password.
   d. Click **Enable**.
   e. Click **OK**.

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

6.3.1 Transmit E2B Attachments

You must Set Up easyPDF before you can transmit E2B attachments.

6.4 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.

6.5 Configure Interchange Service.INI File

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

1. Open ESM Mapping.
2. Select Administrator > Setup INI File from the menu.
3. In the Service INI File Setup dialog box, enter the following parameters, and click **OK**.

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

7 Configure E-mail

Argus Safety Service and Interchange Service use SMTP as an e-mail method if it has been enabled and configured in Argus using Argus Console > System Configuration > SMTP Configuration. Case Letters are also sent using SMTP.

7.1 Configure SMTP

Use the SMTP Configuration utility to send e-mails through the SMTP protocol from Argus Safety Service to the e-mail server.

1. Navigate to Argus Safety Console > System Configuration > SMTP configuration.
2. When the SMTP Configuration dialog box appears, enter the following parameters:
   - SMTP server IP address or name
   - Port number
   - User name
3. Check **Enable SMTP** checkbox.
4. Click **OK**.

Table 7–1 SMTP Configuration dialog box—Field Description

Field Name	Description
Enable SMTP?	Check this checkbox to make sure that the AG Service uses SMTP to send e-mail messages.
Server IP or Name	Enter the SMTP server IP address or name.
Port	Enter the port number. Default value: 25.
Authentication	Select the authentication type. ■ No Authentication—Disables the Username and Password ■ Basic Authentication—Enter the Username and Password (Default) ■ NTLM Authentication—Disables the Username and Password because the authentication of the OS user logged into the system is automatically passed.
Custom SMTP Header	Check this checkbox 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.

Table 7–1 (Cont.) SMTP Configuration dialog box—Field Description

Field Name	Description
Custom SMTP Header Textbox	Enter the customer Header to insert into the SMTP Header.

7.2 Functions Affected by SMTP

7.2.1 Bulk Report Transmit E-mail

1. Navigate to Argus Console > Code Lists > Argus.
2. Select **Reporting Destination**.
3. Enter the e-mail address in the E-mail Address text box under Agency Information.

   The Bulk Report Transmit e-mail is sent to this e-mail address.

7.2.2 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.

7.2.3 Fax E-mail

The Failure E-mail field or the Notify E-mail field in the Argus Safety Service Process screen indicates the e-mail address of the person receiving the e-mail message.

1. On the system where Argus Safety Service is installed, select Start > All Programs > Oracle > Argus Safety Service Configuration.

   The Argus Safety Service dialog box appears.
2. Double-click **E-mail process**.
3. Enter an e-mail address for Failure E-mail or Notify E-mail.

7.2.4 Fax Status E-mail

1. On the system where Argus Safety Service is installed, select Start > All Programs > Oracle > Argus Safety Service Configuration.

   The Argus Safety Service dialog box appears.
2. Double-click **E-mail Status process**.
3. Enter an e-mail address for Failure E-mail or Notify E-mail.

7.2.5 Priority E-mail

From the Argus Console, navigate to Access Management > Argus > Groups.

The E-mail field on the Group Information dialog box contains the e-mail address of the person receiving the e-mail message

7.2.6 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.

- Sender e-mail address represents the normal AG user.
- Receiver e-mail address is the owner of the Dossier template.

  To configure the owner of the Dossier template, navigate to

  Argus Web > Reports > ICH PSUR Reports > Configuration Screen > Template tab.

7.2.7 E-mail Sent by Interchange Service

1. Log in to ESM Mapping.
2. Select Administrator > Setup INI File.
3. For e-mail sent by Interchange Service, the IT E-mail, Business E-mail, and User E-mail fields in the Service INI File Setup window contains the e-mail addresses of those receiving the e-mail message.

   Sender E-mail is the e-mail address that Argus Interchange Service displays as the 'From' address in the e-mails that it sends.

> **Note:** Interchange Service sends e-mail messages to IT, Business, or User e-mail addresses depending on the type of alert/error/warning/information the system encounters.

8

Set Up the Client Browser

8.1 Prerequisites

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

8.2 Install Files Required to View Japanese Text (For Japanese installation only)

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 to view Japanese text correctly.

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

8.3 Configure Internet Explorer

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

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

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

If password encryption is required between Internet Explorer Client and the Web Server, HTTPS must be utilized. Refer to the Section 3.4, "Enable SSL Support for Windows 2012".

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 box. It is recommended to close all other non-Argus Safety Sessions if this problem occurs on an end user machine.

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

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

8.4 Add the Argus Site as a Local Intranet Site

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

   The Internet Options dialog box appears.

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

   The Local intranet dialog box appears.

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

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

5. Click **Add**, and click **Close**.
6. Click **Custom level...**

   The Security Settings dialog box appears.

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

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

   For more information on how to Add Argus Site to the Enterprise Mode.

8.5 Add Argus Site to the Enterprise Mode

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

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

8.6 Set Up Compatibility View with Internet Explorer

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

8.7 Increase the Internet Explorer Timeout Setting to Run Reports

For client machine, increase IE Timeout Setting (from default value of 4 (hours)) to run Periodic or System 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.

9

Post-installation Checks

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

9.1 Post-Installation Tasks

9.1.1 General Checklist

Verify That:

- Oracle 12c is installed.
- the correct modules are installed as follows:
  1. Go to Add/Remove Programs, and select **Argus Safety Web**.
  2. Click **Modify**, and click **Next**.
  3. Verify that the applications that you have installed are checked.
- the Argus.XML file has the same data across all the Web Servers.
- a single domain user account <Domain User> is running Argus Web application on all web servers.
- the login page appears when the server name is entered in your browser.
- you can log in successfully.
- system performance satisfies the requirement

9.1.2 Configure Argus Safety Windows Service to run as a Domain User

1. Select Control Panel > Administrative Tools > Services.
2. Double-click Argus Safety Windows Service.

   The Argus Safety Windows Service Properties (Local Computer) dialog box appears.
3. Click the **Log On** tab.
4. Click **This Account**.
5. Enter the credentials.
6. Click **OK**.

7. Right-click Argus Safety Windows Service, and select **Restart**.

9.1.3 Configure Worklist Intake

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

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

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

```
<InterfaceSchemas>
<add InputXSD="C:\Program Files (x86)\Oracle\Argus\Argus
Safety\Integrations\XSD\v1.0\Base.xsd" />
<add InputXSD="C:\Program Files (x86)\Oracle\Argus\Argus
Safety\Integrations\XSD\v1.0\DataOperation.xsd" />
<add InputXSD="C:\Program Files (x86)\Oracle\Argus\Argus
Safety\Integrations\XSD\v1.0\Dictionary.xsd" />
<add InputXSD="C:\Program Files (x86)\Oracle\Argus\Argus
Safety\Integrations\XSD\v1.0\Case_Intake.xsd" OutputXSLT="C:\Program
Files(x86)\Oracle\Argus\Argus Safety\Integrations\XSLT\v1.0\CaseIntake_
Transform.xsl"/>
</InterfaceSchemas>
```

6. Open the following files:

9.1.3.1 RelsysWindowsService.exe.config

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

Attribute	Description
DBName (Mandatory)	TNS of the Database to which the RelsysWindowsService should connect to. Example: DBName="GOLDDEMO"

Attribute	Description
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, refer to Section 21.2.4, "Generate Encrypted String".
GeneralEmailTo	The e-mail address to which the e-mails will be sent by the Intake Service, using the General Email feature of Argus. Example: GeneralEmailTo ="recepient@oracle.net"
GeneralEmailFrom	The email address from which the e-mails will be sent by the Intake Service, using the General Email feature of Argus. Example: GeneralEmailFrom ="admin@oracle.net"
GeneralEmailCc	This email address will be added to the Cc line when e-mails are sent by the Intake Service, using the General E-mail feature of Argus. Example: GeneralEmailCc ="recepient@oracle.net"
GeneralEmailBcc	The email address will be added to the Bcc line when e-mails are sent by the Intake Service, using the General E-mail feature of Argus. Example: GeneralEmailBcc ="recepient@oracle.net"

9.1.3.2 Service.config

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

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

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

9.1.3.3 Intake.config

The following configuration changes are optional:

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

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

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

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

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

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

AlternatePath: Alternate way of accessing the same folder path.

9.1.4 IIS Checklist

Verify that:

- the properties in the IIS PDFReports virtual directory are correct.
- for Load Balanced Environments only
  - the path under the Virtual Directory is set to Share Path.
  - the correct <Domain User> is in the Connect As option.
- the Read and Write options are checked.
- there is no Red X on the PDFReports folder.
- you can right-click PDFReports, and select Browse.
- you can create a temp file and delete it after browsing.
- for PDFReports:
  - Enable Content Expiration in HTTP Headers is unchecked
  - 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 UploadedLetters: Enable Content Expiration under HTTP Headers is unchecked.
  - Enable Content Expiration under HTTP Headers is unchecked
  - Custom HTTP Headers under HTTP Headers does not have a value of Cache-Control
- the values on the Directory Security tab under Argus Safety Website Properties are correct.

  Click Edit, and verify that:

  - the correct <Domain User> and password are used for Anonymous Access.

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

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

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

Configure MIME Types on IIS 7.0:

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

9.1.5 .INI File Checklist

Verify that:

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

9.1.6 Service Checklist

Go to Control Panel > Administrator Tools > Services, and verify that Argus Report Services is enabled.

9.2 Verify Web Server Installation and IIS Configurations

9.2.1 Verify IIS 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 **HTTP Response Headers**.

   Make sure that there is no value **Cache Control** header.
5. Click **Set Common Headers**.

   Make sure that **Expire Web Content** is unchecked.
6. Verify the same settings for the **UploadedLetters** folder.
7. Click **Argus Safety Web**.
8. Under Actions, click **Basic Settings**.

   Make sure that the website is configured to run under a domain account.

9.3 Verify Files installed on Middle Tier Servers

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

1. Log in to the server as an Admin user.
2. Select Start > Control Panel.

3. Click **Programs and Features**.
4. Hover Argus Safety, and right-click.
5. From the drop-down menu, click **Change**.

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

9.4 Verify Documentum Installation

1. Log in to Console, and verify Documentum is configured in Argus Safety.

   Refer to the *Oracle Argus Safety Administrator Guide* to set up Documentum.
2. Log in to SQL Session on the database <Database>.
3. To verify that the value to enable the Periodic Report Documentum interface is set to 1, execute:

   ```
   select * from cmn_profile where key ='ENABLE_DOCUMENTUM_PERIODIC'
   ```
4. To verify that the correct user has been configured in Documentum, execute:

   ```
   select * from cmn_profile where key = 'DOCUMENTUM_LOGIN'
   ```

   This value is case sensitive and must match the Documentum login.
5. To verify that the password value will be encrypted, execute:

   ```
   select * from cmn_profile where key = 'DOCUMENTUM_PASSWORD'
   ```

   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.
6. To verify that the following information is correct, execute:

   ```
   select *  from DOCUMENTUM_PUSH_INFO
   ```

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

   - TYPE_NAME (<DocumentumType>) is the correct name as specified in Documentum. (This is the table name in Documentum.)
   - All the Attribute names specified here exist in the Documentum table.
   - The SQL_CONTENT SQLs are correct and run without any error when the parameters are filled in. (No Syntax errors.)
   - The ATTRIBUTE_TYPE matches with the one defined in the Documentum table.
7. Log in to the following servers to verify that the Documentum DFC Runtime Environment is installed on the server. This can be verified through Add/Remove Programs.

   - AG Service machine - <ServerName>

- Argus Web Server - <ServerName>
- Interchange Service Server - <ServerName>

9.4.1 Integrate Documentum Completely

1. Open Documentum.
2. Create the following types in Documentum:
   - Attachments
   - 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 Safety.
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 Safety as corresponding Attributes of the Types through Documentum Administrator.

> **Note:** IUSR_<Machine> accounts must be given full access to the shared folder in the DFC installation path where DFC.dll resides.

9.4.2 Run Documentum on Argus Safety

Documentum can be implemented on an Argus Safety system in the following ways:

- Documentum can be successfully run on an Argus Safety 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:
  1. Go to the DFC.config file on the Web Server and change its *dfc.registry.mode* setting.

     The default setting is: *dfc.registry.mode=windows*
  2. Change this setting to: *dfc.registry.mode=file*

     This change ensures that Documentum can run even with minimal security configuration.

10 Other Tasks

10.1 Convert Argus Safety Report Server to Argus Web Server

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

10.2 Configure Argus.xml File

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

<Argus Installation Path>/ArgusWeb/ASP

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

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

10.3 Configure Argus.ini File

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

To configure Argus.ini:

1. Select Start > Run.
2. In the Open field, enter **argus.ini,** and click **OK**.
3. Set the entries in the file as described in the Section 10.3.1, "Argus.ini—Parameters".
4. Save the file.
5. Restart the Internet Information Services (IIS) on the server to reflect the changes.

10.3.1 Argus.ini—Parameters

With some exceptions, the parameters listed in Table 13-2 are used by Argus Web as well as Argus Safety Service (AG Service or Transaction Server).

Parameters specific to the Web Server are:

- MessageCachePath
- Upload
- Template
- ArgusInstallPath
- Timeout
- DB Connection
- Pooling parameters.

Parameters specific to the Transaction (AG) Server are:

- PrintRunTime

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

Section	Parameter	Sample Value	Description
Workstation	Cache*	c:\ArgusReports\PDFReports\	Path for PDF Reports (Expedited/Periodic/Screen Prints etc.). In case of multiple Web Servers, this is a shared path on the network.
Workstation	MessageCachePath*	c:\ArgusReports\MessageCache\	Shared path to save the system level cache such as data for LM tables, CMN Fields, etc. In case of multiple Web Servers, this is a shared path on the network. For use with Web Server.
Workstation	Upload*	c:\ArgusReports\UploadedLetters\	Shared path for uploaded letters. In case of multiple Web Servers, this is a shared path on the network. For use with Web Server.

Section	Parameter	Sample Value	Description
Workstation	Template	C:\Program Files\Oracle\E2BViewer \Templates\	Location that stores the template and report files used to display CIOMS and MedWatch views. For use with Web Server.
Workstation	AcrobatReaderPath	C:\Program Files\Adobe\Acrobat 7.0\Acrobat\Acrobat.exe	Path to the Acrobat Reader exe file.
Workstation	HELP	C:\App\Oracle\Documentation\	Base folder where all the files related to various modules of Argus are placed.
Workstation	ArgusInstallPath	C:\Program Files\Oracle\ArgusWeb\ASP\	Path of the location where the ASP files are placed. For use with Web Server.
Workstation	SCANNED_IMAGES	C:\Temp\Scanned_Images	Location of files that are used by the "New Case from Image" functionality.
PDFReports	TempFileDeleteInterval	1	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.
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.
Argus Server	SQLTimes	1	Enables the Argus Web application to start creating log files for all the SQLs that are fired. These log files are created in C:\Temp folder and can be used for debugging.
Argus Server	Pool_Initial_Size	3	Refers to the DB Connection Pool Initial Size. For use with Web Server.
Argus Server	Pool_Maximum_Size	120	Refers to the DB Connection Pool Maximum Size. For use with Web Server.

Section	Parameter	Sample Value	Description
Argus Server	Connection_Time_Out	120	Refers to the time out time in seconds. The connection times out if it is idle for the given time. For use with Web Server.
Argus Server	Connection_Wait_Time	3	Refers to the connection wait time in seconds. An exception occurs if the system cannot obtain a DB connection in the given time. For use with Web Server.
Argus Server	PeriodicRptMaxRunTime	60000	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).

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

10.4 Install SSO on Oracle Access Manager 11g

Prerequisites:

- 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 Safety.

To install SSO on the OAM:

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

   The Create OAM 10g Webgate screen appears.

2. Enter the following parameters, and click **Apply**.

   a. Name— Name of the WebGate

   b. Access Client Password—Password of the WebGate

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

3. Enter the following parameters, and click **Apply**.

   a. Primary Cookie Domain—FQDN of the machine where you will install WebGate, prefixed by a period.

      For example, .idc.<example.com>. Note the . (dot) before the FQDN.

   b. Preferred Host—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.

   a. Double-click **Resources**.

   b. To create the resource type with the correct host identifier, click **Create** icon.

      (The Create icon is displayed in the Search Results section, with the + symbol in red).

5. Expand the **Authentication Policies** under the newly created WebGate, and double-click the **Protected Resource Policy**.

   a. Select the **Responses** tab, and click the **+** button to add the **Name**, **Type**, and **Value** for the responses.

   b. Select the **Constraints** tab and click the **+** button to add the **Name**, **Type**, and **Class** for the constraints.

      The possible values for Constraint Type to access Argus Safety Services where WebGate is installed are:

      - Allow

      - Deny

Note: If no constraint is added, all the users configured on the LDAP Server will have access to the Argus Safety Services where WebGate is installed.

10.5 Installation Maintenance Tasks

You may need to perform certain installation maintenance tasks on the installed Argus Safety Solution components.

10.5.1 Install New Components

1. Select Start > Control Panel.

2. Click Add or Remove Programs/Uninstall or change a program.

3. Right-click Argus Safety, and from the drop-down menu, click **Change**.

   The Argus Safety InstallShield Wizard opens the Preparing Setup dialog box.

4. Select **Modify**, and click **Next >**.

5. Select **Update installed Argus Components**, and click **Next >**.

6. In the Customer Information dialog box, enter the following parameters, and click **Next >**.

   - User Name

- Company Name

7. In the Select Features dialog box, check the components to install, and click **Next>**.

> **Note:** Make sure the checkboxes for components that are already installed contain a checkmark. If the checkmark is cleared from the checkbox for an existing component, the component will be uninstalled.
>
> Refer to the relevant chapters in this Installation Guide for instructions for installing individual components.

8. When the installation process is complete, the Argus Safety Setup- Maintenance Complete dialog appears.
9. Click **Finish**.

10.5.2 Uninstall Components

1. Select Start > Control Panel.
2. Click Add or Remove Programs.
3. Right-click Argus Safety, and from the drop-down menu, click **Change/Remove**.

   The Argus Safety InstallShield Wizard opens the Preparing Setup dialog box.
4. Select **Modify**, and click **Next >**.
5. In the Customer Information dialog box, enter the following parameters, and click **Next >**.
   - User Name
   - Company Name
6. In the Select Features dialog box, uncheck the components to uninstall, and click **Next >**.

   The Argus Safety Components Installer will uninstall the selected components.
7. Follow the on-screen instructions to uninstall the components.

> **Note:** If a Locked File Detected dialog box appears, select **Don't display this message again**, and click **Reboot**.

10.5.3 Remove All Components

1. Select Start > Control Panel.
2. Click Add or Remove Programs.
3. Right-click Argus Safety, and from the drop-down menu, click **Change/Remove**.

   The Argus Safety InstallShield Wizard opens the Preparing Setup dialog box.
4. Select **Remove**, and click **Next >**.
5. In the Confirm Uninstall dialog box, click **OK**.

   The Argus Safety Components Installer uninstalls the required component(s).
6. Follow the 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**.

10.6 Set Up easyPDF

The easyPDF component is required for printing PDF reports and for use by Interchange features such as transmitting E2B attachments.

The domain account created during the installation of either Argus Web Server, Argus Safety Services or Interchange Services, will be required to continue with the following steps.

10.6.1 Configure Windows Service Settings

Prerequisites:

- The domain account created is part of the local Administrator Group on the server being setup.
- 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 Safety will not be able to function correctly.

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. In the Services dialog box:
   a. Double-click the BCL easyPDF SDK 7 (or 6) Loader.
   b. Click the **Log On** tab.
   c. Enter the parameters.
4. Click the General tab.
5. From the **Startup type** drop-down list, select **Automatic**, and click **OK**.
6. From the Services window, start the BCL easyPDF SDK 7 (or 6) Loader.
7. Close the Services window.

10.6.2 Display PDF in Browser

If you are working on a client machine, you must make sure that you enable or check the **Display PDF in Browser** setting in Adobe Acrobat Reader.

If this setting is not enabled, PDF documents will not appear in Argus Safety user interface. This might cause some information status pop-ups to hang on the client machine.

10.7 Set Up Printer Defaults

When printing Argus Safety reports with Adobe Acrobat, make sure the Page Scaling option in the Print dialog box **(File > Print**) is set to **Shrink to Printable Area.**

10.8 Argus Configuration Files

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

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

Background Processes (AG Server)

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

Argus Web Server:

1. <Argus Install Path>/ArgusWeb/ASP/Web.config
2. <Argus Install Path>/ArgusWeb/Bin/Argussvr2.config
3. <Argus Install Path>/ArgusWeb/ASP/Argus.Net/Web.config
4. <Argus Install Path>/ArgusWeb/ASP/Argus.Net/Bin/RelsysWindowsService.exe.config
5. <Argus Install Path>/ArgusWeb/ASP/ Argus.Net/Bin /Service.config
6. <Argus Install Path>/ArgusWeb/ASP/Integrations/Web.config

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

10.8.1 Backup Configuration Files

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

Commonly modified configuration files are:

.\ArgusWeb\ASP\Argus.NET\bin\Intake.config

.\ArgusWeb\ASP\Argus.NET\bin\RelsysWindowsService.exe.config

.\ArgusWeb\ASP\Argus.NET\bin\Service.config

.\ArgusWeb\ASP\Argus.NET\web.config

.\ArgusWeb\ASP\ArgusConsole\web.config

.\ArgusWeb\ASP\Integrations\Service.config

.\ArgusWeb\ASP\Integrations\Web.config

.\ArgusWeb\ASP\web.config

.\ArgusWeb\Bin\Argusvr2.config

.\ArgusWeb\Bin\Argusvr2a.config

.\Argus Safety\AGProc.config

.\Argus Safety\Intake.config

.\Argus Safety\RelsysWindowsService.exe.config

.\ArgusSafety\Service.config

.\DBInstaller\ArgusDBInstall.exe.config

.\ESMMapping\ESMapping.exe.config

Part III

Install or Upgrade Argus Safety Database Tier

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

11

Install Argus Safety Database

Argus Safety installation requires a database instance that can be set up on:

- Windows—by using Schema Creation Tool or by executing a batch file
- Linux—by executing a shell script

11.1 Run Create DBA User Script

You must run the Create DBA User scripts to create a new DBA user. Use this new DBA user account when running the Schema Creation Tool to create the Argus Safety Schema.

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

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

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

To create the DBA user:

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

   C:\Program Files (x86)\Oracle\Argus\DBInstaller\Utilities\Create_Dba_User\create_dba_user.bat

2. Connect as SYS user.

   a. Enter a new log file name to store the output of the script execution.

   b. Enter the TNSName of the database where the Schema Creation Tool will be run.

   c. Enter the Password for SYS account.

   d. Enter a name for the new DBA User account that will be created.

   e. Enter a password for the new account.

   f. Follow the remaining steps to complete the script.

3. You may also run the script from the DBInstaller.zip:

- For Windows—execute the script from DBInstaller.zip\Utilities\Create_Dba_User\create_dba_user.bat
- For Linux—execute the script from DBInstaller.zip\Utilities\Create_Dba_User\create_dba_user

11.2 Validate the Database Setup Properties File

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

The file is located on the database server at *C:\Program Files (x86)\Oracle\Argus\DBInstaller*.

- #DB Connection Details
  - db_connect_string=<host name>:<port>/<db name>
  - dba_user=<argus dba user or system user>
- #Application Type
  - application_type=MULTI (for multi-tenant setup) or SINGLE (for single-tenant setup)
  - enterprise_name=DEFAULT
  - enterprise_short_name=DEFAULT
- #Complete path of Argus Secure Key ini file
  - argus_securekey_path=c:/windows
  - url—URL for the database connection
  - dbaUser—SYSTEM or DBA privileged user
- #Argus DB Schemas—Schema Name and Password (optional). If the password is left blank, it will be prompted at run-time.
  - To prompt for each password on the screen:
    - appSchema_argus_schema=argus_app
    - appSchema_argususer=argususer
    - appSchema_argus_login=argus_login
    - appSchema_vpd_schema=vpd_owner
    - appSchema_bip_schema=bip_owner
    - appSchema_esm_login=esm_login
    - appSchema_esm_schema=esm_owner
    - appSchema_esmquery_schema=esm_query
    - appSchema_dlp_schema=dlp_owner
    - appSchema_dlp_esmquery_schema=dlp_esm_query
  - To avoid prompt for each password on the screen, set up the password as the login password for each user:
    - appSchema_argus_schema=argus_app/<password>
    - appSchema_argususer=argususer/<password>

        - appSchema_argus_login=argus_login/<password>
        - appSchema_vpd_schema=vpd_owner/<password>
        - appSchema_bip_schema=bip_owner/<password>
        - appSchema_esm_login=esm_login/<password>
        - appSchema_esm_schema=esm_owner/<password>
        - appSchema_esmquery_schema=esm_query/<password>
        - appSchema_dlp_schema=dlp_owner/<password>
        - appSchema_dlp_esmquery_schema=dlp_esm_query/<password>

- #Argus DB Roles—Define the role names present <for upgrade> or to be created <for the new setup> in the database.
- #Argus Data Tablespaces—Define the tablespace and datafile details.

  Similarly ESM and DLP sections Define Data and Index datafiles.
- #Default and Temporary table spaces
  - default_ts=USERS
  - temp_ts=TEMP
- #TableSpace parameters
  - tablespace_encryption=<blank>
  - tablespace_initial_size=10M
  - tablespace_autoextend=ON
  - tablespace_next_size=10M
  - tablespace_block_size=8K
  - securefile=<blank>
- #Logging level (info, debug)
  - log_level=info

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

To create a database account that can connect to the Argus Safety Schema with Read-only privileges, execute the Create Read-only Database User script.

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

   C:\Program Files (x86)\Oracle\Argus\DBInstaller\Utilities\Create_Readonly_User
2. Follow the instructions provided in the script.

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

11.4 Create Argus Safety Database Schema

1. For Windows—To use the interactive user interface, install the Argus Safety Schema Creation Tool.

   For silent installation—execute the **DBInstaller.zip** file available in the shipped software.

2. Create the tablespaces. (Optional)

3. Create the schemas using either Schema Creation Tool or DBInstaller.zip.

   - Use the Argus Safety Schema Creation Tool to create the following database schemas:

     – Argus Schema

     – Interchange Service Schema

     – ESM Query Schema

     – DLP Schema (Optional)—Create this schema if DLP is to be enabled

     – DLP ESM Query Schema (Optional)—Required and created only when DLP is enabled

     ---

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

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

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

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

   - Axway Synchrony Database Instance (Optional)—Required only for Axway Synchrony.

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

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

11.4.1 Install XDB Schema for Interchange

Oracle Schema XDB must be present for Interchange packages to load. To create the XDB schema:

1. Click sqlplus.exe

2. Connect to **sys** as **sysdba**.
3. Execute the **?/rdbms/admin/catqm.sql script**.
4. Enter the following parameters:
   - user password
   - user default tablespace
   - user temporary tablespace

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

11.4.2 Prerequisites to Install Schema Creation Tool

Note: You must disable the UAC (User Account Control) 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.
- database TNS entry should be added in the TNSNAMES.ora file.
- loadjava should be working on the machine.

  From the command prompt, execute loadjava.
- Java 1.8 or higher must be installed and Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8 is applied.

  Note that the Liquibase installer supports both JRE 32 and 64 bit.
- login machine user should have administrative privileges.

To install Java:

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

   .http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html (download jce_policy-8.zip).
2. Unzip the jce_policy-8.zip.
3. Replace **local_policy.jar** and **US_export_policy.jar** files present in all the Java JRE and JDK installation security folder with the local_policy.jar and US_export_policy.jar shipped in **jce_policy-8.zip**.

   For example:

   Location of Java JRE and JDK 32-bit.

   C:\Program Files (x86)\Java\jre1.8.0_121\lib\security

   C:\Program Files (x86)\Java\jdk1.8.0_121\jre\lib\security
4. Or, you may install both JRE and JDK 64-bit. To do so, perform the same steps.
5. From the command prompt verify that Java is properly installed by executing:

   java -version

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

To set Java Installation Path:

1. Right-click the My Computer (or Computer) icon, and from the drop-down menu select **Properties**.
2. From the left-pane, select **Advanced system settings**.

   The System Properties dialog box with Advanced tab appears.
3. In the Startup and Recovery section, click **Environment Variables...**
4. From the System variables section, scroll-down to **Path** variable, and double-click.

   The Edit System Variable dialog box appears.
5. In the **Variable value:** field, enter the location where Java will be installed, and end it with a semi-colon (;).
6. Click **OK** to close the Edit System Variable dialog box.
7. Click **OK** to close the System Properties dialog box.

11.4.3 Install Schema Creation Tool

Note: With Argus Safety 8.1.1, DLP Schema and DLP ESM Query Schema are now part of Argus Database, but DLP setup can be enabled or disabled by executing separate batch files shipped with the software.

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

1. Open Argus Safety Setup.

   The Argus Safety Solution Components dialog box appears.
2. Select the **Schema Creation Tool**, and click **Next**.

   The Setup Status screen appears with the installation progress.

   When the installation process is complete, the Setup Completed screen appears.
3. Click **Finish**.

   The required files are copied to the system.
4. Click **OK** to reboot the system.
5. For silent install use DBInstaller.zip shipped with the software.

11.4.4 Create Tablespaces (Optional)

You can create tablespaces before installing Argus Safety. The schema creation tool creates the tablespaces if they do not exist.

Tablespaces for Argus Safety	Tablespaces for DLP
ARGUS_AEXP_DATA_01	DLP_DATA_01
ARGUS_AEXP_INDEX_01	DLP_DATA_02
ARGUS_AL_DATA_01	DLP_DATA_03
ARGUS_AL_INDEX_01	DLP_DATA_04

Tablespaces for Argus Safety	Tablespaces for DLP
ARGUS_DATA_01	DLP_DATA_05
ARGUS_DATA_02	DLP_DATA_06
ARGUS_DATA_03	DLP_INDEX_01
ARGUS_DATA_04	DLP_INDEX_02
ARGUS_DATA_05	DLP_INDEX_03
ARGUS_INDEX_01	DLP_INDEX_04
ARGUS_INDEX_02	DLP_INDEX_05
ARGUS_INDEX_03	DLP_INDEX_06
ARGUS_INDEX_04	DLP_LOB_01
ARGUS_INDEX_05	
ARGUS_INDEX_06	
ESM_DATA_01	
ESM_INDEX_01	

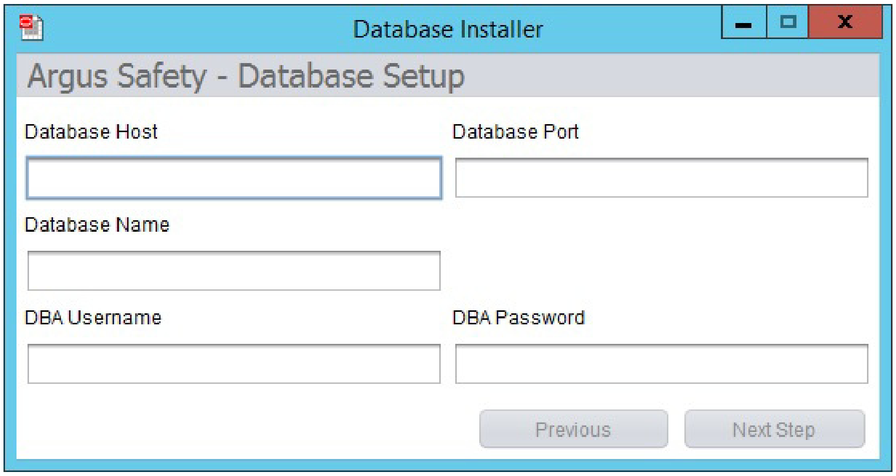
11.4.5 Prerequisites to Create the Schema

- Create the Cryptographic Key, refer to the chapter Argus Password Management - Cryptography Tool
- the Schema Creation Tool is installed
- a blank Oracle database instance is available
- a DBA-privileged or a SYSTEM user account is available
- the Oracle database is available from the machine where the schema creation tool is installed
- Java is installed and JCE policy is applied

To create schema from the user interface:

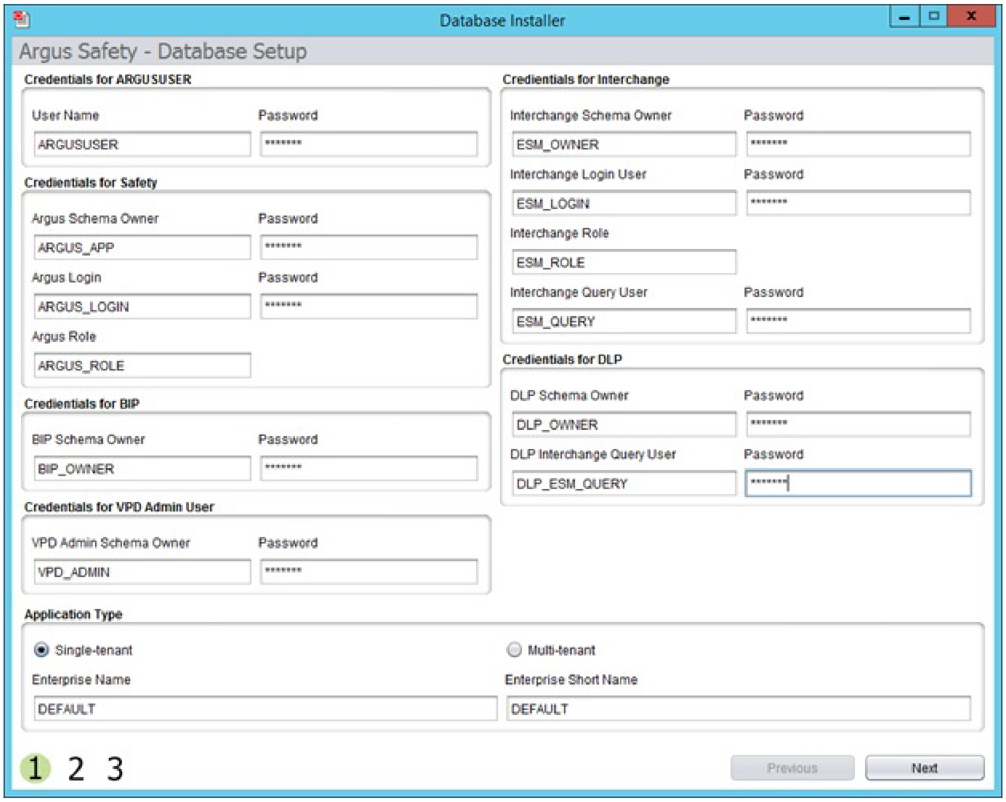
1. Open the schema creation tool, and click **Create/Upgrade DB**.

   The Database Installer dialog box appears.



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

Argus Safety - Database Setup screen appears.



Credentials for ARGUSUSER
User Name: ARGUSUSER
Password: *******

Credentials for Safety
Argus Schema Owner: ARGUS_APP
Password: *******
Argus Login: ARGUS_LOGIN
Password: *******
Argus Role: ARGUS_ROLE

Credentials for BIP
BIP Schema Owner: BIP_OWNER
Password: *******

Credentials for VPD Admin User
VPD Admin Schema Owner: VPD_ADMIN
Password: *******

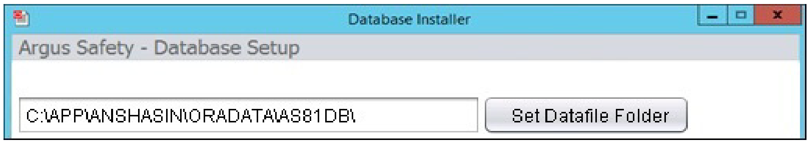
Credentials for Interchange
Interchange Schema Owner: ESM_OWNER
Password: *******
Interchange Login User: ESM_LOGIN
Password: *******
Interchange Role: ESM_ROLE
Interchange Query User: ESM_QUERY
Password: *******

Credentials for DLP
DLP Schema Owner: DLP_OWNER
Password: *******
DLP Interchange Query User: DLP_ESM_QUERY
Password: *******

Application Type
● Single-tenant
○ Multi-tenant
Enterprise Name: DEFAULT
Enterprise Short Name: DEFAULT

3. Enter the parameters, select the Application Type, and click **Next**.
   - Single Tenant—Allows the database to support only single tenant. The options to create multiple tenants in the safety system is disabled.
   - Multi-Tenant—Allows the database to support multiple tenants. Users are able to create multiple tenants using the Global Enterprise setup screens.
4. Create new tablespaces or use the existing tablespaces.
   - Under Complete Path and Data File Name, enter the database server path (complete path including the filename) where the data file is placed.

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



C:\APP\ANSHASIN\ORADATA\AS81DB\

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

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

- Click **Next**.

5. Verify the **Setup Parameters**, and click **Execute**.

   When execution is complete, a message appears in the Execution Log on screen 3 - *Liquibase Update Successfu*l.

6. To view the execution status or errors, open the schema creation log file with the latest timestamp from:

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

To create schema on Windows from the batch file:

1. Make sure the **dbinstaller.properties** are set up correctly.

   (See, Validate the Database Setup Properties File.)

2. From Start menu, select Run, type **cmd**, and click **OK**.

3. In the command prompt, go to the following path:

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

4. Type **DBInstaller.bat**, and press **Enter**.

5. Monitor the execution log and progress on the running window.

6. To view the log file, go to:

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

To create schema on Linux or Unix:

1. Make sure the **dbinstaller.properties** are set up correctly.

   (See, Validate the Database Setup Properties File.)

2. Copy the **DBInstaller.zip** file in your Linux or Unix directory.

   You must have privileges to execute and create files in this directory and /tmp directory.

3. Unzip the **DBInstaller. zip** file in the same directory.

4. Open a Linux or Unix terminal, and execute the following command:

   cd <path>/DBInstaller

5. Type **DBInstaller**, and press **Enter**.

6. Type the DBA user password, and press **Enter**.

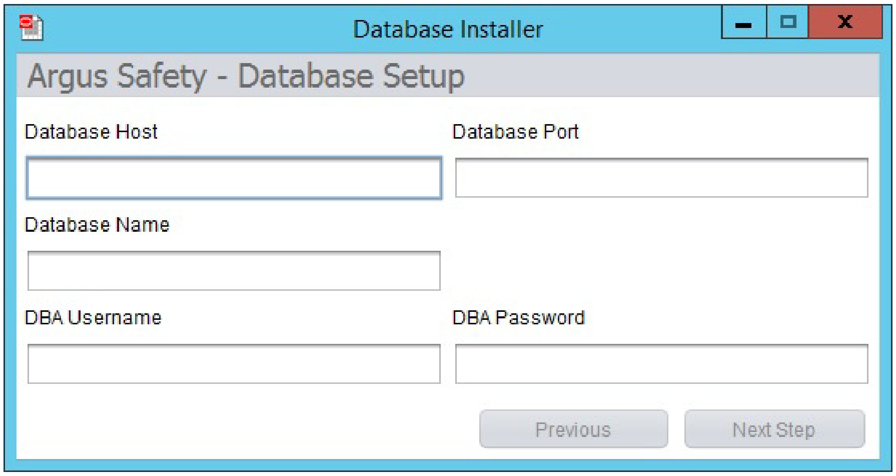
7. View logs from:

   <path>/DBInstaller/logs

11.4.6 Create the Schema on Windows from the User Interface

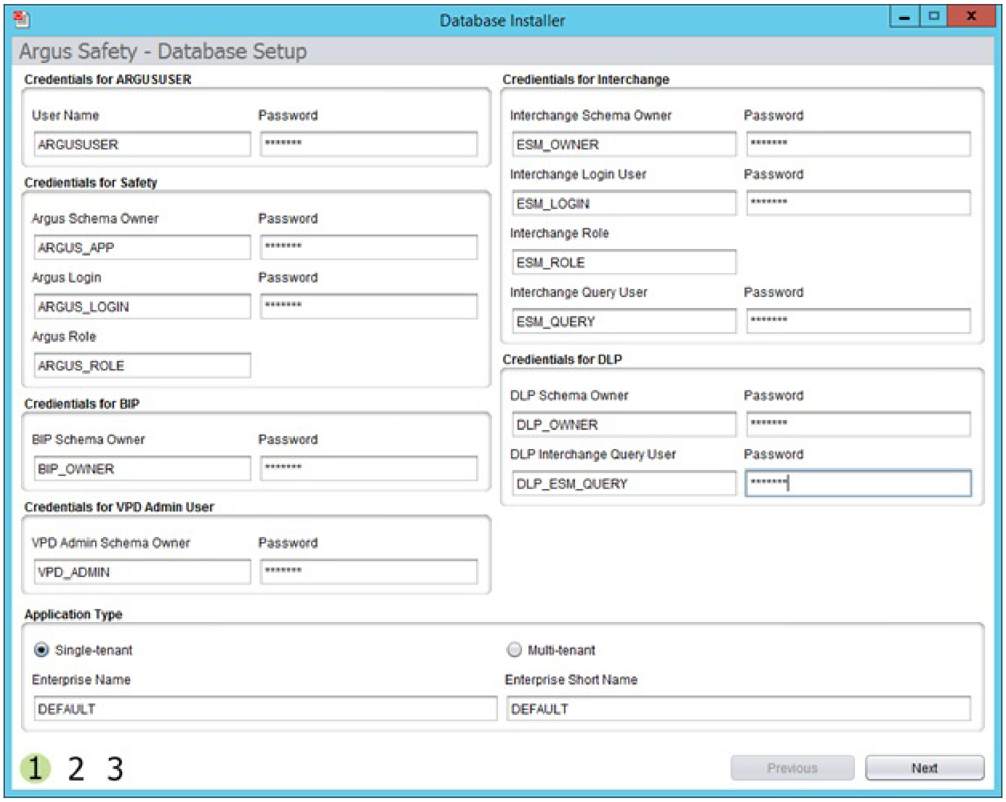
1. Open the schema creation tool, and click **Create/Upgrade DB**.

   The Database Installer dialog box appears.



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

   Argus Safety - Database Setup screen appears.



Credentials for ARGUSUSER

User Name: ARGUSUSER
Password: *******

Credentials for Safety

Argus Schema Owner: ARGUS_APP
Password: *******
Argus Login: ARGUS_LOGIN
Password: *******
Argus Role: ARGUS_ROLE

Credentials for BIP

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

Credentials for VPD Admin User

VPD Admin Schema Owner: VPD_ADMIN
Password: *******

Credentials for Interchange

Interchange Schema Owner: ESM_OWNER
Password: *******
Interchange Login User: ESM_LOGIN
Password: *******
Interchange Role: ESM_ROLE
Interchange Query User: ESM_QUERY
Password: *******

Credentials for DLP

DLP Schema Owner: DLP_OWNER
Password: *******
DLP Interchange Query User: DLP_ESM_QUERY
Password: *******

Application Type

● Single-tenant ○ Multi-tenant

Enterprise Name: DEFAULT
Enterprise Short Name: DEFAULT

3. Enter the parameters, select the Application Type, and click **Next**.

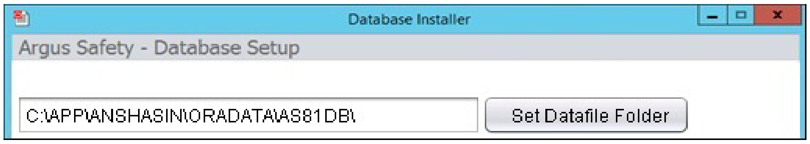
   – Single Tenant—Select this option to allow the database to support only single tenant. The options to create multiple tenants in the safety system is disabled.

   – Multi-Tenant—Select this option to allows the database to support multiple tenants. Users are able to create multiple tenants using the Global Enterprise setup screens.

4. Create new tablespaces or use the existing tablespaces.

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

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



C:\APP\ANSHASIN\ORADATA\AS81DB\

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

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

- Click **Next**.

5. Verify the **Setup Parameters**, and click **Execute**.

   When execution is complete, a message appears in the Execution Log on screen 3 - *Liquibase Update Successfu*l.

6. To view the execution status or errors, open the schema creation log file with the latest timestamp from:

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

11.4.7 Create the Schema on Windows from a Batch file

1. Make sure the **dbinstaller.properties** are set up correctly.

   (See, Validate the Database Setup Properties File.)

2. From Start menu, select Run, type **cmd**, and click **OK**.
3. In the command prompt, go to the following path:

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

4. Type **DBInstaller.bat**, and press **Enter**.
5. Monitor the execution log and progress on the running window.
6. To view the log file, go to:

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

11.4.8 Create the Schema on Linux or Unix

1. Make sure the **dbinstaller.properties** are set up correctly.

   (See, Validate the Database Setup Properties File.)

2. Copy the **DBInstaller.zip** file in your Linux or Unix directory.

   You must have privileges to execute and create files in this directory and /tmp directory.

3. Unzip the **DBInstaller. zip** file in the same directory.
4. Open a Linux or Unix terminal, and execute the following command:

   cd <path>/DBInstaller
5. Type **DBInstaller**, and press **Enter**.
6. Type the DBA user password, and press **Enter**.
7. View logs from:

   <path>/DBInstaller/logs

11.5 Enable Oracle Text

Oracle Text search is an index-based querying solution that improves Duplicate Case search performance.

> **Note:** If you do not use the Schema Creation Tool to install Oracle Text and the Common Profile Switch is enabled, it would lead to an error when you run a search from the Argus Book-in screen.

Enable Oracle Text is part of the Schema Setup. When enabled, Oracle Text performs the following functions:

- DB Installer checks whether Oracle Text is installed. If not, it displays an error message.
- 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, a dialog box appears with the amount of space currently available (in megabytes).

11.6 Table Partitioning (Optional)

> **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.

11.7 Validate Argus Safety Database

You must validate the database after installation.

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

11.7.1 Validate Argus Safety Database on Windows from a User Interface

1. From the Schema Creation Tool, click **Schema Validation**.
2. Enter the SYSTEM or DBA user password, the Database name, and click **OK**.
3. In the Schema Validation dialog box:
   a. Validate the values in the fields.
   b. Locate the Validation CTL File section, and click **Browse** to open the Selection Path for CTL File dialog box.
4. Locate and select the correct folder and CTL file for the database being validated, and click **OK**.
5. Locate the Validation Log Files section, and click **Browse** to open the Selection Path for Creating Log Files dialog box.
6. Choose the folder where you want the system to create the log files, and click **OK**.
7. Click **Validate Schema**.
8. On the command prompt, press **Enter**.
9. On the Oracle Sql*Plus window, press **Enter**.
10. Note the path of the log files created during processing.
11. Exit from the **Schema Creation Tool**.
12. Check the files for errors.

11.7.2 Validate Argus Safety Database on Windows from a Batch file

1. From Start menu, select Run, type **cmd**, and click **OK**.
2. In the command prompt, go to the following path:

   cd C:\Program Files (x86)\Oracle\Argus\DBInstaller\SchemaValidation
3. Type **SchemaValidation.bat**, and press **Enter**.
4. To proceed with the Schema Validation:
   a. Enter TNSNAMES Entry to Connect to the ARGUS Database: <AS811DB>
   b. Enter DBA Username in AS811DB Database: <argus_dba>
   c. Enter password for argus_dba in AS811DB Database:
   d. Enter Validation CTL File [Example VLDN_811.CTL]: <VLDN_811.CTL>
   e. Enter Log Files Folder: <C:\Program Files (x86)\Oracle\Argus\DBInstaller>
   f. Enter Schema Difference Log File [Default SV_Schema_Diffs_qcas8003.log]:
   g. Enter CTL Loader Log File [Default SV_CTLFile_qcas8003.log]:
5. Verify the log file for any error.

11.7.3 Validate Argus Safety Database on Linux or Unix

1. Copy the **DBInstaller.zip** file in your Linux or Unix directory.

   You must have privileges to execute and create files in this directory and /tmp directory.

2. Unzip the **DBInstaller. zip** file in the same directory.

3. Open a Linux or Unix terminal, and execute the following command:

   cd <path>/DBInstaller

4. Type **SchemaValidation**, and press **Enter**.

5. Type the DBA user password, and press **Enter**.

6. View logs from:

   <path>/DBInstaller/logs

11.8 Enable and Disable DLP

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

11.8.1 Pre-requites

Before enabling or disabling DLP, make sure that:

- the Schema Creation Tool is installed
- an Oracle Argus database instance is available
- a DBA-privileged user or a SYSTEM user account is available
- the dbinstaller.properties is correctly updated

  (See, Validate the Database Setup Properties File.)

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

11.8.2 Enable DLP

- For Windows, execute the **enableDLP.bat** file from:

  C:\Program Files (x86)\Oracle\Argus\DBInstaller\Utilities\DLP_Setup

- For Linux or Unix, execute the **enableDLP** shell script

11.8.3 Disable DLP

- For Windows, execute the **disableDLP.bat** file from:

  C:\Program Files (x86)\Oracle\Argus\DBInstaller\Utilities\DLP_Setup

- For Linux or Unix, execute the **disableDLP** shell script

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

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

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

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

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

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

11.9 Enable DLP on a Specific Enterprise

You can enable DLP for:

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

11.9.1 Prerequisites

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

11.9.2 Extract the Custom Scripts

Extract the custom DLP Enable Enterprise Specific script from the following location into a machine's local folder where Argus Safety 8.1.1 is installed:

C:\Program Files\Oracle\Argus\DBInstaller\Utilities\DLP_Enable_Enterprise_Specific

11.9.3 Set Up the Base Database

1. Set up an Argus Safety 8.1.1 multi-tenant or single-tenant database.

   Enable DLP on the Argus Safety 8.1.1 database from Schema Creation Tool > Argus DLP.

2. Validate the schema from Argus Safety 8.1.1 Schema Creation Tool > Schema Validation by selecting the compatible CTL file.

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

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

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

11.9.4 Enable DLP on Specific Enterprise or Delta Cases

To enable DLP on a Specific Enterprise or Delta Cases in a Specific Enterprise, make sure that you use the correct login credentials and set up the appropriate enterprise context.

1. Double-click DLP_Enable_Enterprise.bat from:

   C:\Program Files\Oracle\Argus\DBInstaller\Utilities\DLP_Enable_Enterprise_Specific\Argus\DLP\

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

   - process all cases merged in Argus Safety system due to creation of new enterprise by merge process
   - process of delta cases merged in an enterprise due to any migration activity

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

   For example, DLP_Enable_Enterpirse_Specific.log

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

   A confirmation message appears, whether the database is single-tenant or multi-tenant.

4. Press **Enter**.

   The details entered for the Enable DLP Enterprise Specific process appears.

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

6. Verify the log files for any errors.

   In case of any error during the Enable DLP process, the execution process is paused. Rectify the errors and continue the process from another SQL window.

7. To view the missing cases between Argus Safety and DLP, go to

   \DLP_Enable_Enterprise_Specific\Argus\DLP\DLP_ENABLE_Missing_Cases_in_DLP_log.log.

11.9.5 Validate the Schema

After enabling DLP Enterprise Specific to Argus Safety 8.1.1, validate the schema.

1. Double-click on ArgusDBInstall.exe file from

   C:\Program Files\Oracle\Argus\DBInstaller.

2. Click **Schema Validation**.

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

The following table and related objects will be ignored in Schema Validation if Argus Safety 8.1.1 DLP Enabled system with DLP_Enable_Enterprise_Specific scripts is applied:

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

11.10 Copy Configuration Tool

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

> **Note:** Copy Configuration Tool creates a Database Directory in order to execute. Make sure to create a physical directory on the Database Server where Export and Import dump files are created, and copied respectively. The physical path of these directories is required while performing the export and import.

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 (x86)\Oracle\Argus\DBInstaller\Utilities\Copy_Config to the *C:\CONFIG_EXP_IMP* folder.

3. Export the Source database by running the batch file, and follow the prompts:

   C:\CONFIG_EXP_IMP\Data_ExportConfigOnly.bat

4. Copy ArgusSecureKey.ini (working with source database) from the .\Windows folder, and save it with generated source database file.

5. Move the dump files generated on the source Database Server (physical path provided while performing the export) to the target Database Server (physical path where import will be done).

6. To perform the import on the client machine, in the **Directory Path on DB Server where dump files are placed for import** parameter, use the same folder as entered in the **DB Directory Path for export dump files** while executing the export process for logs.

   Or, move the contents of the export logs folder provided in the **Directory including full path for log/script files** parameter while executing the export process, in the folder being used for the import process for log generation.

7. Create a new database (with/without TDE enabled) using the Schema Creation tool.

8. Import into Target database by running the batch file, and follow the prompts

   C:\CONFIG_EXP_IMP\Data_ImportConfigOnly.bat

Ignore any "ORA-28101: policy already exists" error.

9. Validate Schema on the target database using Schema Validation Tool.
10. 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.
11. In case you do not have ArgusSecureKey.ini, follow the steps listed in the Section 21.2.6, "Reset the Environment if ArgusSecureKey.ini is Lost."

12

Upgrade Argus Safety Database

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

12.1 Prerequisites for Database Upgrade

- The Oracle Database Server version should be upgraded to 12c (12.1.0.2.0).
- Verify that Java is installed and JCE policy is applied.
- Verify that the Oracle TNSNAMES have been configured.
- To avoid errors during upgrade, do either of the following:

  a) KEEP DATA FILES AUTOEXTEND ON, or

  b) Monitor free space and add more space, if required.
- Make sure 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 rollback segments, except SYSTEM, offline.
- The source Argus Safety database must be AL32UTF8 character set database.
- The database semantics must be CHAR and not BYTE.

12.2 Argus Safety Database Upgrade

> **Note:** You will need to generate a key prior to the database upgrade or you can use a key from the existing setup.
>
> You must also make sure that the password information specified in the database is consistent with the information provided in the **ArgusSecureKey.ini** file.

To upgrade the database:

Note that 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. To make sure the upgrade tool detects the roles correctly, login as Argus Schema User, and from SQLPlus execute the following commands:

```
define ESM_ROLE = <Current ESM ROLE NAME>
define ARGUS_ROLE = <Current ARGUS ROLE NAME>

INSERT INTO cmn_profile_global (section, key, value, key_type) VALUES
('DATABASE', 'ARGUS_ROLE',  '&ARGUS_ROLE.', 0);
INSERT INTO cmn_profile_global (section, key, value, key_type) VALUES
('DATABASE', 'INTERCHANGE_ROLE', '&ESM_ROLE.', 0);
COMMIT;
```

2. Connect to Argus Safety database as a SYS user.

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

   Provide the following grants if the DBA user has been created through the Create DBA User script:

   ```
   Define user_dba=SYSTEM
   GRANT EXECUTE on SYS.DBMS_CRYPTO TO &user_dba. WITH GRANT OPTION;
   ```

3. Select Start > Programs > Oracle > Schema Creation Tool.
4. Click **Create/Upgrade DB**.

   The Argus Safety - Database Setup screen appears.

   You cannot modify any details on this screen. In case, any of the information is incorrect, then you must re-create fresh schema.
5. In case of upgrade, all the schema details will be auto-populated based on the schema selection logic. Before proceeding further, you must confirm that all the schema details are correctly populated.

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

6. Click **Next**.
7. Enter the path for Tablespaces, and click **Next**.
8. Verify the Setup Parameters, and click **Execute**.
9. To ignore any error due to customization, check **Ignore Error** checkbox in the Schema Creation Tool, and analyze it later when the upgrade is done.
10. To validate the schema, run the Schema Validation tool.

12.3 Populate J License under Case Form—PMDA tab

If you are already live on Argus Safety English version, you can go live with the Single Global DB and choose to Enable Argus Japan module on the same version or an upgrade version (with both English and Japan).

In such a scenario, some existing cases may need J Reporting and require licenses under PMDA tab. The upgrade script **J_Lic_Upgrade_PMDA** adds PMDA Licenses under PMDA tab (if does not exists already) for the existing drug or vaccine licenses under Event Assessment.

While updating the case:

- The script excludes all the cases that are open or that are deleted.
- The script includes cases in locked state or archived state.
- The updates are audit logged.

To populate J License under Case Form > PMDA tab:

1. Upgrade your database to Argus Safety 8.1 or 8.1.1.
2. Execute the batch file **J_License_PMDA_Upgrade.bat** from

   <Argus Installation Path>\Argus\DBInstaller\utilities\J_Lic_Upgrade_PMDA.
3. Enter the log file name to record the list of cases updated by this upgrade script.

   This is the execution log that is created on the client workstation under the J_Lic_Upgrade_PMDA directory.
4. Enter TNSNAMES Entry to Connect to the source SAFETY Database.
5. Enter the Argus Schema Owner name.
6. Enter the password of the Argus Schema user.

12.4 Enable Local Locking in Argus Safety

Before enabling Local Locking in Argus Safety, you must make sure that you have upgraded your database to Argus Safety 8.1.1 successfully.

12.4.1 Enable Local Locking

1. Execute the batch file **Enable_local_lock.bat** from

   <C>:\Program Files\Oracle\Argus\DBInstaller\utilities\Enable_local_lock directory.
2. Enter the response for *Do you wish to turn on the Local Locking feature for one or more enterprises (Yes/No)?*, enter **Yes** to continue.
3. Enter the log file name to record the results.

   This is the execution log that is created on the client workstation under the Enable_local_lock directory mentioned above.
4. Enter TNSNAMES Entry to Connect to the source SAFETY Database.
5. Enter SAFETY schema owner name in source Database.
6. Enter the password for safety schema name in source Database.
7. Enter comma separated list of enterprises where local locking feature is to be enabled or enter ALL for all enterprises in Source safety Database.

   If no value is entered script will run for enterprise 1 by default.
8. Enter the Agency name for PMDA reporting destination as configured in **Reporting Destination** codelist.
9. To enable the local locking privileges for Argus J users, enter **Yes**.

   Follow the prompts for confirmation.

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

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

12.4.2 Fetch cases in PSUR

To make cases appear in PSUR regardless of past submission:

1. Delete the data from the cmn_per_sub_child table.
2. Execute the following query to restore the data to factory settings as per upgrade:

```
INSERT INTO CMN_PER_SUB_CHILD (id,reg_report_id,rec_type,field,enterprise_id)
SELECT S_CMN_PER_SUB_CHILD.NEXTVAL,reg_report_id,rec_type,field,enterprise_id
FROM (
WITH report_ids AS (
SELECT crr.reg_report_id, crr.report_form_id FROM
v$cmn_reg_reports crr,
v$lm_report_forms lrf
WHERE crr.report_form_id=lrf.report_form_id and crr.enterprise_
id=lrf.enterprise_id
AND crr.state_id=6 AND crr.report_form_id>100
AND lrf.rpt_type in (2,12)
)
, dataview as (
select distinct ri.reg_report_id,cprc.report_form_id,cprc.rec_type,cprc.field,
max(cprc.rec_type) over (partition by cprc.report_form_id) max_rec_type
,cprc.enterprise_id
from v$cfg_per_rpt_child cprc, report_ids ri
where ri.report_form_id=cprc.report_form_id
and cprc.rec_type in (1,8)
)
select reg_report_id,rec_type,field,enterprise_id
from dataview
where rec_type=max_rec_type
);
```

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

Note: You must execute the above steps after setting the enterprise context using PKG_RLS.SET_CONTEXT procedure.

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

12.5.1 Prerequisites to Run the Merge Export Step

- The end user should not use the Source database during export process.
- Install Argus Safety 8.1.1 on a computer where Oracle 12c (12.1.0.2.0) is installed.
- The source databases should be schema validated at Argus Safety 8.1.1.

- The source database should only be a single-tenant database.
- The source database data must contain only one ENTERPRISE.

12.5.2 Merge Export

1. Navigate to the following Path from Start Menu:

   All Programs > Oracle > Merge to Multi-tenant

2. Click **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. Make sure that no error has occurred during the database export, by checking the following log files:

   - Log file name entered as parameter 1 during export step execution.
   - Following Oracle Export log files are created on database server. The path is the value entered on "Enter Directory including full Path to create Source safety database export dump file" during export step:

     SAFETY_EXPORT.log

12.5.3 Export the dmp File Copy to the Target Database Server

Move the export Dmp file created in Merge Export from the source database server to the target database server.

12.5.4 Prerequisites to Run the Merge Import Step

- Create a cold backup of the target database before starting the MERGE IMPORT step.
- The end user should not use the target database during the import process

- Only one MERGE Import process can run on the Target database at a time.
- Auto extend should be set on for all Database files in the target database
- Sufficient space should be available on the target database server to import the new Enterprise Data. The amount of space depends on the number of cases in source Safety database.
- Install the Argus 8.1.1 application. Make sure that Oracle Client version is 12c (12.1.0.2.0).
- The Target databases should be Schema Validated at Argus 8.1.1.
- The target database must be a Multi-tenant database
- All source database dictionaries should be available in target Database. If the dictionary doesn't exist then install missing dictionaries on Target database.
- All existing AG service users on the Source Database must exist on the target Database
- All source database LDAP configured server names should be available in target database.

12.5.5 Merge Import

1. Navigate to the following path from Start Menu:

   All Programs > Oracle > Merge to Multi-tenant

2. Click **Import**, and follow the instructions on the sqlplus screen.

   a. Enter Log File Name to record results.

      This is the execution log that 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 file imports the data from the dump file into the target database.

4. Make sure that no error has occurred during the import, by checking the following log files:

   - Log file name entered as parameter 1 during Import step execution.
   - The following Oracle Import log files are created on database server. The path is the value entered 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 database using Safety Schema Validation tool.

12.5.6 Synchronize Dictionary Manually

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

To synchronize the dictionary data manually on the target database:

1. Log in as 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 is required.

```
Select dict_id
From cfg_dictionaries_enterprise
Where enterprise_id = <Value of New Enterprise ID>
And global_dict_id = -1;
```

5. Log in as the Safety schema owner using sqlplus on the source safety database.

6. Locate the dictionary name of each Dictionary ID where the Dictionary does not exist on the target database using the following sql:

```
Select name from cfg_dictionaries_global
where dict_id in (<List of Dict ID values (comma separated) from Step 4);
```

7. Load the missing dictionaries on the target database.

8. Set the context to new enterprise_id using following sql on target database.

```
Exec pkg_rls.set_context('admin',<Value of new ENTERPRISE_ID> ,'ARGUS_SAFETY');
```

9. Update GLOBAL_DICT_ID data in the target database using the following SQL:

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

13 Work with the Dictionaries

For each dictionary, you need to create a schema with the Schema Creation Tool and then load the dictionary.

Schema Name	Description
MedDRA Schema	To enable MedDRA, create this schema by using the MedDRA Loader Tool when MedDRA is loaded to the new database tables.
J Drug Schema	To enable J Drug, create this schema.
WHO Schema	To enable WHO, create this schema by using the WHO Loader Tool when WHO is loaded to the new database tables.

For more details, refer to the Section 11.4, "Create Argus Safety Database Schema".

13.1 Prerequisites to Load the Dictionaries

- To work with MedDRA and MedDRA J dictionaries, make sure:
  - the system where these dictionaries will be installed has a minimum of 50 MB space
  - the schema creation tool is installed
  - Oracle database instance is available
  - a SYSTEM user account is 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.

- To work with WHO-DRUG dictionary, make sure:
  - Windows workstation PC is available to load the WHO-DRUG data
  - the system 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.

13.2 Load MedDRA Dictionary

1. Open the Schema Creation Tool, and click **MedDRA Loader**.

   The Oracle Database Connect dialog box appears.

2. Enter the SYSTEM user password, Database name, and click **OK**.

   The MedDRA Dictionary Loader dialog box appears.

3. Do the following:

   - To load MedDRA dictionary for the first time, select **Load to New Tables**.
   - To load a MedDRA J dictionary, select **MedDRA J**.
   - In the Tablespace Information section, select the tablespace and index from the respective drop-down lists.
   - To create a new MedDRA user, click **Create User**.

   The New MedDRA User dialog box appears.

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

   The MedDRA Dictionary Loader dialog box appears.

5. Click **Create Role**.

   The New MedDRA Role dialog box appears.

6. Enter the new role name in the **New Role** field, and click **OK**.

   The MedDRA Dictionary Loader dialog box appears.

7. In the Dictionary to Load section, do the following:

   a. Select the **MedDRA Version** being uploaded from the drop-down list.

   b. To locate the dictionary files, click **Browse**, and select the files.

   c. To use this dictionary version in the Argus Safety MedDRA Browser, select the **MedDRA Browser** checkbox.

   d. Select the MedDRA version to be loaded from the MedDRA Version drop-down list, and click **Load**.

   The system loads the dictionary and a confirmation message appears.

8. Click **OK**.

13.3 Overwrite an Existing MedDRA Dictionary

1. Open the Schema Creation Tool, and click **MedDRA Loader**.

   The Oracle Database Connect dialog box appears.

2. Enter the SYSTEM user password, the Database name, and click **OK.**

   The MedDRA Dictionary Loader dialog box appears.

3. Do the following:

   a. Select **Overwrite**.

   b. To load a MedDRA J dictionary, select **MedDRA J**.

   c. From the **Tablespace** and **Index** drop-down lists, select a tablespace and index.

   d. From the **User** drop-down list, select a user.

   e. Enter the user password in the **Password** field; re-enter it in the Verify Password field.

   f. From the **Role** drop-down list, select a role.

   g. From the **Current Version to Overwrite** drop-down list, select the version to overwrite.

   h. From the **MedDRA Version** drop-down list, select the MedDRA version to load.

   i. To go to the directory where the dictionary files reside, click **Browse**, and select the dictionary files.

   j. To use the dictionary version in the Argus Safety MedDRA Browser, check the **MedDRA Browser** checkbox.

   k. Click **Load**.

   The Oracle Database Connect dialog box appears.

4. Enter the SYSTEM user password, the Database name and click **OK**.

   When overwriting the dictionary is complete, the Dictionary Load dialog box appears.

5. Click **OK**.

13.4 Recode Events

1. Open the Schema Creation Tool, click **MedDRA Loader**.
2. Enter the SYSTEM or DBA user password, the Database name, and click **OK**.
3. In the MedDRA Dictionary Loader dialog box, click **Re-Code**.
4. In the Event Re-Coding dialog box, do the following:

   a. 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.

b. 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.

c. Select either or all of the Process Current Terms, Process Non-Current Terms and/or Update dictionary version checkboxes.

d. 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.

e. Select the Output File format.
   - Delimited Text
   - Excel Sheet output

f. Click on the **Execute** button to start the recoding process.

g. 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.

h. The system recodes the following fields from **Case Form** and **Code List**.

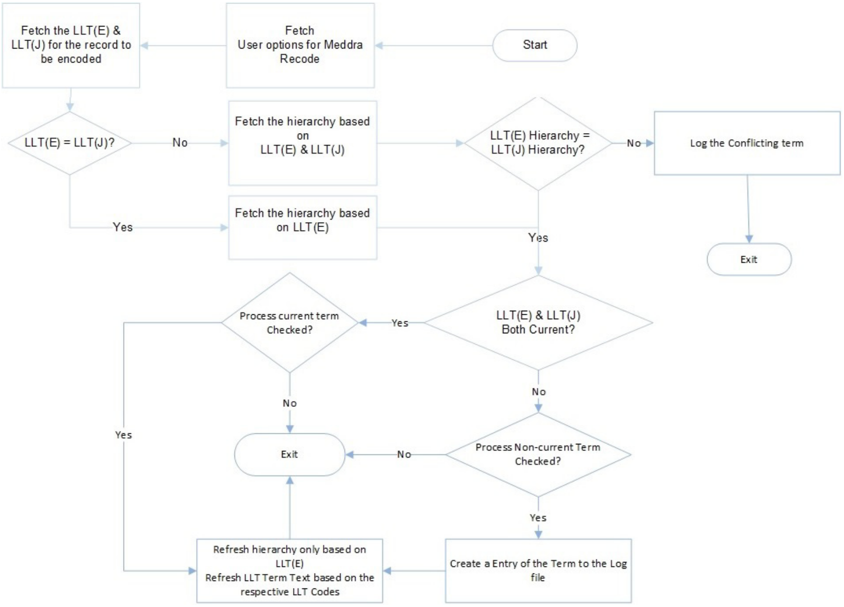
Field Location	Name of Recoded Field
Case Form	Death Details
	Lab Data
	Other Relevant History
	Product Indications
	Events
	Case Diagnosis
Code List	Product Indication
	Lab Test Types

13.4.1 Recode MedDRA for J Dictionary

- If for a record either LLT(E) or LLT(J) term is non-current as per the new upgrading MedDRA Dictionary, then MedDRA recode only refreshes the hierarchy for both LLT(E) and LLT(J).

  Note that for the records for which hierarchy is refreshed, the LLT Term's **text** and **currency** is also be refreshed based on the respective LLT codes.

- Before recoding MedDRA, the re-coding logic verifies if both LLT (E) and LLT (J) belongs to the same hierarchy (that is, under the same PT) in the new upgrading MedDRA or not. And records the term only If they belong to the same hierarchy, else just creates an entry to the logs (for manual update later).
- Re-coding the terms with English MedDRA remains as-is but the application is refreshed for the non-current LLT (E) with PT.
- If you execute the MedDRA Recode with English MedDRA the preferences for executing will be limited as explained in the function flow for re-coding with J MedDRA.



Start
Fetch User options for Meddra Recode
Fetch the LLT(E) & LLT(J) for the record to be encoded
LLT(E) = LLT(J)?
No
Yes
Fetch the hierarchy based on LLT(E) & LLT(J)
Fetch the hierarchy based on LLT(E)
LLT(E) Hierarchy = LLT(J) Hierarchy?
No
Log the Conflicting term
Exit
Yes
LLT(E) & LLT(J) Both Current?
Yes
Process current term Checked?
No
Yes
No
Exit
No
Process Non-current Term Checked?
Yes
Create a Entry of the Term to the Log file
Refresh hierarchy only based on LLT(E) Refresh LLT Term Text based on the respective LLT Codes

- The following log files are created with detailed old and new values:
  - Log files for LLT Terms Non-current in new MedDRA:

    File Name (Case Form): MedDRA_Recode_Success_NonCurrentJ_YYYY_MM_DD_HH_MIN

    File Name (LM Data): MedDRA_Recode_Success_LM_NonCurrentJ_YYYY_MM_DD_HH_MIN
  - Log files for LLT Terms belongs to different PT:

    File Name (Case Form): MedDRA_Recode_Failure_PTMisMatchJ_YYYY_MM_DD_HH_MIN

    File Name (LM Data): MedDRA_Recode_Failure_LM_PTMisMatchJ_YYYY_MM_DD_HH_MIN

13.4.2 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.

Option	Point E
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.

13.5 Load J Drug Dictionary

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

13.5.1 Before loading the J Drug Dictionary

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

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

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

The following is the detailed information:

- **J-drug dictionary distributor organization information**

  Organization Name: MT Kyogikai

  Contact Information:

  URL: http://www.iyaku.info/

  TEL: +81-3-3230-2867

  FAX: +81-3-3239-3954

  e-mail:mtk@iyaku.info

- **J-drug loader load procedure**

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

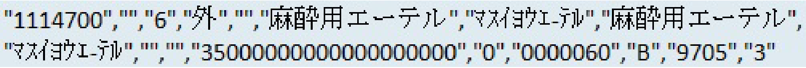
- All_Data.txt
- formulationcode.txt
- drugnameenglish.txt

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

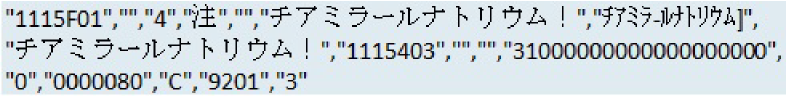
To create file All_Data.txt:

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

Sample All_Data.txt'files:



```
"1114700","","6","外","","麻酔用エーテル","ﾏｽｲﾖｳｴ-ﾃﾙ","麻酔用エーテル",
"ﾏｽｲﾖｳｴ-ﾃﾙ","","","35000000000000000000","0","0000060","B","9705","3"
```



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

To create formulationcode.txt file:

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

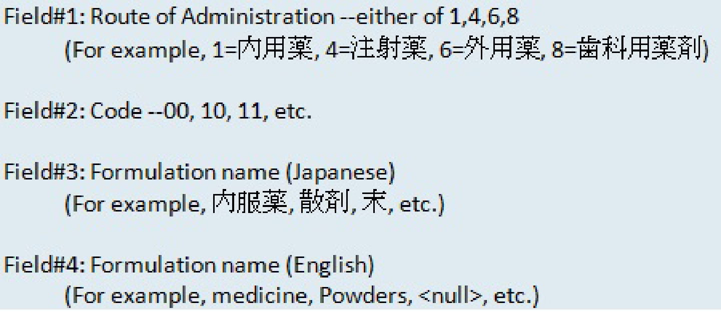
Format of the file formulationcode.txt:

- Physical file name: formulationcode.txt

- File format: CSV (Comma Separated Value) with 4 fields.

- Character Code: Shift-JIS code. (This file contains Kanji.)

- Field Information:



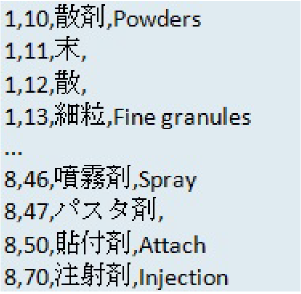
```
Field#1: Route of Administration --either of 1,4,6,8
        (For example, 1=内用薬, 4=注射薬, 6=外用薬, 8=歯科用薬剤)

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

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

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

Sample formulationcode.txt:



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

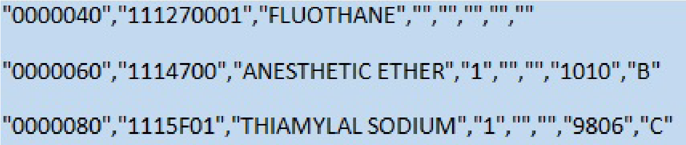
The complete formulationcode.txt file as of Feb.2011 is available at:

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

To create drugnameenglish.txt file:

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

Sample drugnameenglish.txt:



```
"0000040","111270001","FLUOTHANE","","","","",""

"0000060","1114700","ANESTHETIC ETHER","1","","","1010","B"

"0000080","1115F01","THIAMYLAL SODIUM","1","","","9806","C"
```

- **To modify the.MDB file:**

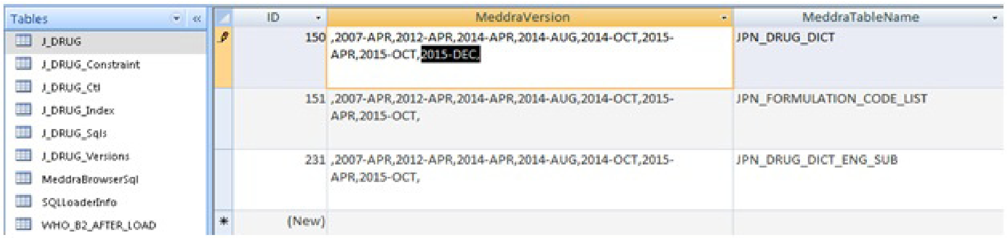
1. Open the **jdrug.mdb** from the following location:

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

   A table appears with J_Drug table supported versions (second column).

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

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



ID	MeddraVersion	MeddraTableName
150	,2007-APR,2012-APR,2014-APR,2014-AUG,2014-OCT,2015-APR,2015-OCT,2015-DEC,	JPN_DRUG_DICT
151	,2007-APR,2012-APR,2014-APR,2014-AUG,2014-OCT,2015-APR,2015-OCT,	JPN_FORMULATION_CODE_LIST
231	,2007-APR,2012-APR,2014-APR,2014-AUG,2014-OCT,2015-APR,2015-OCT,	JPN_DRUG_DICT_ENG_SUB
(New)		

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

13.5.2 Load J Drug dictionary into the database

1. Open the Schema Creation Tool, and click **J Drug Loader**.
2. Enter the SYSTEM or DBA user password, the Database name, and click **OK**.
3. In the J Drug Dictionary Loader dialog box, do the following:

   a. Select **Load to New Tables** if a J-Drug dictionary is not loaded before.
   b. Locate the Tablespace Information section and select the tablespace and index from the drop-down lists.
   c. Click **Create User** to create a new J-Drug user

4. In the New J-Drug User dialog box, enter the parameters, and click **OK**.
5. Click **Create Role**.
6. Enter the **New Role** name, and click **OK**.
7. In 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. Click **OK**.

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

For example, if JDrug_Aug_2015 dictionary and JDrug_OCT_2015 dictionary are loaded in the database, then Argus Safety will use data from the latest dictionary i.e., JDrug_OCT_2015 dictionary.

13.6 Overwrite an Existing J Drug Dictionary

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

1. Open the Schema Creation Tool, click **J Drug Loader**.
2. Enter the SYSTEM or DBA user password, the Database name, and click **OK**.
3. In the J Drug Dictionary Loader dialog box, locate the Loading Options section and do the following:
   a. Select **Overwrite**.
   b. Select the tablespace and index from the Tablespace and Index drop-down lists.
   c. Select the user from the **User** drop-down list.
   d. Enter the user password in the **Password** field; re-enter it in the **Verify Password** field.
   e. Select the appropriate role from the **Role** drop-down list.
   f. Select the J Drug dictionary version to load from the **Dictionary Version** drop-down list.
   g. Click **Browse** to go to the directory where the dictionary files reside and select the appropriate dictionary files.

h. Click **Load**.

4. Enter the SYSTEM or DBA user password, the Database name, and click **OK**.

   The Dictionary Load dialog box appears.

5. Click **OK**.

13.7 Load WHO-DRUG Dictionary

> **Note:** By uploading a version of WHODrug Enhanced, WHODrug Global or other UMC products, you confirm holding a valid license granted by the UMC for the uploaded UMC product.

13.7.1 Before loading the WHO-DRUG dictionary

Verify the following:

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

  SQLPLUS (Exe=sqlplusw)

  SQL*Loader (Exe=sqlldr)
- There is an updated TNSNAMES file and Oracle client to connect to the Argus Safety database.
- The following WHO-DRUG dictionary data files are available:
  - bna.dd
  - ccode.dd
  - dd.dd
  - dda.dd
  - ddsource.dd
  - ina.dd
  - ing.dd
  - man.d
- 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.

13.7.2 Load WHO-Drug Dictionary to New Tables

1. Launch the Schema Creation Tool, click **Who Drug Loader**.
2. Enter the SYSTEM or DBA user password, the Database name, and click **OK**.
3. In the WHO-Drug Dictionary Loader dialog box, do the following:

   a. To load the dictionary into a separate schema, click **Load New Tables**.
   b. To create new user, click **Create User**.

      Enter the information required to create a new user, and click **OK**.
   c. To create new role, click **Create Role**.

      Enter the **New Role** name, and click **OK**.
4. In the Dictionary to Load section, enter the **New Role** name, and click **OK**.
5. Click **Load**.
6. Click **OK**.
7. Enter the SYSTEM or DBA user password, the Database name, and click **OK**.

13.7.3 Overwrite an Existing WHO-Drug Dictionary

1. From the Schema Creation Tool, click **Who Drug Loader**.
2. Enter the SYSTEM or DBA user password, the Database name, and click **OK**.
3. In the WHO-Drug Dictionary Loader dialog box, do the following:
   a. Click **Overwrite**.
   b. Select the dictionary version to load.
   c. Click **Browse** to display the Select Folder dialog box and select the appropriate path, and click **Select**.
   d. Click **Load** to load the dictionary.
   e. View WHO-Drug dictionary log.
4. Enter the SYSTEM or DBA user password, the Database name, and click **OK**.

   A confirmation message that the dictionary is loaded successfully appears.
5. Click **OK**.

13.7.4 Load WHO-Drug Dictionary in Different Format

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. From the Schema Creation Tool, click **Who Drug Loader**.
2. Enter the SYSTEM or DBA user password, the Database name, and click **OK**.
3. In the WHO-Drug Dictionary Loader dialog box do the following:
   a. To load the dictionary into a separate schema, click **Load New Tables**.
   b. To create new user, click **Create User.**

      Enter the parameters, and click **OK**.
   c. Select Dictionary Format**—Format C** or **Format C3**.

Note:

- For Dictionary Format, **Format C3**, WHO Drug schema will have the table named WHO_DRUG_C3_MASTER and WHO_DRUG_C3_MEDICINAL_PRODUCT, instead of table WHO_DRUG_C_MASTER and WHO_DRUG_C_MEDICINAL_PRODUCT. These table will have the DRUG_NAME as Varchar2(1500).

  Besides, this schema will also have views as WHO_DRUG_C_MASTER and WHO_DRUG_C_MEDICINAL_PRODUCT which will point to the tables WHO_DRUG_C3_MASTER and WHO_DRUG_C3_MEDICINAL_PRODUCT but the Drug Name is tranced to Varchar2(250).

- For Dictionary Format, **Format B3,** WHO Drug schema will have the table named WHO_B3_DRUG_DICT and WHO_B3_ATC_CODE, instead of table WHO_DRUG_DICT and WHO_ATC_CODE. These table will have the DRUG_NAME as Varchar2(1500) and ATC_TEXT VARCHAR2(110).

  Besides, this schema will also have views as WHO_DRUG_DICT and WHO_ATC_CODE which will point to the tables WHO_B3_DRUG_DICT and WHO_B3_ATC_CODE but the Drug Name is tranced to Varchar2(250) and Varchar2(110).

4. Click **Create Role**, enter the parameters, and click **OK**.
5. In the WHO-Drug Dictionary Loader dialog box:
   a. Select the Dictionary Version to load from the drop-down list.
   b. Click **Browse** to display the Select Folder dialog box and select the appropriate path.
6. Click **Load**.
7. Enter the SYSTEM or DBA user password, the Database name, and click **OK**.
8. When the dictionary is loaded successfully, click **OK**.

Part IV

Configure Other Products

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

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

Prerequisites:

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

14

Configure and Enable Argus Dossier

14.1 Prerequisites

- Set Up Argus Safety Middle and Client Tiers, and follow all the chapters from 3 to 13.

14.2 Configure Dossier

1. Run Argus Safety Installer, and select **Dossier**.

   Follow the instructions and complete the setup.

2. On the server where Dossier is installed, from the installation folder, open the file **service.config**. By default, the installation folder is

   C:\Program Files\Oracle\ArgusWeb\ASP\Argus.NET\bin

3. Uncomment the entries for **DossierBuilder** in the section:

   <ServiceConfiguration>/<ServiceComponents>

4. From the installation folder, open the file **RelsysWindowsService.exe.config**.

5. Make sure that the <DatabaseConfiguration> section is configured for the following attributes:

Attribute	Description
DBName (Mandatory)	TNS of the Database to which the RelsysWindowsService should connect to. Example: DBName="GOLDDEMO"
DBUser	AGService Username. The RelsysWindowsService logs into the database using this login name. This has to be a user of type AGSERVICE. Example: DBUser="agservice_user1"
DBPassword	Generate new encrypted string, refer to Section 21.2.4, "Generate Encrypted String".
GeneralEmailTo	The e-mail address to which the e-mails will be sent by the Intake Service, using the General Email feature of Argus. Example: GeneralEmailTo ="recepient@oracle.net"

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

14.3 Verify Dossier Installation

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

   The Internet Options dialog box appears.
3. Click the Advanced tab, locate the **Multimedia** section, and verify that:
   - Enable automatic image resizing is **not** checked
   - Show image download placeholders is **not** checked
   - Show pictures is **checked**
   - Smart image dithering is **not** checked
4. Click the Security tab, click **Custom level...**, and scroll-down to the ActiveX controls and plug-ins header.
5. Verify that Download signed ActiveX controls is **enabled**, and 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.

14.4 Enable Dossier

To enable the configured dossier:

1. Go to Argus Safety >Argus Console > System Configuration > Enabled Modules.

2. Select **Dossier**.
3. Click **Save**.

15

Install and Configure Axway Synchrony

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

> **Note:** Either B2B or Axway Synchrony is required for E2B reports exchange. You can choose any one of the software, as required.
>
> You may install EDI Gateway and Interchange Service in any order.

15.1 Create an Axway Synchrony Database Instance

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 Axway Synchrony schema and create the following indexes to improve the interface performance between Argus Interchange and Axway Synchrony:
   - create index fbi_mes_confilename on messageeventsnapshots (direction, upper(consumptionfilename));
   - create index fbi_mes_coreid on messageeventsnapshots (upper(coreid), messageid)

15.2 Install Axway Synchrony Interchange

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

15.3 Start the Axway Synchrony Server

1. Log on to the computer as an Admin user.
2. Go to Local Machine > Services directory.
3. Double-click the GatewayInterchageService.

   The GatewayInterchangeService Properties dialog box appears.
4. To start the Service Status, click **Start**.
5. When the Service Status changes to **Start**, click **OK**.

   You may also start the Axway Synchrony Server from the command prompt.
6. To start the Axway Synchrony Server from the command prompt, select Start > Programs > Axway Synchrony > Start Server.

   The Start Server dialog box appears.

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

15.4 Configure Axway Synchrony Interchange for Axway 5.12

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. In the Axway Synchrony Login screen, enter the Axway Synchrony User ID and Password, and click **Login**.
5. In the Getting Started screen, hover the **Trading Configuration** icon, and select **Recent Communities > Manage Trading Configuration** from the menu.
6. In the Pick a community screen, click **Add a community**.
7. In the Choose the source screen:
   a. Click **Next >>** to continue.
   b. Click the **Manually create a new community profile** option button.
   c. Enter the parameters.
   d. Click **Yes** to add a certificate.

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

   e. Click **Finish**.

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

15.4.1 Configure Axway Synchrony for Binary File Transmission

You can configure 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. In the Axway Synchrony Login screen, enter the Axway Synchrony User ID and Password, and click **Login**.
4. In the Getting Started screen, hover the **Trading Configuration** icon, and from the drop-down menu, select **Recent Communities > <community>**.
5. In the Summary screen, click the **Application Pickup** icon, and add an application pickup.

6. In the Choose transport protocol screen, click File system option, and click **Next** >>.

7. In the From address and To address screens, click **Next >>**.

   Address must be determined by either message attribute configuration or by protocol address only.

8. In the **Configure the file system settings** screen:

   - On the Sender's Axway Synchrony Server, locate Common/Out folder and create the following folder structure:

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

9. In the Exchange Name screen, enter the **Exchange Name**, and click **Finish**.

10. In the **Change this application pickup exchange** screen, click the **Message attributes** tab.

11. In the Message attribute directory mapping tab:

    a. The system moves them to the **Selected attributes** list.

    b. Select **From routing ID** and **To routing ID** and click **Add.**

    c. Locate the **Available Attributes** list.

    d. Click the **From address** tab.

12. Click **To address** tab, and select the **Address determined by message attribute configuration** option or by protocol address only, and click **Save Changes**.

13. 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.

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

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

15.4.2 Configure Axway Synchrony Community

15.4.2.1 Register with the Axway Synchrony Community

1. Open this URL: http://<*Receiver Axway SynchronyServer*>: 6080/ui/.

2. In the **Axway Synchrony Login** screen, enter Axway Synchrony User ID and Password, and click **Login**.

3. In the Getting started screen, hover the **Trading Configuration** icon, and from the drop-down menu, select **Recent Communities > <community>**.
4. In the Summary screen, click **Export this community as a partner profile** at the bottom of the page.
5. Save the file to your local hard drive, and close the **Save** dialog.
6. Click **Logout** in the upper right corner of the page.

15.4.2.2 Add a Partner to the Axway Synchrony Community

1. Open the following URL: http://<*Sender Axway SynchronyServer*>: 6080/ui/.
2. In the Axway Synchrony Login screen, enter the Axway Synchrony User ID and Password, and click **Login**.
3. In the Getting Started screen, hover the **Trading Configuration** icon, and select **Recent Communities > <community>** from the menu.
4. In the Summary screen, click the **Add a Partner to this community** link.
5. In the **Choose the source** screen, select the **Import the profile information from a file** option, and click **Next >>**.
6. In the **Enter profile path** screen, click **Browse** to navigate to the saved file, and click **Finish**.
7. In the **Successful profile import** screen, click **Close**.

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

8. In the Summary screen:
   a. Click the **Partners** menu item, and select the newly imported partner.
   b. Hover the **Trading Configuration** icon.
   c. From the drop-down menu, click **Set up a routing ID**.
9. In the Routing IDs screen:
   1. Click **Add**.
   2. Type the partner (sender) routing ID in the **Routing ID** field.
   3. Verify that the partner **does not** have a routing ID.

      The new routing ID is added to the page.
   4. Hover the **Trading Configuration** icon.
   5. Select **Recent Communities > <community>** from the menu.
10. In the Summary screen, select the sender partner.
11. In the Summary: Sender screen, click the **Default delivery exchange** link.
12. In the **Change this delivery exchange** screen, click the **HTTP Settings** tab, and verify that the URL is correct and that the correct routing ID for the send is appended to the end of the URL

15.4.2.3 Register the Receiver's Community on the Sender Server

Repeat the procedures of the following sections:.

1. Section 15.1, "Create an Axway Synchrony Database Instance"
2. Section 15.3, "Start the Axway Synchrony Server"

15.4.3 Add a Node

1. Open Internet Explorer.
2. Go to the following URL: http://< *Sender Axway SynchronyServer*>:6080/ui/.
3. In the Axway Synchrony Login screen, enter the Axway Synchrony User ID and Password, and click **Login**.
4. In the Getting started screen, click the **System Management** icon.
5. In the System Management screen, click **Add a node**.
6. In the Add a node screen:
   a. Click **Add**.
   b. Select the machine to add the node to from the **Computer name** drop-down list.
   c. Click the **Trading Engine** option.
7. When the System management page opens with the newly created node:
   - Click **Start** to start the node.

     The system updates System management page.

     The status of the node changes to **Starting**.

     The system updates the System management page.

     The status of the node changes to **Running**.
8. Click **Home**, and verify that the node status is **Running**.
9. Repeat the procedure to set up the Receiver Axway Synchrony.

15.4.4 Configure Axway Synchrony Certificates

15.4.4.1 Configure Receiver Axway Synchrony Certificates

1. Open Internet Explorer.
2. Go to the following URL: http://<*Receiver Axway SynchronyServer*>:6080/ui/.
3. In the Axway Synchrony Login screen, enter the Axway Synchrony User ID and Password, and click **Login**.
4. In the Getting Started screen, hover the **Trading Configuration** icon, and select **Manage trading configurations** from the menu.
5. In the Community screen, click the **Community name**.
6. In the Summary screen, click the **Certificates** link.
7. In the Certificate screen, click the **Certificate** listed on the **Personal certificates** tab.

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

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

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

15.4.4.2 Configure Sender Axway Synchrony Certificates

1. Open Internet Explorer.
2. Go to the following URL: http://<*Sender Axway SynchronyServer*>:6080/ui/.
3. In the Axway Synchrony Login screen, enter the Axway Synchrony User ID and Password, and click **Login**.
4. In the Getting Started screen, hover the **Trading Configuration** icon, and select **Manage trading configurations** from the menu.
5. In the Community screen, click the **Community name**.
6. In the Summary screen, click the **Certificates** link.
7. In the Certificate screen, click the **Trusted root certificates** tab, and click the **Add a trusted root certificate** link.

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

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

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

15.4.5 Configuring EVENTS.XML

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

To configure Event.xml on Client machine:

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\Utilities\Cyclone.
3. Locate and double-click the **cyclone_setup.bat** file to open a DOS command prompt window.
4. In the Oracle SQL+ screen:
    a. Enter the Axway Synchrony instance in the **TSNAMES entry**.
    b. Enter the Axway Synchrony DB User Name in the **Axway Synchrony User Name**.
    c. Enter the Axway Synchrony Schema User in the **[USERS]**.
    d. Enter the Axway Synchrony User Password in the **Password for User Axway Synchrony_USER**.
5. When SQL+ connects to the specified database, enter the log file name and the Directory name.

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

To configure Event.xml on Receiver machine:

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

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

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

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

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

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

7. Copy the ArgusRouter.jar file from Argus local directory: \ *SUPPORT* \ *Axway Synchrony* \ *Axway Synchrony 5x* to Axway Synchrony directory: <*Axway Synchrony Install Folder*>*site**jars*\.
8. Open Internet Explorer.
9. Open the following URL: http://<*Receiver Axway SynchronyServer*>: 6080/ui/.
10. In the Getting Started screen, hover the **Trading Configuration** icon, and from the drop-down menu, select **Recent Communities > Community**.
11. In the Summary screen, and click the **Application Pickup** icon.
12. In the Application pickup exchange screen, click the link in the **Name** column.
13. Click the **Inline Processing** tab.
14. In the Inline processing rules screen:
    a. Enter `com.cyclonecommerce.relsys.router.GetMessageInfo` in the **Class name** field.
    b. Enter **Relsys Argus** in the **Parameter** field.
    c. Enter **GetMessagesInformation** in the **Description** field.
15. Click **Save changes**.
16. When the Pick an integration pickup exchange screen appears, click **Logout**.
17. Repeat the preceding steps for the Sender Server.

15.5 Test Communication

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

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

2. Make sure that the Axway Synchrony servers on both sender and receiver are running.
3. Drop the E2B XML file into the out bound folder of the Axway Synchrony Sender server.
4. Log on to a machine where Axway Synchrony is installed.
5. In the Internet Explorer, open the URL:

   http://<Sender Axway SynchronyServer>:6080/ui/

6. In the Axway Synchrony Login screen, enter the Axway Synchrony User ID and Password, and click **Login**.

7. In the Getting started screen, hover the **Message Tracker** icon, and select the **Message Searches > All Messages** from the menu.

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

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

8. When the file is transmitted successfully, click **Logout**.

9. Go to the Axway Synchrony Receiver server, and verify that the E2B file has been received.

10. To verify that the file has been transmitted:

    a. Log in to the receiver Axway Synchrony server.

    b. Select the All Messages option.

    c. View the message payload.

11. Compare the E2B file on the receiving machine (payload version displayed) with the file from the sending machine.

    These files should be identical.

12. 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.

16

Install and Configure Oracle B2B

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

16.1 Install Oracle B2B

Refer to *Oracle B2B Installation Guide*.

16.2 Integrate Oracle B2B with Argus Safety

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

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

16.3 Create Integration tables in B2B Schema

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

After Argus Safety is installed, locate DB Script B2B_setup.bat under *%Argus Installation Folder%\Oracle\Argus\DBInstaller\Utilities\B2B_Setup\*.

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

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

1. B2B_ARGUSSAFETY_INBOUND (table)

2. S_B2B_ARGUSSAFETY_INBOUND (sequence)

16.4 Configure Oracle B2B User Interface

Log in to Oracle B2B UI as an admin user.

16.4.1 General Configuration > Administration > Configuration

1. Under the **Non Purgeable** section, set **Use JMS Queue as default** to **True**.
2. Under the **Miscellaneous** section, set **Additional MIME Types** to **application/octet-stream : application/pdf**.
3. Under the **Performance** section, set **Large Payload Directory** to the desired location.

   It is recommended to set it, even if large payloads are not likely to be received.

16.4.2 Document Configuration > Administration > Document

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

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

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

16.5 Configure Enterprise Manager

16.5.1 Deploy SOA Composite

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

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

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

To deploy SOA composites:

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

16.5.2 Configure SOA Composite

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

16.5.2.1 AS_BPEL_Outbound Composite

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

1. Select AS_FileAdapter.
   a. Change PhysicalDirectory and PhysicalArchiveDirectory to the desired location.

      Do not change other properties.

   b. Argus Safety may create outbound files under the same or under any of the child directories of the above specified directory.
2. B2B_DBAdapter should NOT be changed for any of the properties.
3. B2B_JMSAdapter can be changed, but only if required.

16.5.2.2 AS_BPEL_Inbound Composite

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

1. Select AS_FileAdapter.
   a. Set PhysicalDirectory as the top level folder under which all the incoming files are dropped by B2B.

      Do not change other properties.
2. Select LargeFileReader.
   a. The PhysicalDirectory should be the same as Large Payload Directory under Oracle B2B UI > Administration > Configuration > Performance section.

      Do not change other properties.
3. B2B_DBAdapter should NOT be changed for any of the properties.
4. B2B_Inbound can be changed, but only if required.

16.6 Configure Web Logic Console

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

16.6.1 Data source with JNDI Name as ’eis/DB/ArgusSafety_Outbound’

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

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

16.6.2 Data source as ’jdbc/ArgusSafety_Inbound’

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

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

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

16.6.3 Data source with JNDI Name as ’eis/DB/ArgusSafety_Inbound’

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

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

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

16.6.4 DB Adapters for Data Source

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

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

16.7 Configure Large Payload Exchange

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

Argus Safety can send large files if E2B R2 Attachments are configured or E2B R3 or eVAERS files are exchanged. With other scenarios, generally, large payloads may not be applicable. Each following point specifies if they are needed even if you are exchanging small files.

16.7.1 Outbound Files

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

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

16.7.2 Inbound Files

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

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

16.7.3 Transaction Time

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

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

16.7.4 General B2B Settings for Large Payloads

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

16.8 Configurations for Argus Safety

16.8.1 Configure Oracle B2B

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

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

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

16.8.2 Update for B2B Documents

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

The following table list the sample factory data:

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

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

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

16.8.3 Argus Console > Reporting Destination Code List

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

17

Configure OBIEE or BI Publisher

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

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

17.1 Prepare BI Publisher Server

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

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

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

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

17.2 Set Up BI Publisher for Argus Safety

17.2.1 Install and Configure East Asian Fonts (Optional)

> **Note:** This section is required only if PMDA R3 Paper forms are generated through Argus Safety, or to print any Japanese fonts in any BIP Periodic report or any custom reports having Japanese font.

OBIEE and BI Publisher 12.2.1.0 does not have the fonts that are essential to run PMDA R3 Paper forms. To install and configure these fonts:

1. From My Oracle Support, download the **Patch# 21918899**.

There could be more than one patch listed, based on the applied CPU. It is fine to download any of the listed packages as there is no need to deploy the whole patch.

2. Stop all the OBIEE/BIP services.
3. From the patch zip folder, extract the **fonts.zip** folder into:
   - For Windows—<MW_HOME>\oracle_common\internal\
   - For Linux—$MW_HOME/oracle_common/internal/

   Where, MW_HOME is the location where the OBIEE or BIP middleware is installed.

   Upon extraction, the sub-directory **fonts** is created.
4. Take a backup of the file **setDomainEnv.sh** (or **setDomainEnv.cmd** in Windows) located at $MW_HOME/user_projetcs/domains/bi/bin directory.
5. To edit the file, open the file in a plain text editor, like Notepad, and update the **xdo.font.dir** with the new correct location of the fonts as follows:

   ```
   set EXTRA_JAVA_PROPERTIES=-Dxdo.server.config.dir=C:\Oracle\Middleware\Oracle_
   Home\bi\bin\..\..\user_projects\domains\bi\bidata\components\bipublisher -DXDO_
   FONT_DIR=C:\Oracle\Middleware\Oracle_Home\oracle_common\internal\fonts %EXTRA_
   JAVA_PROPERTIES%
   ```

   Where, C:\Oracle\Middleware\Oracle_Home\ is the MW_HOME.
6. Save and close the file.
7. Start all the OBIEE or BIP services.

   OBIEE or BIP is now ready to run the PMDA R3 Paper forms.

Note: Check the Patch 21918899 readme file for the latest information about the fonts installation settings.

17.2.2 Enable a Local Superuser

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

To enable a local superuser:

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

17.2.3 Database Connectivity

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

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

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

   This displays the **Data Sources** screen.
4. Click **Add Data Source**.
5. In the **Add Data Source** section:
   1. Enter **asbip** in the **Data Source Name** field.

      Make sure that you enter this data source name in lowercase only.
   2. Select the database from the **Driver Type** drop-down list.

      This auto-populates the **Database Driver Class** field.
   3. Enter either of the following connection string in the **Connection String** field.

      - *url="jdbc:oracle:thin:@[host]:[port]/[sid]"*

      - *url="jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=host.com)(PORT=<port number>)))(CONNECT_DATA=(SID=orcl)))"*
   4. Enter the Argus BIP schema username (for example, bip_owner), and the password.

      This user is created as part of the Argus Safety database installation.
   5. Click **Test Connection**.

      If successful, this displays a confirmation message.
6. Click **Apply**. This displays the **asbip** Data Source in the list of already existing data source names.

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

17.2.4 Set Up Runtime BI Publisher Memory

1. Login to BI Publisher.
2. Click **Administration**.
3. From Runtime Configuration section, click **Properties**.
4. Modify the following parameter values to **5000** seconds from 600 seconds:
   - Memory Guard > Process timeout for online report formatting
   - Data Model > SQL Query Timeout
5. Click on **Apply**.

   These values can be increased as needed, for any BIP custom reports that takes longer time-period.

17.2.5 Configure Oracle Fusion Middleware Security Model

> **Note:** If you are using the BI Publisher Security model, it is recommended to move to Oracle Fusion Middleware Security model.
>
> When moving from BI Publisher Security model, you must re-create the users, roles and policies through the Enterprise Manager.

17.3 Manage Users and Roles

17.3.1 Configure Users, Groups and Roles

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

In case you are using the BI Publisher Security Model, refer to Appendix A, "Configure BI Publisher Security Model."

17.3.1.1 Create Groups

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

1. Login to Fusion Middleware Console.
2. Navigate to WebLogic Domain > Security > Users and Groups > Groups.
3. From the Groups section, click **New.**

   The Create a New Group dialog box appears.
4. Create the following groups for Flexible Aggregate Reports by entering the **Name** and **Description**:
   - FARAdminGroup
   - FARSafetyAuthorGroup
   - FARSafetyConsumerGroup
5. Create the following groups for Expedited Reports by entering the **Name** and **Description**:
   - EXPAdminGroup
   - EXPSafetyAuthorGroup
   - EXPSafetyConsumerGroup

17.3.1.2 Create Users

1. Login to Fusion Middleware Console.
2. Navigate to WebLogic Domain > Security > Users and Groups > Users.
3. From the Users section, click **New**.

   The Create a New User screen appears.

4. Enter the following fields, and click **OK**.
   a. Name
   b. Description
   c. Provider
   d. Password
   e. Confirm Password
5. Assign role to the user, and click **Save**.

17.3.1.3 Create Application Roles

1. Login to Fusion Middleware Control Enterprise Manager.
2. Go to WebLogic Domain > Security > Application Roles.

   The Application Roles dialog box appears.
3. From the **Application Stripe** drop-down list, select **OBI**, and click **Search** ▶.

   The default Role available in clean slate installation appears.
4. Click **Create**.

   The Create Application Role dialog box appears.
5. In the **Role Name** field, enter **FARAdminRole**.
6. From the Members section, click **+Add**.

   The Add Principal dialog box appears.
7. From the **Type** drop-down list, select **Group**, and click **Search**.

   A list of principals appears.
8. From the list of Searched Principals, select **FARAdminGroup**, and click **OK**.
9. From the Members section, click **+Add**.

   The Add Principal dialog box appears.
10. From the **Type** drop-down list, select **Application Role**, and click **Search**.

    A list of principals appears.
11. From the list, search Users, select **Weblogic**, and click **OK.**
12. Repeat from Step 4 to Step 11 to create other FAR and Expedited Reports role and add Member to these roles as listed in the table below.

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

Role	Application Roles
FARAdminRole	FARAdminGroup
	Weblogic
FARSafetyAuthorRole	FARSafety AuthorGroup
	FARAdminGroup
FARSafetyConsumerRole	FARSafetyConsumerGroup
	FARSafetyAuthorGroup

Role	Application Roles
	FARAdminGroup
EXPAdminRole	EXPAdminGroup
	Weblogic
EXPSafety Author Role	EXPSafetyAuthorGroup
	EXPAdminGroup
EXPSafety Consumer Role	EXPSafetyConsumerGroup
	EXPSafetyAuthorGroup
	EXPAdminGroup

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

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

17.3.2.1 Create Application Policies

1. Login to Fusion Middleware Control Enterprise Manager.
2. Go to WebLogic Domain > Security > Application Policies.

   The Application Policies screen appears.
3. To create a new application policy, click **Create**.

   The Create Application Grant dialog box appears.
4. From the Grantee section, click **+Add**.

   The Add Principal dialog box appears.
5. From the **Type** drop-down list, select **Application Role**, and click **Search** ▶.
6. From the list of Searched Principals, select **FARAdminRole**, and click **OK**.
7. From the Permissions section, click **+Add.**

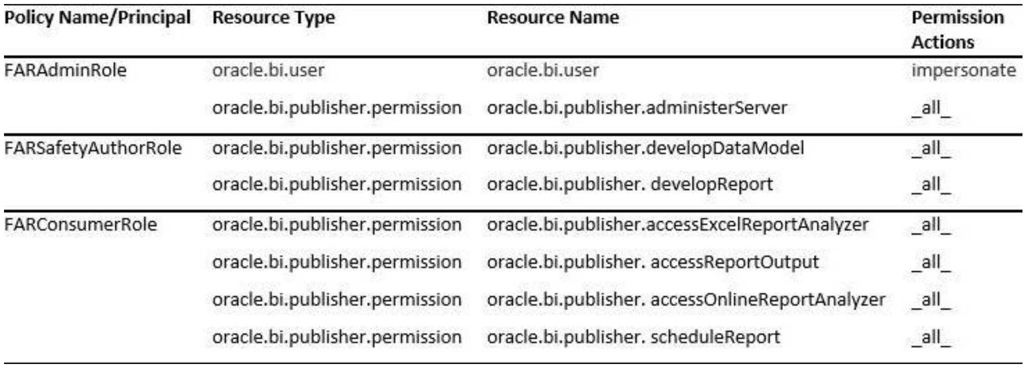
   The Add Permission dialog box appears.
8. Select the **Resource Types** radio button.
9. From the **Resource Type** drop-down list, select **oracle.bi.publisher.permission**, and click **Search**.
10. From the Search Results, select **oracle.bi.publisher.permission** (BIP Administer Server), and click **Continue**.

    The Add Permission dialog box appears.
11. For **Permission Actions**, select **All** (_all_), and click **Select**.
12. Add Resource Name as **oracle.bi.user** with **Impersonate** permission.

    The new FAR Admin policy has all the permissions.

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

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



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

14. Similarly, create roles and policies for Expedited Reports for the following groups:
    - EXPAdminRole
    - EXPSafetyAuthorRole
    - EXPSafetyConsumerRole

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

17.3.2.2 Manage Folder Privileges

To set Catalog Folder-level permissions:

1. Log in to BI Publisher application as a privileged user.

   For example, log in to http://<hostname.domainname>:<port>/xmlpserver, as weblogic.

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

   The Permissions dialog box appears.

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

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

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

4. Go to Catalog > Shared folders > AS_Expedited > Tasks > Permissions.

The Permissions dialog box appears.

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

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

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

6. To add the Data Sources to Roles in BI Publisher:

   a. Login to the BIP with Administrator credentials.

   b. Go to Administration > Roles and Permissions.

      The Roles and Permissions screen appears.

   c. From the list of roles, select **FARAdminRole**, and click the corresponding **Add Data Sources** icon.

      The Add Data Sources screen appears.

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

   e. Click **Apply**.

   f. Repeat the steps to add **asbip** data source for the following roles as well:

      - FARSafetyAuthorRole,

      - FARSafetyConsumerRole,

      - EXPAdminRole,

      - EXPSafetyAuthorRole

      - EXPSafetyConsumerRole

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

17.3.3.1 Create Application Policies

1. Login to Fusion Middleware Control Enterprise Manager.

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

   The Application Policies screen appears.

3. From the **Application Stripe** drop-down list, select **OBI**.

4. Click **Create**.

   The Create Application Grant dialog box appears.

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

   The Add Principal dialog box appears.

6. From the **Type** drop-down list, select **Application Role**, and click **Search** ▶.
7. From the list of Searched Principals, select **FARAdminRole**, and click **OK**.
8. From the Permissions section, click **+Add.**

   The Add Permission dialog box appears.

9. Select the **Resource Types** radio button.
10. From the **Resource Type** drop-down list, select **<Resource Type>**, and click **Search**.
11. From the Search Results, select **<Resource Name>**, and click **Continue**.

    The Add Permission dialog box appears.

> **Note:** If the Resource Name field is blank, enter it manually.
>
> For Principal, Resource Type, and Resource Name, see Table 17–1.

12. For **Permission Actions**, select **All** (_all_), and click **Select**.
13. When all the permissions are added, click **OK**.
14. Repeat Steps 5-13 for other principals and their permissions. (See Table 17–1)

Table 17–1 List of Policies and their Permissions

Policy Name/Principal	Resource Type	Resource Name	Permission Actions
FARAdminRole/EXPAdminRole	oracle.bi.catalog	*	manage
	oracle.bi.server.permission	oracle.bi.server.manageRepositories	_all_
	oracle.bi.presentation.catalogmanger.permission	oracle.bi.presentation.catalogmanger.manageCatalog	_all_
	oracle.bi.delivers.job	oracle.bi.delivers.job	manage
	oracle.bi.publisher.permission	oracle.bi.publisher.administerServer	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.developReport	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.developDataModel	_all_
	oracle.bi.repository	oracle.bi.repository	manage
	oracle.bi.scheduler.permission	oracle.bi.scheduler.manageJobs	_all_
FARSafetyAuthorRole/EXPSafetyAuthorRole	oracle.bi.publisher.permission	oracle.bi.publisher.developReport	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.developDataModel	_all_
	oracle.bi.tech.visualanalyzer.permission	oracle.bi.tech.visualanalyzer.generalAccess	_all_
	oracle.bi.delivers.job	*	schedule

Table 17–1 (Cont.) List of Policies and their Permissions

Policy Name/Principal	Resource Type	Resource Name	Permission Actions
FARSafetyConsumerRole/EXPSafetyConsumerRole	oracle.bi.publisher.permission	oracle.bi.publisher.scheduleReport	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.runReportOnline	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.accessReportOutput	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.accessOnlineReportAnalyzer	_all_
	ESSMetadataPermission	oracle.bip.ess.JobDefinition.EssBipJob	Read,Execute
	oracle.bi.publisher.permission	oracle.bi.publisher.accessExcelReportAnalyzer	_all_

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

17.3.3.2 Manage Folder Privileges

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

   For example: Login to *http://acme.oracle.com:port/analytics* with WebLogic user credentials.

2. Go to Administration > Security > Manage Privileges.

3. Add the following Catalog Roles:

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

Component	Privilege	Default Role Granted
Access	Access to Dashboards	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Access to Answers	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Access	Access to BI Composer	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Access	Access to Delivers	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Access	Access to Briefing Books	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Access to Mobile	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Access to Administration	BI Service Administrator, EXP Administrator Role, FAR Administrator Role

Component	Privilege	Default Role Granted
Access	Access to Segments	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Access to Segment Trees	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Access	Access to List Formats	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Access	Access to Metadata Dictionary	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Access	Access to Oracle BI for Microsoft Office	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Access to Oracle BI Client Installer	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Catalog Preview Pane UI	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Access to Export	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Access to KPI Builder	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Access	Access to Scorecard	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Actions	Create Navigate Actions	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Actions	Create Invoke Actions	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Actions	Save Actions containing embedded HTML	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: Catalog	Change Permissions	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Admin: Catalog	Toggle Maintenance Mode	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Manage Sessions	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Create Dashboards	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Admin: General	See sessions IDs	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Change Log Configuration	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Issue SQL Directly	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	View System Information	BI Service Administrator, EXP Administrator Role, FAR Administrator Role

Component	Privilege	Default Role Granted
Admin: General	Performance Monitor	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Manage Agent Sessions	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Manage Device Types	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Manage Map Data	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	See privileged errors	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	See SQL issued in errors	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Admin: General	Manage Global Variables	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Diagnose BI Server Query	Denied: Authenticated User
Admin: General	Manage Marketing Jobs	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Admin: General	Manage Marketing Defaults	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: Security	Manage Catalog Accounts	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: Security	Manage Privileges	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: Security	Set Ownership of Catalog Objects	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: Security	User Population - Can List Users	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
Admin: Security	User Population - Can List Catalog Groups	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
Admin: Security	User Population - Can List Application Roles	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role,
Admin: Security	Access to Permissions Dialog	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Briefing Book	Add To or Edit a Briefing Book	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Briefing Book	Download Briefing Book	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role

Component	Privilege	Default Role Granted
Briefing Book	Add to Snapshot Briefing Book	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Catalog	Personal Storage (My Folders and My Dashboard)	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Catalog	Reload Metadata	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Catalog	See Hidden Items	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Catalog	Create Folders	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Catalog	Archive Catalog	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Catalog	Unarchive Catalog	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Catalog	Upload Files	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Catalog	Perform Global Search	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Catalog	Perform Extended Search	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Conditions	Create Conditions	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Dashboards	Save Customizations	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Dashboards	Assign Default Customizations	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Dashboards	Create Bookmark Links	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Dashboards	Create Prompted Links	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Dashboards	Export Entire Dashboard To Excel	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Dashboards	Export Single Dashboard Page To Excel	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Formatting	Save System-Wide Column Formats	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Home and Header	Access Home Page	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Access Catalog UI	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Access Catalog Search UI	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Access Rapid Search UI	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role

Component	Privilege	Default Role Granted
Home and Header	Simple Search Field	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Advanced Search Link	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Open Menu	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	New Menu	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Help Menu	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Dashboards Menu	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Favorites Menu	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	My Account Link	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Custom Links	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Access Administration Menu	Denied: Authenticated User
Home and Header	Access User & Role Admin	Denied: Authenticated User
Home and Header	Access Modeler	Denied: Authenticated User
Home and Header	Access Data Loader	Denied: Authenticated User
My Account	Access to My Account	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
My Account	Change Preferences	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
My Account	Change Delivery Options	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Answers	Create Views	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Create Prompts	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Access Advanced Tab	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Edit Column Formulas	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Save Content with HTML Markup	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Answers	Enter XML and Logical SQL	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Edit Direct Database Analysis	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Answers	Create Analysis From Simple SQL	BI Service Administrator, EXP Administrator Role, FAR Administrator Role

Component	Privilege	Default Role Granted
Answers	Create Advanced Filters and Set Operations	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Save Filters	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Save Column	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Add EVALUATE_PREDICATE Function	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Execute Direct Database Analysis	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Answers	Upload Images	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Delivers	Create Agents	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Delivers	Publish Agents for Subscription	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Delivers	Deliver Agents to Specific or Dynamically Determined Users	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Delivers	Chain Agents	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Delivers	Modify Current Subscriptions for Agents	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Proxy	Act As Proxy	Denied: Authenticated User
RSS Feeds	Access to RSS Feeds	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Scorecard	Create/Edit Scorecards	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Scorecard	View Scorecards	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Scorecard	Create/Edit Objectives	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Scorecard	Create/Edit Initiatives	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Scorecard	Create Views	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Scorecard	Create/Edit Causes And Effects Linkages	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Scorecard	Create/Edit Perspectives	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Scorecard	Add Annotations	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Scorecard	Override Status	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Scorecard	Create/Edit KPIs	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role

Component	Privilege	Default Role Granted
Scorecard	Write Back to Database for KPI	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Scorecard	Add Scorecard Views To Dashboards	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
List Formats	Create List Formats	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
List Formats	Create Headers and Footers	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
List Formats	Access Options Tab	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
List Formats	Add/Remove List Format Columns	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Segmentation	Create Segments	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Segmentation	Create Segment Trees	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Segmentation	Create/Purge Saved Result Sets	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Segmentation	Access Segment Advanced Options Tab	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Segmentation	Access Segment Tree Advanced Options Tab	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Segmentation	Change Target Levels within Segment Designer	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Mobile	Enable Local Content	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Mobile	Enable Search	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access SOAP	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Impersonate as system user	BI System
SOAP	Access MetadataService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access ScorecardAssessmentService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access MsgdbService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access ReportEditingService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role

Component	Privilege	Default Role Granted
SOAP	Access KPIAssessmentService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access ConditionEvaluationService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access SecurityService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access Tenant Information	BI System
SOAP	Access SchedulerService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access DashboardService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access ScorecardMetadataService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access JobManagementService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access CatalogIndexingService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access UserPersonalizationService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access AnalysisExportViewsService Service	BI Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access CatalogService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access AdministrationSOAPService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access HtmlViewService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access XmlGenerationService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access IBotService Service	BI Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
View Canvas	Add/Edit Canvas View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Column Selector	Add/Edit Column Selector View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Compound Layout	Add/Edit Compound Layout View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role

Component	Privilege	Default Role Granted
View Contribution Wheel	Add/Edit Contribution Wheel View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Graph	Add/Edit Graph View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Funnel	Add/Edit Funnel View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Gauge	Add/Edit Gauge View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Micro Chart	Add/Edit Micro Chart View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Filters	Add/Edit Filters View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Dashboard Prompt	Add/Edit Dashboard Prompt View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Performance Tile	Add/Edit Performance Tile View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Heat Matrix	Add/Edit Heat Matrix View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Static Text	Add/Edit Static Text View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Javascript view	Edit Javascript View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Legend	Add/Edit Legend View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Map	Add/Edit Map View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Narrative	Add/Edit Narrative View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View No Results	Add/Edit No Results View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Pivot Table	Add/Edit Pivot Table View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Generic Plugin View	Add/Edit Generic Plugin View View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Report Prompt	Add/Edit Report Prompt View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Create Segment	Add/Edit Create Segment View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Selection Steps	Add/Edit Selection Steps View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Logical SQL	Add/Edit Logical SQL View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Table	Add/Edit Table View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Create Target List	Add/Edit Create Target List View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Ticker	Add/Edit Ticker View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role

Component	Privilege	Default Role Granted
View Title	Add/Edit Title View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Treemap	Add/Edit Treemap View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Trellis	Add/Edit Trellis View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View View Selector	Add/Edit View Selector View	BI Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Write Back	Manage Write Back	BI Service Administrator, EXP Administrator Role, FAR Administrator Role
Write Back	Write Back to Database	Denied: Authenticated User

4. To set Catalog Folder-level Permissions:

   a. Login to Analytics with WebLogic user credentials.

      For example, login to *http://acme.oracle.com:port/analytics*.

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

      The Permissions dialog box appears.

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

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

5. To add the Data Sources to Roles in BI Publisher:

   a. Login to the BIP with Administrator credentials.

      The BIP home page appears.

   b. Go to Administration > Roles and Permissions.

      The Roles and Permissions screen appears.

   c. From the list of roles, select **FARAdminRole**, and click the corresponding **Add Data Sources** icon.

      The Add Data Sources screen appears.

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

   e. Click **Apply**.

   f. Repeat the steps to add **asbip** data source for the following roles as well:

      - FARSafetyAuthorRole

- FARSafetyConsumerRole

- EXPAdminRole

- EXPSafetyAuthorRole

- EXPSafetyConsumerRole

17.4 Upload BI Publisher Reports

17.4.1 Flexible Aggregate Reports

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

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

   <Argus Installation Media>\SUPPORT\BIP

2. Log in to BI Publisher using BI Admin User credentials.
3. From the left pane, click **Catalog**.

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

4. Click **Shared Folders** under **Folders**.
5. Click **Upload** under **Tasks**.

   This displays the **Upload** dialog box.

6. Click **Browse** and navigate to the location where you have saved the **Argus Safety.xdrz** file on the local file system.
7. Click **Upload**. Once done, an **Argus Safety** folder is created in **Shared Folders**.
8. Expand the **Argus Safety** folder to verify whether the data model and reports are present.

To set permissions for Argus Safety Shared Folders:

1. Login to Analytics.
2. Go to Shared folders > Argus Safety > Tasks > Permissions.

   The Permissions dialog box appears.

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

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

17.4.2 PMDA R3 Paper Reports

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

The steps to upload the file remains the same as Section 17.4.1, "Flexible Aggregate Reports".

17.5 Integrate Argus Safety with BI Publisher

17.5.1 Configure AG Service

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

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

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

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

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

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

17.5.2 Configure Web Service (Expedited Reports only)

1. Log in to Argus Safety Web Server.
2. Navigate to the ArgusInstallPath in the filesystem.
3. Open the file argusvr2.config for editing.
4. Navigate to the <system.serviceModel> tag in this file.
5. In the endpoint element that lies within the client element, enter the following text in the Address attribute:

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

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

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

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

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

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

This section is applicable for Expedited Reports only.

To auto-schedule the Expedited Reports through AG Services:

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

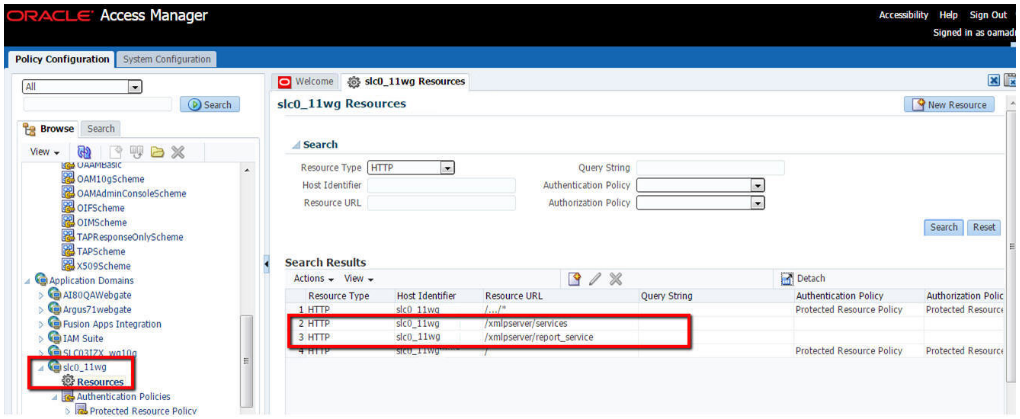
17.5.4 Update SSO Exclusion List

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

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

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

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



slc0_11wg Resources

Resource Type: HTTP

Search Results

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

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

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

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

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

   <Location /xmlpserver/services/>

require valid-user

AuthType Basic

Allow from All

Satisfy any

</Location>

4. Save the file and restart OHS Service.

17.6 Argus Console—BIP Common Settings

17.6.1 Configure BIP Reporting Admin User

1. Navigate to **Argus Console** > **System Configuration > System Management (Common Profile Switches)**.
2. Expand the **Reporting** node on the tree that appears on the left pane.
3. Click **BIP Reporting**.
4. In **Common Settings** section, enter the BIP Common username and password.

   This user is created in BI Publisher with administrator privileges. This user could be an actual Argus Safety user or a user who has No Access to Argus Safety.
5. Save the changes.

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

1. Navigate to **Argus Console** > **Enabled Modules**.
2. Enable the **BIP Aggregate Reports** module.
3. Navigate to **Argus Console > System Configuration > System Management (Common Profile Switches).**
4. Expand the **Reporting** node on the tree that appears on the left pane.
5. Click **BIP Reporting**.
6. Set the Persist data in BIP Aggregate Temp tables to **Yes** or **No**.

   The default value is **No**.
7. Set the Number of days to persist the BIP Aggregate Temp table data. Defaulted to null.
8. Perform **iisreset** on Webserver to make sure that the changes made to enable the BIP Aggregate Reports module are visible in the periodic report configuration.

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

17.6.3 Configure Code Lists

17.6.3.1 Flexible Aggregate Reporting Code Lists

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

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

> **Note:** As the REPPATH is case sensitive, in Unix based Operating System, it must be same as that provided in Report.
>
> For example, in PBRER > Code List, the REPPATH is */Argus Safety/PBRER/Reports/pbrer.xdo*
>
> The same path must be provided in the Reports and vice-versa.

17.6.3.2 PMDA R3 Paper Forms Code lists

1. Navigate to **Argus Console** > **Code Lists > Flexible Data Re-categorization**.
2. Under the **Flexible Data Re-categorization** tree, navigate to **Flexible Re-categorization**.
3. Select the **Code List Name** as **LM_REPORT_FORMS_EXPEDITED,** and click **Search**.
4. Check the **REPPATH** that is pre-configured with the report path of all the PMDA reports.

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

17.7 Configure Flexible Aggregate Reporting Database

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

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

17.7.1 Execute Argus_BIP_Enable

1. From the command prompt, navigate to

   <Argus Home>\DBInstaller\Utilities\BIP_Enable.

2. Execute the batch file Argus_BIP_Enable.bat.

3. Enter the following parameters when prompted:

   a. Enter TNSNAMES Entry to Connect to the Argus Safety Database

      Argus Safety database SID.

   b. Enter SYSTEM or DBA user name in Argus Database.

   c. Enter password for SYSTEM or DBA user password.

   d. Enter Argus schema owner name

      For example: ARGUS_APP.

   e. Enter Argus schema password.

   f. Enter BI Publisher Schema User.

      The BI Publisher Schema owner name created during Argus Safety Database Installation. For example, BIP_OWNER.

   g. Enter Password for BIP Schema User.

   h. Enter BIP Repository Service name

      Database SID of the BI Publisher metadata repository.

   i. Enter BIP Repository User name (Default DEV_BIPLATFORM).

      The BIPLATFORM user created in BI Publisher metadata repository.

   j. Enter BIP Repository Password.

   k. Enter BIP Repository Instance Fully Qualified Host Name

      For example, <hostname>.<domain name>)

   l. Enter BIP Repository Instance Listener Port

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

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

17.7.2 Database Jobs

> **Note:** Both the database jobs should be created and run as BI Publisher Schema Owner.

17.7.2.1 Report Output Pusher

A database job must be created for pushing the completed report output from BI Publisher repository to Argus Safety database. The example below executes the report output pusher for every 3 minutes. The interval can be modified as needed.

```
DECLARE
```

```
n BINARY_INTEGER;
BEGIN
DBMS_JOB.SUBMIT (job => n,
what => ' BEGIN
pkg_agg_rpt_util.p_fetchrptoutput; END ;',
interval => 'TRUNC(SYSDATE + 3/1440,''MI'')',
no_parse => FALSE);

DBMS_OUTPUT.PUT_LINE('Job Number is: ' || to_char(n));
COMMIT;
END;
/
```

17.7.2.2 Persist Data Cleaner

A database job can be created for cleaning the persist data from the BIP Owner schema's RM tables. The example below executes persist data cleaner once in every 3 minutes. The interval can be modified as needed.

```
DECLARE
n BINARY_INTEGER;
BEGIN
DBMS_JOB.SUBMIT (job => n,
what => ' BEGIN
pkg_agg_rpt_util.Purge_RM_Data; END ;',
interval => 'TRUNC(SYSDATE + 3/1440,''MI'')',
no_parse => FALSE);
DBMS_OUTPUT.PUT_LINE('Job Number is: ' || to_char(n));
COMMIT;
END;
/
```

17.8 Upgrade BIP Reports from 8.1 to 8.1.1

If you have enabled Argus Flexible Aggregate Reporting and upgrading from 8.1:

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

1. Login to the BI Publisher console as administrator (or any user who has BI Admin User access).
2. Backup the existing .xdrz files.
   a. From the left pane, click **Catalog**.

      The Catalog screen with the Folders and Tasks sections appears.

   b. Click Folders > **Shared Folders**.
   c. Click Tasks > **Download**.
   d. Click **Browse** and navigate to the location where the backup will be saved.
3. To upload the latest Argus Safety.xdrz file, see Section 17.4.1, "Flexible Aggregate Reports".

   While uploading, click **Overwrite existing files**.

18

Install Argus Unblinding

18.1 Prerequisites

1. Set Up Argus Safety Middle and Client Tiers, and follow all the chapters from 3 to 13.
2. Install Microsoft Visual Basic Power Packs 10.0
3. Tablespace with free space of 500 MB on the Database Server to create Argus Unblinding schema.
4. Set the INIT.ORA parameters as AUDIT_TRAIL=TRUE.

18.2 Install Argus Unblinding Utility

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

1. Copy the installation package files to your local directory, and start **setup.exe**.
2. Click **Argus Safety**, and click **Next**.
3. Enter the customer User Name and Company Name, and click **Next**.
4. To install the Argus Unblinding Generic software, select the Components Default Directory folder, and click **Next**.
5. In the Argus Safety Solution Components screen, select **End of Study Unblinding Module**, and click **Next**.
6. Click **Next** to continue.

   Argus Safety installation process begins and the installation progress appears.
7. In the Setup Complete screen, click **Finish**.
8. You can now run the Argus Unblinding Interface utilities.

   Besides Argus Unblinding installation, the setup also installs an *Operations Guide* and scripts to create Database schema on your computer.

   Refer to the *Operations Guide* to create a new schema to start using Argus Unblinding software. To view the guide:

- Navigate to

  <Installation Folder>\Oracle\End of Study Unblinding\ARGUS_EOSU.pdf

- Or, select Start > Programs > Oracle > End of Study Unblinding > Documentation > End of Study Unblinding Module

9. To set up the Argus Cryptography Key, refer to the section Section 21.1.3, "Argus Safety 8.1.1 Application Servers".

19

Install and Configure Argus Integrations

> **Note:** You must Set Up Argus Safety Middle and Client Tiers before installing Argus Integrations, and follow all the chapters from 3 to 13.

19.1 Install Argus Integrations

1. Click **Argus Safety** to start the installation.
2. Click **Next >**.
3. Enter the customer User Name and Company Name, and click **Next >**.
4. In the Default Directory screen, click **Browse** to select the default installation directory where the Argus Safety Solution Components will be installed, and click **Next >**.
5. In the component list, select the modules to install, and click **Next >**.
6. In the Argus Safety Solution Components Report Directory screen:
   a. Click **Browse**, select the folder to store the temporary reports in, and click **OK**.
   b. Click **Next >**.

      Argus installs and shows the progress of the installation.
7. Enter the **Port** for the Argus website (default is 8083, and can be changed to port 80 at any time), and click **Next >**.

   The installer installs the website and its related components and shows the progress of the installation.
8. In the Setup Completed screen, click **Finish**.
9. Click **OK** to reboot the system.
10. To set up the Argus Cryptography Key, refer to the section Section 21.1.3, "Argus Safety 8.1.1 Application Servers.".
11. to configure Argus Safety Service user passwords, refer to Section 21.2.4, "Generate Encrypted String."

19.2 Reset IIS

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

1. Changes in config files:

- Argus.ini
- Argus.xml

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

19.3 Argus Web Service Interface

Argus Web Service Interface supports outbound Interface (MedDRA, WHO Drug and LOT Number) which provides capability to integrate with customer hosted web services and inbound web services (Product-Study-Load Interface) hosted on Argus Safety web server.

All web service based interfaces communicate with the standard SOAP 1.2 Protocol and use WS-Addressing and WS-Security. Argus web service interface leverage Windows Communication Foundation to generate the WS-Addressing and WS-Security header information. It is recommended to test this message before moving too far into business testing. Information on these specifications can be found at the OASIS and W3C websites.

By leveraging WCF, maximum flexibility is provided to the user allowing the selection of which integrations to enable, the transport protocols to use, authentication, etc. by simply updating a standard .config file.

All errors are handled through a SOAP fault. Should an error occur, logical or otherwise, a SOAP fault should be thrown by the host and caught by the client. The client application (web) of Argus displays the details of the SOAP fault to the user when possible. Argus web services throw SOAP faults when an error occurs. Argus Safety web service interface in this release supports the following integrations through Web Service:

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

In a multi-tenant Argus system:

- Endpoint configuration of central MedDRA and WHO Drug web service is at global level. Enterprise if configured to use MedDRA and WHO Drug web service interface will use same endpoint to connect.

- Endpoint configuration of Lot Number Interface is defined at an enterprise level. Enterprise if configured to use Lot Interface will use enterprise specific endpoint configuration.
- Outbound Interface: Message payload will have 'EnterpriseShortName'.
- Inbound Interface: Argus Safety mandates 'EnterpriseShortName' as part of message payload.

19.3.1 Argus Web Service Interface Framework

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

<Argus Web Install Path>\Integrations\XSD

<Argus Web Install Path>\Integrations\WSDL

(Example: C:\Progam Files\Oracle\ArgusWeb\ASP\Integrations\XSD)

19.4 Basic Configuration Overview

19.4.1 Outbound Interface

The web.config file located in the root of the ArgusWeb directory contains all the configuration required for outbound integrations. Two default bindings have been provided, one for basic HTTP traffic and one for SSL communication. For the most basic configuration, simply updating the "address" attribute of the "endpoint" nodes to point to the correct web service address would be sufficient.

To use encryption, the "bindingConfiguration" attribute of the "endpoint" node can be set to "WSHttpBinding_IRelsysService_Secure", a binding configuration provided out of the box. As the framework utilizes WCF, additional binding configurations may be created and used as well. Note that the binding configurations between the host and the client must be compatible for successful communication.

Basic user authentication is also supported by the framework. Each endpoint has a counterpart in the ClientCredentials section of the web.config. Simply adding the proper credentials here will instruct WCF to transmit the authentication information.

The framework provides the ability to transform messages using either a custom transformation assembly or an XSLT. Some interfaces, like Lot Number and WHO Drug coding, currently leverage this feature. Activating the transformer is a simple matter of updating the 'TransformerConfiguration' section to map an endpoint to a transformer. If multiple transformers are specified for a particular endpoint, they will be executed in the order in which they appear in the configuration file. The transformers configured by Oracle should not be modified, but additional ones may be added if necessary.

19.4.2 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.

19.5 Safety Message

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

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.

19.6 MedDRA Interface

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 uses the same web service endpoint. **EnterpriseShortName** attribute present in the request message payload identifies which Enterprise has initiated the web service request.

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 refer 1.1 (without Japanese current term details) and refer 2.0(to get Japanese current term details for LLT) of MedDRA schema.

19.6.1 Examples of MedDRA Encoding Safety Message

MedDRA Interface supports (v2.0, v1.1 and v1.0) versions of the XMLs. The difference between them is that v2.0 includes support for Japanese Terms including Japanese current term details for LLT. While V1.1 also supports Japanese terms but does not include the detail whether J term is current or noncurrent. The following example uses **Pain** as the search term for encoding for each version of the XML.

19.6.1.1 Request (V 2.0)

```
<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/Rels
ysServiceRequest</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/v2.0"
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:LANG>E</tnsa:LANG>
</tnsa:TERM>
</tnsa:MEDICAL_DICTIONARY>
</tnsa:SAFETY_MESSAGE>
</d4p1:SafetyMessage>
</Msg>
</RelsysServiceRequest>
</s:Body>
</s:Envelope>
```

19.6.1.2 Response(V2.0)

```
<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"
xmlns:s="http://www.w3.org/2003/05/soap-envelope">
<s:Header>
<a:Actions:mustUnderstand="1">
http://www.oracle.com/Argus/Contract/v1.0/IRelsysServic
e/RelsysServiceRequestResponse
</a:Action>
<ActivityId CorrelationId="12dda93b-e6fa-4d3a-8d2f-a5cc34588e8a"
xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">
0000000
0-0000-0000-7600-0060000000f3
</ActivityId>
</s:Header>
<s:Body>
<RelsysServiceRequestResponse
xmlns="http://www.oracle.com/Argus/Contract/v1.0">
<RelsysServiceRequestResult xmlns:b="http://www.oracle.com/Argus/Types/v1.0"
```

```
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
<b:Version>1.0</b:Version>
<b:TransformID />
<b:SafetyMessage>
<tnsa:SAFETY_MESSAGE
xsi:noNamespaceSchemaLocation="http://www.oracle.com/Argus/MedDRA_
Response/v2.0 file:///C:/SS/6 - Argus Interfaces/ASI
6x/RelsysInterfaceLibrary.root/RelsysInterfaceLibrary/RelsysInterfaceComponents/
XSD/v2.0/MedDRA_Response.xsd" tns:Type="Response"
xmlns:tnsa="http://www.oracle.com/Argus/MedDRA_Response/v2.0"
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:TEXT_J>??</tnsa:TEXT_J>
<tnsa:CURRENCY_J>Y</tnsa:CURRENCY_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>
<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>
```

19.6.1.3 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/Rels
ysServiceRequest</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>
```

19.6.1.4 Response (V 1.1)

```
<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"
xmlns:s="http://www.w3.org/2003/05/soap-envelope">
<s:Header>
<a:Actions:mustUnderstand="1">
http://www.oracle.com/Argus/Contract/v1.0/IRelsysServic
e/RelsysServiceRequestResponse
</a:Action>
<ActivityId CorrelationId="12dda93b-e6fa-4d3a-8d2f-a5cc34588e8a"
xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">
0000000
0-0000-0000-7600-0060000000f3
</ActivityId>
</s:Header>
<s:Body>
<RelsysServiceRequestResponse
xmlns="http://www.oracle.com/Argus/Contract/v1.0">
<RelsysServiceRequestResult xmlns:b="http://www.oracle.com/Argus/Types/v1.0"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
<b:Version>1.0</b:Version>
<b:TransformID />
<b:SafetyMessage>
```

```
<tnsa:SAFETY_MESSAGE
xsi:noNamespaceSchemaLocation="http://www.oracle.com/Argus/MedDRA_
Response/v1.1 file:///C:/SS/6 - Argus Interfaces/ASI
6x/RelsysInterfaceLibrary.root/RelsysInterfaceLibrary/RelsysInterfaceComponents/
XSD/v1.1/MedDRA_Response.xsd" tns:Type="Response"
xmlns:tnsa="http://www.oracle.com/Argus/MedDRA_Response/v1.1"
xmlns:tns="http://www.oracle.com/Argus/Base/v1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<tnsa:MEDICAL_DICTIONARY>
<tnsa:PATHS>
<tnsa:PATH Primary="Y">
<tnsa:LLT>
<tnsa:TEXT>Pain</tnsa:TEXT>
<tnsa:CODE>10033371</tnsa:CODE>
<tnsa:TEXT_J>??</tnsa:TEXT_J>
<tnsa:SYNS />
</tnsa:LLT>
<tnsa:PT>
<tnsa:TEXT>Pain</tnsa:TEXT>
<tnsa:CODE>100333712</tnsa:CODE>
<tnsa:TEXT_J>??</tnsa:TEXT_J>
</tnsa:PT>
<tnsa:HLT>
<tnsa:TEXT>Pain and discomfort NEC</tnsa:TEXT>
<tnsa:CODE>10033372</tnsa:CODE>
<tnsa:TEXT_J>????????NEC</tnsa:TEXT_J>
</tnsa:HLT>
<tnsa:HLGT>
<tnsa:TEXT>General system disorders NEC</tnsa:TEXT>
<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>
```

19.6.1.5 Request (V 1.0)

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing">
<s:Header>
<a:Action
s:mustUnderstand="1">
http://www.oracle.com/Argus/Contract/v1.0/IRelsysServic
e/RelsysServiceRequest
</a:Action>
```

```
<a:MessageID>urn:uuid:c5b40ac0-a11e-44ea-b3c5-a39636058d63</a:MessageID>
<ActivityId CorrelationId="1872b16d-c293-4abc-8e5c-9ecdab7d3147"
xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">
0000000
0-0000-0000-3100-0060000000f0
</ActivityId>
<a:ReplyTo>
<a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
</a:ReplyTo>
<a:To s:mustUnderstand="1">http://10.178.87.5/interface/RelsysService.svc</a:To>
</s:Header>
<s:Body>
<RelsysServiceRequest xmlns="http://www.oracle.com/Argus/Contract/v1.0">
<Msg xmlns:d4p1="http://www.oracle.com/Argus/Types/v1.0"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
<d4p1:Version>1.0</d4p1:Version>
<d4p1:TransformID />
<d4p1:SafetyMessage>
<tnsa:SAFETY_MESSAGE xmlns:tns="http://www.oracle.com/Argus/Base/v1.0"
xmlns:tnsa="http://www.oracle.com/Argus/MedDRA_Request/v1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" tns:Type="Request">
<tnsa:MEDICAL_DICTIONARY Action="Auto" Source="INDICATION">
<tnsa:TERM>
<tnsa:REPORTED>pain</tnsa:REPORTED>
<tnsa:CODED>pain</tnsa:CODED>
</tnsa:TERM>
</tnsa:MEDICAL_DICTIONARY>
</tnsa:SAFETY_MESSAGE>
</d4p1:SafetyMessage>
</Msg>
</RelsysServiceRequest>
</s:Body>
</s:Envelope>
```

19.6.1.6 Response (V 1.0)

```
<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"
xmlns:s="http://www.w3.org/2003/05/soap-envelope">
<s:Header>
<a:Action
s:mustUnderstand="1">
http://www.oracle.com/Argus/Contract/v1.0/IRelsysServic
e/RelsysServiceRequestResponse
</a:Action>
<ActivityId CorrelationId="12dda93b-e6fa-4d3a-8d2f-a5cc34588e8a"
xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">
0000000
0-0000-0000-7600-0060000000f3
</ActivityId>
</s:Header>
<s:Body>
<RelsysServiceRequestResponse
xmlns="http://www.oracle.com/Argus/Contract/v1.0">
<RelsysServiceRequestResult xmlns:b="http://www.oracle.com/Argus/Types/v1.0"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
<b:Version>1.0</b:Version>
<b:TransformID />
<b:SafetyMessage>
MedDRA Integration
14-10 Oracle Argus Safety Installation Guide
```

```
<tnsa:SAFETY_MESSAGE
xsi:noNamespaceSchemaLocation="http://www.oracle.com/Argus/MedDRA_
Response/v1.0 file:///C:/SS/6 - Argus Interfaces/ASI
6x/RelsysInterfaceLibrary.root/RelsysInterfaceLibrary/RelsysInterfaceComponents/
XSD/v1.0/MedDRA_Response.xsd" tns:Type="Response"
xmlns:tnsa="http://www.oracle.com/Argus/MedDRA_Response/v1.0"
xmlns:tns="http://www.oracle.com/Argus/Base/v1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<tnsa:MEDICAL_DICTIONARY>
<tnsa:PATHS>
<tnsa:PATH Primary="Y">
<tnsa:LLT>
<tnsa:TEXT>Pain</tnsa:TEXT>
<tnsa:CODE>10033371</tnsa:CODE>
<tnsa:SYNS />
</tnsa:LLT>
<tnsa:PT>
<tnsa:TEXT>Pain</tnsa:TEXT>
<tnsa:CODE>100333712</tnsa:CODE>
</tnsa:PT>
<tnsa:HLT>
<tnsa:TEXT>Pain and discomfort NEC</tnsa:TEXT>
<tnsa:CODE>10033372</tnsa:CODE>
</tnsa:HLT>
<tnsa:HLGT>
<tnsa:TEXT>General system disorders NEC</tnsa:TEXT>
<tnsa:CODE>10018073</tnsa:CODE>
</tnsa:HLGT>
<tnsa:SOC>
<tnsa:TEXT>General disorders and administration site conditions</tnsa:TEXT>
<tnsa:CODE>10018065</tnsa:CODE>
</tnsa:SOC>
</tnsa:PATH>
</tnsa:PATHS>
</tnsa:MEDICAL_DICTIONARY>
<tns:EXTENSION>
<tns:CUSTOM tns:Name="string" tns:Metadata="string">string</tns:CUSTOM>
</tns:EXTENSION>
</tnsa:SAFETY_MESSAGE>
</b:SafetyMessage>
</RelsysServiceRequestResult>
</RelsysServiceRequestResponse>
</s:Body>
</s:Envelope>
```

19.6.2 MedDRA Dictionary: XML Schema

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

Validate the MedDRA Interface request and response for the following schema files.

19.6.2.1 Request: MEDDRA_Request

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

- Schema File

  Version 1.0

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

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

Version 2.0

Top level file: \v2.0\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

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

  where, v 1.0,1.1, 2.0 is the version of the schema

- Node/Attribute Name Description

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

19.6.2.2 Request: MEDDRA_Response

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

Node/Attribute Name	Description
Action	An enumeration supporting the following values (currently only one): Auto **Auto**—This attribute will be present in the request when a full hierarchy is required to be passed back to auto encode the term without using the MedDRA Browser. With an "Auto" message, the system requires that an LLT Term be passed in the request. If the full Hierarchy is not found / returned, the system will open the MedDRA Browsers and display the LLTs returned for manual encoding by the user using the local MedDRA instance. If multiple paths are returned, the Primary SOC path will be used.

Node/Attribute Name	Description
Source	An enumerated value that specifies additional information that may be required for coding based on origination as follows: ■ Reaction Case Form | Patient Tab | Patient Tab | Other Relevant History | Reaction Case Form | Patient Tab | Parent Tab | Other Relevant History | Reaction ■ Indication Case Form | Patient Tab | Patient Tab | Other Relevant History | Indication Case Form | Patient Tab | Parent Tab | Other Relevant History | Indication ■ Condition should be verbatim Case Form | Patient Tab | Patient Tab | Other Relevant History | Verbatim Case Form | Patient Tab | Parent Tab | Other Relevant History | Verbatim ■ Lab Console | Code Lists | Lab Test Type ■ Description Case Form | Events Tab | Event Tab | Description to be Coded Case Form | Events Tab | Death Information | Cause of Death and Autopsy Results | Description as Reported ■ Diagnosis Argus Case Form | Analysis Tab | Analysis Tab| Company Diagnosis Syndrome
Term (v 1.0)1.1/2.0)	The TERM node specifies the information about a specific term that is either being looked up or populated with data and supports Reported and Coded nodes.
Term (v 1.1/2.0)	The TERM node specifies the information about a specific term that is either being looked up or populated with data and supports Reported, Coded, and Lang nodes.

19.6.2.3 Request: MEDDRA_Response

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

- Schema File

  Version 1.0

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

  Sub level file: \v1.0\Base.xsd

  Version 1.1

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

  Version 2.0

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

- Namespace

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

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

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

where, v 1.0,1.1, 2.0 is the version of the schema

- Node/Attribute Name Description

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 without Currency_J (Japanese term is current or noncurrent) Details.
PATHS/PATH (version 2.0)	MedDRA Hierarchy with English and Japanese Terms with Currency_ J(Japanese term is current or noncurrent) Detail for LLT term.

19.6.3 MedDRA Auto Encoding Flow

When Argus Safety makes a call to the web service, it populates the REPORTED and CODED nodes with data entered by the user. The REPORTED term is essentially a verbatim while the coded term is the term that is expected to be coded by the remote system. The returned message contains a PATHS node with PATH sub-nodes that have been encoded by the remote system. Argus Safety displays the returned LLTs in the MedDRA browser from which you can select the correct LLT (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 Safety loads the MedDRA browser with local dictionary information, if the system is configured to allow this.

19.6.4 MedDRA 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">
```

Besides, the Argus .Net/web.config file on each web server should also have the correct Value for the Key MedDRAXMLVersion depending on which version of MedDRA XML is used. For example:

– *<add key="MedDRAXMLVersion" value="2.0"/>*, or

– *<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\v2.0\MedDRA_Response.xsd" />*

– *<add InputXSD="..\..\Integrations\XSD\v2.0\MedDRA_Request.xsd" />*

19.7 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 Generate Encrypted String section.

  A sample configuration would be:

  ```
  <DatabaseConfiguration DBName="ARGOLDDEMO" DBUser="agservice1"
  DBPassword="BC90A10363A26C147DEF172D61AAEC110296FA9E181E7FFA687D58CE08610C08"
  />
  ```

- **Security Configuration**

  If the PSL web service is desired to be run under security, appropriate binding configurations need to be configured in web.config under the Integrations folder. This can be done either manually or through the Service Config Utility.

- **Logging**

PSL Web service performs two kinds of logging. One is file logging using the Relsys Logger. This involves logging information about the errors, warnings, and processing of the PSL web service code. The configuration for this type of logging is present in web.config, under the section <logConfig>. There are four types of logging - Error, Warning, Information, and Verbose. By default, the logger is configured to be of Error level. The logger internally uses log4net component to perform the logging. The RollingLogFileAppender which is by default present in web.config needs to be configured to log information to a specific file on a local folder. Ensure that read/write permissions are available to the web service for this folder.

Another type of logging is the SOAP message logger, called the RequestLogger. This logger logs all the incoming and outgoing SOAP messages of the PSL web service. The messages are stored internally in the Argus Safety Database and are not available for querying in this release. This logging can be turned off by setting the Enabled attribute to false in Service.config as shown below:

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

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

19.8 WHO Drug Coding Interface

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

In a multi-tenant setup, endpoint configuration of central WHO drug coding web service is stored at global level and all enterprises in Argus Safety will use the same web service endpoint. 'EnterpriseShortName' attribute will be present in the request message payload to identify which Enterprise initiated the web service request.

19.8.1 Example of WHO Drug Coding Safety Message

19.8.1.1 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>
```

19.8.1.2 Response

```
<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"
xmlns:s="http://www.w3.org/2003/05/soap-envelope">
  <s:Header>
    <a:Action
    s:mustUnderstand="1">
      http://www.oracle.com/Argus/Contract/v1.0/IRelsysServic
      e/RelsysServiceRequestResponse
    </a:Action>
    <ActivityId CorrelationId="ffb00b07-d1f8-4fa9-ae9f-488d79dda872"
    xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">
      0000000
      0-0000-0000-8f0f-0060010000f1
    </ActivityId>
  </s:Header>
  <s:Body>
    <RelsysServiceRequestResponse
    xmlns="http://www.oracle.com/Argus/Contract/v1.0">
      <RelsysServiceRequestResult
      xmlns:d4p1="http://www.oracle.com/Argus/Types/v1.0"
      xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
        <d4p1:Version>1.0</d4p1:Version>
        <d4p1:TransformID />
        <d4p1:SafetyMessage>
          <tnsa:SAFETY_MESSAGE xmlns:tns="http://www.oracle.com/Argus/Base/v1.0"
          xmlns:tnsa="http://www.oracle.com/Argus/WHODrug_Response/v1.0"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:schemaLocation="http://www.oracle.com/Argus/WHODrug_Response/v1.0
file:///E:/6%20-%20Argus%20Interfaces/ASI%2042%20SP3/RelsysInterfaceLibrary.r
```

```
oot/RelsysInterfaceLibrary/RelsysInterfaceComponents/XSD/v1.0/WHODrug_
Response.xsd" tns:Type="Response">
      <tnsa:DRUG_DICTIONARY>
       <tnsa:DRUGS>
        <tnsa:DRUG>
         <tnsa:DRUG_CODE>000200.01.005</tnsa:DRUG_CODE>
         <tnsa:DRUG_NAME>TYLENOL</tnsa:DRUG_NAME>
         <tnsa:GENERIC_NAME>PARACETAMOL</tnsa:GENERIC_NAME>
         <tnsa:ATCS>
          <tnsa:ATC>
           <tnsa:CODE>65GGH</tnsa:CODE>
           <tnsa:DESCRIPTION>ATC Desc 1a</tnsa:DESCRIPTION>
          </tnsa:ATC>
          <tnsa:ATC>
           <tnsa:CODE>94534</tnsa:CODE>
           <tnsa:DESCRIPTION>ATC Desc 2a</tnsa:DESCRIPTION>
          </tnsa:ATC>
         </tnsa:ATCS>
         <tnsa:INGREDIENTS>
          <tnsa:INGREDIENT>PARACETAMOL</tnsa:INGREDIENT>
         </tnsa:INGREDIENTS>
         <tnsa:MEDICINAL_PRODUCT_ID />
         <tnsa:DRUG_MANUFACTURER>
          MCNEIL LABORATORIES,
          INCORPORATED
         </tnsa:DRUG_MANUFACTURER>
        </tnsa:DRUG>
        <tnsa:DRUG>
         <tnsa:DRUG_CODE>
          004468.01 begin_of_the_skype_highlighting 004468.01
          end_of_the_skype_highlighting.003
         </tnsa:DRUG_CODE>
         <tnsa:DRUG_NAME>TYLENOL ALLERGY SINUS</tnsa:DRUG_NAME>
         <tnsa:GENERIC_NAME />
         <tnsa:ATCS>
          <tnsa:ATC>
           <tnsa:CODE>4UUT1</tnsa:CODE>
           <tnsa:DESCRIPTION>ATC Desc 1b</tnsa:DESCRIPTION>
          </tnsa:ATC>
          <tnsa:ATC>
           <tnsa:CODE>13LLP</tnsa:CODE>
           <tnsa:DESCRIPTION>ATC Desc 2b</tnsa:DESCRIPTION>
          </tnsa:ATC>
         </tnsa:ATCS>
         <tnsa:INGREDIENTS>
          <tnsa:INGREDIENT>PARACETAMOL</tnsa:INGREDIENT>
          <tnsa:INGREDIENT>CHLORPHENAMINE MALEATE</tnsa:INGREDIENT>
          <tnsa:INGREDIENT>
           PSEUDOEPHEDRINE
           HYDROCHLORIDE
          </tnsa:INGREDIENT>
         </tnsa:INGREDIENTS>
         <tnsa:MEDICINAL_PRODUCT_ID />
         <tnsa:DRUG_MANUFACTURER>JOHNSON</tnsa:DRUG_MANUFACTURER>
        </tnsa:DRUG>
       </tnsa:DRUGS>
      </tnsa:DRUG_DICTIONARY>
      <tns:EXTENSION>
       <tns:CUSTOM tns:Name="" tns:Metadata="" />
      </tns:EXTENSION>
```

```
        </tnsa:SAFETY_MESSAGE>
      </d4p1:SafetyMessage>
    </RelsysServiceRequestResult>
  </RelsysServiceRequestResponse>
 </s:Body>
</s:Envelope>
```

19.8.2 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.

19.8.2.1 Request: WHODrug_Request

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

Schema File

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

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.

19.8.2.2 Response: WHODrug_Response

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

Schema File

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

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

19.8.3 Drug Dictionary Coding Flow

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

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

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

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

19.9 Lot Number Interface

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

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

19.9.1 Example of Lot Number Safety Message

19.9.1.1 Request

```
<s:Envelope xmlns:a="http://www.w3.org/2005/08/addressing"
xmlns:s="http://www.w3.org/2003/05/soap-envelope">
  <s:Header>
    <a:Action
    s:mustUnderstand="1">
      http://www.oracle.com/Argus/Contract/v1.0/IRelsysServic
      e/RelsysServiceRequest
    </a:Action>
    <a:MessageID>urn:uuid:4ea4a68c-9930-4681-a3dd-839b04821320</a:MessageID>
    <ActivityId CorrelationId="b7b67964-6e82-46d7-97ed-ff0e9f36dc66"
    xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">
      0000000
      0-0000-0000-0000-000000000000
    </ActivityId>
    <a:ReplyTo>
      <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
    </a:ReplyTo>
  </s:Header>
  <s:Body>
    <RelsysServiceRequest xmlns="http://www.oracle.com/Argus/Contract/v1.0">
      <Msg xmlns:d4p1="http://www.oracle.com/Argus/Types/v1.0"
      xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
        <d4p1:Version>1.0</d4p1:Version>
        <d4p1:TransformID>LOT_NUMBER</d4p1:TransformID>
        <d4p1:SafetyMessage>
          <tnsb:SAFETY_MESSAGE xmlns:tns="http://www.oracle.com/Argus/Base/v1.0"

xmlns:tnsa="http://www.oracle.com/Argus/ProductFamilyEntity/v1.0"xmlns:tnsb="http:
//www.oracle.com/Argus/Lot_Request/v1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" tns:Type="Request">
            <tnsb:LOT_LOOKUP>
              <tnsb:LOT>
                <tnsa:LOT_NUMBER>666</tnsa:LOT_NUMBER>
              </tnsb:LOT>
            </tnsb:LOT_LOOKUP>
          </tnsb:SAFETY_MESSAGE>
        </d4p1:SafetyMessage>
      </Msg>
    </RelsysServiceRequest>
  </s:Body>
</s:Envelope>
```

19.9.1.2 Response

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action s:mustUnderstand="1">
      http://www.oracle.com/Argus/Contract/v1.0/IRelsysServic
      e/RelsysServiceRequestResponse
    </a:Action>
    <a:RelatesTo>urn:uuid:4ea4a68c-9930-4681-a3dd-839b04821320</a:RelatesTo>
  </s:Header>
  <s:Body>
    <RelsysServiceRequestResponse
    xmlns="http://www.oracle.com/Argus/Contract/v1.0">
      <RelsysServiceRequestResult xmlns:b="http://www.oracle.com/Argus/Types/v1.0"
      xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
        <b:Version>1.0</b:Version>
        <b:TransformID />
        <b:SafetyMessage>
          <tnsb:SAFETY_MESSAGE
          tns:Type="Response"
          xmlns:tnsb="http://www.oracle.com/Argus/Lot_Response/v1.0"
          xmlns:tns="http://www.oracle.com/Argus/Base/v1.0"
          xmlns:tnsa="http://www.oracle.com/Argus/ProductFamilyEntity/v1.0"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <tnsb:LOT_LOOKUP>
              <tnsb:LOT>
                <tnsa:LOT_NUMBER>5043AX1</tnsa:LOT_NUMBER>
                <tnsa:EXPIRATION_DATE>2010-06-07</tnsa:EXPIRATION_DATE>
                <tns:CUSTOM tns:Name="Thermisol" tns:Metadata="Thermisol
Indicator">15</tns:CUSTOM>
                <tns:CUSTOM tns:Name="Albumin" tns:Metadata="Albumin
Status">11.4mg/gC</tns:CUSTOM>
              </tnsb:LOT>
              <tnsb:LOT>
                <tnsa:LOT_NUMBER>javascript</tnsa:LOT_NUMBER>
                <tnsa:EXPIRATION_DATE>2014-12-15</tnsa:EXPIRATION_DATE>
                <tns:CUSTOM tns:Name="Thermisol"
tns:Metadata="ThermisolIndicator">22</tns:CUSTOM>
                <tns:CUSTOM tns:Name="Albumin" tns:Metadata="Albumin
Status">19.5mg/gC</tns:CUSTOM>
              </tnsb:LOT>
            </tnsb:LOT_LOOKUP>
            <tns:EXTENSION>
              <tns:CUSTOM tns:Name="string"
tns:Metadata="string">string</tns:CUSTOM>
              <tns:CUSTOM tns:Name="string"
tns:Metadata="string">string</tns:CUSTOM>
            </tns:EXTENSION>
          </tnsb:SAFETY_MESSAGE>
        </b:SafetyMessage>
      </RelsysServiceRequestResult>
    </RelsysServiceRequestResponse>
  </s:Body>
</s:Envelope>
```

19.9.2 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.

19.9.2.1 Request: Lot_Request

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

Schema File

Top level file:

\v1.0\Lot_Request.xsd

Sub level file:

\v1.0\Base.xsd

\v1.0\ProductFamilyEntity.xsd

Namespace

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

where version 1.0 is the version of the schema

Nodes/Attributes

Attribute/Node name	Description
LOT_LOOKUP	First Child node under SAFETY_MESSAGE which represents the Lot integration
LOT	Argus defined complex type element having following elements and attributes: ■ LOT_NUMBER ■ EXPIRATION_DATE

19.9.2.2 Response: Lot_Response

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

Schema File

Top level file:

/v1.0/Lot_Response.xsd

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.

Attribute/Node name	Description
LOT	■ LOT Number ■ Expiration Date ■ Custom Provides a mechanism **Name**: Attribute value is used to identify Case Form field that is to be populated with data in the node **Metadata**: Attribute value is used as labels in the LOT Number selection selection dialog displaying the data

19.9.3 Lot Validation Flow

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

Argus reaction to various counts of returned lots:

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

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

19.9.4 Configuration

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

- **Use Centralized Lot Number Validation**

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

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

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

  Yes—Allows user to enter non-configured Lot Number
  No—Mandates user to only select Lot Number from Lot Lookup Dialog.

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

- **Lot Number Web Service Configuration XML**

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

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

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

  The endpoint configuration might look something like this:

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

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

- **Lot Number Web Service XSLT**

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

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

19.9.5 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.

19.10 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.

19.10.1 Worklist Intake Flow

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

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

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

1. Accept—When the user accepts an Intake, the case form book-in screen is shown which will contain information and attachments pre-populated from the Intake record.

   - If user books in a case, a response is generated which contains the case ID and case number. The attachment details and response XML are placed in the Out folder.

   - If user adds a follow up to an existing case, a similar response is generated as above and the response XML is placed in the OUT folder.

2. Reject—When the user rejects an Intake record, a response is generated which contains the Rejection Reason and the attachment details. This response XML is placed in the OUT folder.

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

19.10.2 Example of Worklist Intake Safety Message

Request—Worklist Intake Safety Message (Multi-Tenant System)

```
<?xml version="1.0" encoding="utf-8"?>
<tnsc:SAFETY_MESSAGE
xmlns:tnszz="http://www.oracle.com/Argus/Base/v1.0"
xmlns:tnsc="http://www.oracle.com/Argus/Case_Intake/v1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
tnszz:Type="Request" tnszz:EnterpriseShortName ="ENT01">
<tnsc:CASE_INTAKE>
<tnsc:CASES>
<tnsc:CASE>
<tnsc:CASE_TYPE>Spontaneous</tnsc:CASE_TYPE>
<tnsc:COUNTRY_OF_INCIDENCE>UNITED STATES</tnsc:COUNTRY_OF_INCIDENCE>
<tnsc:EVENT_PT>Pain</tnsc:EVENT_PT>
<tnsc:EVENT_VERBATIM>Pain</tnsc:EVENT_VERBATIM>
<tnsc:FLTH>LT</tnsc:FLTH>
<tnsc:GENERIC_NAME>D-RIBOSE</tnsc:GENERIC_NAME>
<tnsc:INITIAL_DATE>2012-01-31</tnsc:INITIAL_DATE>
<tnsc:PRIORITY>1</tnsc:PRIORITY>
<tnsc:PRODUCT_NAME>Cure All</tnsc:PRODUCT_NAME>
<tnsc:REPORTER_TYPE>Health Care Professional</tnsc:REPORTER_TYPE>
<tnsc:SITE>US</tnsc:SITE>
<tnsc:STUDY_ID>STUDY 001</tnsc:STUDY_ID>
<tnsc:SUR>No</tnsc:SUR>
<tnsc:ATTACHMENTS xmlns:tnsc="http://www.oracle.com/Argus/Case_Intake/v1.0">
<tnsc:ATTACHMENT>
<tnsc:FILENAME>Case12345.pdf</tnsc:FILENAME>
<tnsc:DOCID>001219988776655</tnsc:DOCID>
<tnsc:CLASSIFICATION>CIRM Case</tnsc:CLASSIFICATION>
<tnsc:ATTACHMENT_DESC>Contains case data for 12345</tnsc:ATTACHMENT_DESC>
</tnsc:ATTACHMENT>
</tnsc:ATTACHMENTS >
</tnsc:CASE>
</tnsc:CASES>
</tnsc:CASE_INTAKE>
<tnszz:EXTENSION>
<tnszz:CUSTOM tnszz:Name="My Name" tnszz:Metadata="My Metadata">My
Value</tnszz:CUSTOM>
</tnszz:EXTENSION>
</tnsc:SAFETY_MESSAGE>
```

Response—Worklist Intake Safety Message (Multi-Tenant system)

```
<?xml version="1.0" encoding="utf-8"?>
<tnse:SAFETY_MESSAGE xmlns:tns="http://www.oracle.com/Argus/Base/v1.0"
xmlns:tnse="http://www.oracle.com/Argus/Case_Intake_Ack/v1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:a="http://tempuri.org/CaseIntakeResponse.xsd"
tns:Type="Response"> tns:EnterpriseShortName="ENT01">
<tnse:CASE_INTAKE>
```

```
<tnse:CASES>
<tnse:CASE>
<tnse:INTAKE_DATE>03-NOV-2014 10:08:49</tnse:INTAKE_DATE>
<tnse:CASE_NUMBER>12US000000001</tnse:CASE_NUMBER>
<tnse:CASE_ID>10285117</tnse:CASE_ID>
<tnse:CASE_PRODUCT>Cure All</tnse:CASE_PRODUCT>
<tnse:DATE_TIME>03-NOV-2014 15:40:07</tnse:DATE_TIME>
<tnsc:ATTACHMENTS xmlns:tnsc="http://www.oracle.com/Argus/Case_Intake/v1.0">
<tnsc:ATTACHMENT>
<tnsc:FILENAME>Case12345.pdf</tnsc:FILENAME>
<tnsc:DOCID>001219988776655</tnsc:DOCID>
<tnsc:CLASSIFICATION></tnsc:CLASSIFICATION>
<tnsc:ATTACHMENT_DESC>Contains case data for 12345</tnsc:ATTACHMENT_DESC>
</tnsc:ATTACHMENT>
</tnsc:ATTACHMENTS>
</tnse:CASE>
</tnse:CASES>
</tnse:CASE_INTAKE>
<tnszz:EXTENSION xmlns:tnszz="http://www.oracle.com/Argus/Base/v1.0">
<tnszz:CUSTOM tnszz:Name="My Name" tnszz:Metadata="My Metadata">My
Value</tnszz:CUSTOM>
</tnszz:EXTENSION>
</tnse:SAFETY_MESSAGE>
```

Request—Worklist Intake Safety Message (Single-Tenant System)

```
<?xml version="1.0" encoding="utf-8"?>
<tnsc:SAFETY_MESSAGE
xmlns:tnszz="http://www.oracle.com/Argus/Base/v1.0"
xmlns:tnsc="http://www.oracle.com/Argus/Case_Intake/v1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
tnszz:Type="Request"
<tnsc:CASE_INTAKE>
<tnsc:CASES>
<tnsc:CASE>
<tnsc:CASE_TYPE>Spontaneous</tnsc:CASE_TYPE>
<tnsc:COUNTRY_OF_INCIDENCE>UNITED STATES</tnsc:COUNTRY_OF_INCIDENCE>
<tnsc:EVENT_PT>Pain</tnsc:EVENT_PT>
<tnsc:EVENT_VERBATIM>Pain</tnsc:EVENT_VERBATIM>
<tnsc:FLTH>LT</tnsc:FLTH>
<tnsc:GENERIC_NAME>D-RIBOSE</tnsc:GENERIC_NAME>
<tnsc:INITIAL_DATE>2012-01-31</tnsc:INITIAL_DATE>
<tnsc:PRIORITY>1</tnsc:PRIORITY>
<tnsc:PRODUCT_NAME>Cure All</tnsc:PRODUCT_NAME>
<tnsc:REPORTER_TYPE>Health Care Professional</tnsc:REPORTER_TYPE>
<tnsc:SITE>US</tnsc:SITE>
<tnsc:STUDY_ID>STUDY 001</tnsc:STUDY_ID>
<tnsc:SUR>No</tnsc:SUR>
<tnsc:ATTACHMENTS xmlns:tnsc="http://www.oracle.com/Argus/Case_Intake/v1.0">
<tnsc:ATTACHMENT>
<tnsc:FILENAME>Case12345.pdf</tnsc:FILENAME>
<tnsc:DOCID>001219988776655</tnsc:DOCID>
<tnsc:CLASSIFICATION>CIRM Case</tnsc:CLASSIFICATION>
<tnsc:ATTACHMENT_DESC>Contains case data for 12345</tnsc:ATTACHMENT_DESC>
</tnsc:ATTACHMENT>
</tnsc:ATTACHMENTS >
</tnsc:CASE>
</tnsc:CASES>
</tnsc:CASE_INTAKE>
<tnszz:EXTENSION>
<tnszz:CUSTOM tnszz:Name="My Name" tnszz:Metadata="My Metadata">My
```

```
Value</tnszz:CUSTOM>
</tnszz:EXTENSION>
</tnsc:SAFETY_MESSAGE>
```

Response—Worklist Intake Safety Message (Single-Tenant system)

```
<?xml version="1.0" encoding="utf-8"?>
<tnse:SAFETY_MESSAGE xmlns:tns="http://www.oracle.com/Argus/Base/v1.0"
xmlns:tnse="http://www.oracle.com/Argus/Case_Intake_Ack/v1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:a="http://tempuri.org/CaseIntakeResponse.xsd"
tns:Type="Response">
<tnse:CASE_INTAKE>
<tnse:CASES>
<tnse:CASE>
<tnse:INTAKE_DATE>03-NOV-2014 10:08:49</tnse:INTAKE_DATE>
<tnse:CASE_NUMBER>12US000000001</tnse:CASE_NUMBER>
<tnse:CASE_ID>10285117</tnse:CASE_ID>
<tnse:CASE_PRODUCT>Cure All</tnse:CASE_PRODUCT>
<tnse:DATE_TIME>03-NOV-2014 15:40:07</tnse:DATE_TIME>
<tnsc:ATTACHMENTS xmlns:tnsc="http://www.oracle.com/Argus/Case_Intake/v1.0">
<tnsc:ATTACHMENT>
<tnsc:FILENAME>Case12345.pdf</tnsc:FILENAME>
<tnsc:DOCID>001219988776655</tnsc:DOCID>
<tnsc:CLASSIFICATION></tnsc:CLASSIFICATION>
<tnsc:ATTACHMENT_DESC>Contains case data for 12345</tnsc:ATTACHMENT_DESC>
</tnsc:ATTACHMENT>
</tnsc:ATTACHMENTS>
</tnse:CASE>
</tnse:CASES>
</tnse:CASE_INTAKE>
<tnszz:EXTENSION xmlns:tnszz="http://www.oracle.com/Argus/Base/v1.0">
<tnszz:CUSTOM tnszz:Name="My Name" tnszz:Metadata="My Metadata">My
Value</tnszz:CUSTOM>
</tnszz:EXTENSION>
</tnse:SAFETY_MESSAGE>
```

19.10.3 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.

19.11 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 fie format)

19.11.1 Literature Intake Flow

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

- Accept
- Reject
- Assign User
- Assign Literature Type
- Modify Product Family

19.11.2 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.

19.11.2.1 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>
```

19.12 Extended E2B Interface

For details, refer to the *ICSR Extension Guide*.

20

Configure Argus Centralized Coding

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

20.1 setup_centralized_coding_interface_schema.bat

This batch file creates the schema objects for the Argus Centralized Coding Interface schema.

This script also updates the coding status field with the current status for existing cases for the following fields. The code status fields displays whether all events are encoded and are in a coding state or if the case has codeable items as not coded.

- LM_LAB_TEST_TYPES.CODE_STATUS
- LM_LABELED_TERMS.CODE_STATUS
- LM_PRODUCT.IND_CODE_STATUS
- CASE_EVENT.CODE_STATUS
- CASE_DEATH_DETAILS.CAUSE_CODE_STATUS
- CASE_PROD_INDICATIONS.IND_CODE_STATUS
- CASE_PAT_HIST.ITEM_CODE_STATUS
- CASE_ASSESS.DIAGNOSIS_CODE_STATUS

To execute the batch file:

1. Double-click the **setup_centralized_coding_interface_schema.bat** file, and enter:

   a. log folder name

   b. database name

   c. DBA user credentials, such as system and password

   d. RLS schema owner name and password

      Execute the following query to get the RLS schema owner name:

      ```
      SELECT owner
      FROM all_objects
      WHERE object_name = PKG_RLS AND object_type = PACKAGE;
      ```

   e. Argus schema owner name, such as ARGUS_APP and password

   f. Argus Safety role name

The script creates two users, ARGUS_DMS and DMS_LOGIN, and their tablespaces.

The Interface schema object is present in the ARGUS_DMS schema.

2. Enter the following:

   a. password for user ARGUS_DMS

   b. password for user DMS_LOGIN

   c. temporary tablespace name.

      If no input is provided, TEMP tablespace is taken by default.

      The script creates two tablespaces: DMS_DATA_01.DBF, and DMS_INDEX_01.DBF..

   d. path and data file name of the tablespaces, such as:

      C:\APP\ORADATA\DBNAMD\DMS_DATA_01.DBF

      C:\APP\ORADATA\DBNAMD\DMS_INDEX_01.DBF

   e. a log file name

3. Press Enter when the Users and Roles are located.

4. Verify the log file to validate the successful completion of the script.

5. Log in to the application and enable the Centralized Coding module.

   Configure Centralized Coding from the dictionary selection page in the Console.

20.2 dms_migration.bat

Execute this script to populate the already encoded terms from all cases to the Interface schema table. This script supports two types of migration:

- Single Enterprise Migration in One Execution
- All Enterprise Migration in One Execution

20.2.1 Single Enterprise Migration in One Execution

To migrate encoded terms for case data for a particular enterprise, enter an enterprise_id such as *1*.

20.2.2 All Enterprise Migration in One Execution

When you have multiple enterprises in the Argus Safety multi-tenant environment:

- To migrate encoded terms of case data for one enterprise only, enter only one enterprise_id such as 1 when prompted.
- To migrate encoded terms of case data for all enterprises in one go, enter input as ALL when prompted.
- To migrate encoded terms of case data for some enterprises (but not all), the number of executions of *dms_migration.bat* = Migration of encoded terms of case data for the number of enterprises.

Note: This migration script does not check whether the Argus Centralized Coding module is enabled for any specific enterprise. You must verify that module is enabled and then migrate data for enterprises.

To populate terms to the Interface table, you must load MedDRA into the Argus schema.

The migration script populates already encoded terms from all cases to the Interface table. Any open cases in the application are processed during migration.

Execute the batch file dms_migration.bat, and enter the following:

1. log folder name
2. log file name
3. TNSNAMES of the Argus Safety database when the Interface schema was created
4. Argus Safety schema owner name and password
5. Based on whether you want to migrate coded terms for all cases, one enterprise or for multiple enterprises:

   i. Enter the enterprise_id of one enterprise to migrate data for that particular enterprise.

   ii. Enter ALL as Input to migrate data for all enterprises.

   iii. To migrate coded terms of cases for more than one enterprise, execute step (i) multiple times and provide different enterprise_ids.
6. application user name

   If no input is provided, *admin* is taken as user input.
7. Verify the log file to validate successful completion of the script.

Part V

Secure Argus Safety

21 Argus Password Management - Cryptography Tool

Argus Safety uses dynamically generated encryption keys for passwords within the system. The Cryptography Key Editor allows you to generate a dynamic key and then encrypt passwords using the said key. The generated key must be installed on each application server and must be common to allow all servers to communicate with the Argus Safety Database.

The key is stored in the ArgusSecureKey.ini file located in the .\Windows folder.

IMPORTANT: During a new environment installation, a key will need to be generated **prior to** creating a database.

During an upgrade, a key will need to be generated prior to upgrading or an existing key from the existing setup can be used to perform the database upgrade. Make sure that the password information specified in the database is consistent with the information provided in the ArgusSecureKey.ini file.

> **Note:** When the ArgusSecureKey.ini file is generated, there is no need to run this tool again while launching 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.

When the key file is created, copy it to the .\Windows folder on all application servers (web, transaction, etc.).

> **Note:** Do not run the Cryptography Key Editor on each application server to generate passwords. It need only be run once during the initial system setup. Subsequent server installations must have the key manually copied to each .\Windows folder.

21.1 Install or Upgrade to Argus Safety 8.1.1

Whether you are upgrading to Argus Safety 8.1.1 or installing a fresh instance of it, you must generate new key using the Cryptography Key Editor.

21.1.1 Generate New Cryptography Key

You must generate ArgusSecureKey.ini key file before running the Schema Creation tool.

1. Launch the **Cryptography Key Editor**.

   The Key Editor Utility screen appears.

2. Click **New**.

   The Generate Key screen appears.

3. In the **Note to be added as comment** field, enter a comment that will be saved in the ArgusSecureKey.ini.

   This can be any form of metadata, such as the reason why this key was generated or for what environments it is used.

4. Enter ARGUSUSER password.

5. Confirm password.

6. Click **OK**.

   The ArgusSecureKey.ini file is created in the

   <Installation folder> \ CryptoKeyEditor\output\<DateTimeStamp>

7. Click the link in the **Argus Secure Key Path** dialog box to open the folder in Windows Explorer.

8. Click **Close, I will copy it manually**, and copy the file manually from the window that gets opened by clicking on the link mentioned above.

9. To move the generated ArgusSecureKey.ini file to the .\Windows folder, click **Copy to windows folder**.

21.1.2 Argus Safety 8.1.1 Database

Run the Argus Safety Schema Creation Tool to create or upgrade the database. If you run the Schema Creation tool before creating the key, a warning message appears that the cryptography key is required.

21.1.3 Argus Safety 8.1.1 Application Servers

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

21.2 Reset Password or Change the Cryptography Key

21.2.1 Reset the ARGUSUSER Password

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

1. Launch the **Cryptography Key Editor**.

   The Key Editor Utility screen appears.

2. Click **Existing**.

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

3. 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**.

   A confirmation 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.

21.2.2 Edit Keys

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

1. Launch the **Cryptography Key Editor**.

   The Key Editor Utility screen appears.
2. Click **Existing**.

   The Key Editor Login or Re-encrypt ARGUSUSER screen appears.
3. Enter the ARGUSUSER password.
4. Enter the Database name.
5. Click **Login**.

   The Key Editor Options for Existing Installation screen appears.
6. Enter the DBA User Name and User Password.
7. Click **Validate**.
8. Select the **Edit Key** checkbox.

   This enables the child checkboxes of **User Key** and **Cookie Key**.

   The User Key is used for all the encrypted strings which are persisted in the database or file server.

   The Cookie Key is only used to encrypt and decrypt the key.

   The user has the option to change either one or both keys.
9. Select the checkboxes in front of the key that you want to change.
10. Change the Key Size drop-down list value, if you wish to change the key size. Key Size is measured in bits of the key used in a cryptographic algorithm.
11. Click **Re-Generate**.

    This will change the value of the checked items and the new value will be visible in the textbox.
12. Click **Execute**.

    The Reason for this Action dialog box appears, prompting the user to add a reason for his action.

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

15. If the operation is successful and the Cryptography key is checked, then the changed key is now stored in the ArgusSecureKey.ini.

    You should now copy this file from the .\Windows folder of the current machine and paste it to the .\Windows folder of all web servers.

16. When the user key is changed, all the encrypted strings in the database are re-encrypted using the new key.

    However, there are still some other file server locations where this key change must also be applied manually. The following is a list of places where the changes must be done manually:

17. Items to be changed from the User Interface:

String	Description
Argus Services	Open Argus Safety Service Configuration: Open all the processes and enter password again.
Cyclone	Open ESM Mapping utility and re-enter the Cyclone password.
ESM Common User	Open ESM Mapping utility and re-enter the ESM Common User password.

18. Re-enter the DBPassword in the configuration files, as explained in the following sections:

    a. Point 2 of the Section 9.1.3.1, "RelsysWindowsService.exe.config.".

    b. Point 5 of the Section 14.2, "Configure Dossier".

    c. The Section 19.7, "Product License Study Interface".

21.2.3 Re-encrypt Common User Passwords

The **Key Editor Options for Existing Installation** screen can also be used to change the common user (ARGUS_LOGIN, ARGUS_LOGIN_I, and ARGUS_LOGIN_IPS) passwords.

1. Launch the **Cryptography Key Editor**.

   The Key Editor Utility screen appears.

2. Click **Existing**.

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

3. Enter the ARGUSUSER password.
4. Enter the Database name.
5. Click **Login**.

   The Key Editor Options for Existing Installation screen appears.

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 box appears, 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.

21.2.4 Generate Encrypted String

Generate the encrypted string from clear text, using the configured UserCryptoKey in ArgusSecureKey.ini.

1. Launch the **Cryptography Key Editor**.

   The Key Editor Utility screen appears.
2. Click **Existing**.

   The Key Edit Login screen appears.
3. Enter the ARGUSUSER password.
4. Enter the Database name.
5. Click **Login**.

   The Key Editor Options for Existing Installation screen appears.
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 box appears, 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.

21.2.5 Reset Administrator and System Application User Password

1. Launch the **Cryptography Key Editor**.

   The Key Editor Utility screen appears.
2. Click **Existing**.

   The Key Editor Login screen appears.
3. Enter the ARGUSUSER password.
4. Enter the Database name.
5. Click **Login**.

   The Key Editor Options for Existing Installation screen appears.
6. Enter the DBA User Name and User Password.

7. Click **Validate**.
8. Check the **Reset password for the default Administrator and System Accounts** checkbox.
9. To set **Administrator** password, select the respective checkbox, and enter the parameters.
10. To set **System** user password, select the respective checkbox, and enter the parameters.
11. Click **Execute**.

    The Reason for this Action dialog box appears, prompting the user to add a reason for his action.

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

21.2.6 Reset the Environment if ArgusSecureKey.ini is Lost

1. To generate a new key and copy it to the Windows folder, follow the steps listed in the Section 21.2.1, "Reset the ARGUSUSER Password."
2. To re-encrypt common user passwords, follow the steps listed in the Section 21.2.3, "Re-encrypt Common User Passwords."
3. Re-encrypt strings in the following locations:

String	Description
LDAP	Clear column LDAP_SEARCH_PASSWORD in all rows from table CFG_LDAP_SERVERS. Now open Argus Console > System Configuration > System Management > LDAP and re-enter passwords for all configurations.
SMTP	Clear column USER_PASSWORD in all rows from table CFG_SMTP. Now open Argus Console > System Configuration > SMTP Configuration and re-enter passwords for SMTP account.
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.

4. Re-enter the DBPassword in the configuration files, as explained in the following sections:
   a. Point 2 of the Section 9.1.3.1, "RelsysWindowsService.exe.config.".
   b. Point 5 of the Section 14.2, "Configure Dossier".
   c. The Section 19.7, "Product License Study Interface".

A

Configure BI Publisher Security Model

Oracle recommends to use Oracle Fusion Middleware Security model. In the case you prefer to use the BI Publisher Security Model, follow the subsequent sections for the set up.

Create Custom Roles and Assign Data Sources

1. Log in to BI Publisher with the administrator credentials.

   The BI Publisher Home Page appears.

2. Click **Administration**.

3. Under Security Center, click **Roles and Permissions**.

   The Roles and Permissions screen appears.

4. Click **Create Role**.

   The Create Role screen appears.

5. Enter a role **Name** and **Description**, and click **Apply**.

   A new custom role is created.

6. To assign data sources to the created role, click the **Add Data Sources** icon .

7. From the Available Data Source section, select a data source (for example, **asbip**), and click **Move (>)** to add it to the Allowed Data Sources section.

8. Click **Apply**.

9. To assign the required roles to the custom role, click **Add Roles** icon .

   The Add Roles screen appears.

10. From the Available Roles, select the roles to be included, and click **Move (>)** to add the selected roles to Included Roles.

11. Click **Apply**.

Create Users and Assign Roles

1. Log in to BI Publisher with the administrator credentials.

   The BI Publisher Home Page appears.

2. Click **Administration**.

   The Administration screen appears.

3. Under **Security Center**, click **Users**.

   The Users screen appears.

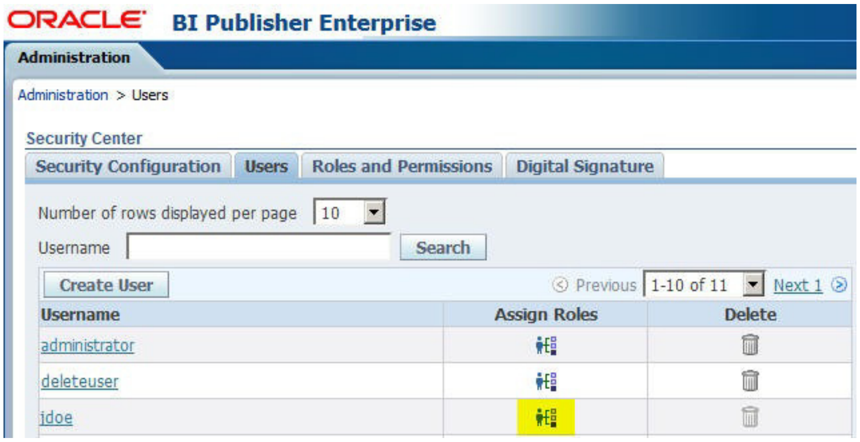
4. Click **Create Users**.

   The Create User screen appears.

5. Enter a **Username** and **Password**, and click **Apply**.

   A new user is created.

6. To assign roles to the user, click the **Assign Roles** icon corresponding to the new user.



Number of rows displayed per page: 10

Username:

1-10 of 11

Username	Assign Roles	Delete
administrator		
deleteuser		
jdoe		

The Assign Roles screen appears with the BI Publisher system roles as the following:

- BI Publisher Administrator
- BI Publisher Excel Analyzer
- BI Publisher Online Analyzer
- BI Publisher Developer
- BI Publisher Scheduler
- BI Publisher Template Designer

  These roles are available by default along with the custom roles you create.

In the above figure, ASAdmin and BIAdmin are custom roles.

7. From the Available Roles section, select a role, and click **Move (>)** to move the selected role to the Assigned Roles section.

8. Click **Apply**.

   The selected role is assigned to the user.