

Oracle® Argus Safety

Administrator's Guide

Release 8.2.1

F21907-01

August 2019

Oracle Argus Safety Administrator's Guide, Release 8.2.1

F21907-01

Copyright © 2019, Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

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

Contents

Preface	xi
Intended Audience.....	xi
Where to Find More Information.....	xi
Documentation Accessibility	xi
1 Introduction	
Introduction	1-1
Argus Safety Configuration Process Overview	1-1
Usage Conventions	1-2
Getting Started.....	1-2
Argus Console Architecture	1-3
Required Fields	1-3
Standard Buttons.....	1-3
Standard Icons	1-4
Administrator Login	1-5
Logging In as an Administrator:	1-5
Changing the Administrator’s Password	1-6
Logging out	1-7
Accessing the Home Page.....	1-7
Launching Online Help	1-7
View the Error Log	1-7
Understanding Argus Console GUI.....	1-7
2 Access Management	
Access Management	2-1
Configuring User Sites.....	2-1
Field Descriptions.....	2-1
Adding User Sites	2-2
About Filtering Criterion.....	2-4
Configuring Groups	2-4
Field Descriptions.....	2-5
Adding User Groups	2-6
Groups Included with the Factory Data.....	2-9
About Filtering Criterion.....	2-10
Printing a User Group.....	2-10

Group Configuration Print Out.....	2-11
About Filtering Criterion.....	2-11
Configuring Users.....	2-12
Field Descriptions.....	2-12
Printing Users.....	2-14
User Configuration - Roles.....	2-15

3 Business Configuration

About Business Configuration.....	3-1
Editable and Non-editable Business Configuration Sections.....	3-1
Type Ahead Fields.....	3-3
Additional Comments Fields.....	3-3
Configuring Product Family.....	3-3
Field Descriptions.....	3-4
Adding Product Families.....	3-4
About Filtering Criterion.....	3-5
Creating Data Sheets.....	3-6
Field Descriptions.....	3-6
Configuring Products.....	3-9
Field Descriptions.....	3-10
Adding Products.....	3-11
About Filtering Criterion.....	3-12
Configuring Licenses.....	3-13
Field Descriptions.....	3-13
Adding Product Licenses.....	3-15
Using the Product Browser.....	3-17
Configuring Clinical Studies.....	3-18
Field Descriptions.....	3-19
Adding Clinical Study Configurations.....	3-22
About Filtering Criterion.....	3-23
Adding WHO Drug Details.....	3-24
Adding Product Details.....	3-25
Configuring Auto Encoding.....	3-26
Configuring Study Reporting.....	3-27
Configuring Expedited Report Rules.....	3-28
Field Descriptions.....	3-30
Expedited Reporting Rules Algorithm.....	3-34
Suppression of Duplicate Reports.....	3-34
Blinded/Forced Distribution.....	3-35
Adding Expedited Report Rules.....	3-36
About the Filtering Criterion.....	3-38
Configure Regulatory Reporting Rules.....	3-39

4 Work with the Dictionaries

MedDRA Dictionary.....	4-1
Prerequisites.....	4-1
Load MedDRA or MedDRA J Dictionary.....	4-2

Overwrite an Existing MedDRA or MedDRA J Dictionary	4-2
Recode MedDRA	4-3
Logic to Recode MedDRA	4-3
Run the Dictionary Management Tool to Recode Events	4-6
Recode MedDRA terms at the Enterprise level	4-7
WHO Drug Dictionary	4-7
Prerequisites	4-7
Load WHO Drug Dictionary to New Tables	4-8
Overwrite an Existing WHO Drug Dictionary	4-8
Load WHO Drug Dictionary Format C	4-9
J Drug Dictionary	4-10
Prerequisites	4-10
Create and Modify Required File	4-11
Create All_Data.txt file	4-11
Create formulationcode.txt file	4-11
Create drugnameenglish.txt file	4-12
Modify the.mdb file	4-12
Load J Drug Dictionary	4-13
Overwrite an Existing J Drug Dictionary	4-13

5 System Configuration

System Configuration Overview	5-1
Configuring Case Priority	5-2
Field Descriptions	5-2
Configuring Field Validations	5-4
Field Descriptions	5-5
Modifying Field Validations	5-6
Configuring LAM System Numbering	5-6
Field Descriptions	5-7
Configuring System Management - Common Profile Switches	5-9
Configuring Advanced Conditions	5-12
Field Descriptions	5-12
Configuring Background Services	5-12
Field Descriptions	5-13
Configuring Case Form (System Management)	5-13
Coding Web Service	5-14
Auto Encoding, Dictionary and Central Encoding	5-14
Automation	5-15
Templates	5-17
Creating a Template in Another Language	5-18
Copying a Template to Another Language	5-18
Deleting Templates	5-19
Duration Calculations	5-19
Documentum Common Login	5-19
Custom Routines	5-19
Table Config Button	5-20
Modify Data Lock Point	5-21

SMTP Configuration	5-21
Configuring Case Processing	5-22
Field Descriptions	5-23
Configuring Database	5-26
Field Descriptions	5-26
GMT Offset Calculation	5-27
Configuring Assessments	5-27
Field Descriptions	5-28
Configuring Auto Archiving	5-29
Field Descriptions	5-30
Configuring Case Numbering	5-30
Field Descriptions	5-31
Configuring Lot Number	5-31
The Custom Node.....	5-33
Configuring the Dictionary Browser	5-34
Field Descriptions	5-34
Dictionaries	5-35
Configuring Group Data Access	5-35
Field Descriptions	5-35
Configuring WHO Drug	5-36
Configuring Performance	5-36
Field Descriptions	5-37
Configuring Documentum	5-37
Field Descriptions	5-41
Local Labeling	5-42
Configuring Local Labeling	5-42
Field Descriptions	5-43
Configuring LAM	5-43
Field Label Updates	5-43
Field Validation Updates.....	5-44
Network Settings	5-45
User Interface	5-47
Configuring User Interface.....	5-47
Configuring Reporting	5-48
Field Descriptions	5-49
Configuring E2B	5-49
Field Descriptions	5-49
Configuring eMDR.....	5-50
Configuring eVAERS	5-51
Expedited Reports Configuration	5-51
BIP Reporting	5-54
Expedited BfArM Reports Configuration	5-55
Expedited Canada Reports Configuration.....	5-56
Expedited CIOMS Reports	5-58
Expedited MedWatch Reports Configuration.....	5-60
Periodic Reports Configuration.....	5-63
Scheduling Reports Configuration.....	5-65

Configuring Security	5-66
Configuring Cryptography within Common Profile > Security	5-69
Configuring Single Sign-On	5-70
Error Messages	5-73
Configuring SMTP	5-73
Field Descriptions	5-73
Configuring Workflow Items	5-74
Field Descriptions	5-76
Configuring Workflow	5-77
Worklist Updates	5-77
Configuring Case Workflow	5-78
Configuring Workflow States	5-78
Configuring Workflow Rules	5-79
Worklist Intake	5-82
Pending Dialog.....	5-82
Worklist Intake View.....	5-84
Worklist.....	5-84
Rejected Cases	5-87
User Site Updates and Access Management.....	5-88
Configuring System Numbering	5-89
Field Descriptions	5-90
Configuring Field Properties	5-91
Field Descriptions	5-92
Adding User Defined Fields.....	5-93
Configuring User Defined Fields	5-94
Configure Local Data Entry	5-95
About Local Fields	5-95
Access Local Case Data Lock Functionality	5-96
Process an Outlier	5-98
Activate Local Locking in Argus Safety	5-99
Enter Local Reports Configuration Seed Data.....	5-99
Enter Local Users Seed Data	5-99
Enter Local Fields Seed Data.....	5-99
Activate Local Reporting in Argus Safety	5-100
Enabled Modules.....	5-100
Interchange Mapping	5-101

6 Code List Configuration

Configuring Code Lists > Argus	6-1
Configuring Autosignals	6-2
Field Descriptions	6-2
Configuring Batch Reports	6-4
Field Descriptions	6-4
Configuring Letters	6-6
Field Descriptions	6-7
Letter Placeholder for the IND Cover Letter	6-8
Configuring Justifications	6-9

Field Descriptions	6-9
Configuring Electronic Transmission	6-10
Field Descriptions	6-10
Configuring Event Groups	6-12
Terms tab	6-12
Event Groups tab	6-14
SMQ tab	6-14
Configuring Literary Citations	6-16
Field Descriptions	6-17
Configuring Message Type	6-18
Field Descriptions	6-19
Configuring Reporting Destination	6-19
Agency Information	6-20
Local Company Contact	6-23
Configuring EDI	6-25
Configuring the Base Directory Path	6-29
SMTP	6-30
Configuring Routes of Administration	6-31
Field Descriptions	6-32
Configuring Study Center	6-33
Field Descriptions	6-34
Configuring Holiday Calendar	6-35
Field Descriptions	6-36
Other Code List Items	6-37
Formulation Factory Data	6-42
Configuring Code Lists > Flexible Data Re-Categorization	6-44
Flexible Code Lists	6-44
Flexible Re-Categorization	6-45
Add custom values to a flexible code list	6-51

7 Accessing Tools

Accessing Tools	7-1
Report Features	7-1
Viewing the ISCR Length Check Report	7-2

8 Using Advanced Conditions

Using Advanced Conditions	8-1
Features within Advanced Conditions	8-2
Using Advanced Conditions	8-3
Creating Advanced Conditions	8-3
Creating a Query Set of Advanced Conditions	8-6
New Action Type Fields and Field Description	8-6
Rename Query Sets	8-9
Use the Advanced Conditions from the Case Selection Dialog Box	8-9
Use the Advanced Conditions Library	8-9
Case Series (former Hit List) Tab	8-10

9 Data Privacy

Personally Identifiable Information	9-1
Personally Identifiable Information and Application Behavior.....	9-4

10 Best Practices

Configuring Argus Safety for ICSR Reports (HL7)	10-1
Configuring Reporting Destination for HL7 ICSR Reports.....	10-1
Customizing Profiles.....	10-3
Configuring ICSR Validation using the New Framework.....	10-3
Configuring Codelists.....	10-4
eMDR Specific Codelist Updates.....	10-4
eVAERS Specific Codelist Updates.....	10-4
PMDA E2B (R3) Flex Codelist.....	10-5
Business Configuration Updates.....	10-6
Setting up the Application Type in Business Configuration -> Products and Licenses (eVAERS specific) 10-6	
Configuring PMDA Specific License Parameters.....	10-6
Configuring PMDA E2B (R3) Specific Study Parameter.....	10-6
System Configuration Updates.....	10-6
.....PMDA E2B (R3) Specific Switches	10-6
Optional Upgrade Scripts for Data Migration to New Fields.....	10-7
eVAERS specific.....	10-7
eMDR Specific.....	10-8
Attachments in HL7 Reports	10-9
Creating and Managing Amendments for eVAERS and E2B (R3) report	10-10
Null Flavor Handling in HL7 Reports	10-10
Best Practices in a Multi-Tenant Environment	10-11
Single Sign-on	10-11
Accessing Argus Safety Directly via URL	10-11
Global Homepage and Portlets	10-11
Global Worklists Columns	10-12
Global User Management	10-12
Global Enterprises.....	10-13
User-Enterprise Association	10-13
New User Creation/Association	10-13
Synchronizable User Attributes.....	10-13
Inactivating an Enterprise	10-16
Add a New Enterprise.....	10-16
New Enterprise Setup	10-16
Data Segregation.....	10-17
Data Segregation by Module.....	10-17
Data Segregation by Enterprise.....	10-20
Maintaining Consistency Across Enterprises.....	10-20
Data Segregation impact on system-level configuration items.....	10-20
Data Shared Across Enterprises	10-24
Applications Access.....	10-25

Pre-upgrade Considerations for Existing Databases.....	10-25
Post-upgrade Considerations for Existing Databases.....	10-25
Documentum Migration	10-26

Preface

This document describes the steps for installing and configuring the components of the Argus Safety Solution application.

A * has been placed before fields that have been introduced in a previous release but are currently non-operational.

Intended Audience

This document is intended for administrators of the Argus Safety system for configuring Argus Safety.

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/MOSHHP/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.

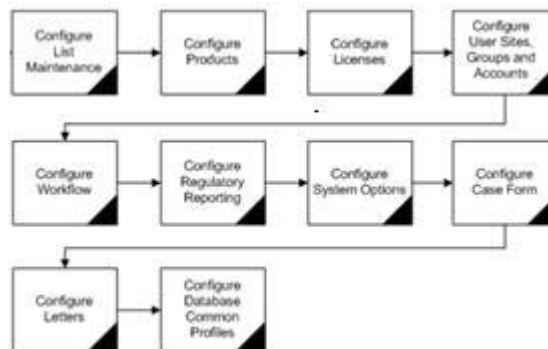
Introduction

Introduction

Argus Safety assists manufacturers of pharmaceuticals and devices by providing a simple and efficient way to comply with international and domestic regulatory safety reporting requirements. It also facilitates internal company safety surveillance by providing tools for signal detection and for analyzing the overall safety profile of both investigational compounds and marketed products.

Argus Safety Configuration Process Overview

To configure Argus Safety, the Administrator must follow a particular sequence of steps. Steps that fall later in the sequence might depend on those that appear earlier. It is, therefore, important for the Administrator to use the following flowchart as a guideline for configuring Argus Safety.



Task	Purpose
Configure User Sites, Groups and Accounts	Enter user sites, create user groups and user accounts, configure group and individual user access rights
Configure Products	Configure Manufacturers, Ingredients, Formulations, Dosage Units, Product Families, and Data Sheets
Configure Licenses	Enter license information, countries and products associated with the license
Configure Code List Items	Configure list maintenance items that are not covered in other topics, like Action Taken, Clinical Studies, Study Centers, etc.

Task	Purpose
Configure Workflow	Configure case workflow states and rules that determine the transition of cases between states
Configure Regulatory Reporting	Configure Regulatory Agency information and expedited reporting rules
Configure System Options	Configure miscellaneous system items like Auto-numbering, Field Labels, etc.
Configure Case Form	Configure Case Form dictionaries, duration calculations, etc.
Configure Letters	Create letter templates by using template placeholders
Configure Database Common Profiles	Configure the Common Profiles Table to customize the Argus Safety application

Usage Conventions

The following conventions are used throughout this document to help you identify specific kinds of information.

Usage Convention	Description
Bold	User interface elements such as Buttons, Dialog boxes, Check boxes, Combo boxes, Drop-down lists, Labels, Option (Radio) buttons, Tabs, Text boxes, etc.
"between quotation marks"	Information that may appear as-is on screen, or information provided by the user.
Note: Text	Information that should be noted before proceeding with the instructions.
Important! Text	Important information that must be noted to ensure accurate, reliable, or safe behavior of the system.
Tip: Text	Information that enables easier completion of the current task or helps in completing other tasks.
ALL CAPITALS	Keyboard keys
Initial Capitals	Names of user interface elements, modules, applications, proper nouns, etc.

Getting Started

This section introduces the basic tasks for configuring Argus Safety. To get started with the configuration process, the person responsible for configuring Argus Safety must log on as Administrator to configure the Argus Console.

Refer to the following sections for information pertaining to:

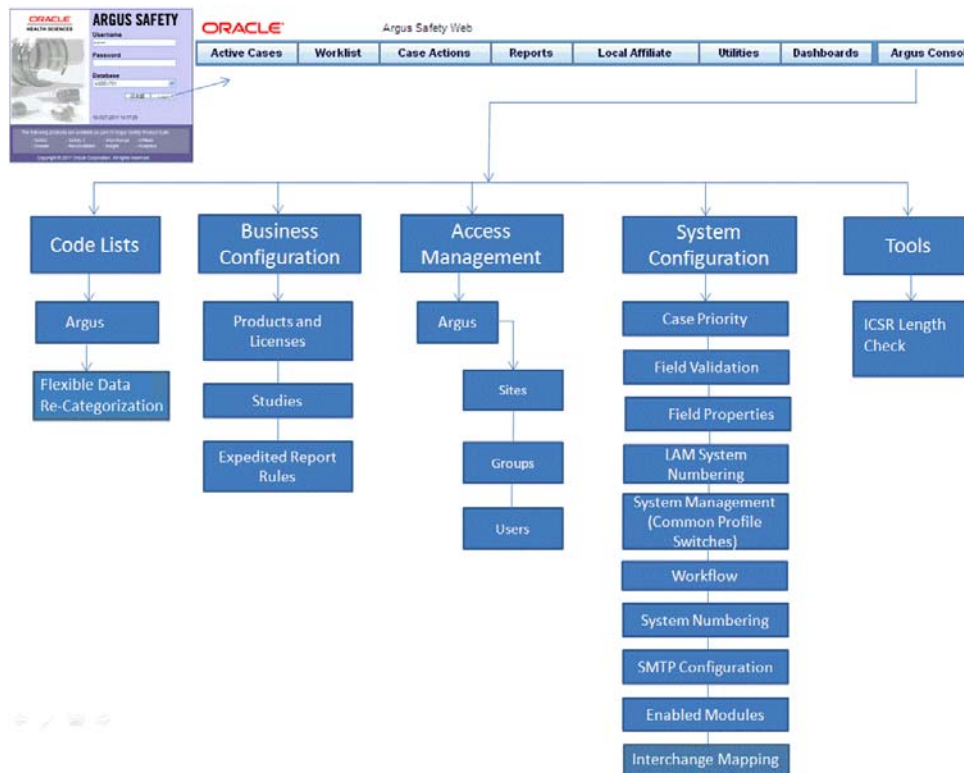
Section	Topics Covered
Administrator Login	<ul style="list-style-type: none"> ■ Logging in and out of the Argus Console ■ Changing the Administrator password ■ Accessing the Home Page and Online Help
Understanding Argus Console user interface	Read this section for an overview of the Argus Console user interface components.

Argus Console Architecture

The Argus Web Administration Console has been designed to enhance ease of navigation for the Argus end-users.

The following illustration shows the design and location of the individual components under the main **Argus Console** Menu.

Note: The menu items that you can access depend on the security permissions that are defined for your account by the administrator



Required Fields

Fields that are marked with a red flag image and associated with an orange boundary are required fields. These fields must be filled in, to proceed with the configuration requirements.

Standard Buttons










The standard buttons used in this console are described in the following table:


Button	Description
Save	Use this button to save changes associated with a section
Cancel	Use this button to cancel changes associated with a section
Print	Use this button to print information associated with a sub-section in a PDF.
Delete	Use this button to delete an item associated with a section
Copy	Use this button to create a new editable copy of an item within a section

Button	Description
OK	Use this button to confirm an action associated with a section
Yes	Use this button to confirm an action associated with a section
No	Use this button to cancel an action associated with a section
Help	Use this button to launch the online manual for the Argus Console
Add New	Use this button to add a new item associated with a section

Standard Icons

The standard icons used in this console are described in the following table:

Icon	Identifies
	A required field
	An item placed inside a folder in the tree-view
	A closed folder containing sub-folders or nodes
	An open folder displaying sub-folders or nodes
	An open folder that does not contain sub-folders or nodes
	A closed folder that does not contain sub-folders or nodes
	An expandable or collapsible browser tree view
	An option to sort columns alphabetically (when placed next to a column header)
	An item appearing under multiple categories (e.g. a user name appearing under multiple groups)

Icon	Identifies
	A withdrawn license in the tree-view of licenses.

Administrator Login

When Argus Safety is installed, an account for the Administrator is automatically created. The installation program assigns **admin** as both the User Name and Password for this account.

Before logging in to the Argus Console, be aware of the following:

- If you enter an incorrect username or password three (3) consecutive times, the system disables the Login button and displays the following message:
The login button has been disabled due to 3 consecutive incorrect entries of Username or Password. Please refresh the page to enable the Login button.
- The Date/Time 24-hour format used by the Web server: DD-MMM-YYYY
HH:MM:SS.

Note: The Administrator or System password can be reset from new Argus Key Management Tool > Reset Password for the default Administrator and System Account.

Logging In as an Administrator:

1. Enter the **Argus URL** in your web browser, to launch Argus Safety. The login screen appears as shown:



Tip:

- The modules displayed in bold text identify the modules you have permission to access.
- Your login user ID and password are valid for all accessible Argus modules.

2. Enter the **User Name** and **Password** to login to Argus Safety.

Note: The password is case-sensitive.

3. Select the database name from the **Database** list.
4. Press **Enter** or click **Login**.
5. When the window opens, click **Yes** to proceed with the login.

Note: If the window does not appear, verify that your browser's Pop-Up blocker is disabled.

6. Click **Argus Console** to launch the Argus Console Administrator screen.

Note: If the window does not appear, verify that your browser's Pop-Up blocker is disabled.

Changing the Administrator's Password

1. Select **Utilities** -> Change Password in Argus Safety.
2. The **Change Password** dialog opens.

3. Enter the current password and the new password.

Note: In case of a Single Sign-On user, the Change Password option is not supported in Argus Safety.

4. Confirm the new password and click **OK**.

Logging out

1. Click **Close** to leave the Argus Console application.
2. To log out at any time from Argus Safety, click **Logout**.

Accessing the Home Page

To go back to the Home page, click **Home**. The default Home page appears.

Launching Online Help

To launch the Online Help click **Help**.

View the Error Log

To view the error log for information about errors that occurred during case processing:

1. From the **Utilities** drop-down menu, go to **Logs > View Error Log**.
2. To search for error logs based on pre-defined or custom date ranges, in the Search Conditions section, enter a value, and click **Search**.

The search results appears in the **Total Number of Rows** section.

3. Locate the error log you want to view, and click to view the error message text.
4. Click the **Zoom** icon to view the complete text.

Understanding Argus Console GUI

This section broadly categorizes the sections of the Argus Console GUI with their associated descriptions.

Section	Sub-Section	Description
Getting Started	~	This section provides information about new keyboard navigation features for the Argus Console.
Access Management	Sites	This section enables the administrator to enter and configure new user sites.
	Groups	This section enables the administrator to enter and configure new user groups.
	Users	This section enables the administrator to configure user accounts.

Section	Sub-Section	Description
Business Configuration	Product and License	This section helps in capturing Product Details (product specifics, product licenses, products involved in the studies. These can be the products marketed, or under investigation, by the company.
	Studies Configuration	This section helps in capturing Study information (study specifics, products involved in the study licensed countries associated with the study and the clinical references used in the expedited reports.
	Expedited Reporting Rules	This section helps in capturing Expedited Reporting Rule configuration. The Reporting Rules configuration feature enables the administrator to define the reporting rules or criteria for the cases to be qualified for expedited reporting.
System Configuration	Case Priority	This section enables the administrator to configure rules to determine the priority of new cases that are entered into the system.
	Field Labels	This section enables the administrator to change field labels, hide and unhide fields in Case form.
	Field Validation	This section enables the administrator to configure field level validations for the case form fields.
	LAM System Numbering	This dialog enables the administrator to specify the case numbering preferences for LAM cases.
	System Management Common Profile Switches	This section enables the configuration of Common Profile Switches that affect the behavior of the Argus application.
	Workflow	The section enables the configuration of workflow states and rules, within the safety department starting from initial case receipt to case closure. The system enables tracking of the progress of cases between users and states of activity.
	System Numbering	This section enables the administrator to specify the case numbering preferences.
	SMTP Configuration	This screen enables the user to configure SMTP settings.
Code Lists	Interchange Mapping	This section enables the user to access the Interchange Mapping client utility from the Argus application to set up and configure the Service INI File.
	Code Lists Argus	This section helps in capturing Code List information. Code lists appear as drop-downs in the Argus application.
Tools	ICSR Length Check	This screen enables the user to view the ICSR Length Check report in PDF format.

Access Management

Access Management

Site, group, and user configuration takes place in the **Access Management** section of Argus Console. Here you can add, copy or delete users, groups or sites.

Each user must be assigned to at least one group in order to determine their security level. Each group is assigned a specific security level. This security level enables members of the group to view, modify, or restrict access rights to various sections of the Case Form, and so on.

The first set of steps in configuring Argus safety is to create the following **exactly in the listed order**:

- Sites
- Groups
- Users

Note: The configuration must occur in the **exact order** specified above.

Configuring User Sites

Addition of Sites is necessary in order to create Users because every user must be assigned to exactly one Site. Site information can also be used in automatic numbering of case IDs.

To configure Sites, use the **Access Management -> Argus -> Sites** section. The following is an illustration of that section.

Field Descriptions

The following table lists and describes the fields on the screen.

ORACLE® Welcome vanessa, Thursday, March 3, 2011 (AS70-DEFAULT) Home Help Close

Code Lists Business Configuration Access Management System Configuration Tools

CODE LIST MAINTENANCE

Browser
Organized by Code List

- Lab Test Group
- Lab Test Type
- Letter Configuration
- Literary Citation
- Local Evaluator Comment Type
- Manufacturers
- Medical Status
- Message Type
- Nature of Event
- Occupations
- Package Units
- Product Group
- Project ID
- Reference Type
- Report Media
- Report Type
- Reporter Information
- Reporter Type
- Reporting Destination
- Reporting Destination Type
- Routes of Administration
- Study Center
- Study Development Phase
- User Sites

Help Text
Defines a list of user sites (e.g. United States, United Kingdom) that are assigned to Argus user accounts. Definition of user sites is required prior to configuring users.

User Sites Filter
Field Description Contains Value Filter

Total Number of Rows (2)

Description	Abbreviation	Site Type	Intake File Path
Common Site	CS	Argus	
United States	US	Argus	

Add New Copy Delete Print

Modify User Site

Description
United States

Abbreviation
US

Site Type
Argus

Intake File Path

Protect Patient Confidentiality - Default
 Protect Reporter Confidentiality - Default
 Bulk Report By Form (Approved Reports) - Default

LAM Sites

Add > < Remove Add All >> << Remove All

Site Printers Add Delete

#	Printer Name	Printer Path
---	--------------	--------------

Save

Field/Control Name	Description
Description	Enter a description of the site.
Abbreviation	Enter an abbreviation of the site name. A one to four character abbreviation is required for each site.
Site Type	Select the Site Type Argus or LAM (Local Affiliate Module).
Protect Patient Confidentiality - Default	Protects or reveals Patient Confidentiality for the specific site.
Protect Reporter Confidentiality - Default	Protects or reveals Reporter Confidentiality for the specific site.
Bulk report By form (Approved reports) - Default	Allows or protects availability of the Bulk Reports by Form for the specific site.
LAM Sites	Select and add previously created LAM sites.
Site Printers	The Site Printers section is used to configure site printers.

Adding User Sites

This screen helps in capturing Site information (such as user site description, abbreviated term, site type and LAM site configuration).

Use the following procedure to add a user site.

1. Click **Access Management->Argus->Sites**.
2. In the left panel, select **User Sites**. The User Sites are listed in the right panel.

Tip: You can alternatively click **Modify** to modify an existing site.
Use **Copy** to make an editable copy of an existing user site.
Use **Delete** to delete a user site.

3. Select a **User Site** and click **Add New**.

The screenshot shows the 'Add New User Site' interface. On the left, there are input fields for 'Description', 'Abbreviation', and 'Site Type' (a dropdown menu). Below these is the 'Intake File Path' field. At the bottom left, there are three checked checkboxes: 'Protect Patient Confidentiality - Default', 'Protect Reporter Confidentiality - Default', and 'Bulk Report By Form (Approved Reports) - Default'. On the right, the 'LAM Sites' section contains two empty boxes and four buttons: 'Add >>', '<< Remove', 'Add All >>', and '<< Remove All'. Below this is the 'Site Printers' section, which includes an 'Add' and 'Delete' button and a table with columns '#', 'Name', and 'Path'. The table has two rows, each with an empty input field for the 'Name' and 'Path' columns. A 'Save' button is located at the bottom right of the form.

4. Enter the user site **Description**.
5. Enter the user site **Abbreviation**.

Note: A maximum four-character abbreviation is required for each user site.

6. Select a **Site Type**.

Note: Each Argus Safety user must be assigned to exactly one user site.

You cannot change the site type from LAM to Central if the current central site has an association with a LAM site, the current site is associated with any user, or the current LAM site has any events assigned to it.

7. Select the following options as required:
 - Select the **Protect Patient Confidentiality - Default** to protect or reveal *Patient Confidentiality* for this specific user site.
 - Select the **Protect Reporter Confidentiality - Default** to protect or reveal *Reporter Confidentiality* for this specific user site.
 - Select the **Bulk Report by Form (Approved Reports) - Default** to enable availability of the *Bulk Reports By Form* for this specific site.
8. Add or remove any **LAM Sites** information.

Tip: To add more **LAM Sites** to the Lam Sites list, use the **Add>>/Add All** options.

To delete the **LAM Sites** from the Lam Sites list, use the **Remove>>/Remove All** options.

9. In the **Site Printers** section, click **Add** to add a site printer.

10. Enter the **Name** of the printer that will be displayed in the application when referring to the printer. The name can have up to 20 characters.
11. To delete a site printer, select the printer and click **Delete**.
12. Click **Print** to print the site information, as shown below:

Site Information			
Description	LAM Site 1		
Abbreviation	LAM1	Site Type	LAM
Intake File Path			
<input type="checkbox"/> Protect Patient Confidentiality-Default	<input checked="" type="checkbox"/> Protect Reporter Confidentiality-Default	<input type="checkbox"/> Bulk Report Report By Form (Approved Reports)-Default	
Site Printers			
#	Name	Path	
1	Printer 1	Printer 1 Path	
2	Printer 2	Printer 2 Path	

13. In the **Path** text box, enter the full path of the printer on the network. This path name can have up to 256 characters. The specified path should be accessible from the machine where Argus Safety Service is installed.
14. Click **Save** to save the information and return to the Code List Maintenance dialog.

About Filtering Criterion The *filtering criterion* is essential as it helps you to search for specific items. The Argus Console provides this option for the Access Management section. The filtering browser is displayed as the **Code Filter List**

Argus Console helps you to filter information further for the Access Management section. Using the **Code Filter List** you can specify whether your search should contain or start with specific alphabets.

For Example: The following filtering criteria enables the system to search for all User Sites that contain A in the abbreviated term.

Field	Operator	Value
Description	Starts with	A

Description	Abbreviation	Site Type	Intake File Path
Argus			

The right panel now displays the list of User Sites based on the filtering criterion.

Configuring Groups

Each user of Argus Safety can be a member of one or more user groups. The access rights of each user group to the menus in the user interface and specific sections of the Case Form can be configured when the group is created.

Configuration of the user site is done using the **Access Management->Argus -> Groups** section.

Field Descriptions

The following table lists and describes the fields in the **Modify Group Information** section.

Field/Control Name	Description
Group Name	Enter a unique name for the group.
Email	Add the group email, used for case priority notification and workflow routing notification.
Supervisor Email	Add the Group's Supervisor Email as applicable. This e-mail address is used to send notifications when the maximum time of a case for a particular workflow state is exceeded.
Menus	Lists the menus and sub menus within a Case Form and allows you to enable or disable each of them.
Case Form	Lists the sections and sub sections within a Case Form and enables you to assign the group Modify; View (Read Only); or No Access (not visible) to each area.
Advanced Condition	Allows you to configure advanced condition settings, as applicable. The options are: No Access to Create Advanced Conditions, No Access to Share Advanced Conditions, No Access to View and Edit SQL.
Listedness Determination - Countries	Assigns Argus users to the group that has rights to change the listedness determination for licenses originating in the selected countries.
Restrictions - Products	Limits the number of products that can be viewed in the trade name lookup and non-study cases.

Field/Control Name	Description
Restrictions - Studies	Limits the number of studies available for selection and the study cases that can be viewed. <ol style="list-style-type: none"> 1. Click the Studies checkbox to enable the Select button 2. Click this button to view a security configuration containing a tree view list of available items 3. Select a study family to select all its constituents
Default report (LAM only)	Lists the expedited report forms in the drop-down list.

Adding User Groups

This section enables the Administrator to configure the security levels for each work group.

Radio buttons enable you to view the group and assign access rights for several specific sections of the case form, menu, case workflow, and report workflow.

If a user belongs to multiple groups, the access rights for the user will be the sum-total of the individual group access rights. Consider the following example:

John Smith is an Argus User and his profile has been added to 2 user groups with different access level permissions for each group.

- John has access rights to the **Patient** Tab in one group and access rights to the **General** Tab in another group.
- In this case, John will be able to access both the **Patient** and the **General** tabs of Argus

Use the following procedure to create a user group

1. Click **Access Management->Argus->Groups**.
2. Select the filtering criterion to display the list of Groups or Users in the left panel.
3. Select a **Group** and click to view the group details in the right panel.

The screenshot displays the Oracle Access Management 'Modify Group Information' window. The top navigation bar includes 'Code Lists', 'Business Configuration', 'Access Management', 'System Configuration', and 'Tools'. The 'Access Management' tab is active, and the 'Argus' application is selected. The left pane shows a 'Browser' view of 'User Groups' under 'ARGUS', with 'Administrator Group(21)' highlighted. The main pane is titled 'Modify Group Information' and contains the following sections:

- Group Information:** Fields for 'Group Name' (Administrator Group), 'Email', and 'Supervisor Email'.
- Menus:** A list of menu items (File, New Case, New Case From Image, Open Case, Save) with 'Enabled' radio buttons.
- Case Form:** A list of case form sections (General Information, Study Information, Reporter Information, Patient Information, Other Relevant History) with radio buttons for 'Modify', 'View', and 'No Access'.
- Advanced Condition:** Three checkboxes for 'No Access to Create Advanced Conditions', 'No Access to Share Advanced Conditions', and 'No Access to View and Edit SQL'.
- Listedness Determination:** A list of countries (AFGHANISTAN, ALBANIA, ALGERIA, AMERICAN SAMOA, ANDORRA, ANGOLA) and a 'Selected Countries' list.
- Restrictions:** Two checkboxes for 'Products' and 'Studies', each with a 'Select...' button.

At the bottom of the window, there are buttons for 'Add User', 'Save', 'Add Group', 'Copy', 'Delete', and 'Print'.

Tip:

- You can alternatively click **Add Group** to create a new group.
 - Use **Copy** to make an editable copy of an existing group.
 - Use **Delete** to delete a group.
4. Enter the **Group Name**. This should be a unique name associated with this Group.
 5. Enter the **Email** address, if applicable.
 6. Enter the **Supervisor Email** address, if applicable.
 7. In the **Case Form** section, select the desired access right option (**Modify**, **View**, or **No Access**) for the group's access to each of the listed items of Case Form.

Note: The following fields are required in order to save a case: **Initial Receipt Date**, **Country of Incidence**, **Report Type**, **Suspect Product**, and **Event Description as Reported**. Therefore, the group responsible for initial case entry must have access to these fields in order to save new cases.

The following user group accesses have been renamed:

- *Case Patient – Personal Patient Information* has been renamed as *Case Patient - Patient Information*.
 - *Case Patient – Patient Information* has been renamed as *Case Patient – Patient Details*.
-

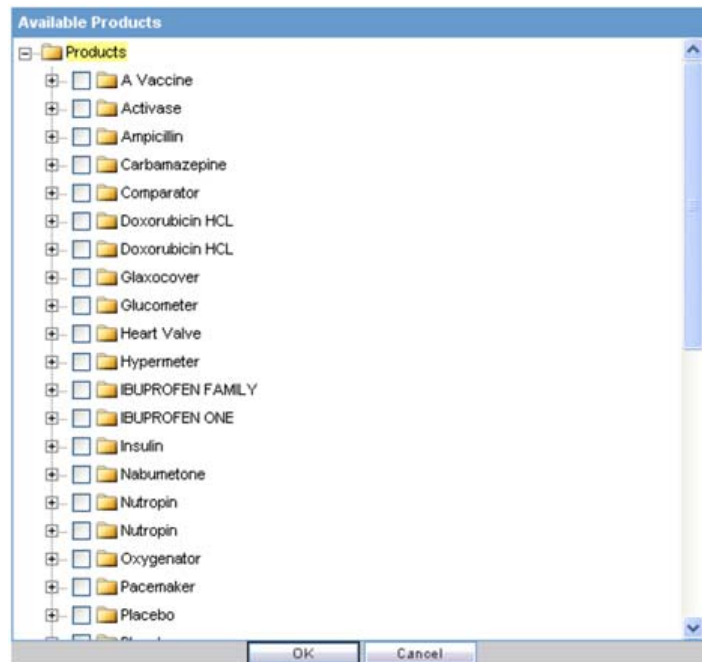
8. In the **Menus** section, enable or disable access of the group, to particular items in the Argus Safety menu.

Tip: Refer to the Argus Safety User Guide for information about the functions of the Case Form sections and the menu items in the Argus Safety user interface.
9. In the **Listedness Determination** section, select a list of countries. This enables the end user to override the listedness determination in the **Event Assessment** section of the Case Form for product licenses that match the countries selected in this step.
10. In the **Advanced Conditions** section, select **No Access to Create Advanced Condition**, **No Access to Share Advanced Conditions**, and/or **No Access to View and Edit SQL**.

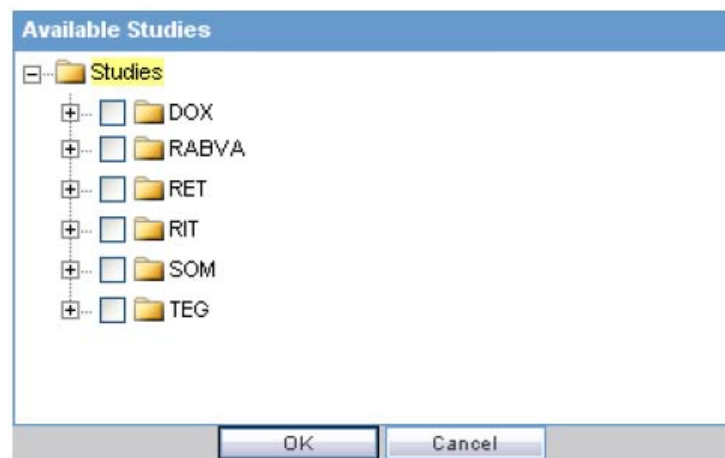
Note: Only trusted users should be given access to Advanced Conditions. This is because users who have this access will have complete access to the information in the Argus Schema.

Tip:

- If you select **No Access to Create Advanced Condition**, **Advanced Conditions** does not appear as an option for that user group.
 - If you select **No Access to Share Advanced Conditions**, the user group does not have access to share Advanced Conditions.
 - If you select **No Access to View and Edit SQL**, the **SQL...** button will not appear as an option for that user group.
11. In the **Restrictions** section, select **Products**.
 12. Click **Add Product**, to open the **Available Products** dialog box.
 13. Select each product you want to add and click **OK**.



14. In the **Restrictions** section, select **Study**.
15. Click **Add Study**, to open the **Available Studies** dialog box.
16. Click the appropriate checkboxes to select the required studies and click **OK**.



17. Click **OK** to save the group.

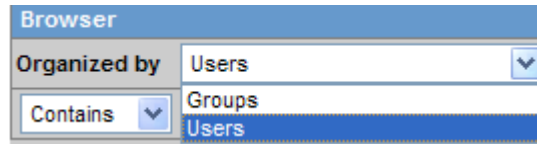
Groups Included with the Factory Data The following table lists and describes the groups included with the factory data.

Group	Description
Administrator	This group has access rights to all areas and all the functionality of Argus Safety.
Investigator	Receives an e-mail alert that can be set up during Clinical Study Configuration.

About Filtering Criterion The filtering criterion is essential as it helps you to search for specific items. The Argus Console provides this option for the Access Management section.

Using Organized by

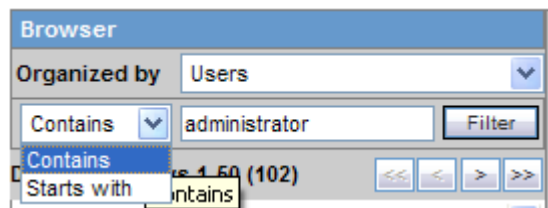
The system displays the filtering browser in the top-left corner of the left panel. You can filter based on either of the two combination shown in the following illustration.



Consider the following.

- If you enable **Organized by Groups**, the generated output displays in a tree-format in the left panel. The structure is based on the entire categorization of Groups and Users
- If you enable the **Organized by Users**, only the User list is available in the tree view in the left panel.

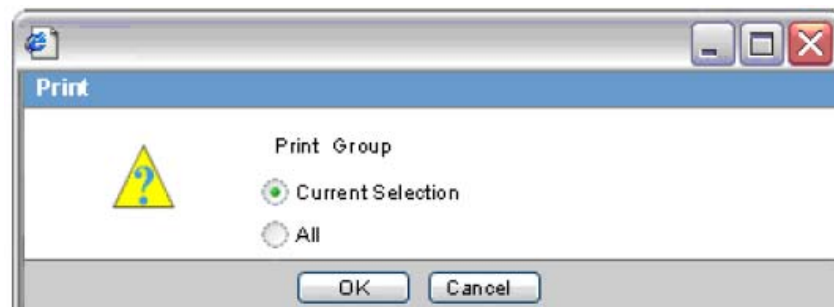
Using **contains** or **starts with** enables you to specify whether your search should contain or start with specific alphabetic characters. For example, filtering criterion shown in the following illustration enables the system to for all Groups that contain the word "administrator."



Printing a User Group

Use the following procedure to print a user group.

1. Select **Access Management->Argus->Groups**.
2. Select the filtering criterion to display the list of Groups or Users (based on the filtering criterion) in the left panel.
3. Select a **Group** and click to view the group details in the right panel.
4. Click **Print** to display a **Print** dialog that enables the user to choose to print the entire window or to print only the text covered by the current selection.



5. Select the appropriate options and click **OK**.
6. The system opens the **Print Groups** to enable the user select the sections to be printed in the **Group Configuration** printout.
By default, the **Group Information** checkbox is selected and disabled so that it always gets printed.
7. Select the appropriate checkboxes, and click **OK**

Group Configuration Print Out The following is an illustration of the **Group Configuration** printout.

- It lists the users which are configured to the groups.
- User are sorted alphabetically by **User Full Name** in the report section

Users		
Full Name	User ID	Site
John Smith	johns	United States

About Filtering Criterion The filtering criterion is essential as it helps you to search for specific items. The Argus Console provides this option for the Access Management section.

Using Organized by

The system displays the filtering browser in the top-left corner of the left panel. You can filter based on either of the two combinations.

Consider the following.

- If you enable **Organized by Groups**, the generated output displays in a tree-format in the left panel. The structure is based on the entire categorization of Groups and Users
- If you enable the **Organized by Users**, only the User list is available in the tree view in the left panel.

Using **contains** or **starts with** enables you to specify whether your search should contain or start with specific alphabetic characters. For example, filtering criterion

shown in the following illustration enables the system to for all Groups that contain the word "administrator".

Configuring Users

User Maintenance enables you to add, copy, or delete users for the system.

- Each user must be assigned to at least one group in order to determine security level.
- Each group is assigned a specific security level that defines whether group members can view, modify, or have no access rights to various sections of the case form, etc.

Configuration of the users is done using the **Access Management->Argus->Users** section. If the Enable LDAP Login checkbox is not checked, you can specify a password when creating or modifying an individual user account. When updating user records, be aware of the following:

- If you enter a value in the **Password** field, the system uses this password to authenticate at login.
- The **Reset Password** field is available **only** when you select **Reset Password**. The new password can be up to 30 characters.
- If you leave the value blank, the system uses the default password as defined in the **Common Profile** for the system.
- When you save the user configuration, the system saves the default password you enter.
- During entry, the system displays the password you type.

The following illustration shows the fields associated with this section.

Field Descriptions

The following table lists and describes the fields in the **Administrator** section

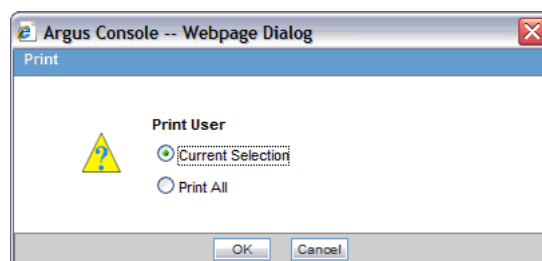
Field/Control Name	Description
User Name	Enter the full name.
User ID	Enter a unique user identification (ID).
Reset Password	Reset the password of a user to a default value specified in the common profile section.
Email Address	Enter the user's e-mail address.
Site	Assigns the user to a site. The values in this field are populated from the codelist item User Sites .
User Group - Select	Attaches the user to pre-configured user groups.
User Type	Select the type of user, such as an Argus J user from the drop-down list.
User Roles - Select	Attaches the user to pre-configured user roles such as Global Admin. By default, a Global Admin role is granted to only an Administrator, who can grant/revoke this role to other Argus users. Such a user role should be assigned to users who need access to the Argus Global application. Similarly, you can also select from other roles present within User Roles.
Application Access	Configure user access settings for Argus Console and Argus Safety. The default application access for the user can be selected from the list.
Worklist to display at login	Configure users to see their worklists immediately upon login. The options are: <ul style="list-style-type: none"> ■ None (default) - Does not open any worklist when the user logs into Argus. Displays personal Argus status on login. ■ Action Items - Opens Worklist - Action Items screen for the user on login into Argus ■ New - Opens Worklist - New screen for the user on login into Argus ■ Open - Opens Worklist - Open screen for the user on login to Argus. ■ Reports - Opens Worklist - Reports screen for the user on login into Argus
Enable site security	If <i>Enable Security</i> is checked, the site-based data security will be enabled for the user. If the box is not checked, the user will have full access to data from all sites.
Enable LDAP Login	Authenticates users against the active directory server. When Enable LDAP Login is selected, all fields inside the Access section are disabled, excluding the Account Disabled option.
Account Disabled	When this option is selected, the user account is temporarily disabled to prevent users from logging in. This option is different from deleting a user as it enables the Administrator to re-activate the account at a later date.
Security Disabled Account	<ul style="list-style-type: none"> ■ When unchecked, the login procedure keeps track of the number of consecutive unsuccessful attempts at logging into the system. If the count reaches three, the login procedure will always fail the password validation to lock the user out. Administrators with rights to user maintenance can reset the login attempts for the user to unlock the account. ■ When checked, the login procedure that tracks the consecutive unsuccessful attempts at logging into the system do not apply.

Field/Control Name	Description
Force password change at login	If this check box is selected, the users must change the password the first time user logs on to the system after the checkbox is checked.
Force password to expire every	Enables the Administrator to force the user's password to expire in the specified number of days.
Days	Enables the Administrator to enter the number of days after which the password should expire.
Allow unblinding of cases	Enables the user to unblind a study case. For example, a user without unblinding rights will not see the Study Drug field. A user with unblinding rights sees a yellow <i>Unblind</i> tag next to concentration of product field and the <i>Broken by Sponsor</i> option in Blinding Status drop-down list is enabled. User will have to enter password when user selects Broken by Sponsor' option.
Protect from unblinded information	When checked, the user cannot view any unblinded information.
Protect from printing unblinded information	When checked, the user cannot print any unblinded information.
Allow locking of cases	Enables the user, to lock/unlock the cases.
Allow local locking	Enables the user, to locally lock/unlock a case for which local Japan data entry/assessment is complete, triggering the scheduling and/or generation of the applicable local reports.
Allow Global Unlock on Pending Local Lock	Allows users to be set up with the privilege to forcibly unlock a case that is still pending a local lock. This option is enabled only if the Allow locking of cases checkbox (above) is checked.
Allow closing of cases	Allows the user to close the cases.
Route on close case	Opens a routing dialog when the user closes the case.
Enable Checklist on Route	By default, this checkbox is selected. If this checkbox is not selected, the checklist for the Workflow is not displayed to the user while routing the cases, even if the rule that is being used has a checklist.

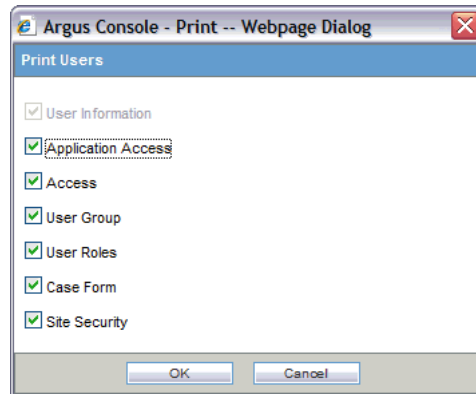
Printing Users

Use the following procedure to print users.

1. Select **Access Management > Argus > Users**.
2. Select a **User** and click to view the user details in the right panel.
3. Click **Print** to display the **Print User** dialog.



- Click OK to display list of Print User options.



- Select the appropriate option(s) and click **OK**.

User Configuration - Roles

Enterprise User	This privilege allows administrators to configure a workflow manager user as an Enterprise user. If Enterprise role is assigned, the user can view cases of any site outside its site.
ESM Admin	This privilege allows the user to access the Interchange Mapping utility in the Argus Console.
Copy Configuration	This privilege lets you copy all the configuration data from the enterprise where they have this role to any new enterprise that they create through the Global Enterprise Management portlet. The factory data Administrator user has this role enabled by default.
Global Admin	This privilege lets the administrator allow users to be designated as Global Users for selected enterprises and not necessarily all enterprises.
AC Library Admin	This privilege lets the administrator allow users to perform specific operation on ACs such as re-assigning the ownership, grant access to various user groups using Permission, Modification, and Deletion.
Workflow Manager	This privilege allows the users to perform specific workflow operations such as routing cases to any workflow state, routing cases to user, viewing all open cases and all action items present in the system, changing the priority of a case and changing the assignee of an action item or a case.

Business Configuration

About Business Configuration

This section explains the Business Configuration of the Argus Console, categorized into the following modules:

Section	Sub-Section	Description
Business Configuration	Products and Licenses:	<p>This section helps in capturing Product Details such as product specifics, product licenses and products involved in the studies.</p> <p>These can be the products marketed, or under investigation, by the company.</p> <p>Refer to the following sections for further information on:</p> <ul style="list-style-type: none"> ▪ Configuring Product Families ▪ Configuring Products ▪ Configuring Licenses
	Studies	<p>This section helps in capturing Study information such as study specifics, products involved in the study licensed countries associated with the study and the clinical references used in the expedited reports.</p>
	Expedited Report Rules	<p>This section helps in capturing Expedited Reporting Rule configuration.</p> <p>The Reporting Rules configuration feature enables the administrator to define the reporting rules or criteria for the cases to be qualified for expedited reporting.</p>

Editable and Non-editable Business Configuration Sections

Each of the three Business Configuration sub-sections supports various views for efficient access to data. Each view consists of a hierarchical tree-structure comprising various nodes such as Family, Product, Licenses, and Countries.

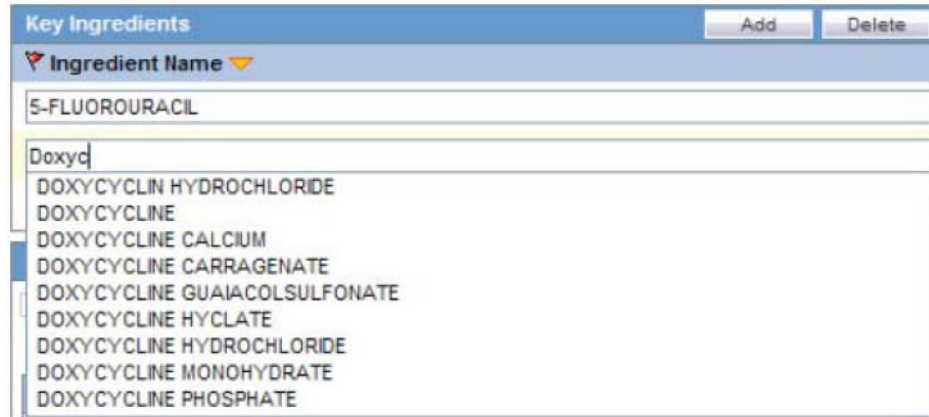
The following table list which nodes can be edited and which cannot.

Business Configuration Sub-Section	Organized By	Node	Editable		
Products and Licenses	Family / Product / Licenses	Family	Yes		
		Product	Yes		
		Licenses	Yes		
	Product / Licenses	Product	Yes		
		Licenses	Yes		
		License / Products	License	Yes	
	Countries / Licenses	Products	Products	Yes	
			Licenses	No	
		Countries / License Type / Licenses	Countries	No	
			License Type	No	
		Studies	Projects / Studies / Products	Projects	No
				Studies	Yes
Products	No				
Studies / Products	Studies		No		
	Products		No		
	Products / Studies		Products	No	
Expedited Report Rules	Countries / Projects / Studies		Studies	No	
			Countries	No	
			Projects	No	
	Country / License Type / Reporting Rule		Country	No	
			License Type	No	
			Reporting Rule	Yes	
	License Type / Reporting Destination / Reporting Rule	License Type	No		
		Reporting Destination	No		
		Reporting Rule	Yes		
Responsible Group / Reporting Rule	Responsible Group	No			
	Reporting Rule	Yes			
	Inactive Rules	Country	No		
License Type		No			
Reporting Rule		Yes			
Active Rules	Country	No			
	License Type	No			
	Reporting Rule	Yes			

Type Ahead Fields

Some fields in the Business Configuration section of Argus Console are enabled with Type Ahead-input. This means that these fields are equipped with the ability to guess what the user is typing.

Based on the text being entered, this feature provides suggestions for the user to choose from.



The following fields have the type-ahead feature:

- Clinical Reference Type (Under **ClinicalStudies Configuration**)
- Ingredients (Under Product Family Configuration)
- Manufacturers (Under Product and License Configuration)
- Project ID (Under Clinical Studies Configuration)
- Reporting Destination (Under **Expedited Reporting Rules**)

Additional Comments Fields

Be aware of the following:

- The system has a **Comments** field that accommodates a maximum of 1000 characters on the **Product Family**, **Product**, and **License and Study** configurations.
- The **Product Configuration** permits a maximum of 50 characters in the PSUR Group Name field. Multiple blank spaces between words will cause the generation of unusable report templates.
- The **License Configuration** permits a maximum of 50 characters in the CTPR Group Name. Multiple blank spaces between words will cause the generation of unusable report templates.
- The **Business Configuration** report prints the **Comments** field, and the system tracks any changes made to these fields in the audit log.

Configuring Product Family

Each company has a set of products to sell and a set of processes unique to its business. The Administrator should be aware of the company business processes and/or workflow rules. The manner of product configuration in Argus Safety will depend on how the company handles its internal workflow related to the release of a product.

Details of the company's products can be added in Argus Safety using the Business Configuration section. This feature helps end-users to retrieve details of company products, without entering significant product information for each case.

Every company product should belong to a product family. Each product within a product family shares the same key ingredient and data sheets but can have a different concentration for the key ingredient.

Configuration of the product is done in the **Business Configuration->Products and Licenses** section.

The following illustration shows the fields associated with this section.

Field Descriptions

The following table lists and describes the fields in this section.

Field	Description
Product Family Name	Enables the user to enter a new product family name.
Product Group	Enables the user to select a product group name.
Ingredient Name	Enables the user to select the multiple key ingredients for the product family <ul style="list-style-type: none"> ▪ The user can sort the field alphanumerically. ▪ Sorting on the ingredient name in the Product Family Configuration updates the sort order in all the products which are part of the same family ▪ A maximum of 25 items are displayed as the search results in the drop-down list. ▪ The Key Ingredients drop-down list enables the user to enter up to 20 active ingredients for a product family.

Adding Product Families

The screen helps in capturing the Product Family information. As per the Argus data model, the Product Family adds the Ingredients, Data Sheets, and the Product group.

Products are associated with Product families and are created using the Data Sheets, Dosage form, Strength and unit of the corresponding Product Family. The **Product Group** field in the Product Family configuration screen enables the Argus administrator to group the product families into various Product Groups.

Use the following procedure to add a product family.

1. In the Business Configuration section, select **Product and Licenses**.
2. In the left panel, select a filtering criterion. The left panel now displays the tree view of the **Family** based on the filtering criterion.
3. Select a Product Family and click to view the product family details in the right panel.

Note: Ensure that you select the top-level folder to view the details of the product family.

Product family details appear in the right panel.

Tip:

- You can alternatively click **Add Family** to create a new family of products.
- Use **Copy** to make an editable copy of an existing product family.
- Use **Copy with Datasheets** to make an editable copy of an existing product family, along with all associated datasheets.

4. Enter the **Product Family Name** as applicable.
5. Select the **Product Group** from the drop-down list. This helps you to group the product families into various product groups.
6. Select the required **Ingredient Name(s)** displayed under the **Key Ingredients** section
7. Select the required Datasheet configuration.
8. Click **Save** to save the changes made to the Product Family.

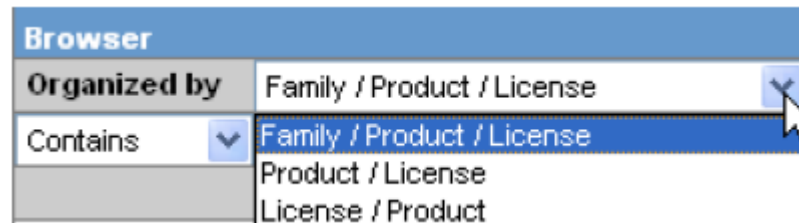
Tip: If you have added a new Product Family, click **Add Family** to save the new **Product Family**.

About Filtering Criterion The filtering criterion is essential as it helps you to search for specific items. The Argus Console provides this option for the Business Configuration section.

Using Organized by

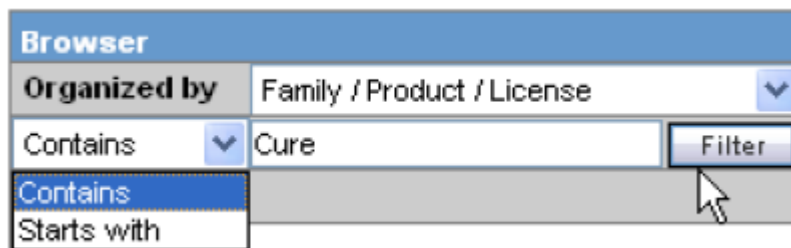
The filtering browser is displayed in the top-left corner of the left panel. The Products and Licenses section can be filtered based on any of the three combinations shown in the following illustration. Consider the following:

- If you enable **Organized by Family/Product/License**, then the generated output will be visible in a tree-format in the left panel.
- If you enable the **Organized by Product/License**, only the Product and License views are available in the tree view in the left panel.



The Argus Console helps you to filter information further for the Business Configuration section. Once you have selected the **Organized by**, you can specify whether your search should contain or start with specific alphabets.

The filtering criterion shown in the following illustration, enables the system to search for all Family/Product/License data that contains the term Cure.



Tip: The number displayed next to the folder indicates the number of Products in the product family.

Creating Data Sheets

Packaged medications (like prescriptions) are marketed with an insert sheet that lists the known contraindications (side-effects) that may occur as a consequence of taking the product. These inserts are also referred to as data sheets. It is important to list these effects in order to ensure accuracy in reporting. An inaccurate report could result in the wrong action taken or bring harm to a patient.

The Listed Events & Indications from the data sheet determine the listedness of the adverse event(s) for the case. Depending on the configured regulatory report rules, the listedness determination will automatically schedule the expedited reports.

The data sheet in the Product Family is configured using the **Business Configuration** -> **Products Family** section.

Field Descriptions

The following table lists the Field Descriptions for this section.

Field/Control Name	Description
Rename	Enables the user to rename the datasheet.
Activate Data Sheet	<p>Enables the user to activate the current data sheet. Be aware of the following:</p> <ul style="list-style-type: none"> ■ When you click the checkbox, the system enables the radio buttons next to Activate Data Sheet. ■ You can either select the option to activate the data sheet with Terms added on the current dates or on another date entered in the Other Date field. ■ Once the datasheet is activated, the system disables the Activate Datasheet text box. ■ If you enter a date greater than the current system date, the system permits you to enable the activation date.
Core Sheet	The Core Sheet checkbox enables the user to indicate that this data sheet is the central data sheet. This checkbox is disabled if another data sheet is marked as the core data sheet.

Field/Control Name	Description
Include	<p>The Include checkbox enables the user to indicate that this data sheet includes the particular datasheet selected in the drop-down list. Be aware of the following:</p> <ul style="list-style-type: none"> ■ The system populates the drop-down list with the list of datasheets that do not include other data sheets. ■ The system enables the drop-down list only when the include checkbox is checked. <p>If a product family has a single datasheet that is marked 'Core', the system disables the Include checkbox.</p>
Other Date	<p>This radio button is enabled if the current date is not to be selected. Select this checkbox and enter any other date, as required.</p>
Global /No local labeling assessment required	<p>Checking this option automatically marks any license using this data sheet, as assessed, and the license does not require any local labeling assessment.</p>
Notes	<p>On clicking the notes icon, a pop-up appears to enable users to enter notes while entering the details of the Datasheet.</p>
Listed Term	<p>This field displays the listed terms (Preferred Term) for the datasheet.</p>
View Revisions	<p>Enables users to view a list of term that were added or removed with the added date.</p>

The View Revisions dialog displays the datasheet revisions, as shown below:

View Revisions

Datasheet Name: CORE

There are more than 1000 terms. Only the first 1000 are displayed, Use "Print" to view all the terms

Rev. No.	Terms	Added On	Active On
1	Pyrexia	22-Jan-2012	22-Jan-2012
1	Nasopharyngitis	22-Jan-2012	22-Jan-2012
1	Rash	22-Jan-2012	22-Jan-2012
2	Headache	25-Jan-2012	25-Jan-2012
2	* Rash	25-Jan-2012	25-Jan-2012
Event Group : Intestinal Disorders			
1	Ageusia	22-Jan-2012	22-Jan-2012
1	Dysgeusia	22-Jan-2012	22-Jan-2012
1	Dyspepsia	22-Jan-2012	22-Jan-2012
2	* Dysgeusia	22-Jan-2012	22-Jan-2012
2	Loss of Taste	25-Jan-2012	25-Jan-2012
2	Epigastric discomfort	25-Jan-2012	25-Jan-2012
Event Group : Skin Disorders			
1	Vitiligo	22-Jan-2012	22-Jan-2012
1	Leukoderma	22-Jan-2012	22-Jan-2012

Print OK

Note: In order to facilitate optimum system performance, you can configure a limit on the number of revised terms that get displayed. If, for example, this value is set to 1000, the datasheet will display only 1000 revised terms in the list. This value is configurable in web.config by using the keyname **DataSheetRevisionTermCount**. The default value is 1000.

Click **Print** to view all other revised terms.

Use the following procedure to create a datasheet.

1. In the **Datasheet** section of the **Product Family** section, click **Activate Datasheet** to activate the data sheet associated with the Product Family.

Note: If you want to make a copy of the datasheet, click **Copy**. Ensure that you enter a new name for the datasheet, if you are making a copy of another datasheet.

2. Select the **Core Sheet** check box, if this data sheet is required to be the core data sheet. Only one core data sheet is allowed per product.
3. Select the **Include** check box and select the value from a drop-down list. This helps you to indicate that this data sheet includes the particular datasheet selected in the drop-down list.
4. Select **Global/No local labeling assessment required** to automatically mark any license using this data sheet as assessed.
5. Click **Add Term** to select the listed terms (Preferred Term) for the datasheet. The MedDRA browser appears.

SOC	HLGT	HLT	PT	LLT	SYN
10027433	10003018	10018067	10059179		

6. The MedDRA Browser available for Datasheets enables the administrator to select either multiple or all Preferred Terms (PTs) in the following way:
 - Click the required High Level Term (HLT) and select multiple PTs by clicking on each required PT.

OR

 - Right-click the HLT to select all entities available under PT.
7. Select the Preferred term from the MedDRA browser and click **Select**.

Tip: You can alternatively click **Select and Close**, in the MedDRA browser to save and exit the Product Family screen.

You can use **Delete Term** to delete the selected listed term(s) from the datasheet.
8. Click **Select** from the **Event Groups** tab of Datasheet to select an event group. The **Event Group Selection** window appears.
9. Press **Save** to save the data sheet. The Data Sheet name displays in the **Data Sheets** list.

Tip: To view the revision history associated with a Datasheet, click **Revisions**. A pop-up appears containing the following information:

- **Rev. No:** Displays the revision number of the datasheet. This number is updated each time the data sheet is activated
- **Terms:** Displays all the terms that were added / removed. In case a term has been deleted, it is marked with * against the term name.
- **Added On:** Displays the date when the terms were added in the datasheet
- **Active On:** Displays the date when the datasheet was made active for that revision

Configuring Products

Each company has a set of products to sell and a set of processes that are unique to its business.

The manner of product configuration in Argus Safety depends on how the company handles its internal workflow, related to the release of a product. Therefore the Administrator should be familiar with the business processes or workflow rules of the company.

Configuration of the product is done in **Business Configuration -> Products and Licenses**.

When configuring a product, be aware of the following:

- When the user clicks the **Notes** link on a data sheet, he/she can enter a maximum of 2000 characters in the **Preferred Terms** section of a data sheet as shown in the following illustration.
- When the user clicks the **Notes** link, he/she can enter one note for each term.
- The user can use the standard spell check function.

- If notes have been entered for the term, the system displays the Notes icon to indicate that notes are present.
- The system also prints the notes on the **Product Family** details.
- A comments field that can contain up to 1000 characters has been added to the **Product Family/Product/License** and **Study** configuration elements.
- The **Product** configuration also has a 50 character PSUR Name.
- The **Business Configuration** reports print the contents of the **Comments** fields.
- The system tracks any updates made to the datasheets in the audit log.

The following illustration shows the fields associated with this section.

Field Descriptions

The following table lists and describes the fields in this section.

Field Name	Description
Product Family Name	Enables the user to enter the unique family name for the product. The Product Family Name must be of at least five (5) characters.
Product Group	Select the product group for the product.
Ingredient Name	Displays the Ingredients of the Product Family to which the Product belongs. The user can alphanumerically sort the field. Sorting on the ingredient name in the Product Configuration updates the sort order in the corresponding Product Family and all the other products which are part of the same family.
Datasheet	To view the description of the fields of this section, see Creating Data Sheets .

Field Name	Description
Preferred Terms	Displays the Listed Term (Preferred Term) for the product, as described in the field description table under Creating Data Sheets .
Event Groups	<p>The Event Group, selected from the Select button > Available Event Groups dialog, is displayed as follows:</p> <p>Event Group Name in English</p> <p>The event group name is displayed in the following format for Japanese users: Event Group Name in English (Event Group Name in Japanese)</p> <p>The count of the total number of Event Group Names present for the case is displayed on the header of the Event Groups tab.</p> <p>For more details about Event Groups, see the section Event Groups tab under Configuring Event Groups.</p>

Adding Products

This screen helps in capturing Product Details (product specifics, product licenses, products involved in the studies. These can be the products marketed, or under investigation, by the company. Every company product should belong to a product family. Each product within a product family shares the same key ingredient and data sheets but can have a different concentration for the key ingredient. This data is reflected in multiple expedited and periodic reports and case form-general information section.

Use the following procedure to add a product.

1. In the Business Configuration section, select **Product and Licenses**.
2. In the left panel, select a filtering criterion.
3. Select a Product and click to view the product details in the right panel.

Note: Ensure that you select the second-level folder to view the details of the product.

4. The details of the product appear in the right panel.

Tip:

- You can alternatively click **Add Product** to create a new product.
 - Use **Copy** to make an editable copy of an existing product.
 - Use **Copy with Licenses** to make an editable copy of an existing product, along with all associated licenses.
5. Enter the Product Name and Product Abbreviation.
 6. Enter the **Dose** information associated with the Ingredient Names in the **Key Ingredients** section.
 7. Select the **Unit** information from the drop-down list, associated with the Ingredient Names in the **Key Ingredients** section.
 8. Enter the **Generic Name**.

Tip: To copy all the Key Ingredients entered in the previous section, click **Copy From Ingredients**. This helps you to modify the list as required, instead of entering all the names manually

9. Enter the Dosage Formulation.
10. Enter the **Strength** of the dosage and select the **Units** from a drop-down list.
11. Click **Encode** to enter the **Primary Indication**. This enables you to display a primary indication for the product using either the MedDRA or the ICD-9 Dictionary.
12. Enter the **Model #** number associated with the product.
13. Select the **Manufacturer** from the drop-down list.
14. Click Select icon to select the **WHO Drug Code** associated with the product.
15. Enter the **Company Code** allotted for the product.
16. Enter the **Lot#** and **Date** associated with the Product.

Tip: You can click **Add** to add new **Lot#** numbers. If you wish to add the current date in the **Date** field, use the = sign on your keyboard as a short-cut.

17. Click **Save** to save the product details.

Tip: If you have added a new Product, click **Add Product** to save the new **Product**.

About Filtering Criterion The filtering criterion is essential as it helps you to search for specific items. The Argus Console provides this option for the Business Configuration section.

Using Organized by

The filtering browser displays in the top-left corner of the left panel. The Products and Licenses section can be filtered on the basis of any of the three combinations displayed below. Consider the following:

- If you enable **Organized by Family/Product/License**, the generated output is visible in a tree-format, in the left panel.
- If you enable **Organized by Product/License**, only the Product and License views are in the tree view in the left panel.

The Argus Console helps you to filter information further for the Business Configuration section. Once you have selected the **Organized by**, you can specify whether your search should contain or start with specific alphabets.

For example, the filtering criterion defined in the following illustration searches for all Family/Product/License data that contains the term Cure.

The left panel now displays the tree view of the **Product Family->Product** based on the filtering criterion.

Tip: The number displayed next to the folder signifies the number of licenses within that product.

Configuring Licenses

Once product configuration is complete, you must create product licenses. Licenses are issued for pre-market and post-market release of a drug, device, or vaccine. Investigational (pre-market) licenses are issued for studies done at study centers and marketed licenses are issued for release of product. Configuration of licenses related to a product is a key step in the configuration of Argus Safety.

Configure licenses in the **Business Configuration -> Products and Licenses** section.

The following illustration shows the fields associated with this section.

Field Descriptions

The following table lists the Field Descriptions for the License configuration section.

Field/Control Name	Description
Trade Name	Enables the user to enter the Trade Name under which this product(s) is (are) authorized by this license.
Award Date	Enables the user to enter the license award date for this license.
Withdrawn Date	Enables the user to enter the license withdrawal date for this license. The withdrawn date cannot be less than the award date.
Market Authorization Holder	Enables the user to select a manufacturer or co-marketing partner for this license of the product.
Biologic / Vaccine	Whether the license is for a Biologic/Vaccine (this can impact reporting rule). If this option is checked MedWatch will print PLA# not NDA# in section G5. It is included to support the Biologic License Application (BLA) and the Product License Application (PLA) requirements.

Field/Control Name	Description
Not in Tradename lookup / Not Auto-scheduled	<p>An option to indicate that this license name should not appear in the filter criteria for Auto Scheduling of Reports or trade name lookup browser.</p> <p>When this checkbox is checked, the trade name will not appear for this license in the Trade Name Lookup dialog and this license will not be evaluated or allowed for auto scheduling of the reports, but will be available for manual scheduling of reports.</p> <p>The license will be displayed in event assessment.</p>
Labeled for Single Use	<p>Whether the drug is for single use (such as disposables)</p> <p>If this option is selected it will mark YES in section H5 of the MedWatch device form, otherwise it will mark NO.</p>
OTC Product	This enables the user to specify if the Product has been bought as an Over-the-Counter Product.
Datasheet URL	User can enter a hyperlink to a site giving information about the datasheet of the product.
Authorization Country	<p>This enables the user to select the Country for which this license applies.</p> <p>The chosen country does not impact the reporting rules algorithm. This field maps to the Country' field in the Reporting rules configuration.</p>
License Type	<p>The user can select one of the possible six types:</p> <p>Investigational Drug/Device/Vaccine or Marketed Drug/Device/Vaccine</p> <p>The chosen license type maps to the License type field under each country on the Reporting rules configuration.</p>
Datasheet Name	<p>The datasheet drop-down enables the user to associate a datasheet with the License.</p> <p>The field lists the datasheets for all the product families of the added products.</p> <p>The Data Sheet drop-down is enabled when one or more products have been added to the Products list.</p>
Application Type	Enables the user to license application type such as IND, NDA, STN etc.
License #	Enables the user to enter the License Number of the Trade name.
Company Item Number	Enables the user to enter the Company Item number corresponding to the license.
Countries List	Enables the user to select all the countries in which the same license was issued. The system adds the authorization country to the Countries List and updates the list when the user updates the authorization country.
TIKEN	Selecting the TIKEN checkbox indicates that the customer will not send the investigational report for the other license.
Status Category of New Drugs	The Status Category of New Drugs field captures the Status category of new drugs. This information is transmitted in the J.2.4k element of PMDA E2B R3.
Risk Category of OTC Dugs	The Risk Category of OTC Dugs field captures the risk category of OTC drugs. This information is transmitted to the J.2.5k element of PMDA E2B R3.
Product Name	The Product List box displays the list of products (product name, dosage form and strength) that this associated license covers for regulatory reporting purposes.

Field/Control Name	Description
Hide	When a product is marked as non display, it will not appear in the Trade Name Product lookup dialogue associated with the license tradename.
PMA/510(k)#	This field is associated with medical device information and prints in expedited reports.
Nomenclature Code	This field is associated with medical device information and prints in expedited reports.
Medical Device Information	This field is associated with medical device information and can contain the following values: <ul style="list-style-type: none"> ■ AIMD Active Implants ■ MDD Class III ■ MDD Class IIb ■ MDD Class IIa ■ MDD Class I ■ IVD Annex II List A ■ IVD Annex II List B ■ IVD Devices for self-testing ■ IVD General ■ Class I ■ Class II ■ Class III ■ Class IV ■ Blank (default)
CE Marked	CE marking is a mandatory conformity marking for certain products sold within the European Economic Area (EEA). For a Marketed or Investigational Device, this field can be set to Yes or No. For all other license types, this field is disabled.
CTPR Group Name	This value is used in Argus Safety when filter periodic report data.
Comments	Enables the user to enter information about the element configuration.
Device Company Identification#	Enables you to capture information about the Device Company Identification number.
Device Identification#	Enables you to capture information about the Device Identification number.

Adding Product Licenses

This screen helps capture License information (License specifics, associated with the License, Countries where the product is marketed or is under investigation). This data is reflected in multiple expedited and periodic reports and in case form-product information section.

Use the following procedure to add a product license.

1. In the Business Configuration section, select **Product and Licenses**.
2. In the left panel, select a filtering criterion.
3. Expand the folders till you reach the license associated with a product.
4. Select a license and click to view the license in the right panel.

5. The system opens the following screen:

1. Enter the **Trade Name** of the license.
2. In the **Manufacturer** list, select the manufacturer of the product.
3. Select the **Authorization Country** in which the license was issued.
4. Select the **License Type**. This is the type of license.
5. Enter the license number in **License#**.
6. If this license is to be reported under the PLA# and not the NDA# select the **Biologic/Vaccine** checkbox. If this checkbox is selected, the PLA# (and not the NDA#) will be printed in section G5 of the MedWatch form.
7. Specify if the drug is **Labeled for Single Use** or not.
8. Specify if the drug has been bought as an **Over-the-Counter (OTC) Product**.

Note: If the **OTC Product** checkbox is checked in **Business Configuration > Products and Licenses** for a product whose **Authorization Country** is US and **Withdrawn Date** is blank, then the **OTC Product** checkbox in the **Case Form > Analysis > Medwatch** tab will be checked automatically on selecting the product license if the **Initial Receipt Date** is equal to or greater than the **Award Date** of the license.

9. Under **Award Date**, enter the date the license was granted to the manufacturer.
10. Enter the **Withdrawn** date, if applicable.
11. Enter the Company item number in **Company item number**.
12. Enter a URL reference for the license under **Data Sheet URL** (A URL reference might be a link to product label or product information).

13. A world wide web address or an appropriate network path (For example: `http://anydomainname/anypath` or `\\FILESERVER\LOCATION`) can be entered in this field.
14. Select **Not in Tradename lookup/Not Auto-Scheduled** if this license is not to be involved in reporting.
15. In the **Countries List**, select the countries that define whether the case will be classified as domestic or foreign for regulatory report scheduling algorithm.

Tip: To modify this list, use the **Modify** option (placed next to the Countries List).
16. Select the **Data Sheet Name** associated with the license, from the drop-down list.
17. Click **Add** in the **Product Name/Dosage Form/Strength** to add a product to the License

Tip: You can alternatively click **Add License** to create a new license.
Use **Copy** to make an editable copy of an existing license.

6. The **ProductBrowser** dialog opens.
7. Enter the name (partial or full) of the product and select **FullSearch**.
8. Select the appropriate product in the search results and click **Select**. Enter all the required products in this manner.

Using the Product Browser

1. Click on **Add Products** to add products.
2. The **Products Browser** window opens:
 - Enter the **Ingredient** key word for the search. The ingredient is displayed in the first column.
 - Select the **Ingredient** to obtain the **Family** it is associated with.
 - Select the **Product Name** to view the associated Trade Names.
 - Select the **Trade Name** required.
3. **Select** is now enabled at the bottom of the window.
4. Click **Select** to add the product details under the **Product Name** section. The Product Name is displayed in under the Product Name section.

The screenshot shows the 'Product Browser' window. At the top, there are search filters: 'Full Search' (checked), 'Clear', 'Drug Code' (empty), 'Country' (UNITED STATES), and 'Search'. Below this is a table with four columns: 'Ingredient', 'Family', 'Product Name', and 'Trade Name'. The first row is highlighted in yellow and contains the following data: 'ALTEPLASE' in the Ingredient column, 'Activase' in the Family column, 'Activase (Injection), 200mg' in the Product Name column, and a list of trade names in the Trade Name column, including 'Activase, 1549 (UNITED STATES 1549)'. Below the table, there is a summary section with fields for 'Family' (Activase), 'Ingredient' (ALTEPLASE), 'Product Name' (Activase (Injection), 200mg), 'Trade Name' (Activase, 1549 (UNITED STATES 1549)), 'Model #', 'Drug Code' (unk), and 'Indication'. At the bottom right of the summary section are 'Select' and 'Cancel' buttons.

5. The product browser available for datasheets, enables the administrator to select either multiple or all Product Names as follows:
 - Click the Family name and select multiple Product Names by clicking on each required Product Name.
 - OR
 - Right-click the Family name to select all entities available under Product Name.
6. Click **Save** to save the changes.

Tip: If you have added a new License, click **Add License** to save the new **License**.

Configuring Clinical Studies

It is important to configure clinical studies in the Argus Console because it helps the system categorize the source of information for the cases that have been registered. This screen helps in capturing Study information (study specifics, products involved in the study licensed countries associated with the study and the clinical references used in the expedited reports).

Configuration of the product is done using the **Business Configuration->Studies** section.

The following illustration shows the fields associated with this section.

Field Descriptions

The following table lists and describes the fields in this section.

Field/Control Name	Description
Study ID	This is the Study ID.
Project ID	This is the project ID for the study.
Other ID	Enter any other ID associated with this study.
Observe Study Type (E2B)	This enables the user to select the study type from a drop-down list. <ul style="list-style-type: none"> This element is populated from the Case Form Clinical Study section of the application. The value selected in Study Configuration, <i>Observe Study Type (E2B)</i> is populated in the Case Form Study section when the user selects the Clinical Study. The system updates the standard E2B profiles (EMA, FDA, and ICH) to populate the tag.
Template Only	Select this checkbox to select only a template for the study.
Study Development Phase	Enables you to choose the study phase.
* Non-Interventional Study	Enables you to identify a study as a non-interventional study. The available options are Yes and No . The default value is set to No . This field is not used in the application (Case Form, Reports) for this release.
Arms	
Study Name	Enter the name of the study. This is a mandatory field. You can add upto 99 Arms to a study.
Study Type	Enter the type of study. Note: The Study Name and the Study Type fields must be unique for a study.

Field/Control Name	Description
Primary License	Select the applicable primary license from the list of licenses available in this drop-down list. These licenses are displayed as per the products that have been selected for the Arm. This drop-down list is displayed as blank for a new Arm.
Copy	Click this button to copy a selected Arm.
Delete	Click this button to delete a selected Arm.
Products	
Product Name (Dosage Form /Strength/Units)	Provides information about the Product Name along with the (Product formulation/Product Concentration/Product Units).
Blinded	Check this checkbox to configure a blinded study. You cannot check this checkbox if the Study Type for that Arm is not blinded. Note: A Study is eligible for Unblinding checkbox is enabled when a study has at least one Arm with Study type as Blinded (Single/Double). The Study is eligible for Unblinding checkbox should be unchecked in study configuration. If this checkbox is checked, the user will be able to see the complete case data even if he has protection enabled.
Product Type	Allows you to select a Product Type from the drop-down list comprising options of 'Investigational Product', 'Placebo', and 'Comparator'.
Products -Add WHO Drug	Opens Search Screen for selecting a non-company product.
Products -Add Product	Opens Search Screen for selecting a company product.
Products -Delete	Deletes the selected product row.
Clinical References	
Reference Type	Shows the various reference types that can be setup for this study.
Country	Enables the user to select a country for the clinical reference type.
Reference Number	Captures the reference number that will be reflected on the regulatory reports.
Add	Enables the user to add another clinical reference.
Delete	Enables the user to delete the selected clinical reference.
Countries	Enables the user to select a country for the clinical reference type.
License	This is the license of the primary (company) product participating in the study.
Product Abbreviation	This enables the user to enter an up to 5 character abbreviation of the study name which would be used in Case numbering when Product' is selected in the system numbering configuration in case of study cases.
Centers	The system displays the selected study centers for the study.
Study Description	Enables the user to enter a brief description of the study. Opens the study description in zoom mode and provides a spell check dialog. Opens the multi lingual dialog allowing the user to choose the language by clicking on the relevant flag of the country.

Field/Control Name	Description
Investigator Alert	Enables the user to select an existing Advanced Condition. Under Investigator alert, an advanced condition can be created / selected. When this condition is satisfied, the system automatically sends an e-mail to the investigator group associated with this study.
Investigator Alert - select	Opens up the Advance Condition browser.
Study is eligible for Unblinding	Check this box if the study can be unblinded. If the Study Type selected is Not Blinded", this field is disabled. This checkbox is enabled when a study has at least one Arm with Study type as Blinded (Single/Double).
Enable Study Specific Encoding	User checks this box if Study specific Auto encoding has to be enabled.
Autoencoding: Drugs(dict)	If unchecked (default state) the study will use the dictionaries configured using the Case form Configuration options. If checked, the Auto encoding button is activated.
Autoencoding: Events & Indications	Select this field to enable the system to encode Events & Indications using the dictionary the user selects from the list.
Study Reporting	
Products -Add Product	Opens the Search screen for selecting a company product.
Products -Delete	Deletes the selected product row.
Inherent Reporting Rules Form	This drop-down list is populated from all the Study templates which are configured for SUSAR Reports. Users can use the pre-defined SUSAR reports by selecting the applicable template from the drop-down list.
Always report	Usually the study-specific reporting is configured to handle reporting requirements for non-company products, e.g. Placebo or a comparator, as the company-based reporting is taken care by the license based reporting logic utilized in Argus. However, checking this checkbox will force Argus to check for qualifying expedited reporting rules based on the country, license type and reporting destination specified even if no non-company products are identified as study drugs. If the checkbox is unchecked then expedited reports based on the study-specific reporting rule will only be scheduled if there is a non-company product identified as a study drug.
Country	Specifies what country's reporting rules the console should consider. The list includes countries for which the expedited reporting rules exist.
License Type	Specifies what license type to consider for the specified country. Only applicable license types, i.e. Marketed Drug, Device, Vaccine or Investigational Drug, Device, Vaccine are displayed in this drop down list. For example if a country Germany" only has reporting rules for investigation drugs, then Investigational Drug" is the valid drop-down element.

Field/Control Name	Description
Reporting Destination	<p>This field is optional and by default will have the value All.</p> <p>Specifying any value in this list limits the reporting rules to be evaluated to the selected country, license type and reporting destination. The drop-down list is filled with valid destinations (regulatory authorities) for the country and license type selected based on the expedited reporting rules.</p> <p>For example, if the user has selected Germany, Investigation Drug and there are reporting rules for Germany with destinations of BfArM¹ and Drugs R us², then only these two destinations (LM: regulatory authorities) are displayed.</p>
Time Frame	<p>This field cannot be searched or altered, but is included for informational purposes.</p> <p>Based on the country, license type and reporting destination selected, the system determines and displays all possible time frames in ascending order separated by a comma.</p>
Possible Report Forms	<p>This field cannot be searched or altered, but is included for informational purposes.</p> <p>Based on the country, license type and reporting destination selected, the system should determine and display all possible report forms in alphabetical order separated by a comma.</p>

Adding Clinical Study Configurations

This screen helps capture study information (study specifics, products involved in the study licensed countries associated with the study and the clinical references used in the expedited reports). Study Information is required if a case has been reported while conducting a study and the participating product(s) belong to the company. This data is reflected in multiple expedited and periodic reports and case form-general information section.

Be aware of the following:

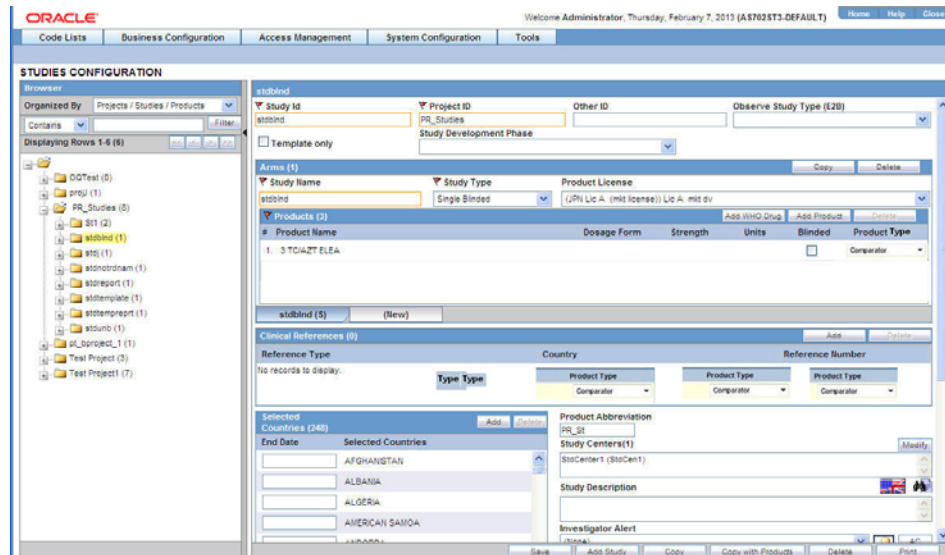
- The IND Reference Number drop down displays only those reference numbers (license numbers) associated with a product with a License Type of Investigational.
 - Console -> Business Configuration -> Studies -> Clinical Reference section (in middle of screen).
 - The **Reference Number** drop down field should be limited to IND (Investigational) US Licenses Number only.
- The Study Name on the Study Configuration can be a maximum 70 Characters (same as the Product name).

Use the following procedure to add a study:

1. In the Business Configuration section, select **Studies**.
2. In the left panel, select a filtering criterion.
3. Select a Study and click to view the study details in the right panel.

Note: Ensure that you select the study-level folder to view the details of the study.

4. The details of the study appear in the right panel.



Tip:

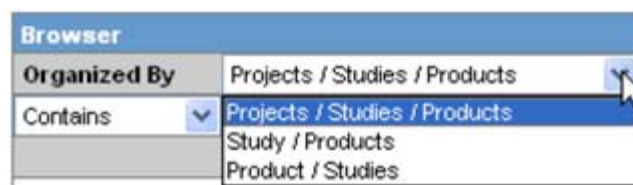
- You can alternatively click **Add Study** to create a new study.
- Click **Copy** to copy of the Study Name and the Study Type data to the new Study.
- Click **Copy with Products** to copy the Study Name and the Study Type data, as well as to copy the blinded and open products.

5. Enter the **Study ID** and **Study Name** associated with the Study.
6. Select the **Project ID** for the Study, from the drop-down list.
7. Select the **Study Type** associated with the Study, from the drop-down list.
8. Enter the **Other ID**. This will be an alternative id for the Study.
9. Select **Template** to associate a template with the Study.
10. Select the **Observer Study Type(E2B)** from the drop-down list.

About Filtering Criterion The filtering criterion is essential as it helps you to search for specific items. The Argus Console provides this option for the Business Configuration section.

Using Organized by

The filtering browser displays in the top-left corner of the left panel. The studies section can be filtered based on of any of the three combinations shown in the following illustration. The generated output is visible in a tree-format, in the left panel, based on the entire categorization of Projects, Studies, Products.



If you enable the **Organized by** Study/Products, only the Study and Product views will be available in the tree view in the left panel.

The Argus Console helps you to filter information further for the Business Configuration section. Once you have selected the **Organized by**, you can specify whether your search should contain or start with specific alphabets.

The filtering criterion shown in the following illustration, enables the system to search for all Projects/Studies/Products data that contain the term Cure.

The screenshot shows a 'Browser' window with a dropdown menu for 'Organized By' set to 'Projects / Studies / Products'. Below it, a 'Contains' dropdown is set to 'Cure', and a 'Filter' button is visible. A second dropdown menu is open, showing 'Contains' and 'Starts with' options.

The left panel displays the tree view of the **Projects/Studies/Products** based on the filtering criterion.

Tip: The number displayed next to the folder signifies the number of studies/products within that project/studies family.

Adding WHO Drug Details

Use the following procedure to add WHO Drug detail information.

1. Select **Add WHO Drug** in the Products section to add the WHO Drug details associated with the Study.
2. Click on **WHO Drug** to add WHO drug details (using the WHO Drug browser window) associated with the Study.
3. The system opens the WHO Drug browser window.

The screenshot shows the 'Drug Coding -- Webpage Dialog' window. It features a search bar with radio buttons for 'Drug Code', 'Medicinal Prod ID', 'Trade Name', and 'Ingredient'. The 'Trade Name' radio button is selected. Below the search bar is a table with columns for 'Trade Name', 'Formulation / Strength', 'Sales Country', and 'Generic?'. At the bottom, there is a 'Drug Detail' section with input fields for 'Trade Name', 'MAH', 'Drug Code', 'ATC Code', 'ATC Description', 'Medicinal Product ID', and 'Ingredients'. 'Select' and 'Cancel' buttons are at the bottom right.

4. Select the **Trade Name** or the **Ingredient** radio-button, to search for the WHO Drug term associated with either the Trade Name or the main Ingredient of the drug.

5. Click **Search** to execute the search. The data is displayed as follows.
6. Select the required component/row (this can be the key **Trade Name** or **Ingredient**).
7. The row now appears highlighted and the **Drug Details** section displays the associated information.
8. Click **Select** to add this drug information in the **Product Name** section of the Studies Configuration window.
9. The WHO Drug browser window closes and the drug appears in the **Product Name** section.

Adding Product Details

Use the following procedure to add details about the Product in the Product Browser.

The screenshot shows the 'Product Browser' window. At the top, there are search fields for 'Drug Code' and 'Country' (set to 'UNITED STATES'). Below this is a table with four columns: 'Ingredient', 'Family', 'Product Name', and 'Trade Name'. The first row is highlighted in yellow and contains the following data: 'ALTEPLASE' in the Ingredient column, 'Actvase' in the Family column, 'Actvase (injection) , 200mg' in the Product Name column, and 'Actvase, 1549 (UNITED STATES 1549)' in the Trade Name column. To the right of the table is a scrollable list of trade names, with 'Actvase, 1549 (UNITED STATES 1549)' selected. Below the table, there are input fields for 'Family', 'Ingredient', 'Product Name', and 'Trade Name', each containing the corresponding data from the highlighted row. At the bottom of the window, there are 'Select' and 'Cancel' buttons.

1. Select **Add Product** in the Products section to add the products associated with the Study.
2. Click on **Add Products** to add products. The Product Browser window appears.
3. Enter the **Ingredient** key word for the search. The ingredient is displayed in the first column.
4. Select the **Ingredient** to obtain the **Family** it is associated with.
5. Select the **Product Name** to view the associated Trade Names.
6. Select the **Trade Name** required.
7. **Select** is now enabled at the bottom of the window. Click **Select** to add the product details under the **Product Name** section. The Product Name is displayed in under the Product Name section.

Tip: To delete a product, select the product and click **Delete** (placed next to Add Product). A pop-up appears asking you to confirm the action.

1. Select the **Reference Type** associated with this Study, from the drop-down list.
2. Select the **Country** associated with this Study, from the drop-down list.

3. Enter the **Reference Number** associated with the Reference Type in this Study.

Tip:

- To add more **Reference Types** in the Clinical Reference section, simply click **Add**. A new row is added to this section.
- To delete the **Reference Type**, select the Reference Type and click **Delete** (placed next to **Add**). A pop-up appears asking you to confirm the action.

4. The **Countries** field is a display only field. You can **Add** or **Delete** this list based on your requirements.
5. Select the **Product License** from the drop down list. This is the license of the primary (company) product participating in the study.
6. Enter the Product Abbreviation.
7. The **Centers** are displayed as per the centers you choose to associate with the Study. To modify this list, click on **Modify** (placed next to **Centers**). Using this option you can add and delete Centers associated with the Study.

Tip:

- To add more **Centers** to the Study Center list, use the **Add>>/ Add All** options.
- To delete the **Centers** from the Study Center list, use the **Delete>>/Delete All** options.

8. Enter the **Study Description** associated with the Study.
9. Click **Select** placed next to **Investigator Alert** to select or create an Advanced Condition for this Study.
10. Select **Study is eligible for Unblinding** to enable the study to be unblinded.
11. Select **Enable Study Specific Encoding** to enable the study specific Auto Encoding.

Configuring Auto Encoding

The Auto Encoding features helps you to configure your own dictionary of encoded data. Using this enables you to:

- Configure studies to use dictionaries different from the dictionaries configured using the Case Form configuration.
- Retrieve coded Events, Drugs and Events & Indications and codes from the lists associated with this section.
- Ensure that the expedited reports display the correct verbatim and coded terms

Use the following procedure to configure Auto Encoding.

1. Click Auto Encoding to open the Auto Encoding dialog. The Auto Encoding dialog opens.

Modify Case Form Configuration

Auto Encoding, Dictionary & Central Encoding

Drugs WHO DDE C3 June 1, 2017

Events & Indications MedDRA J Browns V20.1J **Centralized Coding**

Prevent manual encoding for event terms

Require event term encoding before case closure

Duration Calculations

Event Inclusive Exclusive

Drug Inclusive Exclusive

2. Select the encoding options as required for **Drugs** and **Events & Indications**. Use the items in the list to encode. For Study Encoding, go to **Console -> Business Configuration -> Studies -> Study Encoding** to support Central Encoding for Events & Indications for study cases, in a similar way as for non-study cases. Checking the Central Encoding checkbox (next to the Event & Indications Checkbox) also ensures that Central Encoding also gets reflected (as configured here) in the Argus Case Form, for study cases.

STUDIES CONFIGURATION

Study Encoding - Workpage Editing

Auto Encoding, Dictionary & Central Encoding

Events & Indications **Centralized Coding**

Prevent Manual Encoding for event terms

Require event term encoding before case closure

3. Select **Prevent manual encoding for Events & Indications**, if you want to disable manual encoding by users.
4. Select the **Require event term encoding before case closure**, to ensure that the expedited reports display the correct verbatim and coded terms.

Note: If this feature is not selected, then the study will use the dictionaries configured using the Case Form Configuration options.

Cases where the report type does not include clinical trial cases, will always encode with the dictionaries configured through the Case Form configuration options.

5. Select **Inherit Reporting Rules From** using the drop-down list to configure study-based reporting requirements.

Configuring Study Reporting

Study Reporting is provided in the Study Configuration section to configure study-based reporting requirements.

The reporting rules are not directly defined in the study, but rather identify which reporting rules to check from the already configured expedited reporting rules.

The identification is based on specifying what set of reporting rules to evaluate, as per the criteria of:

- Country
- License Type
- Reporting Destination

Use the following procedure to configure study based reporting.

1. Click **Add** in the **Inherit Reporting Rules From** section. The Study Reporting dialog opens.
2. Select **Always Report** as required.

Tip: Select this checkbox to force Argus to check for qualifying expedited reporting rules. These rules are based on the country, license type and reporting destination specified. Refer to the Field Descriptions for details.

3. Select the **Country** from the drop-down list.

Tip: This field specifies which country's reporting rules should be included. The drop-down list includes countries for which the expedited reporting rules exist.

4. Select the **License Type** from the drop-down list.

Tip: This field specifies the license type to be considered for the specified country. Refer to the Field Descriptions for details.

5. Select the **Reporting Destination** from the drop-down list.

Tip: This field is optional.

6. The **Time Frame and Possible Report Forms** cannot be searched or altered, but is included for informational purposes.

Tip:

- To add information pertaining to inheriting reporting rules in the **Study Reporting** section, click **Add**
- To delete information pertaining to inheriting reporting rules in the **Study Reporting** section, select the reporting rule and click **Delete**. A pop-up appears asking you to confirm the action.

7. Click **Save** to save the changes made to the **Studies** section.

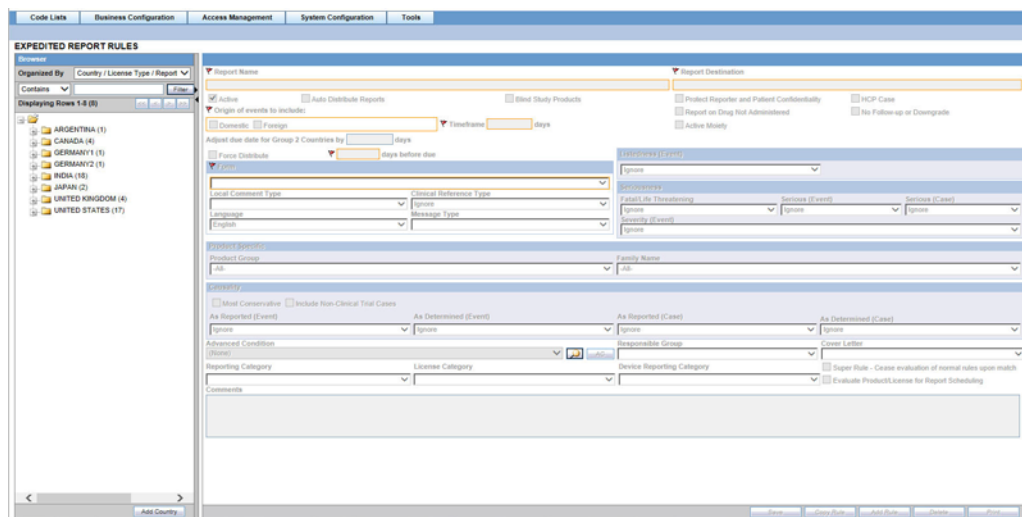
Tip: If you have added a new Study, click **Add Study** to save the new **Study**.

Configuring Expedited Report Rules

This section describes the configuration of Expedited Reports using pre-defined rules. These reports are required by Regulatory Authorities. The Administrator is responsible for entering information about Regulatory Authorities to which regulatory reports will be submitted.

This information is entered in the **Regulatory Agency Information** screen. Information about the local company contact for a regulatory authority can also be entered in this screen.

Configuration of the expedited report rules is done using the **Business Configuration** -> **Expedited Report Rules** section shown in the following illustration.



When configuring expedited reporting rules, be aware of the following:

- If the user **does not** have permission to access **Advanced Conditions** on the **Expedited Reporting Rules**, the system does the following:
 - Displays the advanced condition name instead of displaying a blank.
 - **Does not** permit the user to modify or view advanced condition details.
 - Disables the **Advance Condition** button.
- The system enables the user configure the **Blinding Study Products** option for those included in the case (default unchecked).
 - The system track updates to this field in the audit log.
 - The **Reporting Rules** reports print the new options
- For cases where expedited reports are due, the user can force-distribute expedited reports even if processing is incomplete.
- Due Dates for expedited reports differ from Country to Country regulations. For Group 1 countries, the Due Date is based on the Aware Date received globally for the case.
For Group 2 countries, the Due Date is based on the Aware Date when the affiliate or a company representative of that country received information about the case. In that case, the Due date for these reports could be 15 days after the report was actually generated based on the aware date received globally.
When reports are scheduled and generated, the Due Date for Group 2 countries is calculated. The Due Date for a Group 2 Country = Report Generation Date + Additional days for Group 2 countries.
The Due Date for a Group 2 country can be adjusted as per the holidays and weekends, through the **Adjust Due Date for Group 2 countries by XXX days** field.
- If two or more duplicate reports have different due dates (regardless of license type), the system schedules the report with the earliest due date.
- The reporting rules have a **Force Distribute XXX days before due** checkbox. The default is unchecked.

- If the user checks the **Force Distribute** option, the **# of days before due** field is entered and automatically checks the **Auto Distribute** checkbox on the reporting rule (grayed out).
- The user can enter the number of days from 0 - # of days defined within the time frame.
- If the user enters a value greater than the defined time frame, the system displays the following message:
Please enter a value less than the Time Frame defined for the Reporting Rule.
- If the user has not checked **Force Distribute**, the system disables the days before due.
- The system tracks updates made to the new Argus Console fields in the audit log.
- The system prints an audit log and print out that shows the expedited report rules information as shown in the following illustration.
- A super rule is a rule that overrides other rules when it finds a match. Be aware of the following:
 - The system executes a super rule before executing any other reporting rules.
 - If a super rule matches, it executes all the super rules but does not execute other rules.
 - If the super rule does not match, the application executes the other rules.

Expedited Report Rules	
As of 05 January 2012	
Expedited Report Rule Information	
Country	UNITED STATES
License Type	Marketed Drug
Report Name	US1997000003 & 6
Reporting Destination	CDER
Origin of Events to Include	<input checked="" type="checkbox"/> Domestic <input type="checkbox"/> Foreign
Timeframe	3 days
Adjust Due date for Group 2 Countries by	3 days
Advanced Condition	Adv Condn for investigator alert
Responsible Group	US Distribution
Cover Letter	
<input checked="" type="checkbox"/> Active Rule	<input type="checkbox"/> Auto Distribute Reports
<input type="checkbox"/> Active Moiety	<input type="checkbox"/> Blind Study Products
<input type="checkbox"/> Force Distribute days before due	<input type="checkbox"/> HCP Case <input type="checkbox"/> No Follow-up or Downgrade
<input type="checkbox"/> Protect Reporter & Patient Confidentiality	<input checked="" type="checkbox"/> Report on Study Drug not Administered
Reporting Category	
License Category	
<input type="checkbox"/> Super Rule - Cease evaluation of normal rules upon match	

Field Descriptions

The following table lists and describes the fields in this section.

Field/Control Name	Description
Report Name	Enables the user to view or enter the name of the Report.
Report Destination	Enables the user to select the name of the agency to which the report will be scheduled.

Field/Control Name	Description
Active	<p>Enables the user to specify whether the configured rule is active or inactive.</p> <ul style="list-style-type: none"> Only active rules are considered for report scheduling. Inactive rules are not checked when the report scheduling algorithm runs.
Auto Distribute Reports	<p>Enables you to distribute reports automatically. Except the E2B Reports, all the Expedited Reports that are selected for auto-distribution are tracked under the Worklist-> Bulk Transmit screen. The E2B Reports which are transmitted automatically, are tracked from Worklist-> Bulk Transmit E2B.</p>
Protect Reporter and Patient Confidentiality	<p>Enables the user to configure Protect Reporter and Patient Confidentiality</p> <ul style="list-style-type: none"> If this option checked and a report is generated or draft is viewed, the Patient and Reporter information will be hidden. This option will override the check-boxes on the case form (for Protect Reporter and Protect Patient) if it is checked. If this option is unchecked, the Case Form check-boxes will take effect. The Reports listed below will check for the Reporting Rule Confidentiality Flag: <ul style="list-style-type: none"> EU Device Initial EU Device Final French CERFA Report CIOMS Report MedWatch Report Vaers Report
HCP Case	<p>When checked, the system check for any reporter in the case where HCP=Yes. This enables the report to be scheduled if other parameters for the reporting rules are satisfied.</p> <p>The default is unchecked.</p>
Report on Drug Not Administered	<p>If this checkbox is checked, system schedules report for the suspect products (study or non-study products) that are marked as 'Drug not administered' along with the other suspect products in the case.</p> <p>If this checkbox is unchecked, system ignores suspect products (study or non-study products) that are marked as 'Drug not administered' and Reports are scheduled for other suspect products in the case for which 'Drug not administered' is not marked.</p>
Active Moiety	<p>Enable this check-box to enable rule to act exclusively as an active moiety rule for that country.</p> <p>When this option is enabled the system will disable and ignore the country when evaluating the domestic/foreign causality sections. Listedness will be evaluated at the case level.</p>
No Follow-up or Downgrade	<p>The system does not schedule a follow up or a downgrade report for the case when the the initial report was scheduled based on the current rule.</p>

Field/Control Name	Description
Origin of Events to Include - Domestic	<p>Enables the user to select the inclusion of domestic or foreign cases based on their country of incidence.</p> <ul style="list-style-type: none"> Domestic: The event is marked as Domestic, if the country of incidence appears in the list of selected countries. This list is displayed in the Countries tab, in the List Maintenance Licenses (section) for the license(s) of the suspect product(s) under examination.
Origin of Events to Include - Foreign	<p>Enables the user to select the inclusion of domestic or foreign cases based on their country of incidence.</p> <ul style="list-style-type: none"> Foreign: The event is marked as Foreign, if the country of incidence <i>does not</i> appear in the list of selected countries. This list is displayed in the Countries Tab on List Maintenance License (section) for the license(s) of the suspect product(s) under examination.
Timeframe	This field specifies the report's scheduled due-date based on the number of days, after the initial receipt or significant follow-up date.
Adjust due date for Group 2 countries by xxx days	This field allows the user to specify the number of days by which the due date for a report may need to be adjusted for a Group 2 country.
Form	This is the drop-down list of expedited report forms.
Local Comment Type	This field is used to extract the local evaluator comment from case data (French CERFA 65-0044, CIOMS-I (Local)). This field is only enabled for CIOMS-I (Local) form.
Clinical Reference Type	This field is used to get information from the study configured for a case. This field is enabled for CIOMS-I and other forms.
Language	<p>Enables the user to select language type.</p> <ul style="list-style-type: none"> English is the default language of choice. The system does not support other languages at this time. Reports such as the German BfArM, German PEI, and French CERFA can utilize some field values in their corresponding language (For example: narrative).
Message Type	<p>Enables the user to select the message type.</p> <p>Note: This field is displayed when an E2B or eVAERS report is selected as the Report Form. If the Report Form is selected as eVAERS, then the Message type is set to ICHICSR and is disabled.</p>
Listedness	<p>Enables the user to check if the license being evaluated for reporting is listed. The possible values are:</p> <ul style="list-style-type: none"> Listed Unlisted Ignore (default)
Seriousness - Fatal/Life Threatening	<p>Enables the user to check if case level seriousness assessment is 'Death or Life Threatening'. The possible values are:</p> <ul style="list-style-type: none"> Yes No Ignore (default)

Field/Control Name	Description
Seriousness - Serious (Case)	<p>Enables the user to check if case level seriousness assessment is 'Serious'. The possible values are:</p> <ul style="list-style-type: none"> ■ Yes ■ No ■ Ignore (default)
Seriousness - Serious (Event)	<p>Enables the user to check if the event level seriousness assessment (for any event) is 'Serious'. The possible values are:</p> <ul style="list-style-type: none"> ■ Yes ■ No ■ Ignore (default)
Seriousness - Severity	<p>Enables the user to select a term descriptive of the severity of the event. E.g. Mild, Moderate, severe, unknown.</p>
Product Specific - Family Name	<p>Enables the user to configure product specific reporting rules.</p>
Product Specific - Product Group	<p>Enables the user to configure product specific reporting rules. Product Group drop-down always lists the configured Product Groups.</p>
Causality - Most Conservative	<p>If this checkbox is marked, the system will look at the event level reported causalities, event level determined causalities and case level causalities, and if any of these three causalities is Yes then the case will be considered Reportable.</p> <p>If checked, the following options are hidden and set to Ignore:</p> <ul style="list-style-type: none"> ■ Causality as Reported (Event) ■ Causality as Determined (Event) ■ Causality as Reported (Case) ■ Causality as Determined (Case) ■ Causality is ignored when scheduling reports for non - study cases. This only Study cases.
Causality - Include Non-Clinical Trial Cases	<p>Enables you to include the Spontaneous Cases (Non Clinical Trial Cases) for causality assessments.</p>
Causality - Causality as Reported (Event)	<p>Assesses As Reported causality in conjunction with the Listed value (if any) specified in the rule for the license/event combination being assessed. <i>Ignored for non-study cases. Only applies to Study cases.</i> The possible values are</p> <ul style="list-style-type: none"> ■ Reportable ■ Non-reportable ■ Ignore (default)
Causality - Causality as Determined (Event)	<p>Assesses As Determined causality in conjunction with the Listed value (if any) specified in the rule for the license/event combination being assessed. <i>Ignored for spontaneous, literature and regulatory authority cases.</i></p> <p>Ignored for non - study cases. Only applies to Study cases.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> ■ Reportable ■ Non-reportable ■ Ignore (default)

Field/Control Name	Description
Causality - Causality as Reported (Case)	<p>Most conservative of the As Reported causalities in event assessment for ANY event.</p> <p>Ignored for non - study cases. Only applies to Study cases.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> ■ Reportable ■ Non-reportable ■ Ignore (default)
Causality - Causality as Determined (Case)	<p>Case Level Causality, as observed on the Analysis tab for the Case Level Causality.</p> <p>Ignored for non - study cases. Only applies to Study cases.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> ■ Reportable ■ Non-reportable ■ Ignore (default)
Advanced Conditions	This field enables the selection of an advanced condition to further restrict cases that meet the criteria for the rule.
Advanced Conditions - Select	<p>Enables the user to open the Advanced Condition Browser.</p> <p>You can click this button to open the Advanced Conditions browser to select / create an Advanced Condition.</p>
Responsible Group	Enables the user to select a group to whom reports scheduled by this rule will be assigned.
Super Rule - Cease evaluation of normal rules upon match	Enables the user to provide a super rule.
Reporting Category	Enables the user to configure the relevant reporting category.
Device Reporting Category	Enables the user to configure the relevant device reporting category.
License Category	Enables the user to configure the relevant license category.
Cover Letter	Enables the user to use letters that have been configured for reporting template use.
Comments	Enables the user to enter reporting rule comments, up to 2000 characters.

Expedited Reporting Rules Algorithm

The expedited reporting rules algorithm affects the following:

- Suppression of Duplicate Reports
- Blinded/Forced Distribution
- Letter Placeholder for the IND Cover Letter

Suppression of Duplicate Reports You can suppress duplicate expedited reports to be scheduled at the reporting destination level by using the **Suppress Duplicate Reports** option.

This option:

- Determines the system to use the following attributes to determine whether the reports are duplicates of other reports:

- Report Form
- Reporting Destination
- Aware Date
- Only applies to drug reports. It **does not** apply to device reports.
- **Does not** reduce the number of reporting rules the system evaluates. However, it **does** prevent the system from scheduling and generating expedited reports that match the duplication criteria.

Blinded/Forced Distribution You can configure the **Blinded Study** option for products in a study to blind the products for the report being sent to the reporting destination. The functionality is similar to the corresponding option from the Bulk Reporting dialog box.

- If you select either of the **Blinded Study** product options (**Reporting Rules** or **Bulk Reporting**), the system blinds the study product information on the report form.
- The system blinds only active blinded studies. It does not blind the following case reports even if the Blind Study product is selected.
 - Open Label Studies.
 - Study is eligible for unblinding - If the Study is Unblinding checkbox is not kept as unchecked in study configuration, the user will be able to see the complete case data even if he/she has protection enabled.
- In cases where expedited reports are due, the system permits the user to force-distribute the reports based on user-defined reporting rules, even if case processing is incomplete.
- When you select the **Force Distribution** rule, the following occurs:
 - If a case encounters a rule where a report is due is locked, the system schedules the report based on the rule and does the following:
 - * Generates the report on the due date.
 - * Dynamically replaces the current case comment with the force distribution case comment.
 - * Transmits the report based on the preferences defined by the reporting destinations.
 - * Displays the status in the Worklist Bulk Transmit/Transmit ICSR dialog boxes.
 - The **AG Service Force Reporting** process for expedited reports completes the process by:
 - * Checking the reports required for force distribution.
 - * Locks the case (if it's not already locked).
 - * Generates the reports and makes sure it is ready for transmission.
 - The notes for the **Case Locking/Unlocking** are the same as those defined as the common profile value for the **Forces Distribution** option; **System** is the user.

Adding Expedited Report Rules

The Reporting Rules configuration feature enables you to define the reporting rules or criteria for the cases to be qualified for expedited reporting.

Use the following procedure to add expedited report rules.

1. In the Business Configuration section, select **Expedited Report Rules**.
2. In the left panel, select a filtering criterion. The left panel now displays the tree view of the **Country/License Type/Reporting Rule** based on the filtering criterion.
3. Select a Reporting Rule and click to view the reporting details in the right panel.

Note: Ensure that you select the reporting rule-level icon/folder to view the details of the reporting rule.

Tip:

- You can alternatively click **Add Rule** to create a new reporting rule.
 - Use **Copy Rule** to make an editable copy of an existing reporting rule, along with all associated expedited reporting rule information.
4. Enter the **Report Name**.
 5. Select the **Report Destination** from the drop-down list. This is the name of the agency to which the report will be scheduled.
 6. Select **Auto Distribute Reports** to distribute reports automatically.
 7. Select **Active** to specify if the configured rule is active or inactive.

Note: Only active rules are considered for report scheduling

8. Select **Origin of events to include-Domestic** to include *domestic* cases based on the country of incidence OR Select **Origin of events to include-Foreign** to include *foreign* cases based on the country of incidence
9. Select **Report on Drug not Administered**. This option ensures that all drugs that are not administered are reported.
10. Select **Active Moiety** if you want to enable this option.
11. Select the required **Form** from the drop-down list of expedited report forms.
12. Select the **Local Comment Type** from the drop-down list. This field is used to extract local evaluator comments from case data.
13. Select the **Clinical Reference Type** from the drop-down list. This field is used to obtain information from study configured for a case.

Tip: This field is enabled only for CIOMS-I and other forms.

14. Select the **Language** and **Message Type** from the drop-down list.
15. Select the **Listedness** from the drop-down list. This ensures that the license being evaluated for reporting is listed.

16. Select the **Seriousness- Fatal/Life Threatening** option from the drop-down list. This field ensures that cases that contain *Death* or *Life Threatening* seriousness criteria for an event are evaluated.
17. Select the **Seriousness- Serious (Event)** option from the drop-down list. Enable this field to check if the event level seriousness assessment is *Serious*
18. Select the **Seriousness- Serious (Case)** option from the drop-down list. Enable this field to check if the case level seriousness assessment is *Serious*
19. Select the **Seriousness- Serious (Severity)** option from the drop-down list. This enables you to define the Severity as Mild, Moderate, Severe and Unknown.
20. Select the **Product Specific - Group Name** from the drop-down list. This field enables you to configure product specific reporting rules.
21. Select the **Product Specific - Family Name** from the drop-down list. This field enables you to configure product specific reporting rules.
22. Select **Causality-Most Conservative**. This ensures that the system looks at event level reported causality, event level determined causality and case level causality.
23. Select **Causality-Include Non-Clinical Trial Cases**. This enables you to include the Spontaneous Cases (Non Clinical Trial Cases) for causality assessments.
24. Select **Causality - Causality as Reported (Event)** as required, from the drop-down list.
25. Select **Causality - Causality as Determined (Event)** as required, from the drop-down list.
26. Select **Causality - Causality as Reported (Case)** as required, from the drop-down list.
27. Select **Causality - Causality as Reported (Case)** as required, from the drop-down list.
28. Select or create the **Advanced Condition** to restrict cases to the advanced conditions defined here.

If any of these three causalities are confirmed, then the case will be considered as reportable.

Note: Use the Advanced Conditions browser to select or create an Advanced Condition by clicking **Select**.

29. Select the **Responsible Group** from the drop-down list. This is the group to which the reports scheduled by this reporting rule will be assigned.
30. Select the **Cover Letter** from the drop-down list. Use this field to select cover letters that have been configured for reporting template use.
31. Enter any regulatory report comments under the **Comments** text box.
32. Click **Save** to save the changes made to this section.

Tip: If you have added a new Reporting Rule, click **Add Rule** to save the new **Expedited Reporting Rule**.

About the Filtering Criterion The filtering criterion is essential as it helps you to search for specific items. The Argus Console provides this option for the Business Configuration section.

Using Organized by

The filtering browser is displayed in the top-left corner of the left panel. The Expedited Report Rules section can be filtered on the basis of any of the five combinations shown in the following illustration.



Consider the following examples:

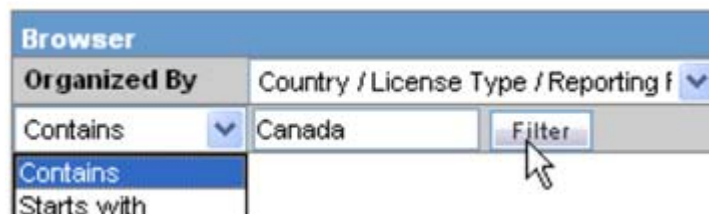
- If you enable **Organized by Country/License Type/Reporting Rule**, then the output generated will be visible in a tree-format, in the left panel, based on the entire categorization of Country, License Type and Reporting Rule.
- If you enable the **Organized by Responsible Group/Reporting Rule**, then only the Responsible Group and Reporting Rule views will be available in the tree view in the left panel.

Tip:

- Enable the **Organized By** filter for **Active Rules**, to obtain the list of active reporting rules.
- Enable the **Organized By** filter for **Inactive Rules**, to obtain the list of inactive reporting rules

The Argus Console helps you to filter information further for the Business Configuration section. Once you have selected the **Organized by**, you can specify whether your search should contain or start with specific alphabets or words.

For example, the filtering criterion defined in the following illustration for all Country/License Type/Reporting Rule data that contain the term Canada.



Sorting of Expedited Report Rules

The Reporting Rules are sorted in an alphanumeric order. The logic of ordering of Reporting rules based on 'Organized by' is as follows:

1. Country/License Type/Reporting Rule

For each country, there will be a folder for license type. Within each folder, the active and inactive reporting rules will be presented together in alphanumeric order.

2. License Type/Reporting Rule

For each license type, there will be a folder for each reporting destination. For each destination, the active and inactive reporting rules will be presented together in alphanumeric order.

3. Responsible Group / Reporting Rule

There will be a folder for each reporting group. Within each folder, the active and inactive reporting rules will be presented together in alphanumeric order.

4. Active Rules

Only active rules will be presented. For each country, there will be a folder for license type. Within each folder, active rules will be presented in alphanumeric order.

5. Inactive Rules

Only inactive rules will be presented.

For each country, there will be a folder for license type. Within each folder, inactive rules will be presented in alphanumeric order.

Configure Regulatory Reporting Rules

The regulatory reporting rules are mainly configured to look at Seriousness, Listedness, Causality, and Outcome. Out of these, Listedness and Causality can be captured and controlled (using the event assessment section) down to an individual license basis.

This granularity allows individual license holders to override the normal listedness and causality assessment to control the need for submissions to their local regulatory authority. Each affiliate could either suppress the need for a report by demoting the criteria, or add the requirement for a report by promoting the listedness or causality.

This serves to promote the global reporting automation while maintaining the level of individual local affiliate control that is often needed.

To obtain an assessment of the adverse event, the product must be in the company's suspect product and the event must be encoded.

Work with the Dictionaries

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

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

For more details, refer to the *Oracle Argus Safety Installation Guide > Section 10.2, Create Argus Safety Database Schema*.

4.1 MedDRA Dictionary

4.1.1 Prerequisites

- The system where these dictionaries will be installed has a minimum of 50 MB space.
- the system has Oracle client installed, including the following:
SQLPLUS (Exe=sqlplus)
SQL*Loader (Exe=sqlldr)
- there is an updated TNSNAMES file and Oracle client to connect to the Argus Safety database.
- The Dictionary Management Tool is installed.
- An Oracle database instance is available.
- A SYSTEM or DBA user account is created.

Note: The `smq_list.asc` and `smq_content.asc` files containing SMQ data must be placed in the same folder as the other dictionary files.

4.1.2 Load MedDRA or MedDRA J Dictionary

Use these instructions to load a new MedDRA or MedDRA-J dictionary while not overwriting any MedDRA dictionary versions you may already have loaded.

1. Open the Dictionary Management Tool and click **MedDRA Loader**.
The Oracle Database Connect dialog box appears.
2. Enter the SYSTEM or DBA username and password, the 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, check **MedDRA J** checkbox.
 - To create a new MedDRA user, click **Create User**, enter the parameters, and click **OK**.
 - To create a new role, click **Create Role**, enter the parameters, and click **OK**.
The New MedDRA Role dialog box appears.
4. In the Dictionary to Load section, do the following:
 - a. From the drop-down, select the **MedDRA Version**.
 - b. Click **Browse** and select the dictionary files.
 - c. Select the **MedDRA Browser** checkbox.
 - d. From the **Tablespace** and **Index** drop-downs, select a table and an index.
 - e. Click **Load**.
The system loads the dictionary and a confirmation message appears.
5. Click **OK**.

4.1.3 Overwrite an Existing MedDRA or MedDRA J Dictionary

1. Open the Dictionary Management 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, check the **MedDRA J** checkbox.
 - c. From the **User** drop-down, select a user.
 - d. Enter the user password in the **Password** field; re-enter it in the Verify Password field.
 - e. From the **Role** drop-down, select a role.
 - f. From the **Current Version to Overwrite** drop-down, select the version to overwrite.
 - g. From the **MedDRA Version** drop-down, select the MedDRA version to load.

- h. Click **Browse** and select the dictionary files.
- i. Check the **MedDRA Browser** checkbox.
- j. From the **Tablespace** and **Index** drop-downs, select a table and an index.
- 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**.

4.1.4 Recode MedDRA

The MedDRA Recoding tool displays the following options for each case with the existing data elements after the case number in the XLS export or tab delimited file:

- Current Workflow State
- Current Workflow Group

These options are available for the end user logs.

The SOC/HLGT/HLT/PT/LLT and Synonym columns in the MedDRA schema and the MedDRA table have been expanded to 250 characters to conform to the ICH guidelines.

Argus Database Table	Location in Argus
CASE_PAT_HIST	Argus Safety > Case Form > Patient Tab > Parent Section > Other Relevant History
CASE_EVENT	Argus Safety > Case Form > Events Tab > Event Information
CASE_PROD_INDICATIONS	Argus Safety > Case Form > Products > Products Indication
CASE_ASSESS	Argus Safety > Case Form > Events Tab > Event Assessment > Event PT (Description)/LLT
CASE_DEATH_DETAILS	Argus Safety > Case Form > Events Tab > Seriousness Criteria > Death Details > Cause of Death & Autopsy Details
CASE_LAB_DATA	Argus Safety > Case Form > Patient Tab > Lab Data
LM_ALWAYS_SERIOUS_TERM	Argus Console > Code Lists > Always Serious Term List
LM_LABELED_TERM	Argus Console > Business Configuration > Products and Licenses > Datasheet
LM_PRODUCT	Argus Console > Business Configuration > Products and Licenses > Primary Indication
LM_LAB_TEST_TYPES	Argus Console > Code Lists > Lab Test Type

4.1.4.1 Logic to Recode MedDRA

1. Get the Lower Level Term (LLT).

For a case or LM data, if LLT (J) is different from the LLT (E), and either of them is moved to a different PT group in new MedDRA version, then the MedDRA

Recode tool resolves the conflict by replacing LLT(J) with LLT(E) and recode as per the new MedDRA dictionary.

2. Check LLT_Code column in the MEDDRA_PREF_TERM_LLT table to see if LLT is not current (LLT_CURRENCY = N).

Decisions:

- If LLT cannot be found in MEDDRA_PREF_TERM_LLT then record as exception to be noted in LOG file.
- If for a record LLT(J) term is non-current as per the new upgrading MedDRA Dictionary but LLT(E) is current, then MedDRA recode only refreshes the hierarchy of 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.

If for a record, LLT(E) becomes non-current, then the MedDRA recode tool when recoded with the MedDRA J dictionary, replaces LLT(E) and LLT(J) with the PT code and recode if the **Process Non-Current Terms** checkbox is checked.

- If LLT is current then keep LLT as it is.
 - If a current LLT can be found in previous step then continue with next step else go to 1 and select the next set of Terms.
3. Based on the LLT, get the Preferred Term (PT_CODE) from MEDDRA_PREF_TERM_LLT. Get the rest of the hierarchy from MEDDRA_MD_HIERARCHY, based on PT_CODE and PRIMARY_SOC_FG = 'Y'.
 4. Match all 5 levels of Code and Description and update the data, if required.
 5. Populate the following columns:
 - DICT_ID = Current MedDRA Dictionary ID, present under Case Form Configuration.
 - CODE_STATUS = 1 (displaying that this set of terms has been encoded).
 6. When you create an Event Group by selecting a term at PT level, and that event group is attached to a datasheet, the hierarchy stored in the datasheet is based on the Primary SOC flag, which is always current.

In the LM_LABELED_TERMS table:

- If only the English hierarchy is populated, then the application fetches data for the Japanese hierarchy based on the English hierarchy populated, and performs recoding based on the new MedDRA dictionary.
- If only the Japanese hierarchy is populated, then the application uses the PT code to populate the English hierarchy, and performs recoding based on the new MedDRA dictionary.
- If neither the English hierarchy, nor the Japanese hierarchy are populated in the table but the PT code or term is populated, then the application uses the PT code or term to populate both the English hierarchy and the Japanese hierarchy, and performs recoding based on the new MedDRA dictionary.

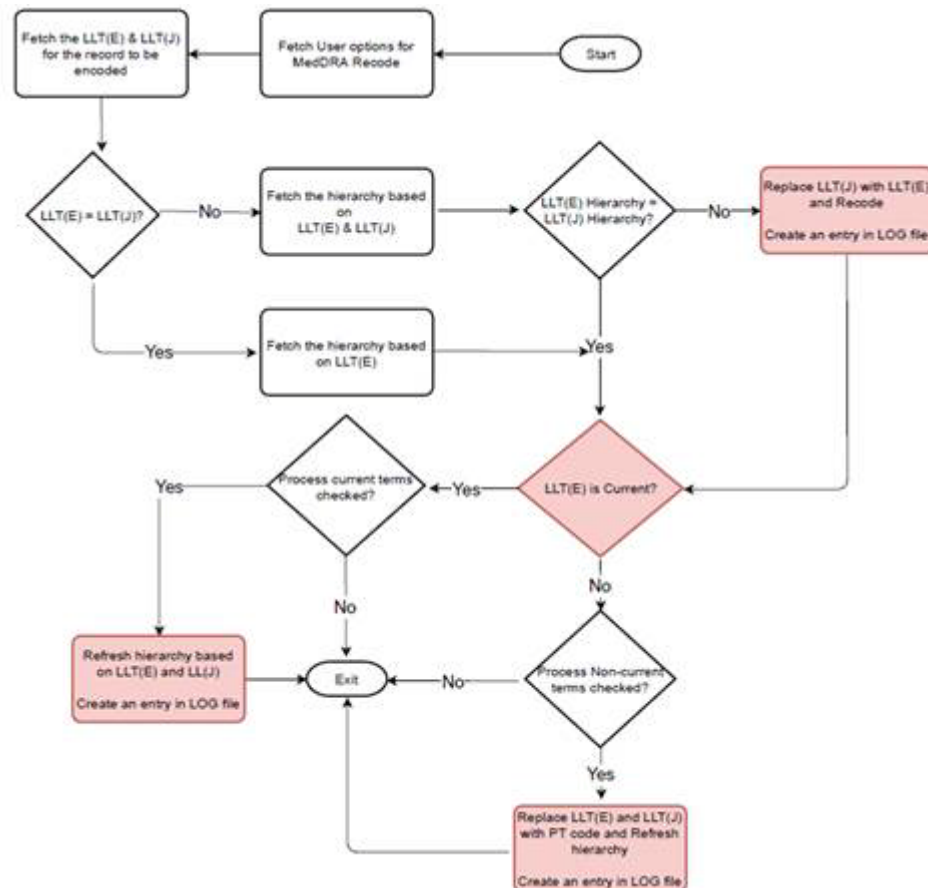
For case or LM data, if LLT(J) is different from LLT(E), and either of them is moved to a different PT group in the new MedDRA version, then the MedDRA Recode tool resolves the conflict by replacing LLT(J) with LLT(E), and recoding based on the new MedDRA dictionary.

For case or LM data, if MedDRA terms are coded with the English dictionary, then during MedDRA Recode, the Japanese hierarchy is populated based on the English hierarchy for both the case and LM data variables.

7. The following log files are created with detailed old and new values:

Log filename	Scenario	Message
(Case Form) - MedDRA_Recode_Success_YYYY_MM_DD_HH_MIN (LM Data) - MedDRA_Recode_Success_LM_YYYY_MM_DD_HH_MIN	When LLT(E) is Non-Current	LLT(E) is non-current in target MedDRA dictionary: LLT(E) and LLT(J) replaced with PT
(Case Form) - MedDRA_Recode_Success_YYYY_MM_DD_HH_MIN (LM Data) - MedDRA_Recode_Success_LM_YYYY_MM_DD_HH_MIN	When LLT(E) and LLT(J) not under same hierarchy	LLT(E) and LLT(J) not under same hierarchy in target MedDRA dictionary: LLT(J) replaced with LLT(E)
(Case Form) - MedDRA_Recode_Success_YYYY_MM_DD_HH_MIN (LM Data) MedDRA_Recode_Success_LM_YYYY_MM_DD_HH_MIN	When LLT(E) is Non-Current and LLT(E) and LLT(J) not under same hierarchy in target MedDRA Dictionary	LLT(E) and LLT(J) not under same hierarchy in target MedDRA dictionary: LLT(J) replaced with LLT(E). LLT(E) is non-current in target MedDRA dictionary: LLT(E) and LLT(J) replaced with PT

8. 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.



4.1.4.2 Run the Dictionary Management Tool to Recode Events

1. Open the Dictionary Management 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. In the Enterprises field, select an 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. In the Argus MedDRA Version to Re-code field, 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. In the Data Update/View Options [Currency determined at LLT Level Only] field:
 - Check one or all of the Process Current Terms, Process Non-Current Terms and/or Update dictionary version checkboxes.
 - Select one of the following options:
 - Update Data to reflect the updates in cases and audit log.
 - View Only to view what events will be coded without making any updates to cases and audit log.
- d. In the Output Log File Options, select an output log file option and directory path for the log files.
 - Delimited Text
 - Excel Sheet output
- e. Click on the **Execute** button to start the recoding process.
- f. 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.
- g. 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

4.1.4.3 Recode MedDRA terms at the Enterprise level

For multi-tenant environment, the Dictionary Management Tool allows recoding of MedDRA terms at the Enterprise level.

The MedDRA Recoding tool displays an additional multi-select list of all active Enterprises. This lists all active Enterprise Short Names in the alphabetical order.

New Schema Owner is no longer required. As per the recoding logic, cases are also re-coded to the MedDRA version that is configured in Console.

Displays a note below the **Existing MedDRA Version to Re-Code** list.

Note: Cases will be re-coded to the MedDRA version configured in Console for the respective Enterprises.

The MedDRA recoding tool only re-codes the items that match the selected Enterprises and values selected in the **Existing MedDRA Version to Re-Code** list.

The log file specifies the Enterprise Short Name with every log record that is processed for a particular Enterprise.

4.2 WHO Drug Dictionary

4.2.1 Prerequisites

- Windows workstation is available to load the WHODrug data.
- the system has Oracle client installed, including the following:
 - SQLPLUS (Exe=sqlplus)
 - 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: WHODrug 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.

- To display the WHO Drug Dictionary version in Argus, the CFG_DICTIONARIES_GLOBAL.VERSION column fetches data from Version.txt file. If Version.txt file is missing during WHO Drug Dictionary load then WHO Drug Dictionary version is displayed based on the value available in CFG_DICTIONARIES.VERSION_NUMBER column only.

4.2.2 Load WHO Drug Dictionary to New Tables

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.

- Open the Dictionary Management Tool and click **Who Drug Loader**.
A disclaimer message pop-up appear. Click **OK**.
- Enter the SYSTEM or DBA user password, the database name, and click **OK**.
- In the WHO Drug Dictionary Loader dialog box, do the following:
 - To load the dictionary into a separate schema, click **Load New Tables**.
 - From the **Dictionary Format** drop-down, select an option.
 - To create new user, click **Create User**.
Enter the information required to create a new user and click **OK**.
 - To create new role, click **Create Role**.
Enter the **New Role** name and click **OK**.
 - From the drop-down, select the **Dictionary Version**.
 - Click **Browse**, navigate to the dictionary files, and click **Select**.
- Click **Load**.
- Click **OK**.
- Enter the SYSTEM or DBA user password, the database name, and click **OK**.

4.2.3 Overwrite an Existing WHO Drug Dictionary

- From the Dictionary Management Tool, click **Who Drug Loader**.
- Enter the SYSTEM or DBA user password, the database name, and click **OK**.
- In the WHO Drug Dictionary Loader dialog box, do the following:

- a. Click **Overwrite**.
 - b. From the **Dictionary Format** drop-down, select an option.
 - c. From the **User** drop-down, select a user.
 - d. Enter the user password in the **Password** field; re-enter it in the Verify Password field.
 - e. From the **Role** drop-down, select a role.
 - f. From the **Current Version to Overwrite** drop-down, select the version to overwrite.
 - g. From the drop-down, select the **Dictionary Version**.
 - h. Click **Browse**, navigate to the dictionary files, and click **Select**.
 - i. From the **Tablespace** and **Index** drop-downs, select a table and an index.
 - j. Click **Load**.
 - k. View the WHO Drug Dictionary log file.
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**.

4.2.4 Load WHO Drug Dictionary Format C

For information about format C, go to <http://who-umc.org>.

1. Open the Dictionary Management Tool and 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. Select Dictionary Format—**Format C** or **Format C3**.

Note:

- For Dictionary Format, **Format C3**, WHODrug 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 updated to Varchar2 (250).

- For Dictionary Format, **Format B3**, WHODrug 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 updated to Varchar2 (250) and Varchar2 (110).

- To create new user, click **Create User**.
Enter the parameters and click **OK**.
 - To create a new role, click **Create Role**.
Enter the parameters and click **OK**.
 - From the drop-down, select the **Dictionary Version**.
 - Click **Browse**, navigate to the dictionary files and click **Select**.
- Click **Load**.
 - From the **Tablespace** and **Index** drop-downs, select a table and an index.
 - Enter the SYSTEM or DBA user password, the database name, and click **OK**.
 - When the dictionary is loaded successfully, click **OK**.

4.3 J Drug Dictionary

4.3.1 Prerequisites

- The system where these dictionaries will be installed has a minimum of 50 MB space.
- The Dictionary Management Tool is installed.
- An Oracle database instance is available.
- A SYSTEM or DBA user account is created.
- The dictionary distribution organization name and contact

- 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

Note: J-Drug Dictionary distributor organization (MT Kyogikai) is a different organization from Oracle thus there is a possibility that their specifications or procedures may change in future as per their own discretion.

4.3.2 Create and Modify Required File

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.

4.3.2.1 Create All_Data.txt file

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

Sample All_Data.txt files:

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

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

4.3.2.2 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 of the formulationcode.txt file.

Format of the file formulationcode.txt:

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

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

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

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

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

Sample formulationcode.txt:

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

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

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

4.3.2.3 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"
```

4.3.2.4 Modify the.mdb file

The current .mdb file shows only a single drop-down value for the release version on the J-drug dictionary loader. Modify this file to use the latest version of the dictionary.

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, add 2015-DEC, (note that you must append a comma).

Tables	ID	MeddraVersion	MeddraTableName
J_DRUG	150	.2007-APR,2012-APR,2014-APR,2014-AUG,2014-OCT,2015-APR,2015-OCT,2015-DEC	JPN_DRUG_DICT
J_DRUG_Constraint			
J_DRUG_Ctl			
J_DRUG_Index			
J_DRUG_Sqls			
J_DRUG_Versions			
MeddraBrowserSql			
SQLLoaderInfo			
WHO_B2_AFTER_LOAD			
	*	(New)	

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

4.3.3 Load J Drug Dictionary

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

- Open the Dictionary Management Tool and click **J Drug Loader**.
- Enter the SYSTEM or DBA user password, the database name, and click **OK**.
- In the J Drug Dictionary Loader dialog box, do the following:
 - Select **Load to New Tables** if a J-Drug dictionary has not already been loaded.
 - To create a new J-Drug user, click **Create User**, enter the parameters, and click **OK**.
 - To create a new role, click **New Role**, enter the parameters, and click **OK**.
- In the Dictionary to Load section and do the following:
 - Select the **J-Drug Version** to be loaded from the drop-down.
 - Click **Browse**, navigate to the dictionary files and select the files.
 - Check the **J-Drug Browser** checkbox.
- In the Tablespace Information section, select a **table** and an **index** from the drop-downs.
- Click **Load**.
- 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 JDrug_OCT_2015 dictionary.

4.3.4 Overwrite an Existing J Drug Dictionary

- Open the Dictionary Management Tool and click **J Drug Loader**.
- Enter the SYSTEM or DBA user password, the database name, and click **OK**.
- In the J Drug Dictionary Loader dialog box, Loading Options section, do the following:
 - Select **Overwrite**.
 - Select the user from the **User** drop-down.

System Configuration

This chapter provides information about configuring the system. It includes information about how to configure the following:

- Case Priority
- Field Validations
- LAM System Numbering
- Common Profile Switches
- Reporting Configuration
- Workflow
- System Numbering
- Field Properties
- User-Defined Fields

System Configuration Overview

The following table describes how the system options are configured:

Section	Description
Case Priority	This screen enables the administrator to configure rules to determine the priority of new cases that are entered into the system.
Field Validation	This screen enables the administrator to configure field level validations for the Case Form fields.
Field Properties	This screen enables the administrator to configure field properties.
LAM System Numbering	This section enables the administrator to specify the case numbering preferences for LAM cases.
System Management (Common Profile Switches)	This screen enables the administrator to configure common profile switches.
Workflow	This screen enables the administrator to configure Workflow states and rules.
System Numbering	This screen enables the administrator to specify the case numbering preferences.
SMTP Configuration	This screen enables the administrator to configure SMTP for e-mails

Enabled modules	This screen enables the administrator to segregate modules per enterprise.
Interchange Mapping	This screen enables the administrator to access the Interchange Mapping Utility in the Argus Console.

Configuring Case Priority

Configure rules to determine the priority of new cases that are entered into the system. Based on these rules, the system assigns each case a priority that is displayed in the Worklist.

Each row in the Case Priority Configuration screen represents the priority level assigned to a case that meets the specific criteria selected for that level. This data is reflected in multiple expedited and periodic reports and case form-product information section.

- The user can select the priority level for which the criterion is to be configured.
- Select **System Configuration -> Case Priority** to view the Case Priority page.

Field Descriptions

The following table lists and describes the fields in this section.

Field/Control Name	Description
Priority	<p>Enables the user to select the priority level whose criterion is to be configured.</p> <p>The user can disable only the last enabled priority. Example: If a user has priority 1-4 checked, the priority can be disabled only in the order of 4-1.</p>
Case Assessment - Serious	<p>Enables the user to configure the seriousness for case assessment.</p> <ul style="list-style-type: none"> ■ Select Yes from the drop-down list to give priority to cases that are serious. ■ Select No for non-serious cases to be considered for this priority level. Seriousness is considered at the case level. ■ Select Ignore from the drop-down list to ignore this condition when assessing the priority of this case.

Field/Control Name	Description
Case Assessment - Unlisted	<p>Enables the user to configure the priority level for unlisted case assessment.</p> <ul style="list-style-type: none"> ■ Select Yes from the drop-down list for unlisted cases to be considered for this priority level. ■ Select No for listed cases to be considered for this priority level. Listedness criteria is considered at the case level. ■ Select Ignore from the drop-down list to ignore this condition when assessing the priority of this case.
Case Assessment - Causal	<p>Enables the user to configure the priority level for causal case assessment.</p> <ul style="list-style-type: none"> ■ Select Yes from the drop-down list for causal cases to be considered for this priority level. ■ Select No for non-causal cases to be considered for this priority level. Causality criteria is considered at the case level. ■ Select Ignore from the drop-down list to ignore this condition when assessing the priority of this case.
Report Due Date-Due Soon	<p>Enables the user to configure the report date due soon.</p> <p>If this option is selected, the case is given the specified priority if at least one expedited report is due after the number of warning days specified from the current system date.</p>
First Report Due Date - Ignore	<p>Enables the user to configure the first report due date to ignore status.</p> <p>This option is used to ignore this parameter when assessing the priority.</p>
No. of Warning Days Before Due	<p>Enables the user to enter the number of days before a case's report due date when the priority is raised to Due Soon.</p>
Advance Condition Drop Down List Box	<p>Enables the user to select an existing advance condition from the drop-down list.</p>
AC Button	<p>Enables the user to create a new advanced condition set or modify an existing one.</p>
Run All Case Priority Determination on Middle Tier	<p>Enables the user to run all case priority determination on Middle Tier.</p> <ul style="list-style-type: none"> ■ If unchecked, the application assesses priority during every case save operation in Web. ■ If checked, the application does NOT assess priority during every case save operation in Web and Client/Server. The initial priority is calculated by the report scheduling and after that, all the priority updates are done by the AG Service Priority process.

Use the following procedure to configure Case Priority

1. Select the priority level whose criterion is to be configured.
2. Select the Case Assessment - **Serious**. The options in the drop-down list are **Yes, No, Ignore**.
3. Select the Case Assessment - **Listed**. The options in the drop-down list are **Yes, No, Ignore**.
4. Select the Case Assessment - **Casual**. The options in the drop-down list are **Yes, No, Ignore**.

5. Select First Report Due Date as Due Soon or Ignore. Enter the #Warning days for Due Soon.
6. Select the **Advanced Conditions** from the drop-down list.
7. Use the **AC** button to create a new Advanced Condition.
8. Select **Run All Case Priority Determination on Middle Tier** to ensure that the application *does not* assess priority when a case is saved in Web and Client/Server.
9. Click **Save** to save the changes made.

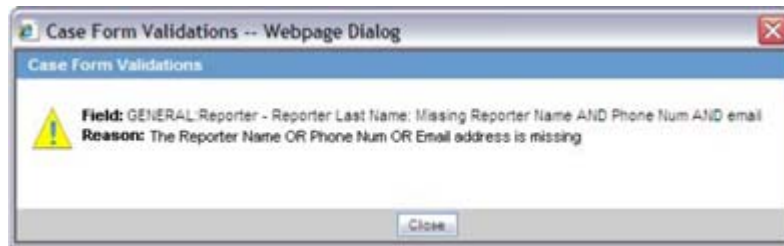
Configuring Field Validations

This screen enables you to configure field level validations for the Case Form fields. Be aware of the following:

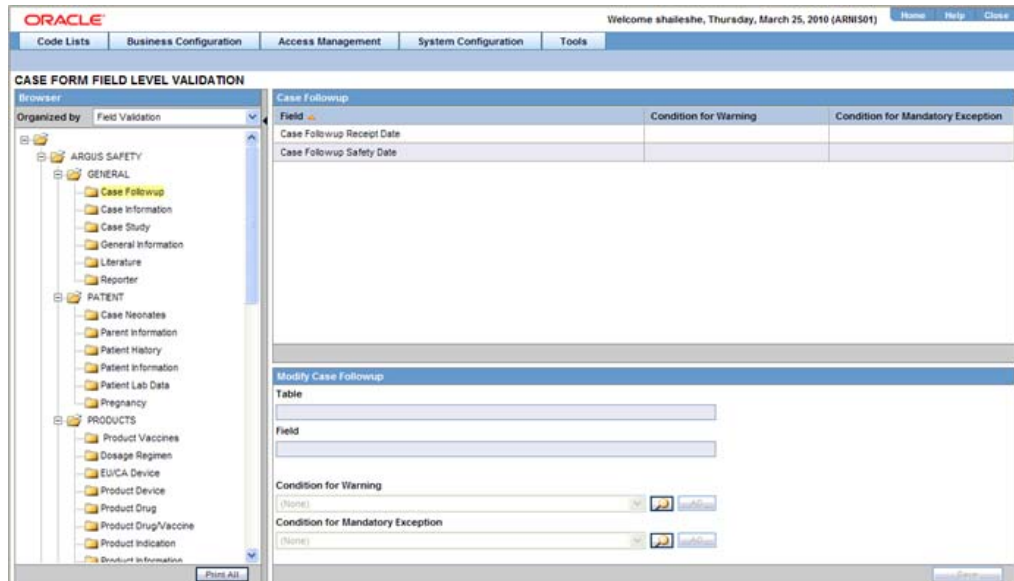
- These validation rules are expressed as an advanced condition, with their criteria marked as required or warning.
- The field level validations feature helps in automatic checking of data as it is entered on the Case Form, to ensure consistency of data as per company requirements. Consider the following example:
Suppose that the year in the patient's date of birth is entered as 1860. The patient's date of birth probably could not have been prior to 1880; hence, a warning is issued to ensure the accuracy of the entered data.
- A field level validation message such as this one is a "warning violation" and the user can therefore enter a justification and continue working on the case.
- An example of a mandatory violation would be a dosage regimen stop date that occurs before the dosage regimen start date. Cases cannot be saved without correcting mandatory violations.
- For dependent fields, Argus Safety is pre-loaded with several field level validations. Some of these validations are protected and cannot be disabled. Others can be disabled, if required by company policy.
- The system displays the Advance Condition Description for field validations on the case form after the Advanced Condition name in the following format: Field: XXXX:YYYYReason: ZZZZ

where:

XXXX	Is the Field Label Tree view followed by the field label as configured in the field label configuration.
YYYY	Is the Advance Condition name configured for the field validation.
ZZZZ	Is the advance conditions descriptions as configured for the Advance conditions. This text prints only if there is a description available for the Advanced Condition. Otherwise, the system disables the field label.



Select **System Configuration->Field Validation** to view the Case Form Field Level Validation screen. The following is an illustration of the screen.



Tip: The Case Form tabs appear on the left panel and are categorized as folders. Each folder contains all the field labels associated with that section.

Consider the following example:

The General Tab in the Case Form contains sections such as Study, Follow-up, Case Literature, etc. To view the list of field names associated with the **Study** section, click **Study** in the left panel. The field names associated with **Study** appear in the right panel.

Field Descriptions

The following table lists and describes the fields in this section.

Field/Control Name	Description
Field	Displays the name of the field.
Condition for Warning	Displays the advanced condition for warning.
Table	Displays the name of the selected sub-folder as displayed in the browser tree view. This field cannot be edited.
Field	Displays the name of the selected field label in the browser tree-view. This field cannot be edited.
Condition for Warning	Displays the advanced condition for warning.

Field/Control Name	Description
Condition for Mandatory Exception	Displays the advanced condition for mandatory exception.
Print All	Displays a list of validations on all tables, fields and advanced conditions of each Group in the Case Form as a PDF.

Modifying Field Validations

This section enables the user to edit the information already entered in fields.

Use the following procedure to modify a field validation.

1. Select the Case Form folder and field for which, the validation rule is to be modified.

Tip: The information of the selected field is displayed in the **Modify** section.

2. Click **Select** icon to create/select advanced conditions for **Condition for Warning** and **Condition for Mandatory Exception**.

Tip: Click here for details on Advanced Conditions.

Note:

- If all validation rules are met, a green icon is displayed.
 - If a condition for warning is met during field validation, an orange icon is displayed.
 - If a condition for mandatory exception is met during field validation, a red icon is displayed.
-
-

3. Click **Save** to save the changes made.

Note: Label Changes will not be reflected in Argus Case Form unless IIS is reset.

Configuring LAM System Numbering

This section enables you to specify the case numbering preferences for LAM cases. The system provides the ability to use multiple case numbering schemes for global use. For example, if site is used in the numbering, the system provides the option to keep separate sequences for each site.

Select **System Configuration->LAM System Numbering** to view the LAM System Numbering screen shown in the following illustration.

Field Descriptions

The following table lists and describes the fields in this section.

Field/Control Name	Description
Manually Number Cases	The option is used to enable the user to manually number the cases on booking or while copying the case, using the save as' option on the case form.
Automatically Number Cases	On selection, the system automatically numbers the cases as defined by the user in the numbering format.
Start at	Enables the user to initialize the counter of the sequence number.
Separate sequence for each site	Enables the user to separate the sequence numbering for cases on site by site basis. If there are cases being entered from two different sites then each site will have different sequencing of case numbers.
Separate sequence for each report type	Enables the user to separate the sequence numbering for cases by the report type of the case.
Separate sequence for each year	Enables the user to reset the sequence numbering for cases after each year, based on the initial receipt date of the case.
Separate sequence for each month	Enables the user to reset the sequence numbering for cases after each month, based on the initial receipt date of the case.
Separate sequence for each product abbreviation	Enables the user to reset the sequence numbering for cases for each different product abbreviation.
Numbering Format	<p>Enables the user to select the numbering format by selecting the different placeholders.</p> <ul style="list-style-type: none"> Define the numbering format by typing in custom keywords to print on every case number and selecting different placeholders. [YY][MM]-[###] is the default format.

Field/Control Name	Description
Placeholder	<p>Enables the user to enter a placeholder.</p> <ul style="list-style-type: none"> ■ Placeholders are used to pickup values from the database to be used in the Case numbering format. ■ The possible values populated in this list are: <ul style="list-style-type: none"> ■ # - Number: defines the digits to be used as the sequence number in the format. The field is used to display the sequence number on the case numbers. ■ CC- Country code: When selected, this uses the A2 code for the country of incidence for the case number. ■ DD - Day: When selected, this uses the date of the Initial receipt date' field of the case. ■ MM - month: When selected, this uses the month of the Initial receipt date' field of the case. ■ P -When selected, this uses either of the two values: If report type is Spontaneous or other during booking: the system uses the value of the Product Abbreviation' field specified in the Product configuration for the selected Primary suspect product. ■ SSS – User Site: When selected this uses the Site abbreviation of the site belonging to the user who booked in the case. ■ TTT – Report Type: When selected this uses the report type abbreviation of the report type selected during bookin of the case. ■ YY- Year: When selected, this uses the year of the 'Initial receipt date' field of the case.

Use the following procedure to configure LAM Numbering.

1. Select the **Numbering** feature as required. This can be manual numbering or automatic numbering of cases.
2. Select the **Sequencing Options** as required.

Tip: For the complete explanation of the sequencing option refer to the Field Descriptions.

3. Select the **Numbering Format**. Use **Placeholders** to enter the required format.

Tip: To customize the **Numbering Format**, use the **placeholder** values. Consider the following example:

To select Country Code, Month and Year (as values to be incorporated from the database) as the Case numbering format, execute the following steps.

1. Click on *Country Code*. This appears in the **Numbering Format** field.
 2. Click on *Month*. This appears in the **Numbering Format** field next to the Country Code.
 3. Click on *Year*. This appears in the **Numbering Format** field next to the Country Code and Month.
 4. The final data listed in the **Numbering Format** field is the Case Numbering Format.
4. Click **Save** to save the changes made.

Configuring System Management - Common Profile Switches

This section lists the configurable sections for Common Profile Switches.

Select **System Configuration** and then **System Management** to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

Note: If any change is made in the System Management (Common Profile Switches) screen, the Argusvr2.exe and Argusvr2a.exe should be killed from each Web Server and the IIS on Argus Web / Report Servers must be reset, in order to reflect the changes made in the Argus application.

The following table provides the list of configurable sections associated with Common Profile Switches.

Section	Sub Section	Description
Advanced Conditions	~	The Advanced Conditions configuration screen enables you to specify the number of rows to be displayed on the Advanced Condition search screen.
Argus Dossier	Report Configuration	The Argus Dossier screen enables you to modify the customizable fields of Argus Dossier.
Argus Insight	~	If Argus Enterprise products are enabled, the Argus Insight URL can be provided here.

Section	Sub Section	Description
Argus J	E2B Reporting ~Device Report Responsible Officer	The Argus J Configuration screen enables you to modify the customizable fields on the Argus J form.
Argus Mart	~	If Argus Enterprise products are enabled, Argus MART related settings can be configured here.
Background Services	~	This screen enables you to configure the Common Profile Switches that affect the behavior of Background Services.
Case Form Configuration	~	This screen enables you to configure Common Profile Switches that affect the behavior of the Argus application
Case Processing	Assessments Always Show Literature Data Auto Archiving Case Numbering Dictionary Browser Enable Local Unlocking Group Data Access Lot Number Processing Performance	This section enables you to configure the case processing fields and items.
Database	~	The database related parameters can be maintained here. Calculation functions for Case Seriousness, Listedness and Causality calculation.
Document Management	~	This screen enables you to configure the Documentum fields and items for Documentum.
Help	~	Centralized Online Help URL.
Local Labeling	LAM	The Local Labeling Configuration screen enables you to modify the options available through local labeling.
Network Settings	~	The Network Settings screen enables you to modify the settings on the Argus Safety Load Balancer Server and Proxy.

Section	Sub Section	Description
Reporting	BIP Reporting E2B eMDR eVAERS Expedited Expedited - BfArM Expedited - Canada Expedited - CIOMS Expedited - MedWatch MedWatch Configuration Periodic Scheduling	The Reporting Configuration screen enables you to modify the options available for reporting.
Security	Cryptography LDAP	The Security Configuration screen enables you to modify the options available for security.
Session Timeout	Session expiration time in minutes	The maximum idle time allowed for a user's session. Valid range for this value is 5-1440. Default value is 30 min. Note that long running processes like CDA are controlled through the table CMN_URL_ACCESS_GLOBAL where user can specify a timeout value local to that process. Further, the user would need to set the process as IS_LONG_RUNNING = 1. By default, the following are categorized as long running: '/REPORTS/CIOMSII/CIOMS2_SAVING.ASP' '/AUDITLOG/AUDITLOGLIST.ASP' ; '/REPORTS/CDA/CDAGENERATE.ASP',
Single Sign-On	~	The Single Sign-On screen enables you to modify the options available for Single Sign-On such as enabling or disabling it, its HTTP Header, Logout URL, and using Oracle Access Server SDK for LDAP Validation. Note that in a SSO configured environment, for the SSO to take effect, the session timeout value should be set to maximum value.
User Interface	~	The User Interface screen enables you to modify the options available for User Interface.
Workflow	~	The Workflow Items screen enables you to modify the options available for Workflow Items.

Configuring Advanced Conditions

Select **System Configuration -> System Management** to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To configure the rows to display on each page of an advanced condition screen, click the **Advanced Conditions** folder in the left panel.



Field Descriptions The following table lists and describes the fields in **Advanced Conditions Configuration**.

Field/Control Name	Description
Number of rows to display per page on the Advanced Condition Search screen	Enables the user to specify the number of rows to be displayed on the Advanced Condition search screen.
Comma separated list of allowable parameters for custom advanced conditions	<p>This feature allows the Advanced conditions to store and execute customer SQLs containing bind variables through the UI. The application supports the bind variables defined in a comma separated format. The bind variables defined here are case insensitive. This switch supports a maximum length of 1000 characters.</p> <p>In OOTB configuration, the following bind variables are supported:</p> <ul style="list-style-type: none"> ■ P_CASE_ID ■ P_SEQ_NUM ■ P_REG_RPT_ID ■ P_REG_REPORT_ID ■ P_REPORT_FORM_ID

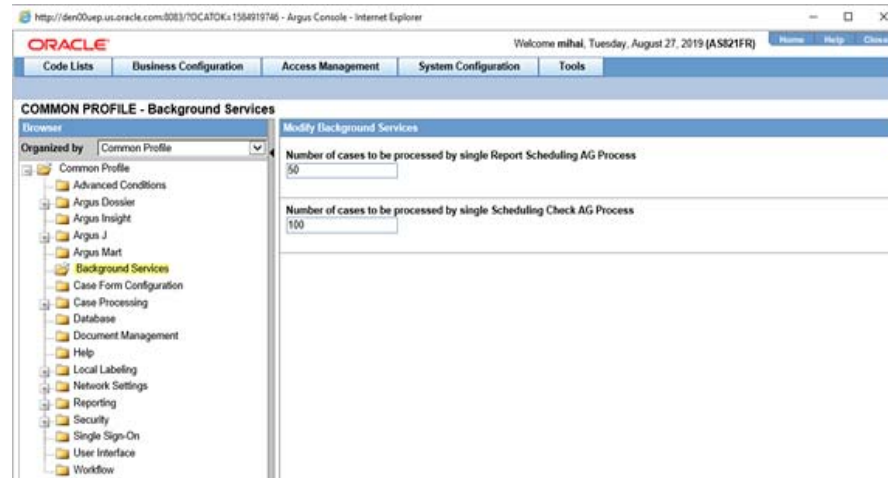
Use the following procedure to configure Advanced Conditions.

1. Enter the Number of rows to display per page on the Advanced Conditions Search screen.
2. Click **Save** to save the changes made.

Configuring Background Services

This screen enables you to configure the Common Profile Switches that affect the behavior of Background Services.

To view the list of field names associated with the **Background Services** section, click the **Background Services** folder in the left panel. The field names associated with the **Background Services** appear in the right panel.



Field Descriptions The following table lists the fields available under **Background Services**:

Field/Control Name	Description
Number of cases to be processed by single Report Scheduling AG Process	The number of cases that can be processed by a single instance of the Report Scheduling AG Process. The range of allowed values is 0-999. The default value is 50.
Number of cases to be processed by single Scheduling Check AG Process	The number of cases that can be processed by a single instance of the Scheduling Check AG Process. The range of allowed values is 0-999. The default value is 100.

Configuring Case Form (System Management)

This screen enables you to configure Common Profile Switches that affect the behavior of the Argus application.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To view the list of field names associated with the **Case Form Configuration** section, click the **Case Form Configuration** folder in the left panel. The field names associated with **Case Form Configuration** appears in the right panel.

The Case Form Configuration dialog helps you customize the case processing activities in order to meet the company's requirements. The Administrator can configure the following items by using the Case Form Configuration dialog shown in the following illustration.

Coding Web Service The **Case Processing Dictionary Browser** common profile switches are segregated by enterprises to allow different configurations for different enterprises. However, the URL and other configuration for WHO Drug and MedDRA web services remain in configuration XML on the Web Servers as per existing design and hence remain common across all enterprises.

In a multi-tenant installation, if the provider chooses to operate using Coding via web service, they should use the same web service across all enterprises.

Auto Encoding, Dictionary and Central Encoding To enable the use of standardized medical terminology throughout the adverse event reporting process, dictionaries can be used to encode certain terms in the Case Form.

The dictionaries that will be used to encode drugs, Events & Indications, and events can be specified in the **Autoencoding** section of the **Case Form Configuration** dialog.

Field Descriptions

The following table lists and describes the fields in this section.

Field/Control Name	Description
Central Coding	<p>You can independently turn On/Off Centralized Coding for individual enterprises from the Argus Console -> System Management -> Case Form Configuration by marking the checkbox next to the Events & Indications MedDRA dictionary version drop-down list.</p> <p>The enterprise can use its own MedDRA version using the Argus Console -> System Management -> Case Form Configuration -> Centralized Coding -> Centralized Coding Configuration.</p>
Drugs	<p>The Drugs dictionary list enables the selection of the WHO-DRUG dictionary. Select the Drugs check box and tab out of the product name field in the Case Form to search the company product followed by the license trade names.</p> <ul style="list-style-type: none"> ■ If no matches are found, the WHO drug dictionary (drug names) is searched. ■ Tab out of the generic name field in the Case Form to search the product/product family ingredients (it displays the select dialog if more than one product is found with the ingredient). ■ If no match is found, the WHO drug dictionary (ingredients) is searched.

Field/Control Name	Description
Events & Indications	Select Events & Indications to be prompted for the term as you enter it to be encoded on the Events & Indications tab. If an exact match is found in the dictionary, the term populates automatically. If an exact match is not found, the Event Coding dialog is displayed to select the desired event. Auto encodes primary indication for the drug encoding, Patient Condition description in Other Relevant History section and Death Details dialog.
Prevent manual encoding for Events & Indications	Prevents users from encoding the Events & Indications manually.
Require event term encoding before case closure	Ensures that users encode the events prior to formally closing a case.

Automation The **Automation** section enables the user to generate an Auto narrative based on one of the templates configured by the method described in this topic.

Field Descriptions

The following table lists and describes the fields in the Automation dialog box.

Field/Control Name	Description
Auto Regulatory Scheduling	This enables the user to configure the manner in which Argus Safety handles the Auto-scheduling of Regulatory Reports. The available options are: <ul style="list-style-type: none"> ■ None ■ Always ■ Significant ■ Manual When the common profile switch is set to <i>Always</i> , the system does not wait for a lock to schedule reports, it tries to auto-schedule each time user the saves the case. However, the only criteria to run auto-scheduling algorithm is that the case must have product, event and event assessment.

Field/Control Name	Description
Report Generation	<p>The Report Generation option helps you to configure how the system responds to new data when generating auto-scheduled regulatory reports.</p> <ul style="list-style-type: none"> When new data is entered, the system re-runs the regulatory report-scheduling algorithm to determine which reporting rules apply to the case. If Overwrite Existing Reports is selected, the system updates the existing scheduled reports with the new data entered. This setting ensures that follow-up numbering is specific to each health authority. If a MedWatch report for the FDA has already been scheduled for this case, that report would then be updated with the new information entered. If Create as Follow-up is selected, the system uses the new data to create new reports marked as follow-up reports. This setting ensures that the same number would identify a follow-up report worldwide. Users will be unable to submit follow-up reports before one of the following events occur on the initial or previous follow-up report. <p>Aware date and Due date of a scheduled report can be overwritten or retained with original dates based on the internal common profile switch "Scheduled Report Update".</p> <p>If "Scheduled Report Update" is set to "Update to current aware date and new due date", the current Aware date is used and due date is updated based on the current aware date while overwriting a scheduled report.</p> <p>If "Scheduled Report Update" is set to "Keep original aware date and due date" the aware date/due date are not updated based on current aware date while overwriting a scheduled report.</p> <p>If the common profile switch Report Generation is set to Create as Follow-up then, system allows generation of follow-up reports irrespective of submission status of previously scheduled reports based on the settings made to the common profile switch Allow Report Generation.</p>
Case Locking for Report	<p>The Administrator has the option of indicating whether cases that are not locked can appear in periodic reports.</p> <ul style="list-style-type: none"> If Allow Unlocked cases to be included is selected, then a check box on the periodic report configuration dialogs will allow unlocked cases to appear in periodic reports. To prevent unlocked cases from appearing in periodic reports, select Prevent unlocked cases from appearing.
Report On	<p>Selecting Diagnoses will only list the events marked as diagnoses plus events unassociated with a diagnosis in Regulatory Reports.</p> <ul style="list-style-type: none"> The Event Assessment section of the case form will only list diagnosis and unrelated events. If there are no diagnoses, all events are listed. You can configure a default setting for selecting the Diagnoses state at a system level. Selecting All Events will always list all events, regardless of their relationship in the Event Assessment section of the case form. The system will take into consideration both events marked as diagnoses and events marked as symptoms when running the regulatory report algorithm.

Field/Control Name	Description
Diagnosis Default on Event	<p>The options are Yes or No</p> <ul style="list-style-type: none"> ■ Selecting Yes will set the default Events Diagnosis to Yes whenever a new event is entered. ■ Selecting No will set the default Events Diagnosis to No whenever a new event is entered.
Event Assessment On	<p>The Event Assessment section of the case form will only list diagnosis and unrelated events. If there are no diagnoses, all events are listed. You can configure a default setting for selecting the Diagnoses state at a system level.</p> <ul style="list-style-type: none"> ■ Selecting Diagnoses will include in Event Assessment only those events that are associated with a diagnosis or symptoms that are not associated with any of the diagnoses. ■ Selecting All Events will include all events when the Event Assessment is performed.
Prevent Modification of Autonarrative	<p>Selecting the Preventing Modification of Autonarrative check box will prevent users from modifying autonarratives.</p>
Case Autonarrative	<p>Selecting the Case Autonarrative check box enables the user to generate an Autonarrative based on one of the templates configured by the method described in this topic.</p>

Templates Clicking the **Templates** button enables the Administrator to create a new Autonarrative template, modify/copy an existing template, or delete an existing template.

Use the following procedure to create a new Autonarrative template.

1. Click the **Templates** button in the **Case Form Configuration** dialog to open the Autonarrative Configuration dialog.
2. Click **New** to open the **Narrative Configuration** dialog.

3. Under **Template Name**, enter a name for this new template.
4. Click the **Add** button at the bottom of the dialog. A new row for entering a phrase and its associated logic will appear.
5. Enter a text phrase in the **Phrase** field. The text can include placeholders that will be substituted by the appropriate case data when the Autonarrative is generated.

For example: A phrase might be entered as: "The patient was [age] at the onset of this event". When the Autonarrative is being generated, the "[age]" placeholder will be substituted for the actual age of the particular patient in the case.

6. Click the ellipsis button to the right of the **Logic** column. Select or enter an Advanced Condition for the logic section.

This search will be used to determine whether or not the corresponding phrase will appear in a narrative for a particular case. For example: An advanced condition can be specified such that only cases involving children younger than five years old will have the phrase "

The patient was [age] at the onset of this event in the Autonarrative.

7. Repeat steps 4 through 6 to add other text phrases to the template. Click **OK** to save the template or **Cancel** to exit the dialog without saving the changes.

Note: Selecting the **Preventing Modification of Autonarrative** checkbox in the Case Form Configuration dialog will prevent users from modifying autonarratives.

Creating a Template in Another Language Use the following procedure to create a template in another language.

1. Once a template is created, double-click the "Narrative Templates" folder to expand the template tree in the **Autonarrative Configuration** dialog.

Tip: To open the Autonarrative Configuration dialog, click the Autonarrative button in the Case Form Configuration dialog.

2. Expand the selected template folder to display the languages for this template. To configure this template in a language other than English, double-click the appropriate language icon.
3. Configure the foreign language template as described in steps 4 through 7 of the procedure for creating the Autonarrative template above.
4. Click Close to exit the Autonarrative Configuration dialog.

Note: Autonarrative placeholders in a language other than English will get substituted by text from that particular language. If no text is available in that language, English language text will be used to substitute the placeholders.

Copying a Template to Another Language Use the following procedure to copy a template to another language.

1. Select the original language from which the target language copy is to be created. The original language can be selected in the tree-view of the **Autonarrative Configuration** dialog.

Tip: To open the Autonarrative Configuration dialog, click the Autonarrative button in the Case Form Configuration dialog.

2. Click **Copy**. The **Autonarrative Copy** dialog will appear.

Note: In the **Autonarrative Configuration** dialog, the **Copy** button for a selected language template will only be available if a template has already been created in that language.

3. Select the language to which the narrative template is to be copied and click **Copy**.
4. The contents of the original language template will now be copied into the selected language template.

Deleting Templates Use the following procedure to delete templates.

1. To delete a language template, select the appropriate language icon for the template in the Autonarrative Configuration dialog and click **Delete**.
2. To delete the entire Autonarrative template, select the template folder icon in the Autonarrative Configuration dialog and click **Delete**.

Duration Calculations The following table lists and describes the fields associated with this section.

Field/Control Name	Description
Event	<p>The Duration Calculations section is used to indicate whether the system should calculate event duration (the time from Event Onset Date to Event Stop Date) in an inclusive or an exclusive manner.</p> <p>For instance, select Inclusive to calculate a range from 01 January to 10 January as ten days. Select Exclusive to calculate a range from 01 January to 10 January as nine days.</p> <p>If the user has entered both the date and time, the exclusive/inclusive designation is ignored.</p>
Drug	<p>The Drug Duration Calculations section is used to indicate whether the system should calculate drug duration in an inclusive manner or an exclusive manner, as described under Event Duration Calculations.</p>

Documentum Common Login The Documentum Common Login information is used to connect to the Documentum server to perform Documentum related activities to the case form. The system uses this information only if the common profile switch to use the common login is set. This option is only available if the system is configured to use Documentum.

The following table lists and describes the fields associated with this section.

Field/Control Name	Description
Username	This is the username associated with the Documentum Common Login.
Password	This is the password associated with the Documentum Common Login username.

Custom Routines The following table lists the Field Descriptions associated with this section.

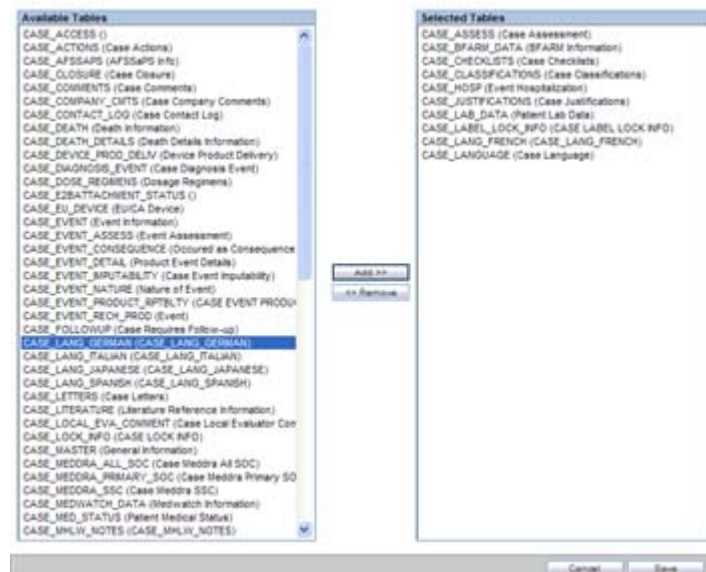
Field/Control Name	Description
Custom Routine Before Save	<p>The function behaves the same way as the Custom Routine Before Commit. The case ID is passed as a parameter to the function. The return value is a string format. If a null string is returned, the system assumes the procedure executed without any error, and continues with the case save operation. If any numeric/string value is returned, the case save routine is aborted and the system displays the returned string as an error message to the user.</p>

Field/Control Name	Description
Custom Routine Before Commit	This is the Custom routine to be called before case save. Ensure that the custom routine is present in the database, and the application has access to it.
Custom Routine After Commit	This is the after-save Custom routine to be called after case save. Ensure that the custom routine is present in the database, and the application has access to it. Select the Table Config button to select the tables that are being modified in the post-save script.
Custom Routine Before Lock	This is the Custom routine to be called before case lock Ensure that the custom routine is present in the database, and the application has access to it.
Attachment File Size Limit (in Megabytes)	The file size entered in this field enables you to specify the maximum size limit for attaching a file. The upload limit defined here can be seen in the Attachments and References section of the Bookin screen. The default size for uploading an attachment is 30 MB. You can also configure the file size as per your requirement, up to 300 MB.

Table Config Button The Table Config button enables you to fetch only the delta table data after post-save, so that the entire case is not reloaded. This button is enabled only when the **Custom Routine After Commit** checkbox is selected.

Use the following procedure to remove case tables.

1. Select the **Custom Routine After Commit** checkbox and click the **TableConfig** button. The following screen appears.



Initially, all case tables open under the **Available Tables** list box.

2. Select the required table(s) and click **Add>>** to include them to the **Selected Tables** list.

Alternatively, you can select the required table(s) and click **<<Remove** to exclude them from the **Selected Tables** list.

3. Click **Cancel** to close the screen without making any changes or click **Save** to save this configuration.

- The **Case Save** routine gets modified to retrieve only the table data from the **Selected Tables** in the configuration.
- If no **Post Save** is configured, the Case Save does not execute the Case Load routine.

Modify Data Lock Point This section is displayed only if the DLP_SETUP switch is set to ON in the database schema in the CMN_Profile_Global table.

Modify Data Lock Point

Enable Data Lock Point

Data Lock Point Revision

Use Last Completed Version

Use Next Completed version (Includes Data Cleaning)

The following table lists and describes the fields in this section.

Field/Control Name	Description
Enable Data Lock Point	Enables you to activate a data lock point by selecting this checkbox. If this checkbox is not selected, the Modify Data Lock Point section displays only this field as editable.
Use Last Completed Version	Enables you to use the last completed version.
Use Next Completed Version (Includes Data Cleaning)	Enables you to use the next completed version that includes data cleaning.

SMTP Configuration

The Argus Safety Service and the Interchange Service use the SMTP configuration utility for e-mail transmission if it has been enabled and configured in Argus Safety. Case Letters are also sent using SMTP.

To configure SMTP:

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 (Default value is 25)
 - User name
3. Check the **Enable SMTP** checkbox.
4. 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.

5. Check the **Custom SMTP Header** checkbox to pass a custom header into the SMTP Header when sending e-mails. This is used if you have a SMTP solution that depends on specific header information for routing.
6. In the **Custom SMTP Header** field, enter a text string (custom header) to insert into the SMTP Header. The Custom SMTP Header text is enabled only when the Custom SMTP Header check box is checked.



All e-mail messages sent using the following processes are sent as Confidential:

- AG Service: Bulk Transmit Email
- AG Service: General Email
- ESM Service: Business / User / IT Email

The Audit Log tracks updates to this field.

Configuring Case Processing

This section enables you to configure the case processing fields and items. **Select System Configuration -> System Management** to view the Common Profile Configuration screen

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders.

Each folder contains all the field labels associated with that section.

To view the list of field names associated with the **Case Processing** section, click the **Case Processing** folder in the left panel.

The field names associated with **Case Processing Configuration** appear in the right panel.

The Case Processing folder has been further categorized into the following sub-folders:

- Configuring Assessments
- Configuring Always Show Literature Data
- Configuring Auto Archiving
- Configuring Case Numbering
- Configuring Dictionary Browser
- Configuring Group Data Access
- Configuring Lot Number Processing
- Configuring Performance

Field Descriptions The following table lists the fields available under **Case Processing Configuration**:

Field/Control Name	Description
Create follow-up on unblinding	The available options are Yes and No.
Manually Schedule reports	The available options are: <ul style="list-style-type: none"> Report scheduling will schedule follow up reports Report scheduling will not schedule follow up reports
Events to Display on Assessment Tab	The available options are: <ul style="list-style-type: none"> Event Assessment will display all Events Event Assessment will display Diagnosis Events only
Enable Local Unlocking	Provides a system level control permitting local users to locally unlock a case and make any corrections to the previously entered local data. Enables you to select whether to locally unlock a case or not. The available options are: <ul style="list-style-type: none"> Yes No
Search product on Case Form	The available options are: <ul style="list-style-type: none"> Product Name product lookup. Based on products configured in the system. Trade Name product lookup. Based on the licenses configured in the system.
Select Type of WHO drug search for auto drug encoding	The available options are: <ul style="list-style-type: none"> Default WHO schema Use alternate who tables
Action Item Code when QC info is entered	The available action item codes are listed in the drop-down list box.
Valid Attachment File Types	Allows users to attach files in Case Form with the file types mentioned in this parameter.

Field/Control Name	Description
SQL to prevent case unlock when reports are pending generation	<p data-bbox="691 228 1451 285">Allows customization to prevent users from unlocking the case from Case Form, E2B, and LAM if there were reports pending generation.</p> <p data-bbox="691 296 1451 352">You can configure this behavior by adding a SQL or database function in the given text field.</p> <ol data-bbox="691 363 1451 940" style="list-style-type: none"> <li data-bbox="691 363 1451 850"> <p data-bbox="691 363 1451 415">1. If the value returned is greater than 0, then the system shall behave as described below:</p> <p data-bbox="737 426 1451 615">If the Value of Allow forced unlock (Global and Local) is Yes, Report Status (Global or Local) is Pending (i.e. the value from SQL check returned > 0), a warning message is displayed. The case is unlocked using the existing "Locked Case" dialog if user selects "Yes" on the warning message. This means that the pending global reports will not be generated on unlock and may be overwritten or removed depending on case data on the subsequent global lock.</p> <p data-bbox="737 625 1451 730">If the Value of Allow forced unlock (Global and Local) is No, Report Status (Global or Local) is Pending (i.e. the value from SQL check returned > 0), the case is not unlocked and an error message is displayed.</p> <p data-bbox="737 741 1451 846">If the Value of Allow forced unlock (Global and Local) is N/A, Report Status (Global or Local) is Generated /Submitted (i.e. the value from SQL check returned 0 or no SQL has been configured), the case is not unlocked.</p> <li data-bbox="691 861 1451 940"> <p data-bbox="691 861 1451 940">2. If the value returned is 0 or no SQL has been configured, the system shall allow users to global unlock the case without any of the other checks.</p> <p data-bbox="691 951 1451 1008">The default for this configuration will stop the users from unlocking the case if there are scheduled reports pending generation.</p> <p data-bbox="691 1018 1451 1102">The checks for reports pending generation is applicable only when DLP_EXPEDITED_E2B_REPORTS is set to 0 (i.e., DLP is not enabled for Expedited Reporting).</p> <p data-bbox="691 1113 1451 1167">Make sure that the name that is being used for the bind parameter is P_CASE_ID.</p>

Field/Control Name	Description
Generate auto-narrative for the other language without user confirmation	<p>This common profile switch helps to suppress user confirmation during generation of auto-narrative for the other language while the user performs the operation in the English side or Japanese side.</p> <p>Click Yes to generate or No (default) to not generate the auto-narrative.</p> <p>If auto-narrative is being performed prior to global lock:</p> <p>If a user is performing the auto-narrative from the Japanese side of the case form and if the auto-narrative template has any other language other than Japanese configured, and if the new common profile switch "Generate auto-narrative for the other language without user confirmation" is set to "No", the system shall first prompt the user if they wanted to generate the English and other language narratives as well. The system shall proceed with all the non-Japanese language narrative generation steps only if the user chose Yes to this dialog (note that existing generation steps and prompts still hold good) or if the new common profile switch "Generate auto-narrative for the other language without user confirmation" is set to "Yes. If they chose No to the user prompt, the system shall proceed with only Japanese narrative generation (note that existing generation steps and prompts still holds true). If they chose Cancel, the system shall not proceed with auto-narrative generation for any language.</p> <p>If a user is performing the auto-narrative from the English side of the case form and if the chosen Narrative template has Japanese language configured, and if the new common profile switch "Generate auto-narrative for the other language without user confirmation" is set to "No", the system shall first prompt the user if they wanted to generate the Japanese narrative as well. The system shall proceed with the Japanese language narrative generation steps only if the user chose Yes to this dialog (note that existing generation steps and prompts still hold good)) or if the new common profile switch "Generate auto-narrative for the other language without user confirmation" is set to "Yes". If they chose No to the user prompt, the system shall proceed with only the non-Japanese (English and all other languages except Japanese) narrative generation (note that existing generation steps and prompts still holds true). Note that the prompt shall not display if Japanese language was not configured in the template. If they chose Cancel, the system shall not proceed with auto-narrative generation for any language.</p>
Truly Local Case (Note: Bind variable :P_CASE_ID must be used in SQL)	<p>Provides a system level control allowing customers to define SQL or PL/SQL block or specify database function to test if a case with suspect Local (Japanese) License product is a Local PRPT case. This field is a multi-line text fields with a limit of up to 1000 characters. It is partitioned by enterprises for multi-tenant customers.</p> <p>The SQL or PL/SQL block or the database function shall accept a bind variable :P_CASE_ID representing the case from which this switch is being invoked. If the value returned from the configured SQL or PL/SQL block or the database function is > 0, the system shall consider the case with suspect products having local (Japanese) license as a Local PRPT case.</p> <p>If the value returned is 0, the system shall not consider the case a Local PRPT case (unless there is already a local report pending generation i.e., Scheduled or New data available report states).</p> <p>If there is no SQL or PL/SQL block or database function configured in this switch, the system shall consider that the switch returns a default value of 1.</p> <p>The system does not allow illegal data manipulations (e.g., UPDATE/INSERT/DELETE statements) to the underlying Argus schema via this switch.</p> <p>This switch is also used to determine if a report is a Local report.</p>

Field/Control Name	Description
Always show Literature Data section on Case Form	When configured to Yes, the application always displays the literature section in the Case Form and Book-in. Default: 0

Use the following procedure to configure the case processing options.

1. Select the required option in **Create follow-up on unblinding**.
2. Select the required option in **Allow User to regenerate reports**.
3. Select the required option in **Manually Schedule reports**.
4. Select the required option in Events to Display on Assessment Tab.
5. Select the required option in **Access on Patient Information**.
6. Select the required option in **Search product on Case Form**.
7. Select the required option in Select Type of WHO drug search for auto drug encoding.
8. Select an action item code from the drop-down list in **Action Item Code when QC info is entered**. This code will be used to populate the **Action Item Code** field of the action item created by the system whenever a user adds QC information to a case through the **Case form > Products** tab. If you do not select any value from the list, then no Action Item Code will be set.
9. The Auto Upload Letters feature is no longer available. You are requested to select only the **Manually Upload Letters** option.
10. Click **Save** to save the changes made to this section.

Configuring Database

This screen enables you to configure the case processing fields and items for the database. **Select System Configuration -> Database** to view the Common Profile Configuration screen.

To view the list of field names associated with the **Case Processing -> Database** section, click the **Database** folder in the left panel.

The field names associated with **Modify Database** appear in the right panel.

The screenshot displays the 'COMMON PROFILE - Database' configuration interface. It features a navigation pane on the left with a tree view containing folders like 'Advanced Conditions', 'Argus Dossier', 'Case Form Configuration', 'Case Processing', 'Database' (highlighted), 'Document Management', 'Help', 'Local Labeling', 'Network Settings', 'Reporting', 'Security', 'Single Sign-On', 'User Interface', and 'Workflow'. The main area is split into two sections: 'Modify Database' and 'Database Server OS Timezone'. The 'Database Server OS Timezone' section has a dropdown menu set to 'US/Central'. Below it, there are three 'Override Case' calculation function settings, each with a text input field: 'Override Case Seriousness Calculation Function' (SF_CASE_SERIOUSNESS), 'Override Case Listedness Calculation Function' (SF_CASE_LISTEDNESS), and 'Override Case Causality Calculation Function' (SF_CASE_CAUSALITY). Each override section includes a note: '(Note: Default function shall be used if left BLANK)'.

Field Descriptions The following table lists the fields available under **Modify Database**:

Field/Control Name	Description
Database Server OS Timezone	The database server timezone can be specified here. This value can be configured during the Argus database installation. Note that the timezone selected here should be in sync with the database, web and transaction servers. For further information, see "GMT Offset Calculation" below.
Override Case Seriousness Calculation Function (Note: Default function shall be used if left BLANK)	If this configured in Common Profile Switches -> Database -> Modify Database, the configured function is executed. (Note: Default function shall be used if left BLANK).
Override Case Listedness Calculation Function (Note: Default function shall be used if left BLANK)	If this configured in Common Profile Switches -> Database -> Modify Database, the configured function is executed. (Note: Default function shall be used if left BLANK).
Override Case Causality Calculation Function (Note: Default function shall be used if left BLANK)	If this configured in Common Profile Switches -> Database -> Modify Database, the configured function is executed. (Note: Default function shall be used if left BLANK).

GMT Offset Calculation

The system uses the time zone of the DB server to perform 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 the CMN_PROFILE table.

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

Assume that Daylight Saving Time starts on the first Sunday of April at 2:00 AM and ends on the last Sunday of October at 2:00 AM.

To find out the time zone offset for the time zone regions, execute the following query:

```
SELECT tzname, tz_offset(tzname) offset, tzabbrev
FROM gv$timezone_names;
----
```

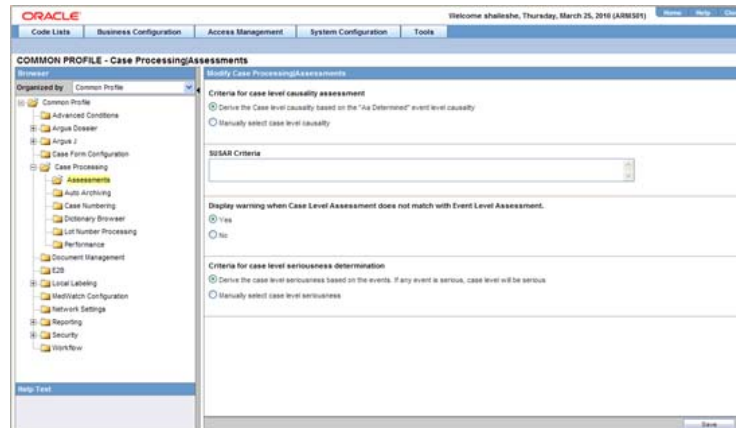
Configuring Assessments

This screen enables you to configure the case processing fields and items for assessments. **Select System Configuration -> System Management** to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To view the list of field names associated with the **Case Processing -> Assessments** section, click the **Assessments** folder in the left panel.

The field names associated with **Assessments Configuration** appear in the right panel.



Field Descriptions The following table lists the fields available under **Assessments Configuration**:

Field/Control Name	Description
Display warning when Case Level Assessment does not match with Event Level Assessment	The available options are Yes and No.
Criteria for case level causality assessment	The available options are: <ul style="list-style-type: none"> Derive the case level causality based on the As Determined event level causality. Manually select case level causality.
Criteria for case level Seriousness determination	The available options are: <ul style="list-style-type: none"> Derive the case level seriousness based on the events. If any event is serious, case level will be serious. Manually select case level seriousness.
SUSAR Criteria	Enables you to enter an SUSAR criteria as an SQL query. An SUSAR is identified as a Serious, Unexpected, Related Case. Note: The SQL should not exceed 2000 characters.

Use the following procedure to Configure the Case Processing Options

1. Select the required option for Display warning when Case Level Assessment does not match with Event Level Assessment.
2. Select the required option for Criteria for case level causality assessment.
3. Select the required option for Criteria for case level Seriousness determination.
4. Enter the **SUSAR Criteria**.
5. Click **Save** to save the changes made.

Configuring Auto Archiving

This screen enables you to configure the auto-archiving. Select **System Configuration** -> **System Management** to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

The default rule requires that the following options must be completed before a case is auto-archived:

- All Action Items Closed
- All Reports Submitted or Marked required for Non-Submission
- All Events are encoded
- All Letters are sent
- All Cases are locked

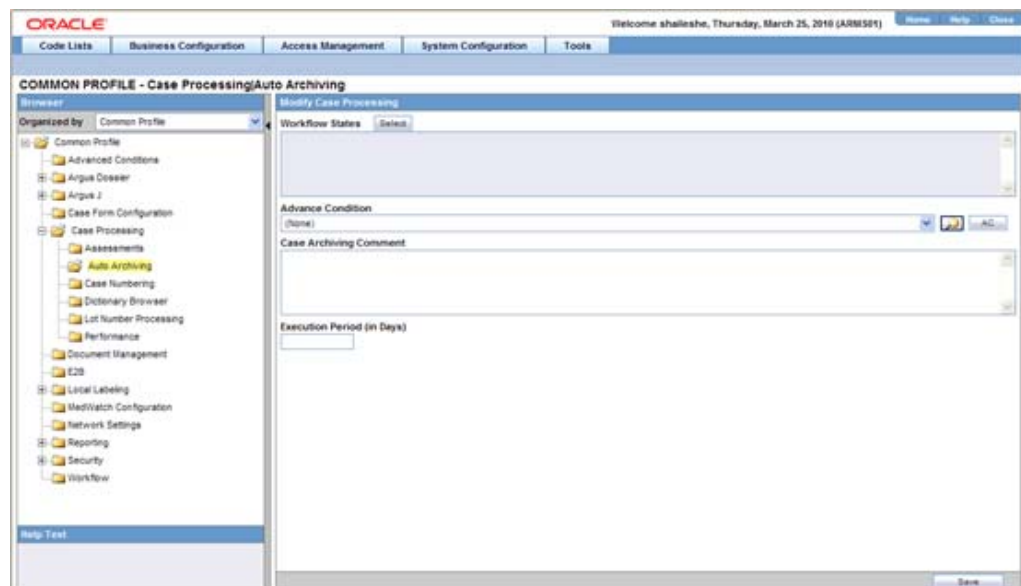
Apart from this default rule, you can also configure additional rules/criteria for auto-archiving cases from this screen.

- Workflow State (Configurable by the user) - This option enables you to select Workflow States. Cases that fall in the specified workflow states can be auto-archived.
- Advanced Conditions selection (Configurable by the user) - This option enables you to specify advanced conditions. Cases that meet the specified advanced conditions, can be auto-archived.

This feature enables you to define rules for automatically archiving those cases that meet the defined rules.

To view the list of field names associated with the **Case Processing** -> **Auto Archiving** section, click the **Auto Archiving** folder in the left panel.

The field names associated with **Auto Archiving Configuration** appear in the right panel.



Field Descriptions The following table lists the fields available under **Auto Archiving Configuration**:

Field/Control Name	Description
Workflow States	The Select button enables you to select workflow states from a list of workflow states. The selected workflow states are displayed in the text box. Cases that belong to these workflow states are marked to be auto-archived.
Advanced Condition	Enables you to specify advanced conditions for auto-archiving cases. Cases that meet the advanced conditions are marked to be auto-archived. Refer to Advanced Conditions for details on creating advanced conditions.
Case Archiving Comment	Enables you to enter a pre-defined case close comment, of up to 200 characters. The information entered in this field is displayed in the Case Routing and Case Archive notes.
Execution Period (in Days)	Enables you to define how often the cases will be archived. Note: You can enter up to 99 days only. If no value is entered, the cases will not be auto-archived.

Use the following procedure to configure the auto archiving options

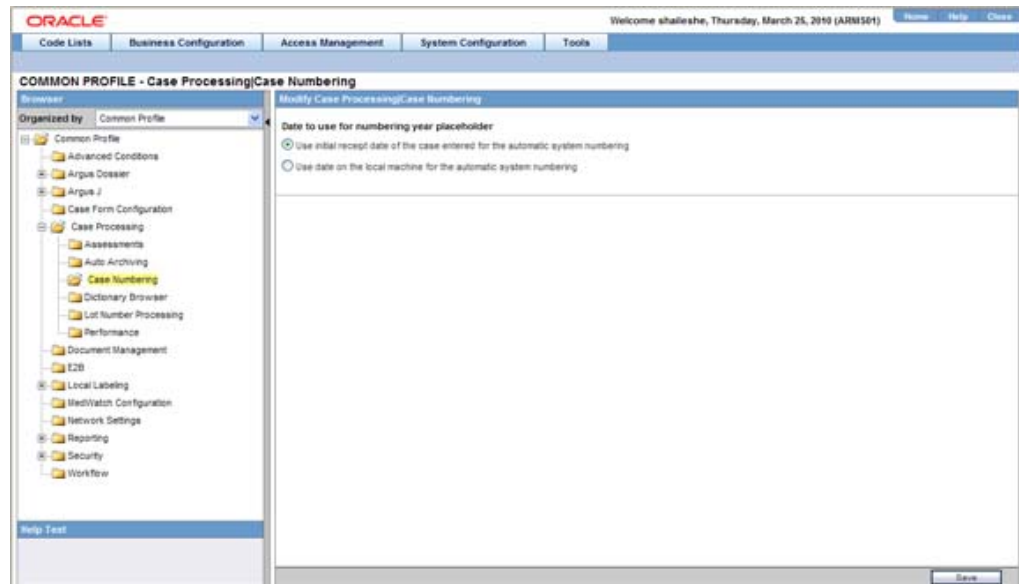
1. Select the workflow states for auto-archiving cases from **Workflow States**.
2. Create the advanced conditions for archiving cases in **Advanced Condition**.
3. Enter the **Case Archiving Comment** as a pre-defined case close comment.
4. Enter how often the cases will be archived, as per number of days, under **Execution Period**.
5. Click **Save** to save the changes made.

Configuring Case Numbering

This screen enables you to configure the case processing fields and items for case numbering. Select System Configuration -> System Management to view the Common Profile Configuration screen

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To view the list of field names associated with the **Case Processing -> Case Numbering** section, click the **Case Numbering** folder in the left panel. The field names associated with **Case Numbering** appear in the right panel.



Field Descriptions The following table lists the fields available under **Case Numbering Configuration**:

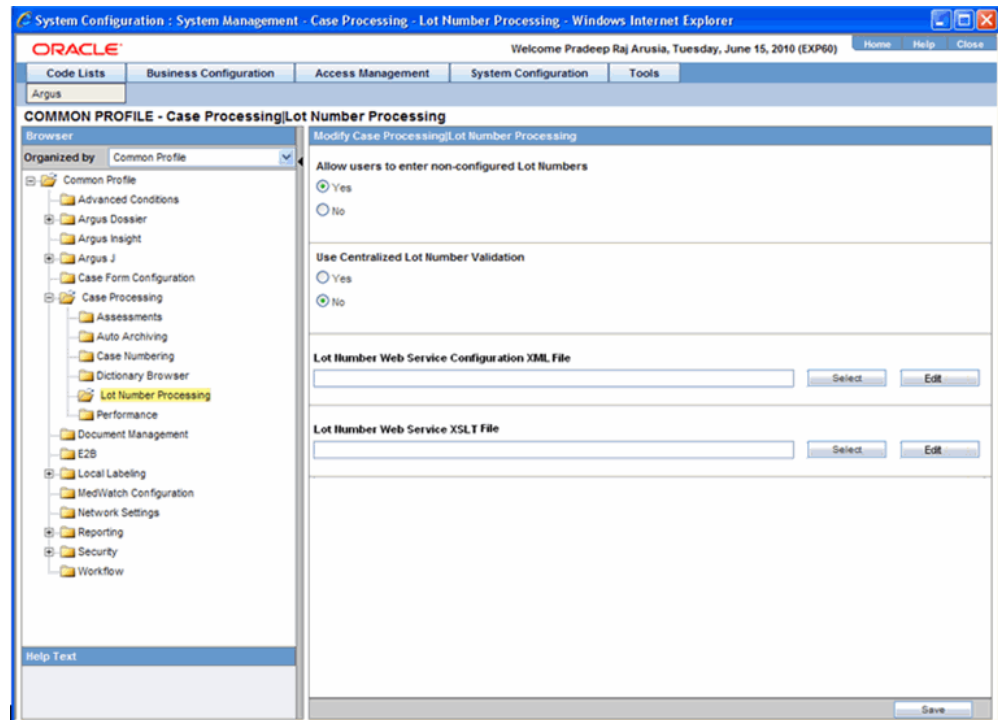
Field/Control Name	Description
Date to use for numbering year placeholder	<p>The available options are:</p> <ul style="list-style-type: none"> ■ Use initial receipt date of the case entered for the automatic system numbering. ■ Use date on the local machine for the automatic system numbering.

Use the following procedure to configure the case numbering options.

1. Select the required option for Date to use for numbering year placeholder.
2. Click **Save** to save the changes made.

Configuring Lot Number

A common profile switch determines whether a user can override an un-validated lot number and enter them in the case form.



The following table lists and describes the fields available under **Lot Number Processing**:

Field/Control Name	Description
Allow Users to enter non-configured Lot Numbers	Enables you to select whether or not to allow users to enter non-configured lot numbers. Select Yes to allow, and No to disallow.
Use Centralized Lot Number Validation	Enables you to select whether or not to allow centralized lot number validation. Select Yes to use, and No to not use this option.
Lot Number Web Service Configuration XML File	Enables you to select and/or edit (if required) the Lot Number Web Service Configuration XML File. The file path textbox is a read-only field, which displays the path of the uploaded file. This field stores the configuration of the Centralized Lot Number Web Service in XML format. The Edit button is enabled only after the XML file has been successfully uploaded.
Lot Number Web Service XSLT	Enables you to select and/or edit (if required) the Lot Number Web Service XSLT File. This field stores the XSLT associated with the Centralized Lot Number Web Service. The file path textbox is a read-only field, which displays the path of the uploaded file. The Edit button is enabled only after the XSLT file has been successfully uploaded.

Yes is the default. This enables the user to select the options for the Lot Number Validation as current functionality. This message box displays the following message:

No matching lot number was found.

If centralized lot search is used, the system hides the Lookup button since a list is automatically returned and displayed.

- **No**: The system does not permit the user to keep the existing value. The user can only obtain it from a Lookup dialog that lists the available Lot Numbers.

- The system hides the Keep button.

A common profile switch determines whether lot validation uses Argus or a centralized lot validation.

- No (default): This enables the user to select the options for the Lot Number Validation as current functionality from within the Argus Product Families Lot Numbers
- Yes: This enables the system to query outside the Argus Safety system through a web service return the following parameters for Lot Number Validation
 - Argus sends the user-entered lot number to central system for validation/look-up and retrieves a response to act on.
 - The message format for the retrieved lot is as follows:

<Lots>

<Lot>

<Lot Number>: Lot number

<Expiration>: Lot expiration date

<Custom name=name metadata=text>: Custom data to a lot number

- If more than one lot number is returned, the system displays a lot selection dialog.

The Custom Node ■ The metadata attribute is as labels in the selection dialog that displays the data. The name attribute is used to identify the case form field to be populated with the data in the node.

- Clients can use an XSLT document to map the custom data to case fields present on the active case form page.

The screenshot shows a dialog box titled "Lot Number Lookup -- Webpage Dialog". Inside, there is a table with the following columns: "Lot Number", "Expiration Date", "Thermisol Indicator", and "Albumin Status". The table contains multiple rows of data, including lot numbers like 5043AX1, 342345, 89653, 4234234, 87653, 78622, and 342345, along with their respective expiration dates, thermisol indicators, and albumin statuses.

Lot Number	Expiration Date	Thermisol Indicator	Albumin Status
5043AX1	2010-06-07	15	11.4 mg/gC
342345	2019-12-15	12	33.5 mg/gC
5043AX1	2010-06-07	15	11.4 mg/gC
89653	2000-11-11	55	9 mg/gC
4234234	2009-09-07	13	7.9mg/gC
87653	2009-12-31	888	7.98 mg/gC
5043AX1	2010-06-07	15	11.4 mg/gC
5043AX1	2010-06-07	15	11.4 mg/gC
342345	2019-12-15	12	33.5 mg/gC
5043AX1	2010-06-07	15	11.4 mg/gC
89653	2000-11-11	55	9 mg/gC
4234234	2009-09-07	13	7.9mg/gC
87653	2009-12-31	888	7.98 mg/gC
5043AX1	2010-06-07	15	11.4 mg/gC
78622	2014-12-15	22	19.5 mg/gC
5043AX1	2010-06-07	15	11.4 mg/gC
342345	2019-12-15	12	33.5 mg/gC
5043AX1	2010-06-07	15	11.4 mg/gC
342345	2019-12-15	12	33.5 mg/gC

If an error occurs during the web service transaction, a message box will appear with the proper error message.

Configuring the Dictionary Browser

This screen enables you to configure the case processing fields and items for MedDRA Browser.

Select System Configuration -> System Management to view the Common Profile Configuration screen

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

A switch in Argus enables you to use either local MedDRA Coding or Central System MedDRA Coding (Web Service Method).

- Local (Default): Current functionality of Dictionary browser using Local Dictionary within the Database.
- Web Services: Returns the MedDRA hierarchy via the configured Web Services.

This enables the User Local MedDRA if term is not found by Web Service function.

COMMON PROFILE - Case Processing|Dictionary Browser

Organized by: Common Profile

Term selection in MedDRA Browser

- Select any term to code if multiple are returned for the search.
- Select the Primary SOC term for encoding if multiple terms are returned from the search.

Argus Safety MedDRA Coding Method

- Local MedDRA
- Web Services
- Use Local MedDRA if Term not found by Web Services
- Use Local MedDRA for Japanese terms

Argus Safety WHO Drug Coding Method

- Local WHO Drug
- Web Services
- Use Local WHO Drug if Term not found by Web Services

Allow User to Add Non-Current MedDRA Terms for

- Case irrespective of Country of Incidence
- Case where Country of Incidence is other than Japan

On change of LLT Term Sync English and Japan LLT's, irrespective of the currency

- Yes
- No

Save

To view the list of field names associated with the **Case Processing -> Dictionary Browser** section, click the **Dictionary Browser** folder in the left panel. The field names associated with **Dictionary Browser** are in the right panel.

Field Descriptions The following table lists the fields available under **Dictionary Browser Configuration**:

Field/Control Name	Description
Term Selection in Dictionary Browser	<p>The available options are:</p> <ul style="list-style-type: none"> ■ Select any term to code if multiple are returned for the search ■ Select the Primary SOC term for encoding if multiple terms are returned from the search.

Allow User to Add Non-Current MedDRA Terms for	The available options are: <ul style="list-style-type: none"> Case irrespective of Country of Incidence Case where Country of Incidence is other than Japan
On change of LLT Term Sync English and Japan LLTs, irrespective of the currency	The available options are Yes or No . This profile switch is enabled only when the user configures the <i>Allow User to Add Non-Current Meddra Terms for</i> to Yes .

Use the following procedure to configure the Dictionary Browser.

1. Select the required option for Date to use for numbering year placeholder.
2. Click **Save** to save the changes made.

Dictionaries All dictionaries are stored in database schema separately outside Argus Safety and Interchange schema. The Argus-supported dictionaries are:

- MedDRA
- MedDRA J
- WHO Drug
- J Drug

Only one copy of each dictionary version is maintained in the database and it is not segregated by enterprise. The dictionary version that is applicable for a particular enterprise/client is defined in these common profile switches: Case Form Configuration' Auto Encoding, Dictionary & Central Encoding. Since these switches are segregated by each Enterprise, these dictionaries can have different versions for different enterprises, as required. J Drug dictionary is not configured through Console common profile switches (Case Form Configuration' Auto Encoding, Dictionary & Central Encoding), and is internally maintained as single version, therefore, it remains a common J Drug dictionary for all enterprises.

Configuring Group Data Access

This screen enables you to configure the case processing fields and items for Group Data Access.

Field Descriptions The following table lists the fields available under **Group Data Access Configuration**:

Field/Control Name	Description
Access on Patient Initials	The available options are: <ul style="list-style-type: none"> Initials part of Patient Details access group Initials part of Patient Information access group
Access on Patient DOB	The available options are: <ul style="list-style-type: none"> Date of Birth part of Patient Details access group Date of Birth part of Patient Information access group
Parent - Initials	The available options are: <ul style="list-style-type: none"> Initials part of Parent Details access group Initials part of Patient Information access group

Access on Parent DOB	The available options are: <ul style="list-style-type: none"> ▪ Date of Birth part of Patient Details access group ▪ Date of Birth part of Patient Information access group
-------------------------	---

Configuring WHO Drug

Argus supports WHO-Drug encoding using a locally installed version of the WHO-Drug dictionary through the WHO-Drug browser.

- A switch in Argus enables you to use either local WHO-Drug Coding or Central System WHO-Drug Coding (Web Service Method) under the Dictionary browser category
 - Local (Default): Uses the current functionality of WHO-Drug browser that uses the Local Dictionary in the Database
 - Web Service: Returns the WHO-Drug fields via the configured Web Services
 - The system enables the User Local MedDRA if term is not found by Web Service"

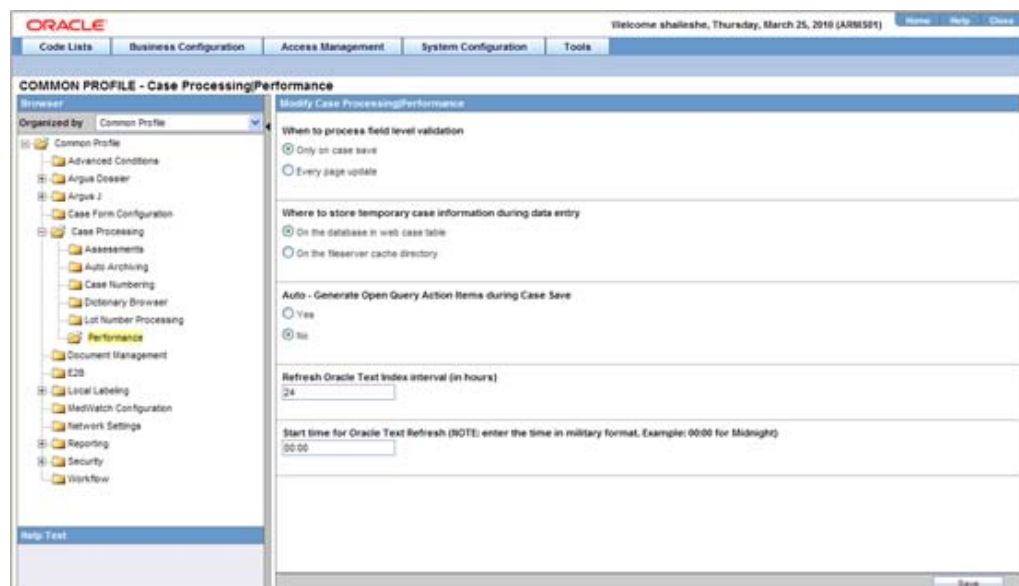
Configuring Performance

This screen enables you to configure the case processing fields and items for performance.

Select System Configuration -> System Management to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To view the list of field names associated with the **Case Processing -> Performance** section, click the **Performance** folder in the left panel. The field names associated with **Performance** appear in the right panel.



Field Descriptions The following table lists and describes the fields available under **Performance Configuration**:

Field/Control Name	Description
When to process field level validation	Enables you to configure the frequency of field level validation. Select Only on case save to validate only when a case is saved. Alternatively, select Every page update to validate fields whenever a page is updated.
Use Oracle Text for duplicate search querying	Enables you to select Oracle Text for duplicate search querying. Click Yes to enable this feature.
Refresh Oracle Text Index interval (in Minutes)	Enables you to configure the interval (in minutes) between each refresh of an Oracle Text Index. This feature is useful while searching for duplicate cases. It is advisable to enter a high interval for low number of cases and vice versa.
Start Time for Oracle Text Refresh	Enables you to specify the time when the Oracle text will be refreshed.

Use the following procedure to configure performance.

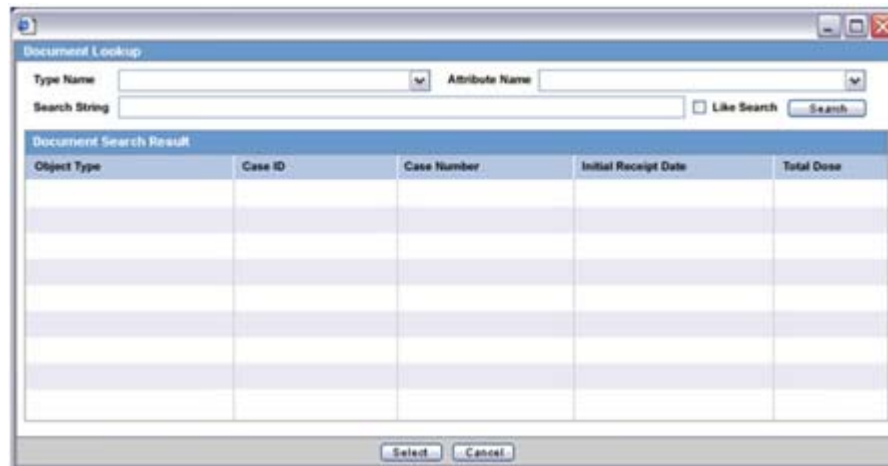
1. Select the required option for **When to process field level validation**, as applicable.
2. Select the required option for **Use Oracle Text for duplicate search querying**, as applicable.
3. Enter the time difference between each refresh (in minutes), under **Refresh Oracle Text Index interval (in Minutes)**.
4. Enter the time (in military format) when the Oracle text refresh will begin, under **Start Time for Oracle Text Refresh**.
5. Click **Save** to save the changes made.

Configuring Documentum

The system enables you to configure to choose Document Management from the Common Profile Switches: Document Management

- You may select from the following:
 - Documentum: Cabinet Name and Document Type textboxes are only enabled when the "Documentum" radio option is selected. These text boxes allow up to 255 characters.
- Docbase and Domain are textbox fields. These fields can be a maximum of 255 characters.
- Configure the following for Document Management:
 - E2B Reports
 - Expedited Paper Reports
 - Periodic Reports
 - Attachments saved within the cases
 - E2B Reports:
- If the E2B switch is enabled and the user transmits an E2B Report (Before submission to the Gateway), the system stores the E2B XML Message in Documentum.
- When the Report Submission is successful and the report is marked as submitted in Argus, the system updates a flag in the Documentum database to designate the same.
- Expedited Reports
 - If the Expedited switch is enabled and the user submits an expedited report, the Argus Safety Service inserts the report into Documentum as a PDF file.
 - When the Report Submission is successful and the report is marked as submitted, the system updates a flag in the Documentum database to signify the same.
- Periodic Reports:

- If the Periodic Switch is enabled and a Periodic Report is approved in Argus, an Argus Safety Service exports the report as a PDF file and saves it in the Documentum database.
- When the Report Submission is successful and the report is marked submitted, the system updates a flag in the Documentum database to indicate the same.
- Attachments:
 - When this switch is enabled, a new button is available on the Argus Attachments screen, **LAM Attachments Section label Attach Documentum Link**.
 - The Argus Bookin dialog has an additional drop down option for attaching to Documentum.
 - When the Links Switch is enabled, the system stores all Argus Attachments in the Documentum database.
 - Clicking the Attach Documentum Link button opens a search dialog to enable the user to search the Documentum database for a document. This document is then linked as an attachment within Argus.



- When the user clicks the Attach Documentum Link button, the following occurs:
 - The system presents a search dialog to enable the user to search for a document in the Documentum database.
 - The user must select a Table to Search. This list is a distinct Table List from the Documentum_table_info Table.
 - After the user selects a Table, the system populates the Column drop down with all the columns available for that table based on configuration from the same table.
 - When the user selects the Full Search option, the system performs a like search in Documentum.
- If LDAP is enabled, the system automatically send the login information from Argus to Documentum.
- After selecting a document from the Search results, the system saves the URL for the Argus attachment.

- If the user clicks the URL, Argus automatically opens the document from Documentum.
- Argus refers to two (2) that enables you to specify which tables/columns can be searched in Documentum and which Table Fields to display in the Search Results.
 - documentum_table_info - This table holds the table / fields the user will be able to search.
 - Type_Name - Table to Search
 - Attribute_Name - Field in the Table to Search
 - Attribute_Type - Type of field being searched.
 - Documentum_display_info - This table stores the Return Search Parameters.
 - Type_Name - Table to Search
 - Attribute_Name - Field in the Table to Search
 - Sort_Id - The order in which the fields will be displayed
 - The Document Management (Central or Documentum) database gets a new document each time a document attachment is added as a new attachment. Existing documents are modified for changes.
 - The system does not create a new document in the Document Management (Central or Documentum) database each time a case /event is saved in Argus or Affiliate
 - When cases are copied, the document copy has the same DOC ID (Object ID) as the original case. If the Document is modified after the cases are copied, the system gets a new DOC ID only for the case attachments that were modified.
 - The icon is similar to the Additional Info requirements for attachment types
 - When the user clicks the attachment to open it, the system retrieves the attachment from Documentum
 - When events from the Affiliate are accepted in Argus as Argus cases, the system keeps the DOC ID(Object ID) from the Affiliate Event
 - Attachments can be entered to the case / affiliate event via
 - Affiliate Events
 - Bookin in Argus or Affiliate
 - Case Form / Affiliate Event Form
 - Intake WL
- Error Messages
 - If the system cannot connect to the document system, it displays the following message:
 - Argus was unable to connect to the document management system. Please contact your Administrator for more details.
 - If the document system does not return any rows, the system returns a dialog with the following message
 - No documents returned.
 - Select System Configuration -> System Management to view the Common Profile Configuration screen

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To view the list of field names associated with the **Case Processing -> Documentum** section, click the **Documentum** folder in the left panel. The field names associated with **Documentum** appear in the right panel.

Field Descriptions The following table lists the fields available under **Documentum Management**:

Section	Field	Description
Common Login	Use Common Login Password	Users use a common login password to access the system
	Docbase	The name of the document database.
	Domain	The name of the domain where the database resides.
Enable Storage of E2B Reports in Document Repository	Documentum	Enables the system to store E2B reports in the document repository.
	Argus	Enables the system to store E2B reports in the Argus document repository. This is the default.
	Cabinet Name	The storage location of the E2B reports.
	Document Type	The type of document that is being stored.
Enable Storage of submitted expedited reports in Document Repository	Documentum	Enables the system to store submitted expedited reports in the Documentum document repository.
	Argus	Enables the system to store submitted expedited reports in the Argus document repository. This is the default.
	Cabinet Name	The storage location of the submitted expedited reports.
	Document Type	The type of document that is being stored.
Enable storage of case attachment files in the Document Repository	Documentum	Enables the system to store case attachment files in the Documentum document repository.
	Argus	Enables the system to store case attachment files in the Argus document repository. This is the default.
	Cabinet Name	The storage location of the case attachment files.
	Document Type	The type of document that is being stored.

Section	Field	Description
Enable storage of submitted periodic reports in the Document Repository	Documentum	Enables the system to store submitted periodic reports in the Documentum document repository.
	Argus	Enables the system to store submitted periodic reports in the Argus document repository. This is the default.
	Cabinet Name	The storage location of the submitted periodic reports.
	Document Type	The type of document that is being stored.

Use the following procedure to configure Documentum

1. Select the Common Login to configure the login for the user.
2. Select the option for Enable Storage of E2B Reports in Documentum.
3. Select the option for Enable Storage of submitted expedited reports in Documentum.
4. Select the option for Enable storage of case attachment files in Documentum and additionally the searching and attaching files already existing in Documentum to a case.
5. Select the option for Enable storage of submitted periodic reports in Documentum.
6. Click **Save** to save the changes made.

Local Labeling

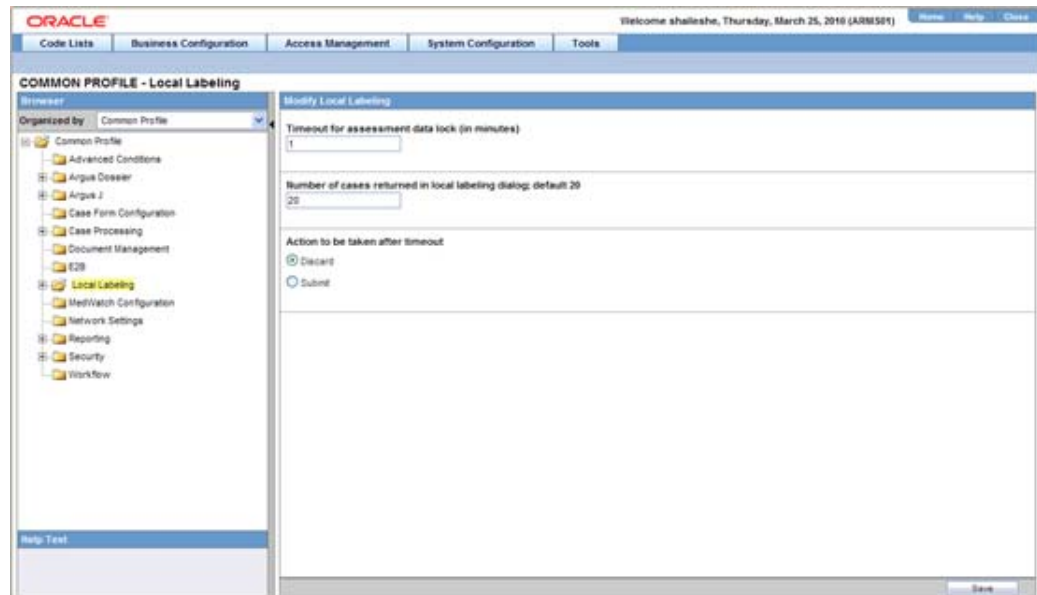
This section enables you to configure the common profile switches for Local Labeling and includes discussions of the following:

- Configuring Local Labeling
- Configuring Local Labeling LAM

Configuring Local Labeling The Local Labeling Configuration screen enables you to modify the options available through local labeling. Select System Configuration -> System Management to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To configure the fields associated with the **Local Labeling** section, click the **Local Labeling** folder in the left panel. The configurable fields associated with **Local Labeling** appear in the right panel.



Field Descriptions The following table lists and describes the fields available under **Local Labeling**:

Field/Control Name	Description
Number of Cases returned in local labeling dialog; default X	This field enables the user to configure the number of cases that are returned in the local labeling dialog. Example: If the value is entered as 20 then 20 cases are returned in the local labeling dialog.
Action to be taken after timeout	The available options are : <ul style="list-style-type: none"> ■ Discard ■ Submit
Timeout for assessment data lock (in minutes)	This field enables the user to enter the minutes after which the time-out for assessment data lock is applicable.

Use the following procedure to configure local labeling

1. Enter the number in Number of Cases returned in local labeling dialog; default.
2. Select the option for Action to be taken after timeout.
3. Enter the value in minutes for Timeout for assessment data lock (in minutes).
4. Click **Save** to save the changes made.

Configuring LAM The Local Labeling LAM Configuration screen enables you to modify the options available through local labeling for LAM.

Field Label Updates The **Argus Console Field Labels** option enables the user to modify the field labels for the **Argus Affiliate Event Information** form.

- The existing Argus fields are under the **Argus Safety** folder structure.
- Please refer to the tables in the **LAM Information** section for the details about the Help Text for the fields.
- The system enables the user to hide the field on the LAM form.

- The system prints the Affiliate field labels.
- The system tracks all field label updates in the audit log.

Field Validation Updates Argus Affiliate enables the user to configure Field **Validations for Mandatory and Warning for the LAM Event** fields.

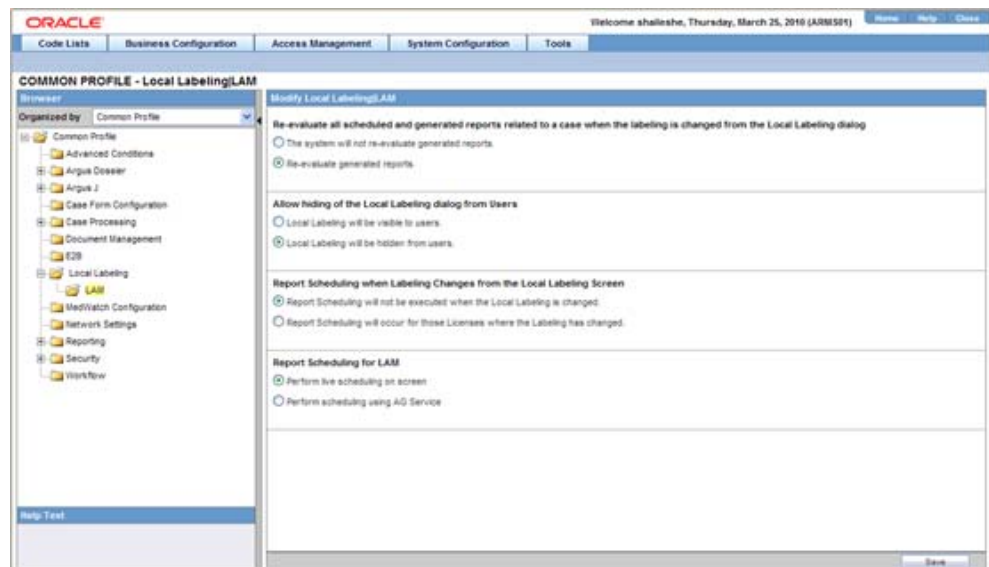
- The existing Argus fields are under the **Argus Safety** folder structure.
- Please refer to the table for **LAM Event Info** for the fields in the **Field Validations**.
- The Affiliate fields for advanced conditions are **only** visible for field validations. They are not visible to the rest of the application.
- The system prints the information for the configured field validations.
- The system tracks all updates to field validations in the audit log.
- The system displays the standard **Justifications** dialog to enable the user to enter the justifications for overriding the warnings, but **does not** permit the user to save the case for a mandatory error.

Select System Configuration -> System Management to view the Common Profile Configuration screen

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To configure the fields associated with the **Local Labeling LAM** section, click the **Local Labeling** folder in the left panel.

- The **LAM** sub-folder is displayed in the left panel.
- Click on LAM sub-folder to configure the LAM options.
- The configurable fields associated with **Local Labeling Lam** appear in the right panel.



Field Descriptions

The following table lists and describes the fields available under **Local Labeling LAM**:

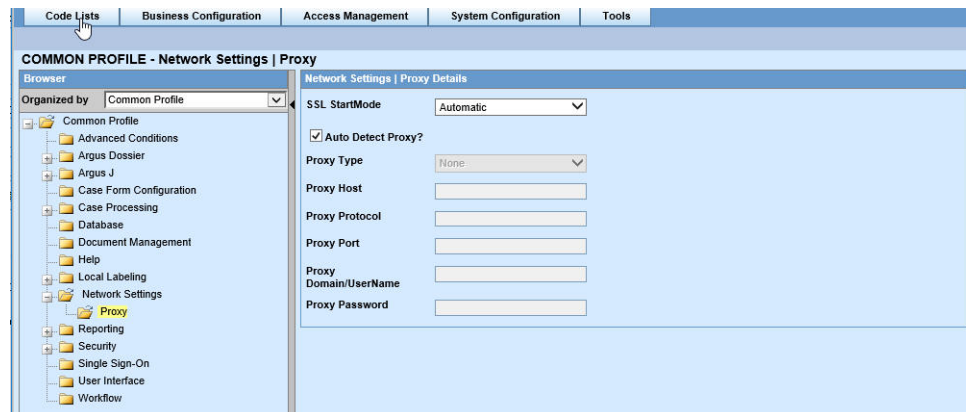
Field/Control Name	Description
Report Scheduling when Labeling Changes from the Local Labeling Screen	<p>The available options are:</p> <ul style="list-style-type: none"> Report Scheduling will not be executed when the Local Labeling is changed Report Scheduling will occur for those Licenses where the Labeling has changed
Re-evaluate all scheduled and generated reports related to a case when the labeling is changed from the Local Labeling dialog	<p>The available options are:</p> <ul style="list-style-type: none"> The system will not re-evaluate generated reports Re-evaluate general reports.
Report Scheduling for LAM	<p>The available options are:</p> <ul style="list-style-type: none"> Perform live scheduling on screen Perform scheduling using AG service

Use the following procedure to configure local labeling for LAM.

1. Select the option for Allow hiding of the Local Labeling dialog from Users.
2. Select the option for Report Scheduling when Labeling Changes from the Local Labeling Screen.
3. Select the option for Re-evaluate all scheduled and generated reports related to a case when the labeling is changed from the Local Labeling dialog.
4. Click **Save** to save the changes made.

Network Settings

The settings for Proxy set up can be configured under **Network Settings > Proxy**.



The following table lists the fields available:

Configuration Parameter	Valid Values	Description	Default Value
SSLStartMode (Determines how the component starts the SSL negotiation.)	Automatic	If the remote port is set to the standard plain text port of the protocol (where applicable), the class will behave the same as when SSLStartMode is set to sslExplicit. In all other cases, SSL negotiation will be implicit (sslImplicit).	
	Implicit	The SSL negotiation starts immediately after the connection is established.	
	Explicit	The class first connects in plaintext, and then explicitly starts SSL negotiation through a protocol command such as STARTTLS.	
	None	No SSL negotiation, no SSL security. All communication will be in plaintext mode.	Yes
Auto Detect Proxy Checking this field lets the application detect the proxy automatically if applicable.			
Proxy Type Determines the type of Proxy to connect through	None - No proxy (Default)		
	Tunnel - Connect through a tunneling proxy. ProxyPort is set to 80		
	SOCKS4 - Connect through a SOCKS4 Proxy. ProxyPort is set to 1080		
	SOCKS5 - Connect through a SOCKS5 Proxy. ProxyPort is set to 1080		
Proxy Host Holds the Name or IP address of Proxy serve			

Configuration Parameter	Valid Values	Description	Default Value
Proxy Protocol Holds the HTTP_ PROTOCOL component of Proxy URL. Maximum length is 20 characters.			
Proxy Port TCP Port for the Proxy Host			
Proxy Domain/UserName		If the Proxy Host is specified, this property along with Proxy Password is used to connect and authenticate to the given Proxy Server.	
Proxy Password		If the Proxy Host is specified, this property along with Proxy Domain/UserName is used to connect and authenticate to the given Proxy Server. This field expects the password to be in encrypted state, use Cryptography Key Editor to encrypt the password.	
Use Proxy settings for ESM DTD Validation	Checked Unchecked	Enables or disables the usage of Proxy settings for ESM.	Checked (Enabled)
Use Proxy settings for SMTP/S	Checked Unchecked	Enables or disables the usage of Proxy settings for SMTP/S.	Unchecked (Disabled)

User Interface

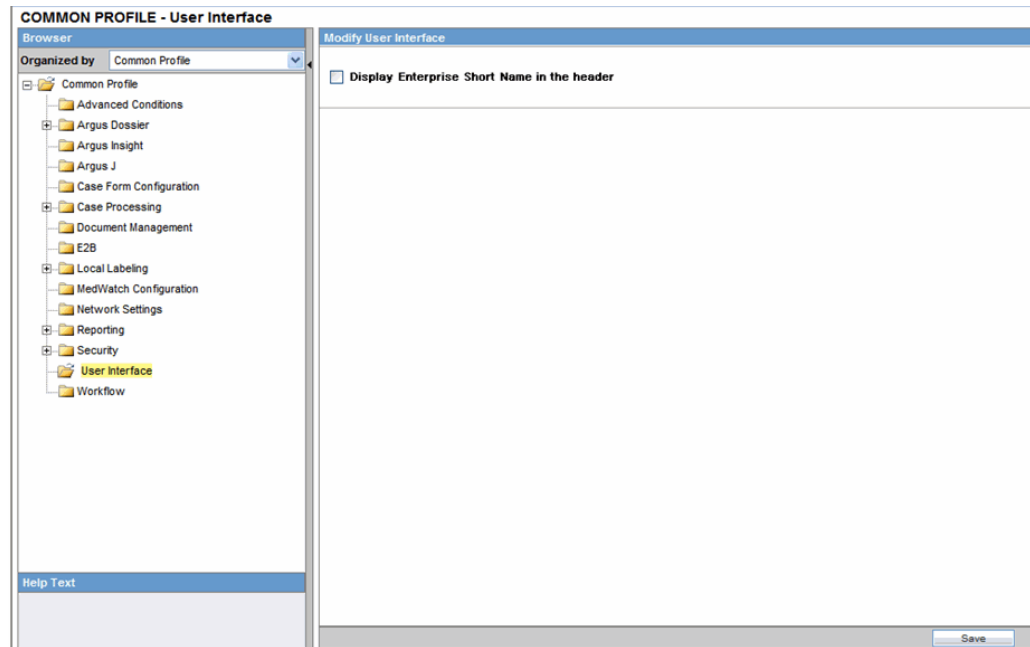
This section enables you to configure the common profile switches for User Interface.

Configuring User Interface

The User Interface Configuration screen enables you to configure the user interface, as per the options available. Select System Configuration -> System Management to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To configure the fields associated with the **User Interface** section, click the **User Interface** folder in the left panel. The configurable fields associated with **User Interface** appear in the right panel.

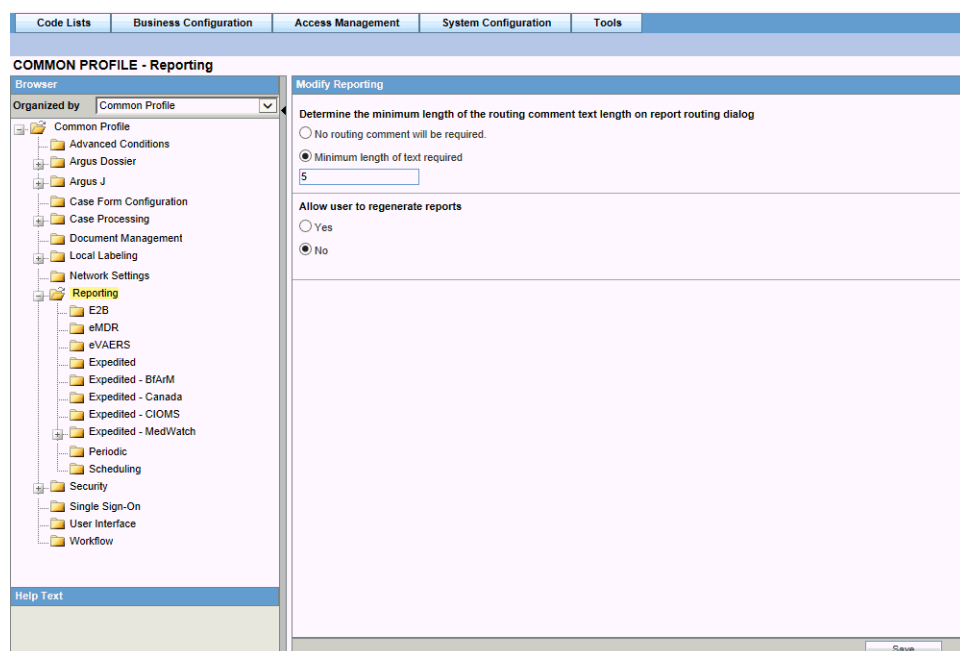


Configuring Reporting

The Reporting Configuration screen enables you to modify the options available for reporting. Select System Configuration -> System Management to view the Common Profile Configuration screen

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To configure the fields associated with the **Reporting** section, click the **Reporting** folder in the left panel. The configurable fields associated with **Reporting** appear in the right panel.



Field Descriptions The following table lists the fields available under **Reporting**:

Field/Control Name	Description
Allow User to regenerate reports	The available options are Yes and No.
Determine the minimum length of the routing comment text length on report routing dialog	The available options are: <ul style="list-style-type: none"> ■ No routing comment will be required ■ Minimum length of text required

Use the following procedure to configure reporting.

1. Select the option for Determine the minimum length of the routing comment text length on report routing dialog.
2. Enter the numeric value in the **Minimum length of text required** text-box, if applicable.
3. Click **Save** to save the changes made to this screen.

Configuring E2B This screen enables you to configure the E2B fields and items for E2B. Select System Configuration -> System Management to view the Common Profile Configuration screen

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To view the list of field names associated with the **E2B** section, click the **E2B** folder in the left panel. The field names associated with **E2B** appear in the right panel.

Field Descriptions The following table lists the fields available under **E2B**:

Field/Control Name	Description
Auto Accept Notes	Enables the user to enter notes (up to 190 characters). It is required for these notes to be entered for the acceptance of the E2B. The notes entered here, are automatically provided during E2B acceptance.
Blind status during E2B report generation	The available options are: <ul style="list-style-type: none"> ■ Blinded ■ Unblinded
Default DTD	Enables the user to select the Default DTD from the drop-down list box.
Default view for E2B (R3)	Specifies the default view of E2B (R3) reports in the ICSR viewer. Decoded, HL7, and XML are the available options.
Default viewing format of the E2B report (used in E2B (R2) reports)	The available options are: <ul style="list-style-type: none"> ■ SGML ■ CIOMS ■ MEDWATCH ■ DECODED VIEW
Drug assessment method (used by E2B/Interchange module)	Enables the user to incorporate the drug assessment method used by E2B/Interchange module.

Field/Control Name	Description
File attachments allowed for ICH E2B (R3) Profile	Verifies the applicable files that can be attached with an E2B (R3) report generated using the ICH profile.
File attachments allowed for EMA E2B (R3) Profile	Verifies the applicable files that can be attached with an E2B (R3) report generated using the EMA profile.
Onset Date Calculation	Enables the user to configure if the onset date is to be calculated based on any suspect drug or on the primary suspect drug only.
Perform E2B Check on Save	Performs data check on Argus fields against E2B standard while saving the case. The available options are: <ul style="list-style-type: none"> ■ Yes ■ No
Send E2B nullification report	Enables the user to send an E2B nullification report. You can select whether to automatically schedule it or to not send the report.
Enable stripping of line breaks in attachment data for EMA E2B(R3) profile	Enables you to strip line break characters in encoded attachment data. The parameter applies only to the EMA E2B (R3) Profile and has 'Yes' and 'No' values. The default value is 'Yes'.

Use the following procedure to configure E2B

1. Enable the check-box option for **Drug assessment method (used by E2B/ESM module)**, if required.
2. Select the option for Blind status during E2B report generation.
3. Select the option for Perform length check of Argus fields against E2B standard.
4. Select the option for Default viewing format of the E2B report (used with Electronic Submission Module (ESM)).
5. Select the option for **Default DTD**.
6. Select the required radio button under **Onset Date Calculation**, as applicable.
7. Enter the comments for the automatically generated notes, when an E2B is accepted, under **Auto Accept Notes**.
8. Click **Save** to save the changes made to this screen.

Configuring eMDR The eMDR Reporting Configuration screen enables you to modify the options available for eMDR reporting.

Select System Configuration -> System Management to view the Common Profile Configuration screen.

To configure the fields associated with the **Reporting** section, click the **Reporting** folder in the left panel. The **eMDR** sub-folder is displayed in the left panel. Click this sub-folder to configure the reporting options. The configurable fields associated with eMDR appear in the right panel.

Field Descriptions

The following table lists and describes the fields available under eMDR:

Field/Control Name	Description
Default Reporting Destination for draft eMDR generation	Displays all Reporting Destinations in the drop-down list. It is used only when the user generates a draft eMDR using the Draft icon or Medical Review eMDR View Draft options.
Default Timeframe for draft eMDR generation	Displays a time frame that the Draft report generation required for populating G7 (gtypeofreport). Without this information, eMDR throws a validation error and the report cannot be generated. The default setting for this parameter is 5. The allowed values for this parameter are 5, and 30. Based on the value entered, the corresponding NCI code is populated for data element Type of Report (G7) in eMDR.
File attachments allowed for eMDR	Verifies the files that are attached to an eMDR. Only configured file types are allowed to be attached to an eMDR.
Default view for eMDR	Specifies the default view of eMDR in ICSR viewer.

Configuring eVAERS The eVAERS Reporting Configuration screen enables you to modify the options available for eVAERS reporting.

Select System Configuration -> System Management to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To configure the fields associated with the **Reporting** section, click the **Reporting** folder in the left panel. The **eVAERS** sub-folder is displayed in the left panel.

Click this sub-folder to configure the reporting options. The configurable fields associated with eVAERS appear in the right panel.

Field Descriptions

The following table lists and describes the fields available under eVAERS:

Field/Control Name	Description
Default view for eVAERS	Enables you to select either XML View or HL7 view as the default view for eVAERS.
File attachments allowed for eVAERS	Enables you to specify the types of files which are allowed as attachments for eVAERS.
Allowed file size for eVAERS (in MB)	Enables you to specify the maximum file size (in MB) allowed in eVAERS.
Default Reporting Destination for draft eVAERS generation	Enables you to select the default Reporting Destination for draft eVAERS generation.

Expedited Reports Configuration The Expedited Reporting Configuration screen enables you to modify the options available for expedited reporting. When configuring expedited reporting rules, be aware of the following:

- If the user **does not** have permission to access **Advanced Conditions** on the **Expedited Reporting Rules**, the system does the following:

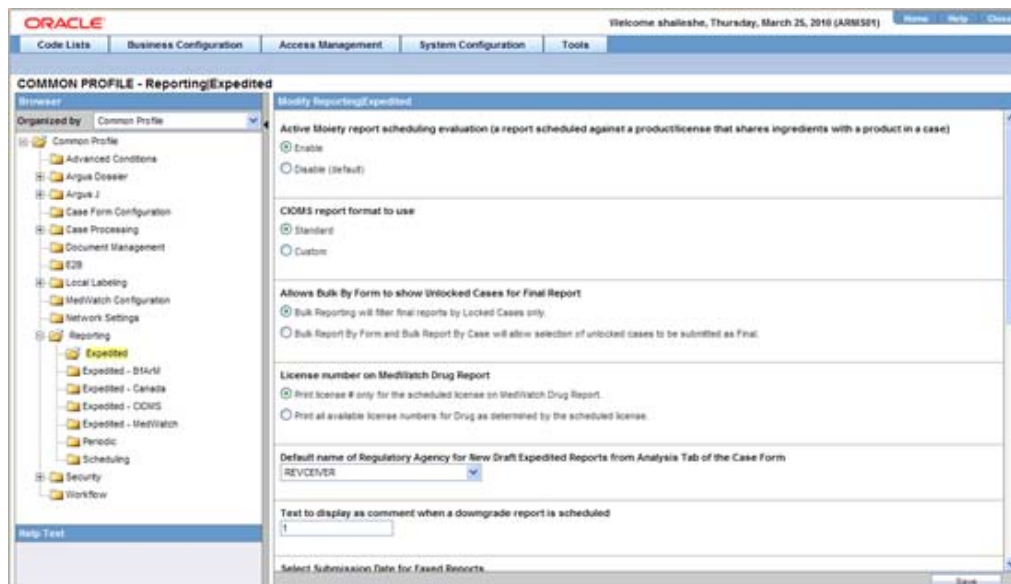
- Displays the advanced condition name instead of displaying a blank.
- **Does not** permit the user to modify or view advanced condition details.
- Disables the **Adv Condition** button.
- The system enables the user configure the **Blinding Study Products** option for those included in the case (default unchecked).
 - The system track updates to this field in the audit log.
 - The **Reporting Rules** reports print the new options
- For cases where expedited reports are due, the user can force-distribute expedited reports even if processing is incomplete.
- The reporting rules have a **Forced Distribute XXX days before due** check box. The default is unchecked.
 - If the user checks the **Force Distribute** option, the **# of days before due** field is entered and automatically checks the **Auto Distribute** check box on the reporting rule (grayed out).
 - The user can enter the number of days from 0 - # of days defined within the time frame.
 - If the user enters a value greater than the defined time frame, the system displays the following message:
 - Please enter a value less than the Time Frame defined for the Reporting Rule.
 - If the user has not checked **Force Distribute**, the system disables the days before due.
- The system tracks updates made to the new Argus Console fields in the audit log.
- The system prints the new fields on the **Reporting Rules** report.

Select System Configuration -> System Management to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To configure the fields associated with the **Reporting** section, click the **Reporting** folder in the left panel. The **Expedited** sub-folder opens in the left panel.

Click on **Expedited** sub-folder to configure the expedited reporting options. The configurable fields associated with **ExpeditedReporting** open in the right panel.



Field Descriptions

The following table lists and describes the fields available under **Expedited Reporting**:

Field/Control Name	Description
Active moiety report scheduling evaluation (a report scheduled against a product/license that shares ingredients with a product in a case)	The available options are: <ul style="list-style-type: none"> Enable Disable (default)
Allows Bulk Reporting screen to show Unlocked Cases for Final Report	The available options are: <ul style="list-style-type: none"> Report by Form and Bulk Report By Case will filter final reports by Locked Cases only Bulk Report By Form and Bulk Report By Case will allow selection of unlocked cases to be submitted as Final
Allows Bulk Reporting screen to show Generated Reports Only	Enables the administrator to allow the Bulk Reporting screen to display only the generated reports.
Nomenclature System on EU Device Vigilance Form	Nomenclature system (Preferable GMDN)" box of EU Device Vigilance Form. By default, this common profile switch is set to 'GMDN'.
Default name of Regulatory Agency for Draft Expedited English Reports	This enables the user to select the Default Name of the Regulatory agency from the drop-down list.
Text to display as comment when a downgrade report is scheduled	This enables the user to enter the text to display when a downgrade report is scheduled.
Auto Distribution Transmission Comments	Enables the user to enter transmission comments of up to 2000 characters, for Expedited Reports Transmission. These comments are auto-distributed, based on Expedited Reporting Rules or Reporting Destinations.

Field/Control Name	Description
Auto Distribution Submission Comments	<p>Enables the user to enter submission comments of up to 2000 characters, for Expedited Reports Transmission.</p> <p>These comments are auto-distributed, based on Expedited Reporting Rules or Reporting Destinations.</p>
Print Case Version of Expedited Reports (x.y.z)	This switch enables the user to enable or disable the printing of the case version of expedited reports.
SQL mapping for CIOMS/CERFA/MHRA Spontaneous/EU EMEA Spontaneous/Spanish Clinical/Spanish Spontaneous Literature Report Source (Parameters: P_CASE_ID)	For more details on the default mapping, refer to the Mapping Document.
Allow Generation of report	<p>If the <i>Allow generation of report</i> is set to Only when previously scheduled reports are submitted or marked for <i>submission not required</i> (default), then follow-up reports are not generated if the previously scheduled report are not yet submitted or not marked as <i>Submission not required</i>.</p> <p>If the <i>Allow generation of report</i> is set to Even when previously scheduled reports are neither submitted nor marked for <i>submission not required</i>, then follow-up reports are generated even if the previously scheduled report are not yet submitted or not marked as <i>Submission not required</i>.</p>

Use the following procedure to configure expedited reports.

1. Select the option for Active moiety report scheduling evaluation (a report scheduled against a product/license that shares ingredients with a product in a case).
2. Select the option for enables Bulk by Form to show Unlocked Cases for Final Report.
3. Select the option for Default name of Regulatory Agency for New Draft Expedited Reports from Analysis Tab of the Case Form from the drop-down text-box.
4. Enter the text in the Text to display as comment when a downgrade report is scheduled text-box, if applicable.
5. Enter the transmission comments in **Auto Distribution Transmission Comments**.
6. Enter the submission comments in **Auto Distribution Submission Comments**.
7. Select whether to enable or disable printing the case version of expedited reports in **Print Case Version of Expedited Reports (x.y.z)**.
8. Click **Save** to save the changes made to this screen.

BIP Reporting Argus Safety uses the BI Publisher reporting technology for the PMDA (R3) Paper reports and Flexible Aggregate reports (DSUR, PBRER and PMAR). This screen contains the common fields that are needed for integrating the BI Publisher server with Argus Safety.

Select System Configuration -> System Management to view the Common Profile Configuration screen.

To configure the fields associated with the **Reporting** section, click the **Reporting** folder in the left panel. The **BIP Reporting** sub-folder is displayed in the left panel.

Click this sub-folder to configure the reporting options. The configurable fields associated with BIP Reporting appear in the right panel.

Field Descriptions

The BIP Reporting fields are grouped into *Common* and *Aggregate* reporting. The following table lists and describes the fields available under these sections:

Common

The fields under this section are common to both PMDA (R3) Paper Reports and Flexible Aggregate Reporting. These fields are critical to authenticate Argus Safety with BI Publisher.

Field/Control Name	Description
BIP Common User	Enables you to enter the name of the BIP common user.
BIP Common User Password	Enables you to enter the password of the BIP common user.

Aggregate Reporting

The fields under this section are applicable only to Flexible Aggregate Reports.

Field/Control Name	Description
Persist data in BIP Aggregate Temp Tables	<p>Enables you to select whether to persist data in BIP Aggregate Temporary Tables.</p> <p>The available options are:</p> <ul style="list-style-type: none"> ■ Yes ■ No
Number of days for which data of BIP Aggregate Temp Tables should be persisted	Enables you to specify the number of days for which data in BIP Aggregate Temporary Tables should be persisted.

Expedited BfArM Reports Configuration The Expedited BfArM Reporting Configuration screen enables you to modify the options available for expedited BfArM reporting.

Select System Configuration -> System Management to view the Common Profile Configuration screen.

To configure the fields associated with the **Reporting** section, click the **Reporting** folder in the left panel. The **Expedited- BfArM** sub-folder is displayed in the left panel.

Click on the **Expedited-BfArM** sub-folder to configure the expedited BfArM reporting options. The configurable fields associated with **Expedited - BfArM Reporting** appear in the right panel.

Field Descriptions

The following table lists and describes the fields available under **Expedited - BfArM Reporting**:

Field/Control Name	Description
Causality Value on BfArM Report	The available options are: <ul style="list-style-type: none"> beh.Azrt Hersteller Arznel.Komm
Value of field "Grunderkrankung" on the BfArM/PEI form	The available options are: <ul style="list-style-type: none"> Do not output suspect and concomitant product indication in this field Output additional suspect and concomitant product Events & Indications.

Use the following steps to configure the expedited BfArM reports.

1. Select the option for Causality Value on BfArM Report.
2. Select the option for Value of field "Grunderkrankung" on the BfArM/PEI form.
3. Click **Save** to save the changes made to this screen.

Expedited Canada Reports Configuration The Expedited Canada Reporting Configuration screen enables you to modify the options available for expedited Canada reporting.

Select System Configuration -> System Management to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To configure the fields associated with the **Reporting** section, click the **Reporting** folder in the left panel. The **Expedited- Canada** sub-folder is displayed in the left panel.

Click on the **Expedited-Canada** sub-folder to configure the reporting options. The configurable fields associated with **Expedited - CanadaReporting** appear in the right panel.

Field Descriptions

The following table lists and describes the fields available under **Expedited- Canada Reporting**:

Field/Control Name	Description
SQL used to populate the "Health Canada assigned company identification number" field on the Canadian Device report form	This field enables the user to enter the associated SQL syntax.
SQL used to populate the "Establishment License Number" field on the Canadian Device report form	This field enables the user to enter the associated SQL syntax.
SQL used to populate the "Device Identification No" field on the Canadian Device report form	This field enables the user to enter the associated SQL syntax.
SQL used to populate the "Age of Device" field on the Canadian Device report form	This field enables the user to enter the associated SQL syntax.
SQL used to populate the "How long was the device in use?" field on the Canadian Device report form	This field enables the user to enter the associated SQL syntax.
Offset from GMT used to calculate Canada date/time fields (in hours)	This switch enables the GMT offset to the Submitted dates getting printed in Canadian Device Form.
SQL used to populate the "If "preliminary" only, anticipated date for the final report" field on the Canadian Device report form	This field enables the user to enter the associated SQL syntax.
SQL used to populate the "Name of Health Care Facility" field on the Canadian Device report form	This field enables the user to enter the associated SQL syntax.
SQL used to populate the "Name and Address for Manufacturer(A7)" field on the Canadian Device report form	This field enables the user to enter the associated SQL syntax.

Field/Control Name	Description
SQL used to populate the "Is there a new drug submission for this drug under review in Canada" field on the Canadian Expedited ADR report form	This field enables the user to enter the associated SQL syntax.
SQL used to populate the "Is there a clinical trial application for this drug under review in Canada" field on the Canadian Expedited ADR report form	This field enables the user to enter the associated SQL syntax.
SQL used to populate the "Is there an ongoing clinical trial for this drug in Canada" field on the Canadian Expedited ADR report form	This field enables the user to enter the associated SQL syntax.
SQL used to populate the "Report ADR occurred in Phase I-IV Study" field on the Canadian Expedited ADR report form	This field enables the user to enter the associated SQL syntax.
SQL used to populate the "Report ADR occurred in Phase I-III Study" field on the Canadian Expedited ADR report form	This field enables the user to enter the associated SQL syntax.

Use the following procedure to configure expedited Canada reports.

1. Enter the SQL syntax for SQL used to populate the "Is there an ongoing clinical trial for this drug in Canada" field on the Canadian Expedited ADR report form.
2. Enter the SQL syntax for SQL used to populate the "Is there a clinical trial application for this drug under review in Canada" field on the Canadian Expedited ADR report form.
3. Enter the SQL syntax for SQL used to populate the "Is there a new drug submission for this drug under review in Canada" field on the Canadian Expedited ADR report form.
4. Enter the SQL syntax for SQL used to populate the "Report ADR occurred in Phase I-III Study" field on the Canadian Expedited ADR report form.
5. Enter the SQL syntax for SQL used to populate the "Report ADR occurred in Phase I-IV Study" field on the Canadian Expedited ADR report form.
6. Click **Save** to save the changes made to this screen.

Expedited CIOMS Reports The Expedited CIOMS Reporting Configuration screen enables you to modify the options available for expedited CIOMS reporting. Select System Configuration -> System Management to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To configure the fields associated with the **Reporting** section, click the **Reporting** folder in the left panel.

The **Expedited- CIOMS** sub-folder is displayed in the left panel. Click on the **Expedited-CIOMS** sub-folder to configure the expedited CIOMS reporting options.

The configurable fields associated with **Expedited - CIOMS Reporting** appear in the right panel.

Field Descriptions

The following table lists the fields available under **Expedited- CIOMS Reporting**:

Field/Control Name	Description
CIOMS Form Selection	This enables the user to select the CIOMS form to be used across the application for Expedited Reporting / Periodic Reporting.
CIOMS report format to use	<p>The available options are:</p> <ul style="list-style-type: none"> ■ Standard ■ Custom <p>When Custom is selected, a second version of the CIOMS form is used. This form is almost identical to the Standard form.</p> <p>The only difference is that the Custom form includes superscripts in the label text for boxes 15, 16, 18 and 19. The superscript is simply an asterisk (*) to draw the user's attention to the following footnote also included in the Custom form:</p> <p>*Boxes 15, 16, 18, and 19 on page 1 contain first dose regimen information for suspected product #1 and #2. Suspected Drug(s) information is continued on Additional Information page, if applicable.</p> <p>Thus, the Custom form simply provides the user the option to clearly identify fields that have overflow information on the Additional Information page.</p>
Print Patient ID, Study ID, Center ID in 26. REMARKS section of the CIOMS form	Enables the user to print the Patient ID, Study ID and Center ID fields in the "26. REMARKS" section of the CIOMS form.
Print Medically Confirmed in the 26. REMARKS section of the CIOMS form	Enables the user to print Medically Confirmed in the 26. REMARKS section of the CIOMS form.

Field/Control Name	Description
Print World Wide Number in the 26. REMARKS" section of the CIOMS form	Enables the user to print World Wide Number in the "26. REMARKS" section of the CIOMS form.

Use the following procedure to configure the expedited CIOMS reports.

1. Select the Print Patient ID, Study ID, Center ID in the "26. REMARKS" section of the CIOMS form checkbox to print these fields in the CIOMS form.
2. Select the Print Medically Confirmed in the "26. REMARKS" section of the CIOMS form checkbox to print this field in the CIOMS form.
3. Select the Print World Wide Number in the "26. REMARKS" section of the CIOMS form checkbox to print this field in the CIOMS form.
4. Select the option for CIOMS report format to use.
5. Select the relevant CIOMS form, from CIOMS Form Selection.
6. Click **Save** to save the changes made to this screen.

Expedited MedWatch Reports Configuration The Expedited MedWatch Reporting Configuration screen enables you to modify the options available for expedited MedWatch reporting.

Select System Configuration -> System Management to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To configure the fields associated with the **Reporting** section, click the **Reporting** folder in the left panel. The **Expedited- MedWatch** sub-folder is displayed in the left panel.

Click on the **Expedited-MedWatch** sub-folder to configure the expedited MedWatch reporting options. The configurable fields associated with **Expedited - MedWatch Reporting** appear in the right panel.

Field Descriptions

The following table lists the fields available under **Expedited- MedWatch Reporting**:

Field/Control Name	Description
Value for Field E4 on MedWatch	Select the applicable value from the available options.
Data to print on follow up MedWatch Device form	The available options are: <ul style="list-style-type: none"> All information (initial + follow-up) is displayed. (Previous Behaviour). Only Display changed information from the initial report.
Number from LM_REF_TYPES.REF_TYPE_ID for Reference Type containing Legacy Case Number (to print MedWatch forms)	This field enables the user to select the required option from the drop-down list.
SQL used to print the BLA #	Enables you to enter the SQL query used to print the BLA#.
SQL used to print Unique Identifier (UDI #) in MedWatch Device Form	Enables you to enter the SQL query used to print the UDI# in MedWatch Device Forms.
License number on MedWatch Drug Report	The available options are: <ul style="list-style-type: none"> Print License # only for the scheduled license on MedWatch Drug Report Print all available license numbers for Drug as determined by the scheduled license
License number on MedWatch Drug Report	This field enables the user to select the option for License number on MedWatch Drug Report.
SQL mapping for MedWatch Literature Box 3. Report Source (Parameters: P_CASE_ID)	SQL mapping for the field: "This type includes cases from literature" for MedWatch. For more details on the default mapping, refer to the Mapping Document.
Value for Field G8 on MedWatch	Select the applicable value from the available options.

Use the following procedure to configure expedited MedWatch reports.

1. Select the option for the **Value for Field E4 on MedWatch**.
2. Select the option for the Data to print on follow up MedWatch Device form.
3. Select the required option for Number from LM_REF_TYPES.REF_TYPE_ID for Reference Type containing Legacy Case Number (to print MedWatch forms) from the drop-down list box.
4. Select the option for License number on MedWatch Drug Report.
5. Add an SQL for BLA# and UDI#, if there is a need to change the default logic for these fields in MedWatch report.
6. Click **Save** to save the changes made to this screen.

Configuring MedWatch

The MedWatch Configuration screen enables you to modify the customizable fields on the MedWatch form. Select System Configuration -> System Management to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To view the list of field names associated with the **MedWatch Configuration** section, click the **MedWatch Configuration** folder in the left panel.

Mfr. Site FDA Number	Year	# of Reports	Reset Number
001QRDD	2014	0	<input type="radio"/> Yes <input checked="" type="radio"/> No
REG-001	1999	0	<input type="radio"/> Yes <input checked="" type="radio"/> No
TEG-001	1999	3	<input type="radio"/> Yes <input checked="" type="radio"/> No
VE-001	2014	0	<input type="radio"/> Yes <input checked="" type="radio"/> No

The field names associated with **MedWatch Configuration** appear in the right panel.

Field Descriptions

The following table lists and describes the fields available under **MedWatch Configuration**:

Field/Control Name	Description
Firm Name as it Should Appear at the Top of Each Page	Enables the user to enter the name of the reporting firm on the MedWatch form.
Use Manufacturer of the License Used for Report scheduling	Enables the user to use the manufacturer of the license that was used for report scheduling, by checking this checkbox.
Date of FDA Approval to Appear on the First Page	Enables the user to enter the FDA approval date of the manufacturer.
Disclaimer to appear at the Bottom of the First Page	Enables the user to enter a brief disclaimer.
Default text to appear on Block H10	Enables the user to enter default text.
Address to be printed at the bottom of Second page of MedWatch Device Form	Enables the user to enter the address to be printed at the bottom of Second page of MedWatch Device Form. The default address is as follows: Department of Health and Human Services Food and Drug Administration Office of Chief Information Officer Paperwork Reduction Act (PRA) Staff PRAStaff@fda.hhs.gov
Reset MedWatch Numbering	Enables the user to reset the sequence number that appears on the MedWatch form for the manufacturer.

Field/Control Name	Description
Mfr. Site FDA Number	Displays the FDA number for the Manufacturer Site which submitted the MedWatch 3500 Device report in the year.
Year	Displays the year of report submission.
# of Reports	Displays the number of submitted reports for products associated with a Manufacturing Site in that year
Reset Number	Enables the user to reset the Sequence Number.

Use the following procedure to configure the MedWatch form options.

1. Enter the Firm Name as it Should Appear at the Top of Each Page.
2. Enter the Date of FDA Approval to appear on the first page.
3. Enter the Disclaimer to appear at the bottom of the first page.
4. Enter the Default text to appear on Block H10.
5. Click **Reset MedWatch Numbering** to reset the sequence number that appears on the MedWatch form, for the manufacturer as required.

Periodic Reports Configuration The Periodic Reporting Configuration screen enables you to modify the options available for periodic reporting.

Select System Configuration -> System Management to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To configure the fields associated with the **Reporting** section, click the **Reporting** folder in the left panel. The **Periodic** sub-folder is displayed in the left panel.

Click on the **Periodic** sub-folder to configure the periodic reporting options. The configurable fields associated with **Periodic Reporting** appear in the right panel.

The screenshot displays the Oracle System Configuration interface. The top navigation bar includes 'Code Lists', 'Business Configuration', 'Access Management', 'System Configuration', and 'Tools'. The main window title is 'COMMON PROFILE - Reporting/Periodic'. On the left, a tree view shows the 'Common Profile' folder expanded to 'Reporting', with the 'Periodic' sub-folder selected. The right pane, titled 'Modify Reporting/Periodic', contains several configuration sections:

- Print footnote "Non-Serious Listed" for non-serious listed cases in ICH PSUR report:** Radio buttons for 'Yes' (selected) and 'No'.
- Inclusion criteria for case in the ICH PSUR report:** Radio buttons for 'Use lateness of the primary event' (selected) and 'Use case level lateness'.
- Inclusion criteria for cases in the ICH PSUR report:** Radio buttons for 'Use causality of the primary event', 'Use case level causality', and 'Use causality of all the events against products in the PSUR' (selected).
- Seriousness determination for event in the PSUR:** Radio buttons for '(Default) Seriousness from other case level or primary event level' (selected), 'Product Primary Event Seriousness is used', and 'Case Level Seriousness is used'.
- Determine Possible Causality from causality score:** A text input field containing the value '1'.
- Determine Probable Causality from causality score:** A text input field containing the value '4'.

A 'Save' button is located at the bottom right of the configuration pane.

Field Descriptions

The following table lists and describes the fields available under **Periodic Reporting**:

Field/Control Name	Description
Determine Primary Event for use in ICH PSUR/CTPR report	<p>The available options are:</p> <ul style="list-style-type: none"> Primary Event (Left Most Diagnosis or the left-most Event if there is no Diagnosis on the Case Form). Most severe event for the product (First left most Diagnosis Related Serious Event with most weight on Diagnosis then relatedness and then seriousness).
Listedness grouping logic for ICH PSUR/CTPR report output	<p>The available options are:</p> <ul style="list-style-type: none"> Primary Event (refer to Inclusion criteria of event for a product in the PSUR/CTPR switch). Case level Listedness
Seriousness grouping logic for ICH PSUR/CTPR report output	<p>The available options are:</p> <ul style="list-style-type: none"> Primary Event (refer to Inclusion criteria of event for a product in the PSUR/CTPR switch). Case level seriousness
Inclusion Criteria for cases in the ICH PSUR/CTPR report	<p>The available options are:</p> <ul style="list-style-type: none"> Evaluate seriousness, listedness, relatedness, fatal across all diagnoses/events against product <p>When this option is selected, the case inclusion criteria logic in ICH PSUR/CTPR scans all the diagnoses in the case and matches all the Seriousness, Listedness, Relatedness, Fatal values for the diagnosis in the case against the product(s) for which the report is being run, with the corresponding values selected by the user in the Report configuration.</p> <p>When there are no diagnosis in the case, the system scans all the events in the case and matches all the Seriousness, Listedness, Relatedness, Fatal values for the events in the case against the product(s) for which the report is being run, with the corresponding values selected by the user in the Report configuration.</p> <p>When multiple products are configured in the report, a match of all the Seriousness, Listedness, Relatedness and Fatal values against even one product-diagnosis is considered as a match for including the case.</p> <ul style="list-style-type: none"> Evaluate case inclusion based on following seriousness, listedness, causality option groups - Case Inclusion criteria for the ICH PSUR/CTPR report based on Seriousness OR Case Inclusion criteria for the ICH PSUR/CTPR report based on Causality OR Case Inclusion criteria for the ICH PSUR/CTPR report based on Listedness.
Determine Possible Causality from the causality score	This field enables the user to enter a numeric value.
Determine Probable Causality from the causality score	This field enables the user to enter a numeric value.
On PSUR, NDA, IND, Medical Review List Reports	<p>The available options are:</p> <ul style="list-style-type: none"> Use Initial Receipt Date for date range search Use Safety Date for date range search

Field/Control Name	Description
Print footnote 'Non-Serious Listed' for non-serious listed cases in ICH PSUR report	The available options are: <ul style="list-style-type: none"> ■ Yes ■ No
Assessment of Listedness and Causality when both Licenses and Studies are selected in CTPR	The available options are: <ul style="list-style-type: none"> ■ Based on selected licenses ■ Based on selected studies

Use the following procedure to configure periodic reports.

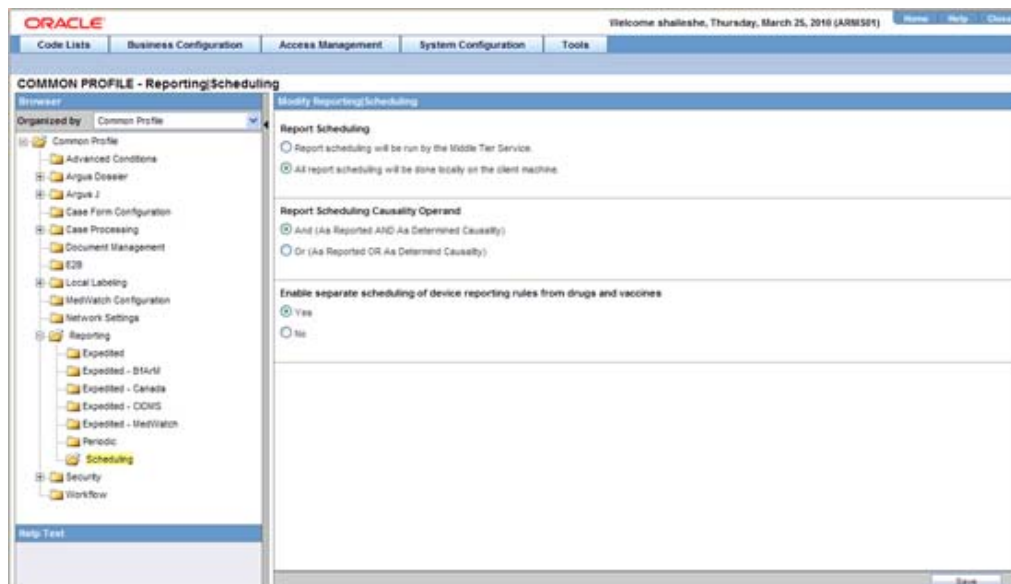
1. Select the option for Inclusion Criteria for cases in the ICH PSUR report.
2. Select the option for Print footnote "Non Serious Listed" for non-serious listed cases in ICH PSUR report.
3. Select the option for Inclusion criteria of event for a product in the PSUR.
4. Enter the value for Determine Possible Causality from the causality score.
5. Enter the value for Determine Probable Causality from causality score.
6. Select the option for On PSUR, NDA, IND, Medical Review List Reports.
7. Click **Save** to save the changes made to this screen.

Scheduling Reports Configuration The Scheduling Reports Configuration screen enables you to modify the options available for scheduling reporting. Select System Configuration -> System Management to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To configure the fields associated with the **Reporting** section, click the **Reporting** folder in the left panel. The **Scheduling** sub-folder is displayed in the left panel.

Click on the **Scheduling** sub-folder to configure the scheduling report options. The configurable fields associated with **Scheduling Reports** appear in the right panel.



Field Descriptions

The following table lists and describes the fields available under **Schedule Reports**:

Field/Control Name	Description
Report Scheduling	The available options are: <ul style="list-style-type: none"> Report Scheduling will be run by the Middle Tier Service All report scheduling will be done locally on the client machine
Enable separate scheduling of device reporting rules from drugs and vaccines	The available options are: <ul style="list-style-type: none"> Yes No
Report Scheduling Causality Operand	Enables the user to select from the causality operands AND/OR to use for scheduling a report.

Use the following procedure to configure scheduling.

1. Select the option for **Report Scheduling**.
2. Select the option for Enable separate scheduling of device reporting rules from drugs and vaccines.
3. Select the operand to use for scheduling a report from **Report Scheduling Causality Operand**.
4. Click **Save** to save the changes made to this screen.

Configuring Security

The Security Configuration screen enables you to modify the options available for security. Select System Configuration -> System Management to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To configure the fields associated with the **Security** section, click the **Common Profile-> Security** folder in the left panel. The configurable fields associated with **Security** appear in the right panel.

Field Descriptions

The following table lists the fields available under **Security**:

Field/Control Name	Description
Number of previous passwords that cannot be repeated	<p>Enables you to configure the number of passwords that can be allowed.</p> <p>For example, if you enter 4 in this field, it configures the system to enable up to 4 previous passwords that cannot be used as passwords again.</p>
Number of non-alpha characters in password	<p>Enables you to configure the number of non-alpha characters that should exist in a password. Non-alpha characters include characters such as @, \$, etc.</p> <p>Note: To avoid bad configuration, we recommend that the value of this switch is kept as 0 or 1 only.</p>
Minimum number of characters in the password	<p>Enables you to configure the minimum number of characters that a password must have.</p> <p>For example, if you enter 8 in this field, it configures the system to ensure that every password contains at least 8 characters.</p>
Use Secure property for cookies	<p>Enables you to select whether to use secure property for cookies.</p>
Number of consecutive failed login attempts before account is locked out	<p>Enables you to configure the number of consecutive failed login attempts that can be allowed before an account is locked out.</p> <p>For example, if you enter 3, it means that up to 3 consecutive failed login attempts are allowed. If the fourth consecutive login attempt also fails, the account gets locked out.</p>

Use the following procedure to configure security.

1. Enter the value for the number of unique previous passwords in **Number of previous passwords that cannot be repeated**.
2. Enter the value for the number of non-alpha characters in **Number of non-alpha characters in password**.
3. Enter the value for the minimum number of characters for a password in **Minimum number of characters in the password**.
4. Enter the value for the number of consecutive failed login attempts in **Number of consecutive failed login attempts before account is locked out**.
5. Click **Save** to save the configured values.
6. Click **LDAP** to configure the LDAP fields.

The configurable fields associated with **LDAP** appear in the right panel.

Field Descriptions

The following table lists and describes the fields available under **LDAP**:

Field/Control Name	Description
Enable LDAP at system level	The available options for this are : <ul style="list-style-type: none"> ■ Yes ■ No

Use the following procedure to configure security:

1. Select the option for Enable LDAP at system level.
2. Click **Yes** to enable the LDAP Search Domain Account. This displays the **LDAP Search Domain Account** dialog.

The screenshot shows the Oracle System Configuration interface. The left pane displays a tree view of configuration categories, with 'Security' > 'LDAP' selected. The main area is titled 'COMMON PROFILE - SecurityLDAP' and contains a 'Modify SecurityLDAP' dialog. The 'Enable LDAP at system level' section has radio buttons for 'Yes' (selected) and 'No'. Below this is the 'LDAP Server Details' section with the following fields:

LDAP Server Alias	DEFAULT	Server Name		User DN (ex CN=...OU=...DC=...)	CN=...
<input type="checkbox"/> Use Secure Socket Layer (SSL)		Port Number	0	Password	
<input type="checkbox"/> Force anonymous binding for search?		Base DN		LDAP Search Key (CN=...)	CN=...
		Time Out (Sec)	0		

The following table describes the fields of the LDAP Search Domain Account dialog:

Field/Control Name	Description
Use Secure Socket Layer	If your LDAP Server is configured to use SSL for communication, please check this box. Use of SSL enables for a Secure communication between the client and the server using secure keys.
Force Anonymous Binding for Search	When setting up the LDAP Server, you have the option to force users to bind (authenticate) to the LDAP Server prior to being able to search the LDAP Tree. If this option has been setup in your LDAP server, this option must be checked.
UserDN	During the setup of the LDAP server, the distinguished name and tree structure is created for users to be configured under. Enter in the defined structure as defined in your LDAP server into this box. This is required only if the server is setup for Force Anonymous Binding for Search".
Password	Enter in the password for the User entered in the UserDN box for the bind to the server.
Server Name	Enter in the LDAP Server name or IP Address to which LDAP Authentication needs to occur on.
Port Number	Enter the port on which the LDAP Authentication Services are enabled on the LDAP Server (Default Value: 389).
BaseDN	Enter in the topmost distinguished name of your tree defined on the LDAP Server for which you would like to search for users under.
Time Out (Sec)	Enter a value in seconds, which will tell Argus how long to wait for a response from the LDAP Server during any authentication before timing out (Default Value: 10).
LDAP Search Key	Enter the key to authenticate the user name against in the LDAP Tree structure. For Example, when using Microsoft Active Directory, to authenticate using the Windows Username (Not Full Name), enter in sAMAccountName.

- If you select the **Use Secure Socket Layer (SSL)** checkbox, the **Port Number** is auto-populated with the value **636**.
 - If this checkbox is not selected, the **Port Number** is auto-populated with the value **389**.
 - A generic LDAP server can accept anonymous as well as non anonymous binding, based on the configuration.
 - If the **Force anonymous binding for search?** checkbox is not selected, both **UserDN** and **Password** are enabled.
3. Enter the LDAP username and password in the **UserDN** and **Password** fields, respectively.
 4. Enter the values for Server Name, Port Number, Base DN, Time Out and LDAP Search Key, as required.
 - The field length for **Port Number** and **Time Out** is 5 characters, while the **Server Name**, **BaseDN**, **LDAP Search Key**, **UserDN** and **Password** can be up to 255 characters.
 5. Click **Save** to save the changes made to this screen.

Configuring Cryptography within Common Profile > Security

Common Profile > Security > Cryptography contains two key settings:

1. Configured hashing algorithm to use - This setting determines the Hashtag algorithm that will be used in encrypting passwords.
2. *De-optimizer counter for hashtag routine* - This setting determines the strength of encryption (for example, the higher the value of this setting, the stronger will be the encryption, and vice-versa). The default/recommended value is 1000.

Configuring Single Sign-On

A common profile switch determines whether the system uses the Single Sign-On function. The Enable Single Sign-On checkbox enables you to configure the system to use the single sign-on feature.

Before enabling the single sign-on feature, you must enter the Single Sign-On HTTP Header element that the Argus application uses for authentication. This field can contain a maximum of 40 characters.

1. The following new entries which are common across all enterprises have been added in Argus Console -> System Management (Common Profile Switches) -> Single Sign-On:

A checkbox called **Enable IAMS Integration** has been introduced. IAMS is an Oracle suite of products used for Identity and Access Management mainly for Oracle Argus Cloud releases. Enabling this switch allows the application to integrate with IAMS.

A checkbox called **Use Oracle Access Server SDK for LDAP Validation** under Single Sign-On tree will become available for selection only when 'Enable Single Sign-On' is checked.

This configuration is used to identify use of Oracle ASDK for user action confirmation , ESM login and EOSU Login functionality.

- If this checkbox is checked, Oracle ASDK is user for action confirmation , ESM Login and EOSU Login when Argus Safety is configured for Single Sign-On.
 - If this checkbox is not checked, LDAP server information is used from Argus Safety database for user action confirmation, ESM Login and EOSU Login.
2. A new textbox called **Oracle Access Server Login URL** has been added under the **Use Oracle Access Server SDK for LDAP Validation** checkbox.
 - This is the base URL which is be passed to Oracle ASDK for user validation against Oracle Access Manager.
 3. A new textbox called **Short Org ID HTTP Header** has been added under the **Use Oracle Access Server SDK for LDAP Validation** checkbox.
 - This is an HTTP Header variable for retrieving the short org ID which is to be passed with ASDK Login URL.
 4. If the **Use Oracle Access Server SDK for LDAP Validation** checkbox is checked, the application ignores any LDAP configuration present in the Argus Safety database and you cannot select **LDAP Server Alias** for any user from the user configuration screen (**Access Management > Argus > Users**) in the Argus Console.

The following table lists dialog boxes in the Argus Application that require passwords. In such cases, the system Single Sign-On feature redirects the password to Argus for validation. When single sign-on is enabled, the system locks the user account if the user enters an incorrect password three consecutive times. You must then unlock the account to enable the user to log in to the application.

Function	Section	Procedure
Case Locking	Activities Lock	Locking a case
Case Unlocking	Activities Lock	Unlocking a case
Case Closing	Activities Close	Closing a case
Case Unclosing	Activities Close	Unclosing a case.
Case Unblinding	General Blinding Status	Breaking a blind
E2B Incoming Accept	Reports Incoming E2B Reports	Accepting E2B Reports
E2B Incoming Reject	Reports Incoming E2B Reports	Rejecting E2B Reports
E2B Incoming Follow-up Accept	Reports Incoming E2B Reports	Accepting E2B Follow-up Reports
E2B Incoming Follow-up Reject	Reports Incoming E2B Reports	Rejecting E2B Follow-up Reports
E2B Incoming Nullification Accept	E2B Incoming Nullification Accept	Accepting E2B Nullification Reports
E2B Incoming Nullification Reject	E2B Incoming Nullification Reject	Rejecting E2B Nullification Reports
LAM Incoming	Local Affiliate Incoming Review	Accepting an Affiliate Event
Workflow Routing	Workflow Routing on Password on Route	Workflow Routing on Password on Route

Oracle Access Server SDK Support for LDAP Validation in a Single Sign-On Environment

Argus Safety has been enhanced to support action confirmation (user id/password) using Oracle Access Server SDK.

If customers do not want to store the LDAP information in the Argus database for a single sign-on environment, this new feature of Argus Safety can be used to validate a user's actions through ASDK.

This feature is available only while using Oracle Access Manager as the Single Sign-On tool.

The following is a list of places where the Argus Safety web dialog which requires action confirmation to perform respective actions, has now been enhanced to validate a user using Oracle ASDK:

1. Case Lock/Unlock
2. Case Routing
3. Case Delete/Undelete
4. Case Archiving
5. LAM Routing
6. Study Unblinding
7. ESM Login
8. EOSU Login

There is no change in the user experience while performing actions which require password validation for a logged-in user.

The following modules launched in the Argus application continue to use the Single Sign-On feature:

- Argus Insight
- Argus Affiliate
- Argus J

The following modules **do not use** the Single Sign-On feature:

- End of Study Unblinding
- Argus Safety Services
- Argus Interchange Services (ESM)
- Argus Interchange Mapping (ESM Mapping Utility)

Configuring Single Sign-On re-authentication

Before you can configure Single Sign-On re-authentication, make sure that the Service Provider IDM (for example, Oracle Access Manager) supports Re-Authenticate URL and sets the last re-authentication header every time a user is re-authenticated.

To configure re-authentication, use the following common profile switches under **Console > System Management > Single Sign-On**:

1. The **Enable Re-Authentication** checkbox (selectable only when the **Enable Single Sign-On** checkbox is checked), which enables Single Sign-On re-authentication. You can edit the re-authentication fields only if this checkbox is checked.
2. The **Re-Authentication URL** text field, where you enter the re-authentication URL of the corporate LDAP system. The URL must be in the following format:
`<protocol>://<hostname>:<port>/oamreauthenticate?redirect_url=` (for example, `https://acme.idm.com:8787/oamreauthenticate?redirect_url=`).
3. The **Re-Authentication HTTP Header** text field, which is populated by default. The default setting is `OAM_LAST_RE-AUTHENTICATION_TIME`.
4. The **Re-Authentication HTTP Header Date Time Format** text field, which is populated by default. The default setting is `Dy Mon dd hh24:mi:ss TZD YYYY`.

If re-authentication is enabled, user association with LDAP is not required, and you can configure Argus Safety users without providing LDAP details.

Single Sign-On re-authentication has the following impact on the LDAP settings at the user configuration level, which you can access under **Console > Access Management > Argus > Users**:

1. The **Enable LDAP Login** checkbox is available if either LDAP is enabled at the system level (under **Argus Console > System Configuration > System Management > Security > LDAP** node), or Single Sign-On re-authentication is enabled. If neither is enabled, then the checkbox is disabled.
2. The **LDAP Server Alias** drop-down list is disabled and blank when the **Enable Re-Authentication** checkbox is checked.

3. If both re-authentication and LDAP are configured, then priority is given to re-authentication.

Error Messages

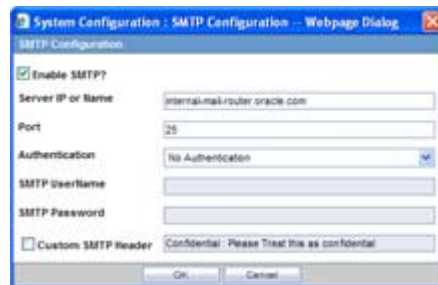
Once the user is configured, the system automatically logs the user into the Argus Application without requiring re-authentication on the Argus Login application. If there is an authentication error, the system displays the current login page so the user can log in manually.

Configuring SMTP

This screen enables you to configure SMTP.

Currently there are multiple issues such as, Outlook related problems with AG Service due to new security features introduced by Microsoft. Due to these security enhancements, a new method to submit emails from AG Service has been implemented using the SMTP Protocol.

Select **System Configuration -> SMTP Configuration** to view the SMTP configuration pop-up dialog. The pop-up dialog opens as shown.



Field Descriptions The following table lists and describes the fields associated with this section.

Field/Control Name	Description
Server IP or Name	Enables the user enter the SMTP server name / IP address.
Port	Enables the user to enter the port number to use for SMTP server.
Authentication	Enables the user to select the Authentication mode for SMTP configuration
SMTP User Name	This is the username that the AG Service authenticates with for SMTP Emailing.
SMTP Password	This is the password that the AG Service authenticates with for SMTP Emailing. This field is required when Basic Authentication is selected in Authentication.
Enable SMTP	When this checkbox is checked, SMTP is used by AG Service to send emails.

Use the following procedure to modify SMTP.

1. Enter the **SMTP Server IP or Name**.
2. Enter the **Port** number to use for SMTP server.

3. Select the **Authentication** mode for the SMTP configuration, from the drop-down list.
4. Enter the **SMTP User Name**.
5. Enter the **SMTP Password**.
6. Select **Enable SMTP?** to ensure that the AG Service implements SMTP to send e-mails.
7. Click **OK** to save the changes made.

Note: If Argus Safety needs to use the proxy set up for SMTP configuration, ensure that the Proxy setting is configured under System Configuration > System Management > Network Settings > Proxy.

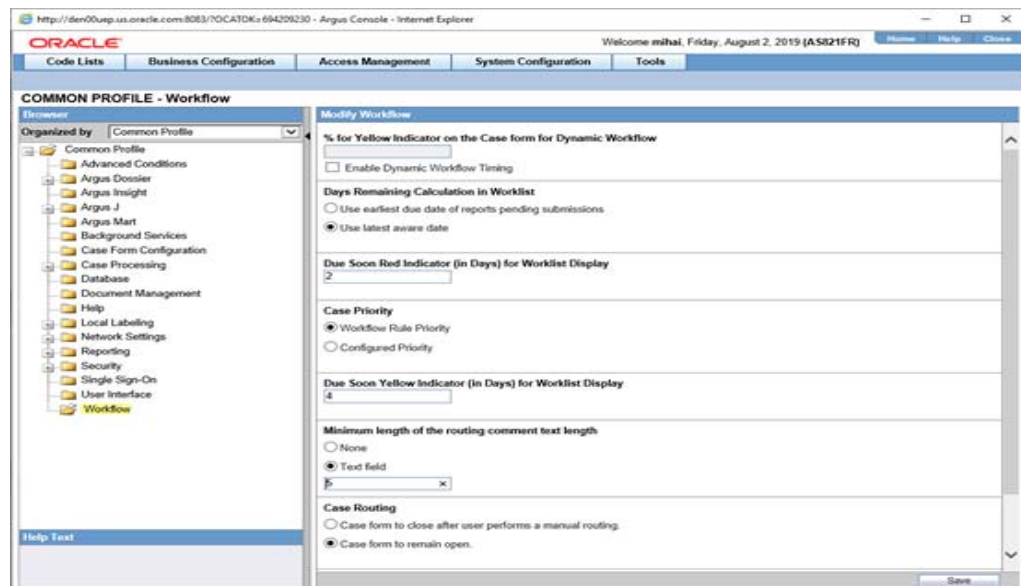
Configuring Workflow Items

The Workflow Items screen enables you to modify the options available for Workflow Items.

Select System Configuration -> System Management to view the Common Profile Configuration screen.

Tip: The Common Profile folder appears in a tree-view on the left panel. The components are categorized as folders. Each folder contains all the field labels associated with that section.

To configure the fields associated with the **User Interface** section, click the **Common Profile-> Workflow** folder in the left panel. The configurable fields associated with **Workflow** appear in the right panel.



This section enables you to configure the total number of hours remaining for the present workflow state as well as the Total Number of hours remaining for the case lock.

- The first element displays the number of hours remaining for the case to be processed with the current workflow state.

- The second element displays the number of hours remaining for the entire workflow for the case till Case Approval (Case Lock).
- If the time remaining is less than the specified value in % for **Yellow Indicator on the Case form for Dynamic Workflow**, the elements are highlighted in yellow.
- If the time remaining is more than the specified value in % for **Yellow Indicator on the Case form for Dynamic Workflow**, the elements are highlighted in green.
- If the time remaining has exceeded the allocated time for the case process, the value is displayed in red, with the time displayed in negative.
- The exceptions to this feature are those cases, which are archived and locked.

The **Worklist > New** and **Worklist > Open** also display a ! status beside **Priority**, denoting that the time remaining has exceeded the allocated time.

Priority	Lock State	Initial Date	Assess Date	Days Open	Remaining	Case Number	Workflow State	Product Name	Generic Name	Treat PT	Event Verbatim	SAR	Case Type	Study ID	Reporter Type	Assigned To
		30-NOV-2007		03		2007150000		Atorvastatin	ATORVASTATIN CALCIUM	Spontaneous		No	Spontaneous		Physician	(Assigned)
		30-NOV-2007		0		2007150000		Atorvastatin	ATORVASTATIN CALCIUM	Spontaneous		No	Spontaneous		Physician	(Assigned)
		30-SEP-2007		13x		2007150000		Lipitor	ATORVASTATIN CALCIUM	Spontaneous		No	Spontaneous		Physician	(Assigned)
		30-SEP-2007		0		2007150000		Lipitor	ATORVASTATIN CALCIUM	Spontaneous		No	Spontaneous		Physician	(Assigned)
		30-NOV-2007		03		2007150000		Atorvastatin Calcium (H)	ATORVASTATIN CALCIUM	Spontaneous		No	Spontaneous		Physician	(Assigned)
		30-NOV-2007		0		2007150000		Atorvastatin Calcium	ATORVASTATIN CALCIUM	Spontaneous		No	Spontaneous		Physician	(Assigned)
		30-NOV-2007		03		2007150000		Lipitor	ATORVASTATIN CALCIUM	Spontaneous		No	Spontaneous		Physician	(Assigned)
		30-NOV-2007		03		2007150000		Lipitor	ATORVASTATIN CALCIUM	Spontaneous		No	Spontaneous		Physician	(Assigned)
		30-NOV-2007		03		2007150000		Lipitor (H)	ATORVASTATIN CALCIUM	Spontaneous		No	Spontaneous		Physician	(Assigned)

The total number of units is calculated by navigating across the possible routes the case can traverse. In case a case has to traverse through multiple possible routes, the preferred route is selected.

- The Days Remaining Calculation in Worklist common profile switch enables you to select either of the following options:
 - Use earliest due date of reports pending submissions (default)

When...	...populate Due Soon date based on:
Auto-scheduling is done for the reports and the case contains scheduled reports.	Earliest due date of the report
Auto-scheduling is done for the reports but the case does not contain any scheduled reports.	Latest aware date and duration as specified in the Due Soon Duration (in Days) for Worklist Calculation common profile switch
Neither auto-scheduling is done for the reports nor likely to schedule a report.	Latest aware date and duration as specified in the Due Soon Duration (in Days) for Worklist Calculation common profile switch
Auto-scheduling is not done for the reports but the reports are likely to be scheduled.	Earliest due date of the possible reports

– Use latest aware date

When...	...populate Due Soon date based on:
Auto-scheduling is done for the reports, and may or may not contain any scheduled reports.	Latest aware date and duration as specified in the Due Soon Duration (in Days) for Worklist Calculation common profile switch
Neither auto-scheduling is done for the reports nor likely to schedule a report.	Latest aware date and duration as specified in the Due Soon Duration (in Days) for Worklist Calculation common profile switch.
Auto-scheduling is not done for the reports but the reports are likely to be scheduled	Earliest due date of the possible reports

Field Descriptions The following table lists the fields available under **Workflow**:

Field/Control Name	Description
Case Routing	The available options are: <ul style="list-style-type: none"> ■ Case form to close after use performs a manual routing ■ Case form to remain open
Days Remaining Calculation in Worklist	The available options are: <ul style="list-style-type: none"> ■ Use earliest due date of reports pending submissions ■ Use latest aware date
Minimum length of the routing comment text length	The available options are: <ul style="list-style-type: none"> ■ None ■ Text field
Due Soon Duration (in Days) for Worklist Calculation	Enter the number of days in which the worklist calculation is due.
Due Soon Red Indicator (in Days) for Worklist Display	Enter the number of days in which the red indicator is to due to be displayed for the worklist.
% for Yellow Indicator on the Case form for Dynamic Workflow	Enter the percentage for the yellow indicator on the case form for dynamic workflow. This field cannot have a value more than 99.
Enable Dynamic Workflow Timing	Select this checkbox to view the dynamic workflow indicators on the case form.

Use the following procedure to configure workflow items.

1. Select the option for **Case Routing**.
2. Select the option for Display Locked/All cases on the worklist.
3. Enter the Minimum length of the routing comment text length in the text box.

4. Select the option for Display date for cases in the worklist.
5. Enter the number of days in which the worklist calculation is due in **Due Soon Duration (in Days) for Worklist Calculation**.
6. Enter the number of days in which the red indicator is to due to be displayed for the worklist in **Due Soon Red Indicator (in Days) for Worklist Display**.
7. Enter the percentage for the yellow indicator on the case form for dynamic workflow in % for **Yellow Indicator on the Case form for Dynamic Workflow**.
8. Select the **Enable Dynamic Workflow Timing** checkbox to view the dynamic workflow indicators on the case form.
9. Click **Save** to save the changes made to this screen.

Configuring Workflow

When a case is received by the company and initial details have been entered and saved into Argus Safety, its status in the system becomes 'New' or 'Data Entry'. Various actions may be required before a case makes the transition from one workflow state to another.

Example: The case may require review, letters may need to be issued, the case may need to be reported elsewhere in the company, or regulatory reports need to be submitted to regulatory authorities. The case can be closed after all outstanding actions have been carried out and it flows through its life cycle.

For each stage in case processing, Argus Safety enables responsibility for cases to be assigned to specific user or group of users. Click the following link for information about how worklist permissions have changed.

Worklist Updates

The Worklist is driven by the group permissions defined for each user.

- Granular permissions have replaced the current worklist options for the following worklist elements in group permissions:
 - Worklist - New
 - Worklist - Open
 - Worklist - Reports
 - Worklist - Action Items
 - Worklist - Coding Action Items
 - Worklist - Contacts
 - Worklist - Bulk Transmit
 - Worklist - Bulk Print
 - Worklist - Bulk E2B Transmit
 - Worklist - Local Labeling
 - Worklist - Coding Status
 - Worklist - Letters
 - Worklist - Intake (default is disabled)
- If the worklist is disabled during the upgrade, then all the sub-elements are disabled; otherwise, all are enabled.

- The default for **New Group Creation** is enabled.
- The **User Group Permissions Report** has been updated to reflect granular permissions.

Configuring Case Workflow

Configuring case workflow involves configuration of:

- Workflow States
- Workflow Rules

Configuring Workflow States This screen enables you to configure the workflow states. The following illustration shows the fields associated with this section.

State Name	State Description	Site
Closed	Closed	<Not Associated>
Data Entry	Data Entry	<Not Associated>
Deleted	Deleted	<Not Associated>
New Case	New Case	<Not Associated>
US Data Entry	US Data Entry	United States
US Medical Review	US Medical Review	United States
US Reporting	US Reporting	United States

Field Descriptions

The following table lists and describes the fields available under **Total Number of Rows**:

Field/Control Name	Description
State Name	Displays the name of a workflow state.
State Description	Displays a brief description about the workflow state.
Site	Displays the site associated with a workflow state.

Tip: Click **Add New** to add a new workflow state to the list of existing workflow states.

Use the following to modify workflow states

1. Enter the name of the workflow state under **State Name**.

Tip: This name is displayed as **Case Status** in the General Information section of the Case Form.

2. Enter the description of the workflow state under **Description**.

3. Select the site to be associated with the workflow state from the **Site** drop-down list.
4. The drop-down list is populated with the configured user sites.
5. Click **Save** to save the changes made.

Configuring Workflow Rules This screen enables you to configure workflow rules. The following illustration shows the fields associated with this section.

The screenshot displays the 'WORKFLOW' configuration interface. At the top, there are tabs for 'Code Lists', 'Business Configuration', 'Access Management', 'System Configuration', and 'Tools'. The 'WORKFLOW' section has sub-tabs for 'States' and 'Rules'. Below this is a 'Filter Criteria' section with several dropdown menus and checkboxes. A table below shows a list of workflow rules with columns: From, To, A/C Name, Group, Normal Time-Max Time, User Defined Attribute 1, and User Defined Attribute 2. Below the table is a 'Modify Workflow Rules' form with fields for 'From', 'To', 'Group', 'Preferred State', 'Product Group', 'Time(days) Norm. / Max. / Units', 'Privileges to others', 'Advanced Conditions', 'Reason for Not Being Able to Route', 'User Defined Attribute 1', 'User Defined Attribute 2', and several checkboxes like 'Restrict to Workflow Group', 'Email', 'Lock Case on Route', and 'Require Password on Route'.

From	To	A/C Name	Group	Normal Time-Max Time	User Defined Attribute 1	User Defined Attribute 2
New Case	Germany Data Entry	Workflow: Case number contains DE	Germany Data Entry	1Q		
New Case	US-Data Entry	Workflow: Case Number contains US	United States Data Entry # not Validation	1/04		
New Case	Japan Data Entry	Workflow: Case Number contains JP	Japan Data Entry	1Q		
Data Entry	US Medical Review	CDI - US	AJ - Medical Review Group	01/01		

Field Descriptions

The following table lists the Field Descriptions for this section.

Field/Control Name	Description
From	Defines the original state for the transition.
To	Defines the destination state for the transition.
Group	Specifies the group which will own the case once it moves from the From state to the To state (via this transition). The drop-down list displays all the configured user groups of Argus.

Field/Control Name	Description
Normal Time (days)	<p>The workflow system monitors the time frames of each case in a state with respect to the Normal and Maximum parameters through AG Service.</p> <ul style="list-style-type: none"> ■ The AG Service evaluates the status of each open case. ■ If a case has existed in its current state longer than the Normal time specified for the transition, the system raises the priority of the case by one level. <p>This escalation occurs only once for a case within a given state.</p> <ul style="list-style-type: none"> ■ The case priority is not reset to its assigned priority upon transition. ■ If a case has existed in its current state longer than the Maximum time specified for the transition, the system raises its priority to level one (the highest priority). ■ In addition, an email notification is sent to the group's supervisor, indicating that the case has exceeded its maximum time. ■ The email message identifies the Case ID, Current State, Current Owner, and the time it has spent in its current state.
Max Time (days)	
User Defined Attribute 1 /	Lets a user define a custom attribute for a work flow rule such as logically grouping workflow rules. Used only for filtering purposes on the same screen.
User Defined Attribute 2	
Units	Enables the user to specify the number of units.
Product Group	Enables the user to associate a specific Product group as additional criteria for the workflow transition.
Restrict to Workflow Group	Enables the user belonging to the identified workflow rule group to have case access rights, based on the definitions of only the identified group.
Email	<p>When checked, the system sends an email notification to the user group address specified in group information whenever a case makes this particular transition.</p> <p>By default, the checkbox is unchecked.</p>
Require Password on Route	<ul style="list-style-type: none"> ■ If the switch "PASSWORD_ON_ROUTING" is disabled (0), the password option on the Workflow Dialog is not displayed and the Routing dialog does not ask the user for a password. ■ If the switch "PASSWORD_ON_ROUTING" is enabled (1), the password option on the Workflow Dialog is displayed to users. If the Workflow Rule has the password option checked and the case being routed passes that workflow rule criteria, the password option is displayed on the routing dialog. ■ If the Workflow Rule that the case has passed does not have the Password option checked, no password option is displayed on the routing dial.
Lock Case on Route	Enables the user to lock the case on routing. Users might need to enter a password when routing to the case.
Reason for not being able to route	Enables the user to enter the description needed by the system to display while routing the case, when the case is ineligible to be routed to any of the configured To State.

Field/Control Name	Description
Privileges to others	Specifies the access rights for groups other than To Group' of the transition have to the case when it follows that transition. The choices are: <ul style="list-style-type: none"> ■ No Access ■ Read-Only ■ Read/Write (default)
Preferred State	Enables the user to specify the preferred state for the rule.

Use the following procedure to modify workflow rules.

1. Select the appropriate **Filter Criteria**.
 - Execute the following steps to apply a filtering criteria to search for specific workflow rules.
 - Select the check boxes to enable the drop-down lists containing a filtering criteria.
 - Select the appropriate filtering criteria from the drop-down lists.
 - Click **Search** to remove the selected criteria or click **Apply Filter** to apply the selected criteria. This displays the search results under **Total Number of Rows**.
2. The entities in **Total Number of Rows** display the **From** and **To** states, the Advanced Condition, Group, Normal Time/Max Time and Number of User Defined Attributes in the Workflow.
3. Select the rule displayed under **Total Number of Rows** that needs to be modified.
4. The **ModifyWorkflow Rules** section is populated with information about the selected rule.
5. Select the original state of the workflow rule from the **From** drop-down list.
6. Select the destination state of the workflow rule from the **To** drop-down list.
7. Select the group from the **Groups** drop-down list.
8. Select the product from the **Product Group** drop-down list.
9. Select the **Email** checkbox, if required.
10. Select the **Lock Case on Route** checkbox, if required.
11. Select the **Require Password on Route** checkbox, if required.
12. Enter the number of days in the **Normal Time** (days) field.
13. Enter the number of days in the **Max. Time** (days) field.
14. Enter the number of units in the **Units** field.
15. Select the preferred state for the rule from **Preferred State**.
16. Select the relevant **Advanced Condition**, if any from the button.

Tip: Click here for details on Advanced Conditions

17. Enter the reason for not being able to route, if applicable, under **Reason for not being able to route**.

18. Specify the access levels available to others from the **Privilegesto others** drop-down list. The options available under this list are No Access, Read-Only and Read/Write.

Tip: Select the No Access option to disallow users outside the transition's group to open the case when it follows the transition.

Select the Read-Only option to enable users outside the transition's group to view the case, but not to modify it.

Select the Read/Write option to enable users outside the transition's group to modify the case when it follows the transition.

19. Specify the checklist of items to appear under **Checklist**.

Tip: The Checklist row cannot be left blank. Click **Add** and **Delete** to add and delete checklist items.

20. Define custom attributes for a workflow rule under **User Defined Attribute**.

21. Click **Save** to save the changes made.

Worklist Intake

This section provides information about the Worklist Intake feature.

Pending Dialog The system enables the user to view a list of incoming attachments in Worklist View. In this view, the user can select an attachment for the case creation for Argus and Affiliate cases in the Pending dialog.

Priority	Initial Date	Intake Date	Product Name Generic Name	Event PT Event Verbatim	Serious F, LT or R	Case Type Study ID	Reporter Type Country	Central Site Attachment Name	Classification Description
8	08-NOV-2004		Wander Drug	Bradycardia	N	Other	Physician US	United States CASE02	Source Case US Source Case
8	17-NOV-2004		Super Drug	Dyspnea (BREATHLESS)	Y	Spontaneous	Physician UNITED KINGDOM	United States CASE03	Source Case US Source Case
8	06-DEC-2004		Tetanus and Diphtheria Vaccine	Swarmen (Slight spotted, itchy xan)	N	Spontaneous	GERMANY	United States CASE04	Source Case US Source Case
1	06-DEC-2004		Td-PUR (Tetanus Diphtheria Vaccine)	Swarmen (Slight spotted, itchy xan)	Y	Spontaneous	GERMANY	United States CASE05	Source Case US Source Case
8	14-DEC-2004		Wander Drug	Disease progression (DISEASE PROGRESSIO)	N	Other	Physician US	United States CASE06	Source Case US Source Case
8	14-DEC-2004		Wander Drug	Gastrointestinal increase (BOWEL INCREASE)	Y	Spontaneous	Physician US	United States CASE07	Source Case US Source Case
8	14-DEC-2004		Wander Drug	Cardiac tamponade	N	Other	Physician US	United States CASE08	Source Case

The following table lists and describes the fields available for the worklist

Field/Control Name	Description	Bookin Field	Property
Priority	Enables you to view the priority of a case	N/A	Non-scrollable field label
Initial Date	Enables you to view the Initial Receipt Date of the case.	Initial Receipt Date	Non-scrollable field label
Intake Date	Enables the user to view the date the system imported the attachment in the Intake Worklist	N/A	Non-scrollable field label

Field/Control Name	Description	Bookin Field	Property
Product Name	Enables you to view the suspect product in questions.	Product Name	Scrollable field label
Generic Name	Enables you to view the generic name of the suspect product in question.	Generic Name	Scrollable field label
Event PT	Enables you to view the primary event and verbatim as reported	N/A	Scrollable field label
Event Verbatim	The following format will be used: Primary Event (Verbatim as Reported)	N/A	Non-scrollable field label
Serious	Enables you to view the Case Level Assessments Serious (Y/N)	N/A	Non-scrollable field label
F, LT, or H	Fatal (F) or Life Threatening (LT) or Hospitalized (H) <ul style="list-style-type: none"> ■ If the case is Fatal, print F ■ If the case is Life Threatening, print LT ■ If the case is Hospitalized, print H ■ If any of the preceding are present together, Fatal takes precedence followed by LT, followed by H ■ If the case is neither, display No 	Death for F Hospitalized for H Life Threatening for LT	Non-scrollable field label
Case Type	Enables you to view report type information.	Report Type	Non-scrollable field label
Study ID	Enables you to view the Study ID for the study cases This field is empty for cases where the Study ID is not available.	Study ID	Non-scrollable field label
Reporter Type	Enables you to view the reporter type for the primary reporter in the case. This field is empty if the reporter type is not available.	N/A	Non-scrollable field label
Country	Enables you to view the country of incidence	Country of Incidence	Scrollable field label
Central/Affiliate Site	Enables you to view the current Argus or Affiliate site of the case. You can view all the source documents from the site folder the user belongs to Workflow enterprise users can view all cases across all site	N/A	Scrollable field label

Field/Control Name	Description	Bookin Field	Property
Attachment	Enables you to view the attachment associated with the case. If there are multiple files, they are separated by a comma.	N/A	Non-scrollable field label link
Classification	Enables you to view the attachment classifications associated with the attachment.	Classification	Scrollable field label
Description	Enables you to view the attachment description associated with the case.	Description	Scrollable field label
View All	Enables the administrator and workflow manager/enterprise to see all items in the system across all sites.	N/A	Radio button
View Individual	Enables you to view all items assigned to this user site. <ul style="list-style-type: none"> ■ If there are no sites defined then all users have access to the case attachment. ■ This button is disabled if the user is not a workflow manager or enterprise user. 	N/A	Radio button

Worklist Intake View The following table describes the Worklist Intake View:

Argus Site	Folder	Worklist Intake View
US	C:\USINTAKE	All users belonging to the US site can see the case and workflow enterprise users.
DE	C:\EUINTAKE	All users belonging to the DE, FR, CH site can see the case and workflow enterprise users.
CH	C:\EUINTAKE	All users belonging to the DE, FR, CH site can see the case and workflow enterprise users.
FR	C:\EUINTAKE	All users belonging to the DE, FR, CH site can see the case and workflow enterprise users.
JP	C:\JPINTAKE	All users belonging to the JP site can see the case and workflow enterprise users.

Worklist ■The system reads the XML that contains the preceding fields as tags and creates the Worklist based on the tags.

<Cases>

<Case>

<PRIORITY>: Single number from 1 - 8. All others to be ignored

<INITIAL_DATE>: Format of Date DD-MMM-YYYY

<PRODUCT_NAME>: Text Field up to 70 Characters

<GENERIC_NAME>: Text Field up to 70 Characters

<EVENT_PT>: Text Field up to 250 Characters

<EVENT_VERBATIM>: Text Field up to 250 Characters

<SERIOUS>: Yes / No. All others are ignored

<FLTH>: Format of F. All other after that are ignored

<LT>: Format of LT All other after that are ignored

<H>: Format of H. All other after that are ignored

<CASE_TYPE>: Text field of report type

<STUDY_ID>: Text field of Study ID

<REPORTER_TYPE>: Text field of Reporter Type

<COUNTRY_OF_INCIDENCE>: Text field of Country

<ASSIGNED_TO>: Text field of User

<GROUP>: Text field of Group

<SITE>: Text field of Site

<ATTACHMENTS>

<ATTACHMENT>:

<FILENAME>: Text field of Attachment File Name

<DOCID>: Document ID from Document Storage System

<CLASSIFICATION>: Text field of Attachment Classifications

<DESCRIPTION>: Text field of Attachment Classifications Descriptions

- The text on the worklist prints as specified in the XML and no lookup is performed.
- If any of the Tag elements are empty they will be empty in the Intake Worklist.
- If any fields are not available on the initial case entry, the system ignores them.
- If there are multiple tags for the same element, the system retrieves the first tag element.
- If the values do not match any elements in the Initial Case entry, the system ignores them.
- The minimum fields required for the Attachment to be visible in the Intake Worklist are
 - Filename
 - DocID
 - DocID is only required if a central document system is enabled. If DocID is blank then the physical file with the same name as specified in the tag <Filename> is also required in the same folder.
- If there is an error occurs while processing the Worklist, AG Service sends an e-mail to the General E-mail address.
- The system enables you to select only one case at a time when creating cases in the Initial Case entry dialog.
 - When you select an attachment row and click Create case, the system locks the file to prevent others users from booking in the same case.

- The system displays the following message:
The case attachment is being currently used by XXXX user.
where:
XXXX is the full name of the user who has locked the attachment row
- The system displays the standard Initial Case Entry where the system populates the fields within the XML Properties to the Initial Case entry dialog and display the PDF file for 40% of the screen.
- If multiple attachments are available, the system opens them. The end user system must be setup to open multiple documents in the same window in Internet Explorer.
- If the system is setup to use a central document storage system and the user clicks Create Case, the system retrieves the PDF from the central document system.
- The system adds the attachment to the Initial Case entry dialog and also includes the Classifications and Descriptions for the attachment.
- If the system is setup to use a central document storage system, Argus stores the document ID from the central document system. The file attachment will not be stored in Argus.
- The system fills all available fields in the Initial Case Entry dialog with data from the XML Messages.
- If you choose to open the cases after book-in, the system keeps the Attachment open in the split screen to enable the user to complete the case data entry.
- If you book in the case from the Worklist Intake and chooses not to open the case from the Initial Case Entry dialog after book in is complete, the system returns to the Worklist Intake dialog.
- When you perform a Duplicate Search and select a Case from the list, you can attach an incoming file to an existing case.
 - The system displays the Accept As Follow-up button and enables it when the user selects a case from the Duplicate search for the current Attachments to be added.
 - When you click Accept as Follow-up, the system opens the selected case and continues to display the Source attachments.
 - The system adds the attachments with the Classification and description (if provided) to the follow up case
 - The system opens multiple attachments if they are available. The end user system must be setup to open multiple documents in the same window.
- Once you accept the initial or Follow up case and successfully create the case in Argus / Affiliate, the system generates an Acknowledgement in the OUT folder at the same level. For example, if the incoming folder for Site US is C:\USSITE\Incoming, the system generates ACKS in the C:\USSITE\OUT folder.
 - a. The Message format for the ACK is as follows:
<CASES>
<CASE>
<CASE_NUMBER>: Argus Generated Case Number

<PRODUCT_NAME>: Text Field up to 70 Characters for Primary Suspect Product of Case

<DATETIME>: The Date and time in the DD-MMM-YYYY hh:mm:ss format when the file was accepted / rejected by the system

<ATTACHMENTS>

<ATTACHMENT>:

<FILENAME>: Text field of Attachment File Name

<DOCID>: Document ID from Document Storage System

- If you click Copy to copy a case in Argus, the system generates an ACKS and puts it into the out folder for the site the original case belongs to. For example, Case A belongs to US Site and the user copies the case to Case B. The system creates an ACK in the US\Out Folder as configured in the US Site.

Rejected Cases In Argus Safety, the Workflow Manager or Enterprise User can click Reject Case to reject cases from the Intake Worklist.

- Affiliate Users can reject cases in the Intake Worklist.
 - When you try to reject a case, the system presents the Standard Justification dialog.
 - The Status row displays the following message:
Case Rejected by XXXX on YYYY at MMM due to: ZZZZ
where:
XXX is the User Full Name,
YYYY is the Date when the case was rejected in GMT
MMM is the time in GMT
ZZZ is the justification for rejecting the case as entered by the user.
 - Rejected Date: Date in GMT when the user rejected the case
 - Rejected By: User Full Name who rejected the case.
- The system displays the **Total number of Rows** in the Worklist header section.
- You can select the number of cases to display on the by selecting a value from page size drop-down list on the Worklist dialog.
- The page drop-down list contains the following values:
 - 50
 - 100 (default)
 - 250
 - 500
 - 1000
 - 2000
- The system displays the number of cases currently in view and updates the range automatically. For example, if you select 100 from the page size drop-down list, the system separates the displaying rows into groups of 100 cases.

- The system enables you to go directly to a range of cases from the **Displaying Rows** drop-down list.
- The system enables you to scroll through the Worklist page-by-page increments as defined by the **Page Size** drop-down list.
- The system enables you to sort on ALL the columns in the Worklist view by clicking the header column. The system displays a triangle to show which column is sorted currently.
 - The initial sorted column is Initial Date.
 - The default sort order is ascending
 - Clicking the column header again, toggles between ascending and descending order.
- The system maintains the worklist view with the sorting and filtering options defined by the user.
- The Intake Worklist enables you to filter on each element.
- The system enables you to filter on any element when you click the **Filter** button.
 - The system provides a Type Ahead feature to enables users to filter on any text/date element.
 - The system enables you to Close the filtering options by clicking the **X** icon on the filtering options.
 - If filtering criteria are specified, the **Filter** icon has the **paper clip** icon to indicate there are filtering elements.
 - The system permits a Like search (e.g. if you search for Cure, it returns all elements starting with Cure).
 - The system enables wild card searches . For example, if the user searches for %Cure, the system returns all elements containing Cure.
 - Clicking the **Search** button enables you to filter for the reports in the list of reports.
 - These are filtering options are available from Worklist-specific views and when you drill down for cases or reports.
- The system saves all user preferences for future use.
- Clicking the Search button enables you to filter the elements on the dialog.

User Site Updates and Access Management You can configure the Path for the File Intakes per Site (Argus and LAM) in the Site configuration.

- When you click the **Browse** button, the system enables you to browse to the Folder for the Site where the XMLS and the PDFs are stored.
- The Path length is up to 255 characters.

ORACLE® Welcome vanessa, Thursday, March 3, 2011 (AS70-DEFAULT) Home Help Close

Code Lists Business Configuration Access Management System Configuration Tools

CODE LIST MAINTENANCE

Browser
Organized by Code List

- Lab Test Group
- Lab Test Type
- Letter Configuration
- Literary Citation
- Local Evaluator Comment Type
- Manufacturers
- Medical Status
- Message Type
- Nature of Event
- Occupations
- Package Units
- Product Group
- Project ID
- Reference Type
- Report Media
- Report Type
- Reporter Information
- Reporter Type
- Reporting Destination
- Reporting Destination Type
- Routes of Administration
- Study Center
- Study Development Phase
- User Sites

Help Text
Defines a list of user sites (e.g. United States, United Kingdom) that are assigned to Argus user accounts. Definition of user sites is required prior to configuring users.

User Sites Filter
Field Description Contains Value Filter

Total Number of Rows (2)

Description	Abbreviation	Site Type	Intake File Path
Common Site	CS	Argus	
United States	US	Argus	

Add New Copy Delete Print

Modify User Site

Description
United States

Abbreviation
US

Site Type
Argus

Intake File Path

Protect Patient Confidentiality - Default
 Protect Reporter Confidentiality - Default
 Bulk Report By Form (Approved Reports) - Default

LAM Sites

Add > < Remove Add All >> << Remove All

Site Printers Add Delete

#	Printer Name	Printer Path
---	--------------	--------------

Save

- The current Worklist options are replaced with granular permissions for Worklist elements in the Group Permissions as per the following:
 - Worklist Intake (default is disabled).
 - The Audit Log tracks the updates made to Site Configuration.
 - The User Site print out displays the File Intake Path.

Configuring System Numbering

This screen enables you to specify the case numbering preferences. Select **System Configuration -> System Numbering** to view the LAM System Numbering screen.

The screen appears as shown.

Code Lists Business Configuration Access Management System Configuration Tools

SYSTEM NUMBERING

System Numbering

Numbering
 Manually number cases
 Automatically number cases
 Start at 10002

Sequencing Options
 Separate sequence for each site
 Separate sequence for each report type
 Separate sequence for each year
 Separate sequence for each month
 Separate sequence for each product abbreviation

Format
 Numbering Format
 Fmt_Bd-[YY]MM[]#####

Placeholder	User Site
SSS	User Site
CC	Country Code
DD	Day
MM	Month
P	Product
YY	Year
TTT	Report Type
#	Number

Save Print

Field Descriptions

The following table lists and describes the fields for this section.

Field/Control Name	Description
Manually Number Cases	Enables the user to manually number the cases on booking or while copying the case, using the save as' option on the case form.
Automatically Number Cases	On selection, the system automatically numbers the cases as defined by the user in the numbering format.
Start at	Enables the user to initialize the counter of the sequence number.
Separate sequence for each site	Enables the user to separate the sequence numbering for cases on site by site basis. If there are cases being entered from two different sites then each site will have different sequencing of case numbers.
Separate sequence for each report type	Enables the user to separate the sequence numbering for cases by the report type of the case.
Separate sequence for each year	Enables the user to reset the sequence numbering for cases after each year based on the initial receipt date of the case.
Separate sequence for each month	Enables the user to reset the sequence numbering for cases after each month based on the initial receipt date of the case.
Separate sequence for each product abbreviation	Enables the user to reset the sequence numbering for cases for each different product abbreviation.
Numbering Format	<p>Enables the user to select the numbering format by selecting the different placeholders.</p> <p>Define the numbering format by typing in custom keywords to print on every case number and selecting different placeholders.</p> <p>[YY][MM]-[###] is the default format.</p>
Placeholder	<p>Placeholders are used to pickup values from the database to be used in the Case numbering format.</p> <p>The possible values populated in this list are:</p> <p># - Number: defines the digits to be used as the sequence number in the format. The field is used to display the sequence number on the case numbers.</p> <p>CC- Country Code: When selected, this uses the A2 code for the country of incidence for the case number.</p> <p>DD - Day: When selected, this uses the date of the Initial receipt date' field of the case.</p> <p>MM - month: When selected, this uses the month of the Initial receipt date' field of the case.</p> <p>P - When selected , this uses either of the two values:</p> <p>If report type is Spontaneous' or other' during booking: the system uses the value of the Product Abbreviation' field specified in the Product configuration for the selected Primary suspect product.</p> <p>If report type is of the type report from study' during booking: the system uses the Product Abbreviation' field specified in the study configuration.</p> <p>SSS - User Site: When selected this uses the Site abbreviation of the site belonging to the user who booked in the case.</p> <p>TTT - Report Type: When selected this uses the report type abbreviation of the report type selected during booking of the case.</p> <p>YY- Year: When selected, this uses the year of the Initial receipt date' field of the case.</p>

Use the following procedure to configure LAM system numbering.

1. Select the **Numbering** feature as required. This can be manual numbering or automatic numbering of cases.
2. Select the **Sequencing Options** as required.

Tip: For the complete explanation of the sequencing options refer to the Field Descriptions

3. Select the Numbering Format.

Tip: To customize the **Numbering Format**, use the **placeholder** values.

Example: To select Country Code, Month and Year (as values to be incorporated from the database) as the Case numbering format, execute the following steps.

- Click on *Country Code*. This appears in the **Numbering Format** field.
- Click on *Month*. This appears in the **Numbering Format** field next to the Country Code.
- Click on *Year*. This appears in the **Numbering Format** field next to the Country Code and Month.

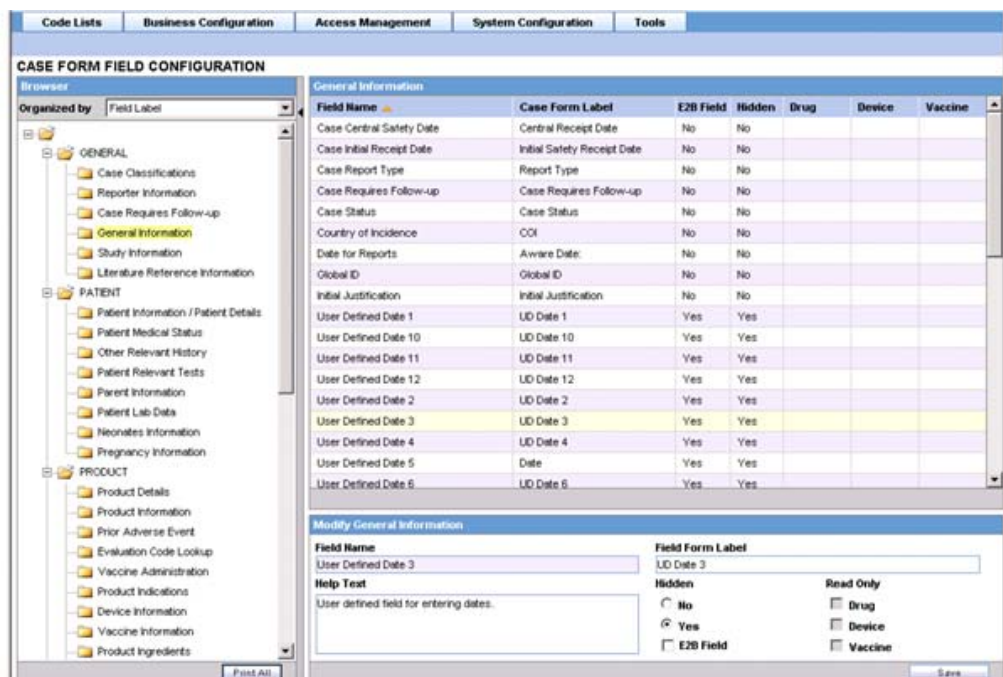
The final data listed in the **Numbering Format** field is the Case Numbering Format.

4. Click **Save** to save the changes made.

Configuring Field Properties

This section enables you to change field label names and hide or display fields in the Case Form.

Select **System Configuration -> Field Properties** to view the Case Form Field Configuration screen shown in the following illustration.

**Tip:**

The Case Form tabs appear in the left panel and are categorized as folders. Each folder contains all the field labels associated with that section.

Example: The General Tab in the Case Form contains sections such as Study, Follow-Up, Case Literature etc.

- To view the list of field names associated with the Study section, click **Study** in the left panel.
- The field names associated with Study appear in the right panel.

Field Descriptions

The following table describes the fields associated with this section.

Field/Control Name	Description
Field Name	Enables the user to view the field name. This is a read only field.
Field Form Label	Enables the user to enter the field label names for those fields that can be edited.
Help Text	Enables you to enter help text for fields that can be edited.
Read Only	Enables you to make drug, device, or vaccine field read-only.
Drug	Enables the user to make a field Read only in the Product tab, when the Argus user chooses "Drug" option on the Product screen.
Device	Enables the user to make a field Read only in the Product tab, when the Argus user chooses "Device" option on Product screen.
Vaccine	Enables the user to make a field Read only in the Product tab, when the Argus user chooses "Vaccine" option on Product screen.

Field/Control Name	Description
Hidden	<p>Enables the user to hide or unhide a field by selecting the radio button.</p> <p>Select Yes to hide the field on case form; select No to unhide the field on case form.</p> <p>Note: Some fields cannot be hidden. Hidden fields do not appear in the case form printout.</p>
E2B Field	When checked, displays which fields are required for E2B.
Max Length	Displays the maximum data length allowed for the fields. This information is displayed for all fields except for Date and Codelist fields.
Null Flavors	This drop-down list displays the Null Flavor sets that are configured in Null Flavor codelist. Null Flavors are displayed in the Case Form field as per Null Flavor set associated.
* Safe Length	<p>Allows the user configure the safe length for all fields except for Date and Codelist fields. Safe length is populated by default for E2B R2 fields which have been extended as per the E2B R3 Regulation.</p> <p>This field is not used in the application for this release.</p>

Use the following to modify case form field names.

1. Select the folder (or section) in the left pane, for which the field names are to be modified.
2. The places the list of field labels associated in the right panel.
3. Click on the **Field Name** to be modified.
4. The system highlights the selected row is highlighted and puts the details about this field in the **Modify** section at the bottom of the screen.
5. Enter the new field name in **Field Form Label**.

Tip: This label will appear in the Case Form section.

6. Select the **Hidden** preference. Select **Yes** if you want to hide the field on the Case Form.
7. Click this checkbox to indicate which fields are required for E2B.
8. Select any or all of the following options **Drug**, **Device** or **Vaccine** as **Read Only** based on your requirement.
9. Click **Save** to save the changes made.

Note: Label Changes will not be reflected in Argus Case Form unless IIS is reset.

Adding User Defined Fields

User defined fields of type Text, Date, and Number may be added to a Case Form. Follow the steps listed below to add a user defined field to a Case Form and/or confirm that the Case Form supports user-defined fields:

1. In Argus Console, navigate to System Configuration > Field Labels.
2. In the left-hand section, select a Case Form by clicking on its name.

3. In the right-hand section with a title bar matching the selected Case Form, scroll down till the words "User Defined.." are visible in the Field Name column.
4. Click on the desired Field Name.
5. In the lower, right-hand section, make the appropriate corrections and save any changes.

Note: Oracle Argus Safety controls the total number of User Defined Fields on any given Case Form by only allowing a single occurrence of each sequence number. Therefore, if "User Defined Number 1" is used, "User Defined Text 1" and "User Defined Date 1" cannot be activated. If a Date and/or Text field is desired the user must select from the fields that have a higher sequence number such as User Defined Date 2, User Defined Date 3, etc., thus always ensuring that the sequence number is unique.

Configuring User Defined Fields

The Argus Safety administrator can customize a user-defined field as a drop-down list. These drop-down lists may contain customized lookup data which can be independent of Argus data.

Use the following procedure to create a user-defined field.

1. Identify the User Defined field in the CMN_FIELDS table.
2. Create a custom table containing lookup information.
3. Create a custom index and specify the required values for the table.
4. Update the record in the CMN_FIELDS table for the User Defined Field.
5. Create a Role and Synonym for the table.
6. Restart IIS.
7. Verify the update made in the application.

Consider the following example that show a sample set of scripts required to configure User Defined Fields as a drop-down list. Assume the requirement is for a **User Defined Field** (UDF) with the following features:

Requirement: A User Defined field *SOURCE_OF_INFORMATION* to be created, with its drop-down values as Fax, E2B, Letter, Email and Telephone under Case Form -> General Tab -> General Information.

Attribute	Value
Field Name	SOURCE_OF_INFORMATION
Field Type	Numeric (Text field type would not work)
Drop-down Values	Fax, E2B, Letter, Email and Telephone
Field Location	Case Form => General tab => General Information

Use the following procedure to create a user-defined field:

1. Login to Argus -> Argus Console -> System Configuration -> Field Labels.
2. Select User Defined Number <N> at desired page from tree shown in the left pane.

3. Choose *No* at *Hidden*.
4. Check **Selectable**.
5. Click **Add** and specify items stored in the drop-down in both English and Japanese if the field is multi-language, otherwise specify only in the English text box.

Go to **General** tab -> **General Information** and check that the configured user-defined fields display the updated drop-down text.

Configure Local Data Entry

Argus Safety supports a concept of global lock that indicates the readiness of case data for global reporting, and a concept of local data locks that indicates the readiness of case data for local reporting having fulfilled the local data entry and assessment needs.

The application allows local users to open a case for entering local data without globally unlocking the case and at the same time maintain the integrity of the “global” case data.

In order to achieve this:

1. The fields in the application are categorized into global and local fields. The local fields have been identified as local to one or more countries. The local fields for only Japan are supported in this release.
2. All Argus J users are considered as Japan Local user in this release and as having access to edit the Japan local fields.

About Local Fields

A field is identified as a Local field to one or more countries based on a new attribute in the CMN_FIELDS table. The local fields for only Japan are supported in this release.

Customers can configure any field in the Case Form > General, Patient, Products, Events tabs, and in the Analysis > PMDA tab as a Local field for Japan through back-end updates to the CMN_FIELDS table.

The Enterprise copy configuration action will copy these updates as per existing functionality.

If a customer configures a field that could update global value as a local field, it is expected that the customers maintain the integrity of the global data by business SOPs or custom software processes.

All the fields in a case that is not a Local PRPT case are simply treated as global fields.

All Argus J users are considered as having access to edit the Japan local fields.

All Japanese text fields, including J User-Defined fields are considered as Local fields for Japan.

- i. All Japanese text fields are the fields that currently has separate _J columns.
- ii. All fields from PMDA tab, PMDA Device Information section.

Argus Safety allows selection of secondary LLT (stored in LLT_J or LLT_CODE_J field) or Synonym (SYN_CODE_J) encoding using MedDRA J browser that does not change the base MedDRA hierarchy of English.

The Event Assessment > Listedness field in the tab for the licenses of the local country corresponding to the local user is considered as local field. However, this field is available for editing for the user only when the local user has listedness privilege for

that local country assigned to them via the User Group > Listedness Determination - Countries access and the datasheet associated with that local country license is configured with "Global /No Local Assessment Required" checkbox as unchecked.

The Events tab > Infection and Event Exclusion checkbox are also considered as local field for Japan.

Any field where an update to a global field can occur is NOT considered as Local field.

All numeric fields, date fields, drop-down fields which share same data value for English and Japan sides are not considered as Local fields.

However, there are exceptions to this rule where some fields that contain global values are available for update to local users and in such a scenario, it is expected that the global value should be protected by customer's business SOPs.

Case classification is such a field that can cause update to global value and it is available as a Local field in the application out-of-the-box.

Study section under General tab requires special handling by the application during local editing. Study Name, Study Description, Protocol Number, Clinical Compound Number and Center Name are local fields.

When the study is a configured study, all these fields are disabled for local editing except Center Name (J). Center Name (J) is available as an editable local field.

Product Information section in Products tab requires special handling by the application during local editing. J Drug Code type and the corresponding J Drug Code/OTC Drug Code/Temporary Code (i.e., DRUG_CODE_TYPE_J, DRUG_CODE_J), J Generic Name and J Product Name fields are local fields.

Any field that is already editable after case lock will remain editable even after local lock.

An auto-narrative generation performed during Japan Local data entry (after global lock) only updates the J field value and does not update the English or any other language field value.

Access Local Case Data Lock Functionality

This section lists the different sections where the functionality for Local Case Data Lock has been documented in the Argus Safety suite of documentation.

Refer to the following table for the list of features and the corresponding Guides where they have been documented:

Local Lock Feature	Overview	Documented in
Local Locking and Local Unlocking - Configuration	<p>Introduction of new switches: Allow Local Locking - to allow a local user to be set up with the privilege to locally lock or unlock a case.</p> <p>Enable Local Unlocking - to provide a system level control permitting local users to locally unlock a case and make any corrections to the previously entered local data.</p>	<p>Oracle Argus Safety Administrator's Guide > 2 Access Management > Configuring Users</p> <p>Oracle Argus Safety Administrator's Guide > 4 System Configuration > Configuring System Management - Common Profile Switches</p> <p>Oracle Argus Safety User's Guide > Global User Management</p>
Changes to the Case Locking Mechanism in Argus Safety - Case Form Changes	Introduction of action icon - Local Lock - to allow a user to locally lock or unlock a case	Oracle Argus Safety User's Guide > 1 Getting Started > Quick Launch Toolbar
Changes to the Case Locking Mechanism in Argus Safety - Changes to global locking, One Step Global and Local Lock	Allow Global locking and triggering of global and local reports, and allow one step global and local locking	Oracle Argus Safety User's Guide > Locking a Case
Changes to the Case Locking Mechanism in Argus Safety - Changes to Global Unlocking - Configuration	<p>Introduction of new switches:</p> <p>Allow Forced unlock (Global and Local) - to allow users to be set up with the privilege to forcibly unlock a case that been globally and/or locally locked but pending report generation.</p> <p>Allow Global Unlock on Pending Local Lock - to allow users to be set up with the privilege to forcibly unlock a case that is still pending a local lock.</p>	<p>Oracle Argus Safety Administrator's Guide > 2 Access Management > Configuring Users</p> <p>Oracle Argus Safety Administrator's Guide > 2 System Configuration > Configuring System Management - Common Profile Switches</p> <p>Oracle Argus Safety User's Guide > Global User Management</p>
Changes to the Case Locking mechanism in Argus Safety - Changes to global unlocking - Case Form changes	Control globally unlocking a case based on local/global reports pending generation and /or cases pending local lock.	Oracle Argus Safety User's Guide > Unlocking a Case

Local Lock Feature	Overview	Documented in
Case Form changes - Local Reports Configuration - Local Reporting Rule and Local Reports	Configuring Local Reporting Rules and Local Reports.	Oracle Argus Safety Japanese Administrator's Guide > 3 System Configuration > Configuring Local Reports - Local Reporting Rule and Local Reports
Triggering Local Reports - Changes to Report Scheduling and Generation Algorithm - Auto Scheduling	Changes to report auto-scheduling for scheduling local reports.	Oracle Argus Safety User's Guide > Report Scheduling - Auto-Scheduling
Triggering Local Reports - Changes to Report Scheduling Algorithm - Manual Scheduling	Changes to report manual scheduling for scheduling local reports.	Oracle Argus Safety User's Guide > Report Scheduling - Manual Scheduling
Triggering Local Reports - Changes to Report Generation Algorithm	Changes to report generation for generating local reports.	Oracle Argus Safety User's Guide > Triggering Local Reports - Report Generation Algorithm
Changes to Expedited Reports and Periodic Reports on DLP	Changes to DLP while generating local expedited and periodic reports.	Oracle Argus Safety Japanese User's Guide > Reports

Process an Outlier

When a suspect product with local license is removed on a follow-up, the case remains a Local PRPT Case (Local Potential Reportable Case) until the corresponding nullification/downgrade local reports is generated.

If a customer wants to change Local Reports configuration data after being in production with this release, it is recommended that customers ensure that cases/reports under processing be completed before changing configuration data to avoid unpredictable results. Note that if a customer changes the Local Reports configuration data mid-way where the reports are mid-way processing (e.g., scheduled), the reports will be determined as local/global based on what type it was at the time when the report was scheduled and will be completed processing that way irrespective of current configuration even if inconsistent with the configuration. Also note that presence of local reports will determine that the case is local case.

It is also recommended that customers ensure that cases/reports under processing be completed before up taking the Local Locking feature and (thereby) installing the local lock configuration data (refer to [Activate Local Locking in Argus Safety](#)). Note that if the case was mid-way processing (e.g., case was open in data entry workflow) when customer up took the Local Locking feature, a subsequent case save will determine if the case is local or global.

Activate Local Locking in Argus Safety

In order to activate the Local Locking feature in Argus Safety, the installer provides the users with an option to install the underlying metadata that enables the local lock feature in the application. A customer, who may not prefer to turn on the local locking feature due to existing business processes that already handle the local processing needs for a company, could choose not to install the metadata and thus not uptake the local lock feature in the application.

A separate database script is provided so that the user can run to turn on the Local lock feature after an upgrade or fresh install. On executing this script, it prompts the user to choose to turn on the local locking feature and uptake the Local Locking seed data.

The application assumes the default value of 1, parses the user input and installs the Local Locking seed data for each of the enterprise specified in the comma separated list.

Enter Local Reports Configuration Seed Data A new table is seeded to identify Local Reports for Japan:

- **Country** — The seed data is the country id for Japan (from codelist Countries) for this release.
- **Reporting Destination** — The script prompts the customer to provide the default value of reporting destination for PMDA.

Prompt - "Please enter Agency Name for the PMDA reporting destination as configured in the "Reporting Destination" codelist. This name will be used to identify Local Reports for all enterprises".

- **Report Form** — The seed data is the following Japan reports:

- i. 医薬品 症例報告書 別紙様式 1・2 (Mktd 1, 2)
- ii. 医薬品 研究報告調査報告書 別紙様式 3・4 (Mktd 3, 4)
- iii. 医薬品 外国での措置報告 別紙様式 5・6 (Mktd 5, 6)
- iv. 治験薬 症例報告書 別紙様式 1・2 (Inv 1, 2)
- v. 治験薬 研究報告調査報告書 別紙様式 3・4 (Inv 3, 4)
- vi. 治験薬 外国での措置報告 別紙様式 5・6 (Inv 5, 6)
- vii. 報告様式8: 医療機器不具合・感染症症例報告書
- viii. 報告様式10: 医療機器の研究報告調査報告書/外国措置調査報告書
- ix. E2B

Enter Local Users Seed Data The upgrade installer script prompts the user to choose if all the Argus J users will be updated to have local locking privileges.

Enter Local Fields Seed Data Note that the CMN_FIELDS are always seeded as part of install/upgrade factory data to identify the Local Fields for Japan and will be present irrespective of if the customer chooses local locking feature or not.

In case of Multi-tenancy, the customer input value is used to set the seed values across all enterprises.

This seeding of Local users data is audit logged with the system user.

After install/upgrade, if customer has turned on the local locking, the icons in the applicable screens start reflecting the local/global lock status of the case.

Activate Local Reporting in Argus Safety

The changes described below are applicable only when there are local reports configured in the application (i.e. there is data in the Local Reports Configuration table).

The Report Generation functionality does not generate any Japan Local reports, including the reports that were scheduled by the local reporting rules that were marked as Active Moiety or Super Rules, until a local lock occurs. The global reports are generated on global lock.

In Case Form > Regulatory Reports tab, the Final hyper link for a local report is NOT available for a case that is not yet locally locked (similar to the existing functionality for global report on a global unlocked case).

In Case Form > Regulatory Reports tab, the Regenerate Report menu for a local report is NOT available for a case that is not yet locally locked (similar to the existing functionality for global report on a global unlocked case).

The **Final** checkbox in Case Actions > Case Open > Batch Print dialog box will remain disabled and grayed out when any of the case selected is locally unlocked as it does today when a case is globally unlocked.

If report generation is invoked from the Batch Report Generation AG Service, the AG Service skips the case that is not yet locally locked similar to the existing global unlocked cases.

Note that Worklist > Bulk ICSR Transmit > Re-Transmit and Re-Transmit Multiple Reports put a failed report back in generation to be picked up for processing by Batch Report Generation AG Service. The above point will apply in this scenario.

If report generation is invoked from other AG Services listed below, the AG Service today ignores the global locked status and generates reports. This has been corrected so that the AG Service skips the case that is not yet globally locked when generating global reports similar to the existing Batch Report Generation AG Service. Similarly, the AG Services listed below skip the locally unlocked cases while generating local reports:

- Bulk Report Transmit
- Bulk Report Transmit Email
- Bulk Report Print
- Bulk Report Transmit Fax
- Bulk Report Transmit ICSR

Enabled Modules

You can use this menu option to enable or disable the usage of particular Argus modules such as Affiliate, Centralized Coding, FAR, or Interchange.

The the new CFG_MODULES table stores module names in individual columns. Enabling or disabling a module in the UI checks or unchecks the module flag in the table. For fresh installations, license keys are created in the table without any CMN_PROFILE key entries. Enabled modules are migrated per user setup during upgrade. CMN_PROFILE key entries are removed from the table as part of the upgrade.

The out of the box configuration of the following modules is as follows:

Module Name	Enabled/Disabled
Affiliate	Enabled
Dossier	Disabled
Insight	Disabled
Interchange	Enabled
Japanese	Disabled
BIP Reporting	Disabled
Central Coding	Disabled
Affiliate	Enabled

The Reconciliation and the Documentum modules are no longer part of the configurations list.

Interchange Mapping

You can use this menu option to access the ESM Mapping Utility from the Argus Console Web instead of from the client server network. The ESM Mapping desktop utility is part of the Argus Cloud hosting and is used only for the setup and configuration of the Service INI File.

Code List Configuration

This chapter allows administrators to configure and maintain code lists in Argus Safety through Argus and the Flexible Data Re-categorization feature.

These are detailed in the following sections:

- [Configuring Code Lists > Argus](#)
- [Configuring Code Lists > Flexible Data Re-Categorization](#)

Configuring Code Lists > Argus

Code List items appear at several locations in the Case Form. It is essential to configure relevant Code List items in order to ensure that case entry in Argus Safety is done according to your company's policies. Before configuring Code List items, the Administrator should consult the company's policies and the terminology used by the company.

To ensure that the Administrator does not have to enter excessive amounts of data during Code List configuration, Argus Safety is shipped with factory data for many of the Code List items.

Tip: The following Code List Items have been described to familiarize you with the Code List configuration.

- For the complete set of Code Lists refer to the **Argus Console->Code List** section.
- The default help text associated with each code list item is displayed at the bottom of the left panel.

Code List Item	Description
Autosignals	This screen helps in capturing Auto Signal information. Users can define the criteria that triggers Autosignal within Argus
Batch Reports	This screen helps in capturing Batch Reports information.
Letters	The screen helps in configuring the system to create and schedule letters automatically, according to pre-defined business rules.
Justification	This screen helps in capturing justification information.
Electronic Transmission Recipient	This screen helps in capturing electronic transmission recipient information.
Literary Citation	This screen helps in capturing information about Literary Citations.

Reporting Destination	This screen helps in capturing Reporting Destination information.
Routes of Administration	This screen helps in capturing Routes of Administration information.
Study Center	This screen helps in capturing Study Center information.

Configuring Autosignals

This screen enables you to capture the Auto Signal information. Using this screen, you can define the criteria that triggers Autosignal within Argus.

Example: If an event is reported within x number of days, an email is sent to the defined individual or workgroup. The system checks for patterns each time new data is entered, and sends e-mails to the appropriate individuals or departments on finding a matching pattern.

Select Code Lists -> Argus to view the Code List Maintenance screen.

Tip: The code list items are displayed in the left-panel. Click on the required Code List folder to be configured. The details of this code list item appear in the right panel.

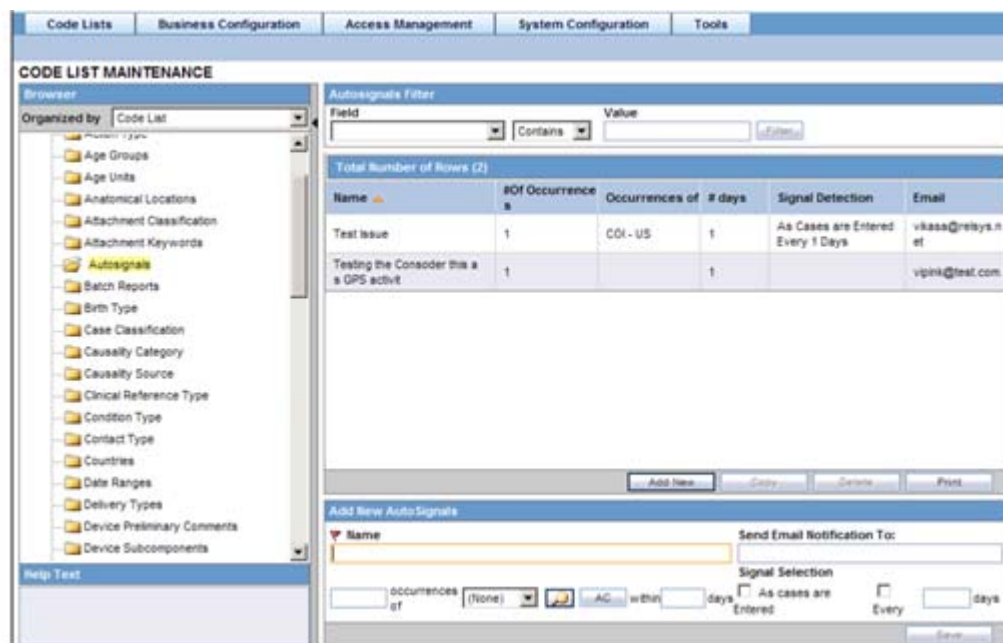
Field Descriptions

The following table describes the fields associated with this section.

Field/Control Name	Description
Name	Enables the user to enter the name of the Autosignal. This is a required field.
Number of Occurrences	Enables the user to enter the number of occurrences of the autosignal.
Occurrences of	Enables the user to enter the user to select or create an advanced condition for the autosignal through Select icon.
Number of days	Displays the number of days for the autosignal.
As cases are entered	Enables the user to perform autosignal as cases are entered.
Every N Days	Enables the user to enter the number of days, when autosignal should be executed.
Email	Enables the user to enter the email address of Argus users to whom the email about autosignal occurrence should be sent.

Use the following procedure to configure Autosignals.

1. Click on the **Autosignals** folder in the left panel. The associated autosignal data appears in the **Total Number of Rows** section in the right panel.



- Click on the **Name** (or row), to view the details associated with the selected autosignal. The details appear in the **Modify Autosignal** section.

You can use the **Autosignals Filter** to make your search specific to an autosignal. The filtering criterion is essential as it helps you to search for specific items.

- Select the appropriate **Field** as the filtering criteria from the drop-down list.
- Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.
- Enter the search criteria in **Value**.
- Click **Filter** to apply the selected criteria.

This displays the search results under **Total Number of Rows**.

Tip: You can alternatively click Add New to create a new auto signal.: Click **Copy** to make an editable copy of an existing autosignal.

Click **Delete** to delete a selected autosignal.

- Enter the name of the autosignal in the **Name** field.
- Enter the number of occurrences of the autosignal in the **Number of Occurrences** field.
- Select or create an Advanced Condition, if any from the button in the **Occurrences of field**.

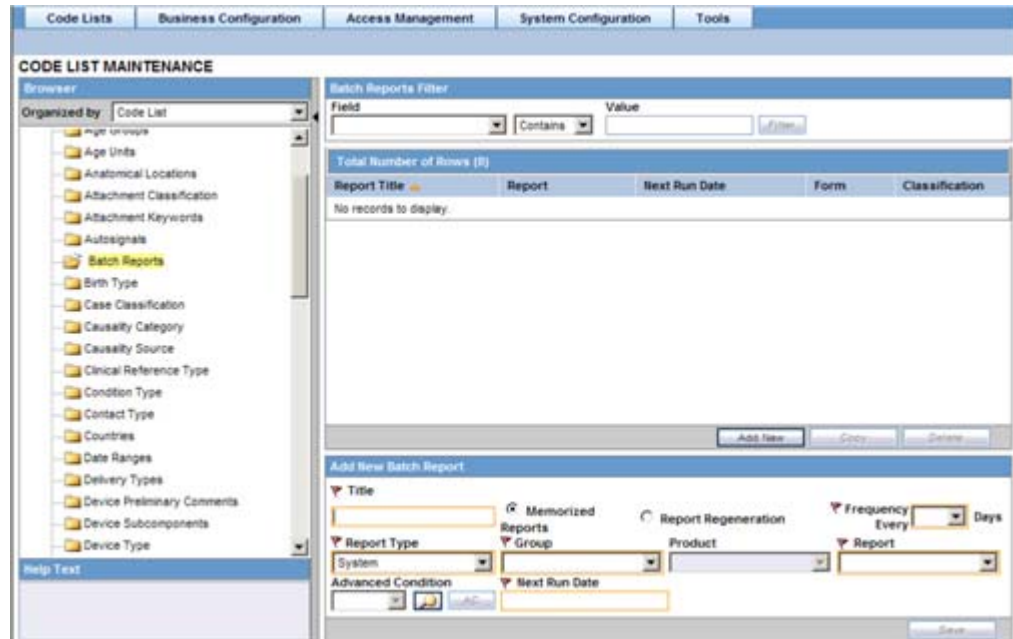
Tip: Click here for details on Advanced Conditions

- Enter the number of days for the autosignal under the **Number of days** field.
- Select the **As cases are Entered** checkbox to perform autosignal as cases are entered.
- Enter the number of days when the autosignal should perform under the **Every N Days** field.

13. Enter the e-mail address that receives email about autosignal occurrence in the **Email** field.
14. Click **Save** to save the changes made to this screen.

Configuring Batch Reports

This screen enables you to configure Batch Reports information.



- Scheduled reports can be automatically generated and stored in the database by Argus Safety Service. This screen displays a list of all the existing Batch Reports.
- By default the Batch reports shown are memorized reports. The Argus user can see the list of scheduled reports for memorized reports, using the Memorized Reports option.
- Select Code Lists -> Argus to view the Code List page.
- Click on the **Batch Reports** folder in the left panel.

The associated report data appears in the **Total Number of Rows** section in the right panel.

Tip: The code list items are displayed in the left-panel. Click on the required Code List folder to be configured. The details of this code list item appear in the right panel.

Field Descriptions

The following table describes the fields associated with this section.

Field/Control Name	Description
Title	This is the unique name for the batch report name.
Report	Enables the user to select a report that has to be scheduled.
	Report Regeneration
	Memorized report

Field/Control Name	Description
Product	Enables the user to select a product for which the report is generated.
Frequency: Every Days.	Enables the user to enter the number of days after which the report is to be generated. The value has to be > 0.
Next Run Date	Enables the user to enter the next date from which the report has to be scheduled.
Advanced Condition	Enables the user to select the Advance Condition that satisfies the criteria which will trigger the Signal. You can either select an existing criteria or create a new one.
Report Type	Enables the user to select the type of the report.
Group	Enables the user to select the group to which the report must be assigned.

Use the following procedure to configure Batch Reports

1. Click on the **Report Title** (or row), to view the details associated with that report. The details appear in the **Modify Batch Report** section.

You can use the **Batch Reports Filter** to make your search specific to a batch report. The filtering criterion is essential as it helps you to search for specific items.

2. Select the appropriate **Field** as the filtering criteria from the drop-down list.
3. Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.
4. Enter the search criteria in **Value**
5. Click **Filter** to apply the selected criteria.
6. This displays the search results under **Total Number of Rows**.

Tip:

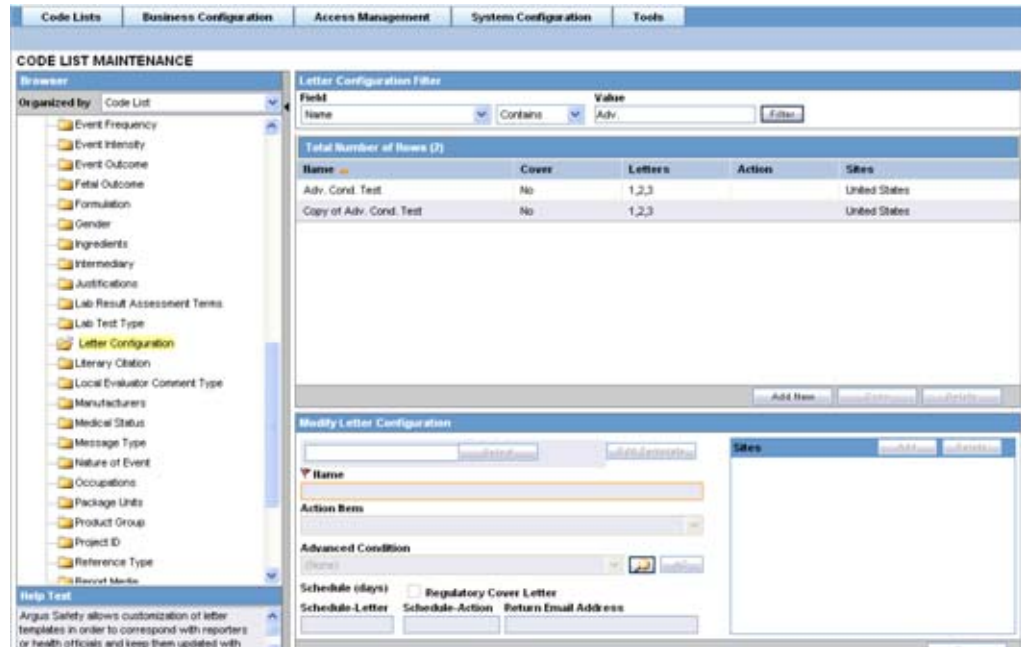
You can alternatively click **Add New** to create a new report.

- Use **Copy** to make an editable copy of an existing report.
 - Use **Delete** to delete an existing report.
7. Enter the **Title Name** for the batch report.
 8. Select the **Report Type** from the drop-down list.
 9. Select the **Group** to which the report must be assigned.
 10. Select the report to be scheduled as **Memorized Reports** or **Reports Regeneration**.
 11. Select the **Frequency** of generating the report after the specified number of days have elapsed.
 12. Select the **Product** for which the report is to generated, from the drop-down list box.
 13. Select the **Report** from the drop-down list.
 14. Enter the **Next Run Date**. This is the next date from which the report has to be scheduled.
 15. Select the **Advanced Condition** associated with the report configuration.
 16. Click Select icon to launch the Advanced Conditions browser.

17. Click **Save** to save the changes made to this section.

Configuring Letters

Argus Safety enables the customizing of letter templates in order to correspond with reporters or health officials and keep them updated with case activity. Access to the **Letter Configuration** dialog can be granted to any user or user-group, as found appropriate by the Administrator.



- To automatically generate a letter, the system reads a template that specifies the information that must appear in the letter.
- The template is a file in Rich Text Format (.rtf format) that contains the letter text and some field identifiers (also called placeholders). The system substitutes information specific to the current case for the placeholders in the template. Thus, a letter containing case-specific information is automatically generated.
- The administrator can set up the system to create and schedule letters automatically, according to pre-defined business rules. This section discusses the creation, modification, and deletion of letter templates.

Select **Code Lists-> Argus** to view the Code List page.

Tip: The code list items are displayed in the left-panel. Click on the required Code List folder to be configured.

The details of this code list item appear in the right panel.

Configuring letter (RTF) templates

RTF Document can be created using the required placeholders such as:

[patient_last_name], [product_name]:[n], [rec_vacc_date]:[n]:[m], [event_prior_hist:primary_event], [reg_report_timeframe]

Most of the placeholders have one parameter or two and these are almost always linked to sort order.

Here are some examples of how these placeholders extract data:

For single value columns:

[age],[case_id],[comments],[case_status],[country_of_inc]

For multiple value columns:

[event_death:primary_event] picks data from case_primary_event table

[event_death]:[n] picks data from case_event/lam_event table based on Sort order

[case_notes]:[n], [concentration]:[n],[drug_code]:[n]

For multiple parameter columns:

[ingredient]:[n]:[m] - It lists nth case product and lists its mth ingredient

Field Descriptions

The following table describes the fields associated with this section.

Field/Control Name	Description
Name	Enables the user to specify the name of the letter as it will appear in the Letters menu.
Name (J)	Enables the user to specify the Japanese name of the letter as it will appear in the Letters menu.
Edit Template	Enables the user to open the letter (template) for editing. Use only WordPad for editing letter templates.
Regulatory Cover Letter	Enables the user to indicate whether this letter template should appear in the Regulatory Rules dialog Cover letter drop-down list box. The available options are: No , Yes – RTF Format , and Yes – PDF Format .
Schedule - Letter	Enables the user to enter the number of days (from the receipt date) when the letter will be due.
Schedule - Action	The Action field enables the Administrator to specify the number of days (from the current date) after which the Action Item for following up on this letter will be due.
Sites	Argus Console provides the ability to configure letters to user sites. Enables users to select single or multiple sites for that letter. The system will only allow users to see letters that are configured to their site.
Action Items	The action items list is a drop-down list of action item codes from the Action Type List Maintenance.
Return Email Address	Enables the user to enter a default email address where the mails will be sent. This address is displayed by default in the Activities tab of the Case Form.
Advanced Condition	Enables the user to configure Advanced Conditions. If the case matches with the Advanced Condition, the configured letter is scheduled for the case.

Use the following procedure to configure letters.

1. Click on the **Letter Configuration** folder in the left panel. The associated data appears in the **Total Number of Rows** section in the right panel.
2. Click on the **Name** (or row), to view the details associated with that letter. The details appear in the **Modify Letter Configuration** section.

3. You may use the **Letter Configuration Filter** to make your search specific to a letter. The filtering criterion is essential as it helps you to search for specific items.
4. Select the appropriate **Field** as the filtering criteria from the drop-down list.
5. Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.
6. Enter the search criteria in **Value**.
7. Click **Filter** to apply the selected criteria.
8. This displays the search results under **Total Number of Rows**.

Tip: You can alternatively click **Add New** to create a new letter.

- Use **Copy** to make an editable copy of an existing letter.
- Use **Delete** to delete an existing letter.

9. Click **Select** to specify the path of the letter template to be used.

Tip: Click **Edit Template** to save the existent template on to your local drive of the system.

You can edit this template and repeat the step listed above, to ensure that the updated template is used for letters.

10. Enter the name of the letter, as it will appear, in the **Letters Menu** section in **Enter a new item**.
11. Click **Add** or **Delete** to configure letter to the user **Sites**.
12. Select the **Action Item** from the drop-down list box. The action items list is a drop-down list of action item codes, from the **Action Type List Maintenance**.
13. Configure the **Advanced Condition** for the case.
14. Enter the **Schedule (days)-Letter**. This is the number of days from the receipt date when the letter is due.
15. Enter the **Schedule (days)-Action**. This is the number of days from the current date, after which the Action Item for the follow up on this letter will be due.
16. Enable the **Regulatory Cover Letter** option to indicate whether this letter template should appear in the Regulatory Rules dialog.
17. Enter the default e-mail address in **Return Email Address**.
18. Click **Save** to save the changes made for this section.

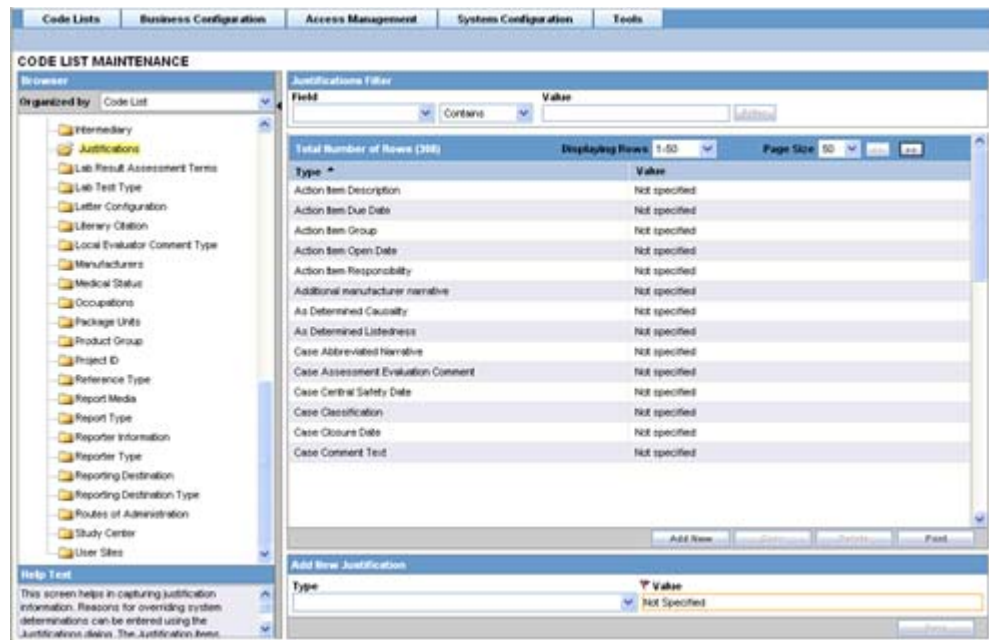
Letter Placeholder for the IND Cover Letter

- You can define a placeholder for the **IND_SIMILAR_EVENTS** table. The system uses data from this table to populate the **Case Number**, **Protocol Number**, **Subject ID**, and **Adverse Event** terms for previously submitted cases reporting the same events.
- If no reports were submitted, the system prints **None Submitted** instead of the table.

The placeholder only prints this information when it is used in the cover letter for the **Regulatory Report**. The system uses the license associated with the scheduled report to track other cases where the same product license was previously submitted for the same events in the current case.

Configuring Justifications

This screen enables you to capture justification information.



Argus Safety users can enter the reasons for overriding system determinations using the Justifications dialog. The Justification items appear on the Action Justification dialog on the screen.

Select **Code Lists**-> **Argus** to view the Code List page.

Tip: The code list items are displayed in the left-panel. Click on the required Code List folder to be configured.

The details of this code list item appear in the right panel.

Field Descriptions

The following table describes the fields associated with this section.

Field/Control Name	Description
Type	Enables the user to configure the type.
Justification	Enables the user to enter the justification.

Use the following procedure to configure justification.

1. Click on the **Justifications** folder in the left panel. The associated report data appears in the **Total Number of Rows** section in the right panel.
2. Click on the **Type** (or row), to view the details associated with that justification. The details appear in the **Modify Justification** section.
3. You may use the **Justifications Filter** to make your search specific to a justification. The filtering criterion is essential as it helps you to search for specific items.
4. Select the appropriate **Field** as the filtering criteria from the drop-down list.
5. Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.

6. Enter the justification reason in **Justification**.
7. Click **Filter** to apply the selected criteria. This displays the search results under **Total Number of Rows**.

Tip: You can alternatively click **Add New** to create a new justification.

- Use **Copy** to make an editable copy of an existing justification.
- Use **Delete** to delete an existing justification.

8. Select the **Type** from the drop-down list.
9. Enter the **Value** for the justification.
10. Click **Save** to save the changes made for this section.

Configuring Electronic Transmission

This screen enables you to configure electronic transmission recipient information.

- Details of electronic transmission recipient such as name, title, address etc. are submitted here.
- Select **Code Lists-> Argus** to view the Code List page.

The screenshot shows the 'CODE LIST MAINTENANCE' application. On the left is a tree view of code lists, with 'Electronic Transmission Recipient' selected. The main area is titled 'Electronic Transmission Recipient Filter' and contains a search bar with 'Field' and 'Value' dropdowns and a 'Filter' button. Below this is a table showing 'Total Number of Rows (4)'. The table has columns for Name, Title, Address (City, State, Province), Country, Postal Code, Phone, Fax, and Email Preferred Method. Three rows of recipient data are visible. At the bottom, there is an 'Add New Electronic Transmission Recipient' form with fields for Name, Address, State, Phone, Title, Country, Fax, Preferred Method, City, Postal Code, and Email.

Name	Title	Address	Country	Postal Code	Phone	Fax	Email Preferred Method
Joan Miller	Regulatory Reporting Consul	PO Box 6720 Stanford CA	94309				jml@et@etrys-inc.com Electronic Mail (Email)
Joe Smith	Safety Surveillance Consul	8973 Oakbridge Newton MA	AFGHANISTAN	04938	617-485-9283	617-485-9283	jsmith@consulting.com Fax
Marcus Orlando	Regional Office	1074 Little River Drive Orange CA	92876		949-387-5643	949-453-1817	orlando@cc.regional.com Electronic Mail (Email)

Tip: The code list items are displayed in the left-panel. Click on the required Code List folder to be configured. The details of this code list item appear in the right panel.

Field Descriptions

The following table lists and describes the fields associated with this section.

Field/Control Name	Description
Name	Enables the user to enter the name of Electronic Transmission Recipient.

Field/Control Name	Description
Title	Enables the user to enter the title of Electronic Transmission Recipient.
Address	Enables the user to enter the address of Electronic Transmission Recipient.
City	Enables the user to enter the city of Electronic Transmission Recipient.
State/Province	Enables the user to enter the state/province of Electronic Transmission Recipient.
Country	Enables the user to select the country of the user.
Postal Code	Enables the user to enter the postal code of Electronic Transmission Recipient.
Phone	Enables the user to enter the phone number of Electronic Transmission Recipient.
Fax	Enables the user to enter the fax of Electronic Transmission Recipient.
Email	Enables the user to enter the email of Electronic Transmission Recipient.
Preferred Method	Enables the user to select the preferred method of transmission from the drop-down list. This can be by fax or by email.

Use the following procedure to configure the electronic transmission recipient.

1. Click on the **Electronic Transmission Recipient** folder in the left panel. The associated data appears in the **Total Number of Rows** section in the right panel.
2. Click on the **Name Title** (or row), to view the details associated with that electronic transmission. The details appear in the **Modify Electronic Transmission Recipient** section.
3. You may use the **Electronic Transmission RecipientFilter** to make your search specific to an electronic transmission recipient. The filtering criterion is essential as it helps you to search for specific items
4. Select the appropriate **Field** as the filtering criteria from the drop-down list.
5. Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.
6. Enter the search criteria in **Value**.
7. Click **Filter** to apply the selected criteria. This displays the search results under **Total Number of Rows**.

Tip: You can alternatively click **Add New** to create a new electronic transmission recipient.

- Use **Copy** to make an editable copy of an existing electronic transmission recipient.
 - Use **Delete** to delete an existing electronic transmission recipient.
8. Enter the **Name** of the electronic transmission recipient.
 9. Enter the **Title** of the electronic transmission recipient.
 10. Enter the **Address** of the electronic transmission recipient.

11. Enter the **City** of the electronic transmission recipient.
12. Enter the **State/Province** of the electronic transmission recipient.
13. Select the **Country** of the electronic transmission recipient, from the drop-down list.
14. Enter the **Postal Code** of the electronic transmission recipient.
15. Enter the **Phone** of the electronic transmission recipient.
16. Enter the **Fax** of the electronic transmission recipient.
17. Enter the **Email** of the electronic transmission recipient.
18. Select the **Preferred Method** of communication (by fax or email) for the electronic transmission recipient.
19. Click **Save** to save the changes made to this section.

Configuring Event Groups

This screen enables you to configure Event Groups information.

- The list of terms which are used across labeledness determines are defined in a central location for users. These users can update these event groups (list of terms) when the product configuration updates are required or when MedDRA versions are upgraded when MSSO releases the new MedDRA updates.
- The values entered here and marked as **Display** appear in the **Console > Business Configuration > Products and Licenses > Product Family > Datasheet > Add Event Groups** section.

Terms tab

The following table describes the fields associated with Event Groups > Terms tab.

Field Name	Description
Event Group Name	Allows the user to enter a new Event Group name.
Event Group Name (J)	Allows the user to enter a new Event Group name in Japanese. This screen and its print form will be visible to only the Japanese users.

Field Name	Description
Display	Allows the user to display the Event Group in Business Configuration > Products and Licenses > Product Family > Datasheet.
Terms	<p>The Terms tab contains terms selected from the MedDRA browser. These terms are displayed in the following format for English users: MedDRA Term in English</p> <p>These terms are displayed in the following format for Japanese users: MedDRA Term in English (MedDRA Term in Japanese)</p> <p>The count of the total number of MedDRA terms present for the case is displayed on the header of the Terms tab.</p>
Term Type	Displays the type of the MedDRA term. This field can contain the MedDRA term type values such as PT, HLT, HLGT or SOC.

Use the following procedure to configure Terms:

1. Click **Event Groups** on the left pane of the Code List.

You can use the **Event Group Filter** on the right pane, to make your search specific to an event group. The filtering criterion is essential as it helps you to search for specific items.
2. Select the appropriate **Field** as the filtering criteria from the drop-down list.
3. Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.
4. Enter the search criteria in **Value**.
5. Click **Filter** to apply the selected criteria.
6. This displays the search results under **Total Number of Rows**.

Tip:

You can alternatively click **Add New** to create a new event group.

 - Use **Copy** to make an editable copy of an existing event group.
 - Use **Delete** to delete an existing event group.
7. Enter the name of the event group under **Event Group Name**.
8. If it is also required for a Japanese user, enter the Japanese name of the event group under **Event Group Name (J)**.
9. Check the **Display** checkbox to display the Event Group in **Business Configuration > Products and Licenses > Product Family > Datasheet**.
10. Click **Export** (or **Import**) to export (or import, respectively) a file in a valid file format from (or into) your local system. Valid file formats require that the file be in .xls, .xlsx, or .csv formats.

Important: The format of the data in the csv, xls or xlsx file must be as follows:

It must have only a single column of data. An import file can have ~ 16 K Terms.

The first/header row must have text as "PT" or "HLT" or "HLGT" or "SOC" in upper or lower case.

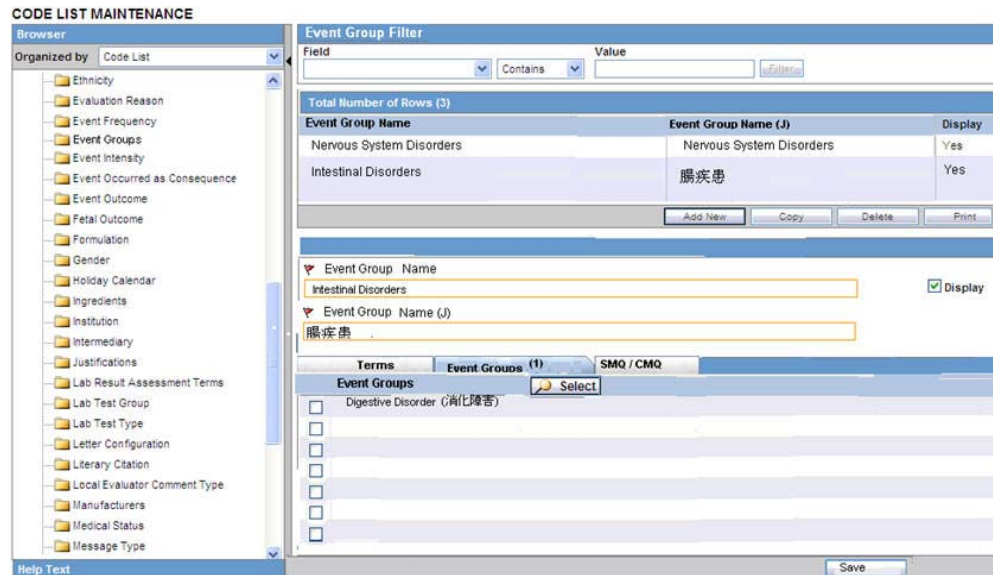
All the rows below the header row must contain corresponding terms (text) such as PT text or HLT text or HLGT text or SOC text.

11. Click **Save** to save the changes made to this tab.

Event Groups tab

Click the **Event Groups** tab to configure event groups.

The following screen is displayed:



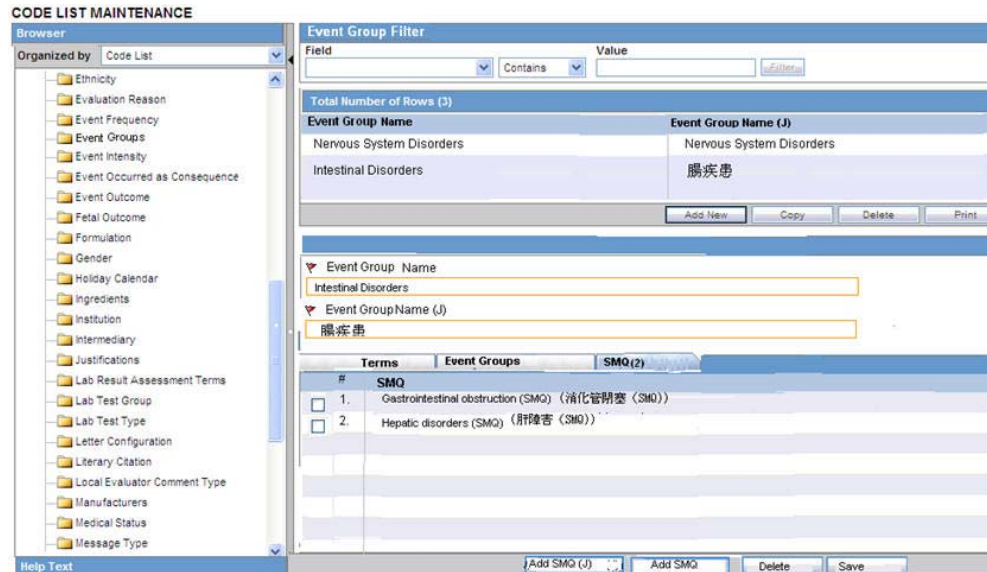
The following table describes the fields associated with Event Groups > Event Groups tab.

Field Name	Description
Event Groups	<p>The Event Group, selected from the Select button > Available Event Groups dialog, is displayed as follows:</p> <p>Event Group Name in English</p> <p>The event group name is displayed in the following format for Japanese users:</p> <p>Event Group Name in English (Event Group Name in Japanese)</p> <p>The count of the total number of Event Group Names present for the case is displayed on the header of the Event Groups tab.</p>
Select button	<p>Click this button to select the relevant event groups from the Available Event Groups dialog.</p> <p>This dialog displays the event groups in a tree-format, with the child event groups being paired under the parent event groups.</p>

SMQ tab

Click the **SMQ** tab to configure SMQ terms.

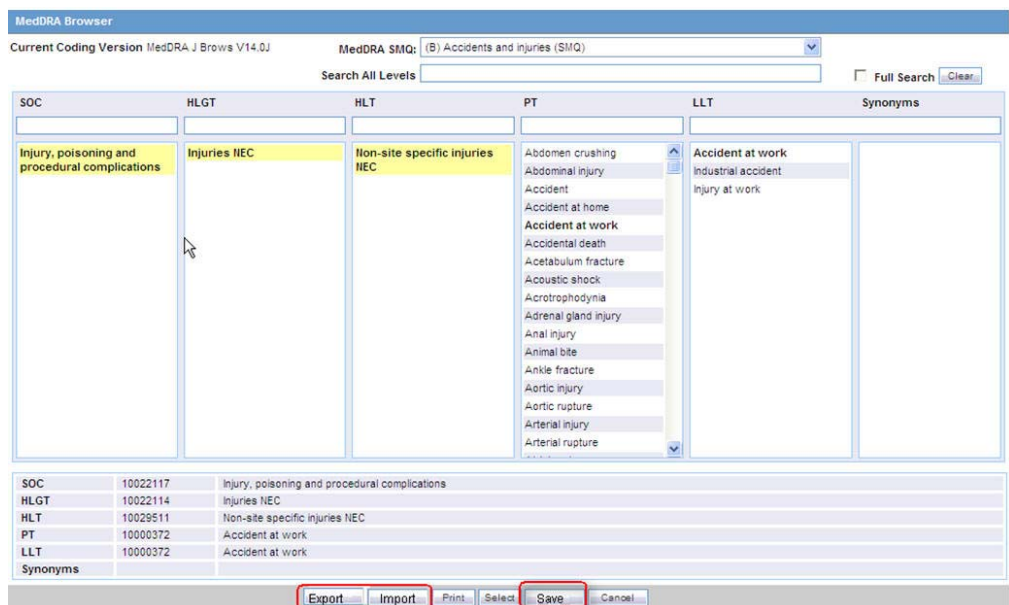
The following screen is displayed:



The following table describes the fields associated with Event Groups > SMQ tab.

Field Name	Description
SMQ	The SMQ term is selected from the Add button > MedDRA Browser dialog.

On clicking the **Add** button, the **MedDRA Browser** is displayed, as shown below:



Export:

The Export button is enabled in two scenarios - when MedDRA is opened from:

i) Argus Console > Business Configuration > Products and Licenses > Product Family > Datasheet

or, from:

ii) Argus Console > Code Lists > Argus > Event Group

MedDRA terms are selected at any level of the MedDRA hierarchy.

On clicking this button, a dialog is displayed, that allows you to select the file type - .csv / .xls / .xlsx file.

On specifying the file type, the selected PT terms are then exported in the Export file. in the <PT terms> format.

Import:

This button is enabled in two scenarios - when MedDRA is opened from:

i) Argus Console > Business Configuration > Products and Licenses > Product Family > Datasheet

or, from:

ii) Argus Console > Code Lists > Argus > Event Group

MedDRA terms are selected at any level of the MedDRA hierarchy.

On clicking this button, a dialog is displayed, that allows you to browse and upload a .csv / .xls / .xlsx file from the desired location on your local machine.

The format of the data in the selected file should be as follows:

It should have only one column of data

The first header/row must display 'PT' or 'HLT' or 'HLGT' or 'SOC'.

All the rows under the header row should contain corresponding terms such as PT text, or HLT text, or HLGT text, or SOC text.

The MedDRA terms in the file should be matched against the MedDRA terms table at the level specified in the header row. Duplicate terms within the import file should be ignored.

If the user enters a search criteria at any levels of the MedDRA hierarchy and continues to search for terms, the results obtained from the Import will be lost. The user may need to import terms again, using the **Import** button.

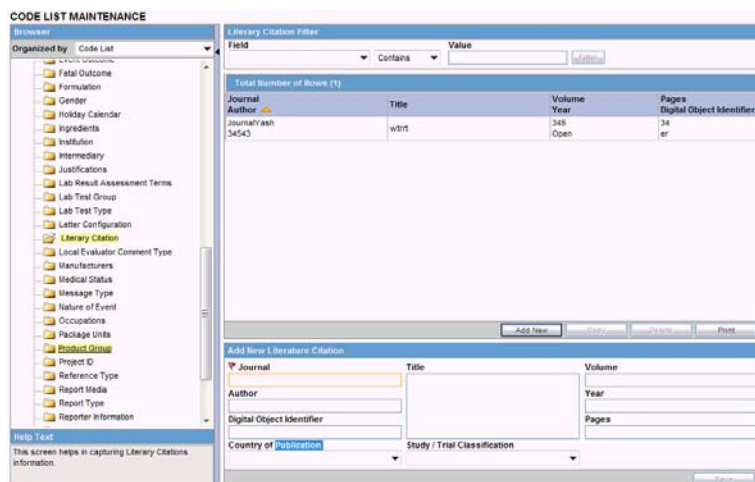
Save:

The Save button is enabled only on selection of the PT term(s).

Configuring Literary Citations

This screen enables you to configure information about Literary Citations.

- The information configured in this form is displayed in the **Literature Info** section of the **Case Form**.
- Select Code Lists -> Argus to view the Code List Maintenance screen.



Tip: The code list items are displayed in the left-panel. Click on the required Code List folder to be configured. The details of this code list item appear in the right panel.

Field Descriptions

The following table lists and describes the fields associated with this section.

Field/Control Name	Description
Journal	Configures the name of the journal where the citation appears. This is a required field.
Author	Configures the name of the author.
Title	Configures the title of the citation.
Volume	Configures the volume number of the journal where the citation appears.
Year	Configures the publication year of the journal where the citation appears.
Digital Object Identifier	Configures the digital object identifier.
Pages	Configures the number of pages in the journal where the citation appears.
Country of Publication	Captures the country of publication of the literature.
Study/Trial Classification	Captures the Study / Trial classification for the literature.

Use the following procedure to configure literary citations.

1. Click on the **Literary Citations** folder in the left panel. The associated data appears in the **Total Number of Rows** section in the right panel.
2. Click **Journal/Author** (or row) to view the details associated with the literary citation. The details appear in the **Modify Literature** section.
3. You may use the **Literary Citation Filter** to make your search specific to a citation. The filtering criterion is essential as it helps you to search for specific items.
4. Select the appropriate **Field** as the filtering criteria from the drop-down list.

5. Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.
6. Enter the search criteria in **Value**.
7. Click **Filter** to apply the selected criteria. This displays the search results under **Total Number of Rows**.

Tip: You can alternatively click **Add New** to create a new citation.

- Click **Copy** to make an editable copy of an existing citation.
 - Click **Delete** to delete a selected citation.
 - Click **Print** to print the selected information as a PDF.
8. Enter the name of the journal in the **Journal** field.
 9. Enter the name of the author of the citation in the **Author** field.
 10. Enter the title of the citation in the **Title** field.
 11. Enter the Volume Number in the **Volume** field.
 12. Enter the year in the **Year** field.
 13. Enter the digital object identifier in the **Digital Object Identifier** field.
 14. Enter the number of pages in the **Pages** field.
 15. Click **Save** to save the changes made.

Configuring Message Type

This screen enables you to configure information about message type.

- The message type specified in this section enables you to specify auto-submission of reports.
- Select Code Lists -> Argus to view the Code List Maintenance screen.

The screenshot shows the 'CODE LIST MAINTENANCE' interface. On the left, a tree view lists various code list categories, with 'Message Type' highlighted. The main area displays a table of existing message types. Below the table are buttons for 'Add New', 'Copy', 'Delete', and 'Print'. At the bottom, there is a form to add a new message type with fields for 'Message Type', 'Description', 'Expedited', 'Mark as Auto Submit', and 'Display'.

Message Type	Description	Expedited / Periodic	Auto Submit	Display
Master		Expedited	Yes	Yes
Recorded		Expedited	Yes	Yes
Master Recorded		Expedited	Yes	Yes
ichscr		Expedited	No	Yes
backlogct		Periodic	No	Yes
backlog		Periodic	No	Yes
psur		Periodic	No	Yes
clar		Periodic	No	Yes
mhwadmintermiscsr		Periodic	No	Yes

Tip: The code list items are displayed in the left-panel. Click on the required Code List folder to be configured. The details of this code list item appear in the right panel.

Field Descriptions

The following table lists and describes the fields associated with this section.

Field/Control Name	Description
Message Type	Displays the message type for a report.
Expedited/Periodic	Displays if the message type is expedited or periodic. Note: By default, ICHICSR is considered as Expedited, while the other message types are considered as Periodic.
Description	Displays a description about the message type.
Auto Submit	Displays if the report has been auto submitted.
Display	Displays if the report needs to be displayed or hidden.

Use the following procedure to configure message type.

1. Click on the **Message Type** folder in the left panel. The associated data appears in the **Total Number of Rows** section in the right panel.
2. Click **Message Type** (or row) to view the details associated with the message type. The details appear in the **Modify Message Type** section.
3. You may use the **Message Type Filter** to make your search specific to a message type. The filtering criterion is essential as it helps you to search for specific items.
4. Select the appropriate **Field** as the filtering criteria from the drop-down list.
5. Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.
6. Enter the search criteria in **Value**.
7. Click **Filter** to apply the selected criteria. This displays the search results under **Total Number of Rows**.

Tip: You can alternatively click **Add New** to create a new message type.

 - Click **Copy** to make an editable copy of an existing message type.
 - Click **Delete** to delete a selected message type.
 - Click **Print** to print the selected information as a PDF.
8. Enter the type of message in the **Message Type** field.
9. Enter the description for the message type in the **Description** field.
10. Click the **Expedited** checkbox if the message type is for an expedited report.
11. Click the **Mark as Auto Submit** checkbox if you wish to mark for auto submission.
12. Click the **Display** checkbox if you wish to display the message type.
13. Click **Save** to save the changes made.

Configuring Reporting Destination

Regulatory reports are submitted to the Reporting Destination. Local company contact information is also provided on this screen.

Use the following procedure to configure reporting destination:

Select Code Lists -> Argus to view the Code List Maintenance screen.

Click **Reporting Destination** on the left pane of the Code List screen.

Agency Information

The **Agency Information** tab is displayed by default, on selecting **Reporting Destination**.

Field Descriptions

The fields under the **Agency Information** tab are described in the following table:

Field/Control Name	Description
Address 1	Enables the user to enter the address of the regulatory contact in line 1.
Address 2	Enables the user to enter the address of the regulatory contact in line 2.
Agency Name	Displays the name of the agency. This is a required field.
Agency Type	Enables the user to select the agency type.
Allow WHO Drug reporting	Enables the user to schedule a report for WHO Drug Reporting.
Attachments	Enables the user to select single or multiple attachments.
City	Enables the user to enter the city of the regulatory contact.
Contact Type	<ul style="list-style-type: none"> ■ Manufacturer - Enables the user to select manufacturer as the type of contact ■ Importer - Enables the user to select importer as the type of contact ■ Distributor - Enables the user to select distributor as the type of contact
Country	Enables the user to enter the country of the regulatory contact.
Country Code	Enables the user to enter the country code of the regulatory contact.
Department	Enables the user to enter the name of the department.
Email Address	Enables the user to enter the email address of the agency.
Email Text Body	<ul style="list-style-type: none"> ■ Select - Enables the user to select a .txt or .rtf file to be uploaded. Note: The file should be in .txt, or .rtf format. After the uploaded file is saved, the Edit button displays a clip button, denoting an attachment. ■ Edit - Enables the user to open the uploaded file / text in a word document from the server and edit the text inside it. If no file was uploaded earlier, a blank document is opened. Note: You can save the edited document on the local machine and click Select to save the file.
Ext	Enables the user to enter the extension number of the regulatory contact.
FAX	Enables the user to enter the FAX Number.
FAX Cover	Enables the user to enter the FAX Cover.
First Name	Enables the user to enter the first name of the regulatory contact.
Last	Enables the user to enter the last name of the regulatory contact.

Field/Control Name	Description
Middle	Enables the user to enter the middle name of the regulatory contact.
Offline Recipient	Enables the user to configure the regulatory agency as an offline agency.
Phone	Enables the user to enter the phone number of the regulatory contact.
Postal Code	Enables the user to enter the postal code of the regulatory contact.
Preferred Method	Enables the user to select the preferred method of agency information.
Registration #	Enables the user to enter the registration number.
Report for Investigational Licenses	Enables the user to select if the reports are to be investigational always or only for clinical case or no marketed license.
Report for Marketed Licenses	Enables the user to select whether reports are to be marketed always or only for the Spontaneous cases or no Investigational.
Report per Email	Enables the user to enter the number of reports to be received in each email.
State/Province	Enables the user to enter the state/province of the regulatory contact.
Title	Enables the user to enter the title of the regulatory contact.
FAX	Enables the user to enter the fax number of the regulatory contact.

Use the following procedure to configure agency information.

1. Select the **Agency Name** (or row) of the reporting destination displayed under **Total Number of Rows** that needs to be modified. The **Modify** section displays the information about the selected code list.
2. You may use the **Reporting Destination Filter** to make your search specific to an agency. The filtering criterion is essential as it helps you to search for specific items.
3. Select the appropriate **Field** as the filtering criteria from the drop-down list.
4. Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.
5. Enter the search criteria in **Value**
6. Click **Filter** to apply the selected criteria. This displays the search results under **Total Number of Rows**.

Tip: **Tip:** You can alternatively click **Add New** to create a new agency information.

- Click **Copy** to make an editable copy of an existing agency information.
 - Click **Delete** to delete the selected agency information.
 - Click **Print** to print the selected information as a PDF.
7. Enter the name of the agency in the **Agency Name** field.
 8. Select the type of agency in the **Agency Type** field.
 9. Enter the department in the **Department** field.

10. Enter the email address in the **Email** field. Multiple e-mail addresses must be separated by a comma (,), and not by a semi-colon (;). If you separate the email addresses by a semi-colon, the transmission service will fail.
11. Select the preferred method from the **Preferred Method** drop-down list. The options available are **Fax** or **Email**.
12. Enter the registration number in the **Registration #** field.
13. Enter the Fax Number in the **FAX** field.
14. Enter the Fax Cover in the **FAX Cover** field.
15. Select the preferred contact type by clicking the checkboxes available under **Contact Type**.
The options available are **Manufacturer**, **Importer** and **Distributor**.
16. Select the **Offline Recipient** checkbox to configure the regulatory agency as an offline agency.
17. Select the **Title** of the regulatory contact. The options available are **Mr.**, **Miss** and **Mrs.**
18. Enter the first name of the regulatory contact under the **First Name** field.
19. Enter the middle name of the regulatory contact under the **Middle** field.
20. Enter the last name of the regulatory contact under the **Last** field.
21. Enter the postal contact address of the regulatory contact under the **Address 1** field.
22. Enter the phone number of the regulatory contact under the **Phone** field.
23. Enter the extension number of the regulatory contact under the **Ext** field.
24. Enter the country code to be dialed in calling up the regulatory contact under the **Country Code** field.
25. Enter the fax number of the regulatory contact under the **FAX** field.
26. Enter the fax extension number of the regulatory contact under the **Ext** field.
27. Enter the country code required in faxing up the regulatory contact under the **Country Code** field.
28. Enter the name of the city where the regulatory contact lives in the **City** field.
29. Enter the name of the state/province where the regulatory contact lives in the **State/Province** field.
30. Enter the name of the country where the regulatory contact lives in the **Country** field.
31. Enter the postal code of the place where the regulatory contact lives in the **Postal Code** field.
32. Enter the number of reports that need to be sent in every email to the regulatory contact in the **Report per Email** field.
33. Select whether to send single or multiple attachments with emails through the **Attachments** drop-down list.
34. Select how the report is to be marketed from the **Report to be marketed** drop-down list.
35. The options in this list are **Always** or **Spontaneous** or **No Investigational**.

36. Select the **Allow WHO Drug Reporting** checkbox to schedule the report for WHO Drug Reporting.
37. Select the type of reports as Investigational always or Only for clinical case or No marketed license from the Report for Investigational drop-down list.
38. Click **Save** to save the changes made.

Local Company Contact

This section lists the Field Descriptions and configuration steps for the **Local Company Contact** tab.

Field Descriptions

The fields the following table lists and describes the fields on the **Local Company Contact** tab.

Field/Control Name	Description
Company Name	Displays the name of the company. This is a required field
Sender Type	Enables the user to select the sender type
Department	Enables the user to enter the name of the department
Email Address	Enables the user to enter the email address of the agency
Lab Code	Enables the user to enter the lab code
Event Term on Expedited Reports	Enables the user to select the event term on expedited reports.
Title	Enables the user to enter the title of the local company contact
First Name	Enables the user to enter the first name of the contact
Middle	Enables the user to enter the middle name of the contact
Last	Enables the user to enter the last name of the contact
Address	Enables the user to enter the address of the contact
Phone	Enables the user to enter the phone number of the contact
Ext	Enables the user to enter the extension number of the contact
Country Code	Enables the user to enter the country code of the contact
FAX	Enables the user to enter the fax number of the contact
Ext	Enables the user to enter the fax extension number of the contact
Country Code	Enables the user to enter the fax country code of the contact
City	Enables the user to enter the city of the contact
State/Province	Enables the user to enter the state/province of the contact
Country	Enables the user to enter the country of the contact
Postal Code	Enables the user to enter the postal code of the contact

Use the following procedure to configure the local company contact.

1. Select the **Agency Name** (or row) of the reporting destination displayed under **Total Number of Rows** that needs to be modified. The **Modify** section is populated with information about the selected code list.

2. You can use the **Reporting Destination Filter** to make your search specific to a company. The filtering criterion is essential as it helps you to search for specific items.
3. Select the appropriate **Field** as the filtering criteria from the drop-down list.
4. Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.
5. Enter the search criteria in **Value**
6. Click **Filter** to apply the selected criteria. This displays the search results under **Total Number of Rows**.
 - Tip:** You can alternatively click **Add New** to create a new company contact.
 - Click **Copy** to make an editable copy of an existing company contact.
 - Click **Delete** to delete a selected company contact.
 - Click **Print** to print the selected information as a PDF.
7. Enter the name of the company in the **Company Name** field.
8. Select the type of sender in the **Sender Type** drop-down list.
9. Enter the name of the department under the **Department** field.
10. Enter the email address of the agency under the **Email Address** field.
11. Enter the lab code of the agency under the **Lab Code** field.
12. Select the type of event term on preferred reports from the **Event Term on Preferred Reports** drop-down list. The options available under this list are **Preferred** and **Lower Level**.
13. Select the **Title** of the regulatory contact. The options available are **Mr.**, **Miss** and **Mrs.**
14. Enter the first name of the regulatory contact under the **First Name** field.
15. Enter the middle name of the regulatory contact under the **Middle** field.
16. Enter the last name of the regulatory contact under the **Last** field.
17. Enter the postal contact address of the regulatory contact under the **Address** field.
18. Enter the phone number of the regulatory contact under the **Phone** field.
19. Enter the extension number of the regulatory contact under the **Ext** field.
20. Enter the country code to be dialed in calling up the regulatory contact under the **Country Code** field.
21. Enter the fax number of the regulatory contact under the **FAX** field.
22. Enter the fax extension number of the regulatory contact under the **Ext** field.
23. Enter the country code required in faxing up the regulatory contact under the **Country Code** field.
24. Enter the name of the city where the regulatory contact lives in the **City** field.
25. Enter the name of the state/province where the regulatory contact lives in the **State/Province** field.

26. Enter the name of the country where the regulatory contact lives in the **Country** field.
27. Enter the postal code of the place where the regulatory contact lives in the **Postal Code** field.
28. Click **Save** to save the changes made.

Configuring EDI

This section lists the field descriptions and configuration steps for the **EDI** tab.

Use the following procedure to configure reporting destination:

1. Select Code Lists -> Argus to view the Code List Maintenance screen.
2. Select **Reporting Destination** on the left pane of the Code List screen. The screen appears as shown below.

Field Descriptions

The following table lists and describes the fields on the **EDI** tab.

Field/Control Name	Description
SGML/XML	Enables the user to select whether to send the report in SGML or XML format. When SGML is disabled and XML is selected, it is populated with default values and is displayed in the read-only mode for the PMDA E2B R3 profile.
Agency Identifier	Enables the user to enter the routing ID configured in Cyclone for the sender community.
Identification Code	Enables the user to enter the agency Duns code, a unique identification code that identifies the trading partner. This field is disabled for the E2B (R3), eVAERS, and eMDR profile. Populated with default values and is displayed in the read-only mode for the PMDA E2B R3 profile.
Code Qualifier	Enables the user to enter the code qualifier here. The code qualifier is used to interpret the identification code. This field is disabled for the E2B (R3), eVAERS, and eMDR profile. Populated with default values and is displayed in the read-only mode for the PMDA E2B R3 profile.
Message Profile	Enables the user to select a message profile. The available options now include the ICH-ICSR V3.0 MESSAGE TEMPLATE - PMDA template.
Mark as Auto Submit	Enables the user to mark the report for auto submission.
Auto Accept ICSRs	Click this checkbox to auto accept ICSRs. This checkbox is visible only when case numbering is set to Automatic .

Field/Control Name	Description
Submission date for ICSRs	Enables the user to select the submission date for ICSRs. It is blanked out and disabled if user selects the eVAERS or eMDR profile in the EDI Tab.
ACK Profile	Enables the user to select the acknowledgement profile. This field is disabled for the eMDR and eVAERS profile. The PMDA E2B R2 Ack profile is also available now.
Primary Receive Agency	Enables the user to select the primary receiving agency.
Imported Cases are assigned to	Enables the user to select the country, where the imported cases need to be assigned. Note: This list comprises the configured Argus sites. The default value is the site of the importing user.
Initial Workflow State	Enables the user to configure the initial workflow state of the case. Note: This list comprises Argus workflow states, with the default value being blank. If you select blank as the workflow state, it is treated as a new case being booked-in.
XML Source Classification	The system enables the user to configure the XML Source Classification and the PDF Source Classifications used for classifications defined while the Source E2B File / PDF for Initial Intake or E2B Differences report is classified. When a case is accepted as an initial or follow-up case, the system attaches the source XML and the Initial Selection PDF to the case on the Additional Info tab.
Selection Source Classification	Enables the user to select the source classification from the drop-down.
Transmit E2B Attachments	Click this checkbox to transmit E2B attachments. If this checkbox is checked in the Reporting Destination Code List, case form attachments are sent to the specified reporting destination.
Attachment Classification	Enables the user to select the attachment classification.
Identification Code	Enables the user to enter the company Duns code, a unique identification code that identifies the trading partner. This field is disabled for the E2B (R3), eVAERS, and eMDR profile.
Company Identifier	Enables the user to enter the company identifier
Code Qualifier	Enables the user to enter the code qualifier here. The code qualifier is used to interpret the identification code. This field is disabled for the E2B (R3), eVAERS, and eMDR profile.
File Name	Enables the user to enter the file name
SGML Declaration File	Enables the user to enter the SGML Declaration File. This field is disabled for the E2B (R3), eVAERS, and eMDR profile.
Maximum # of reports to include in the msg	Enables the user to enter the maximum number of reports that will be transmitted in one message. This field is disabled for the E2B (R3), eVAERS, and eMDR profile and set to 1. Populated with default values and is displayed in the read-only mode for the PMDA E2B R3 profile.
Method	Enables the user to select a method here. This field contains E2B ESTR1 Gateway and E2b Media values.
EDI Header Required	Enables the user to generate the EDI Header. This field is disabled for the E2B (R3), eVAERS, and eMDR profile. Populated with default values and is displayed in the read-only mode for the PMDA E2B R3 profile.

Field/Control Name	Description
XML Version	Enables the user to enter the XML Version. This field is disabled for the E2B (R3) and eMDR profile and set to 1.0. Populated with default values and is displayed in the read-only mode for the PMDA E2B R3 profile.
"URL for Message Schema"	Enables the user to enter the path where the message schema resides on the internet or enter full path if it is located on the disk. This field is disabled for the E2B (R3), eVAERS, and eMDR profile. Populated with default values and is displayed in the read-only mode for the PMDA E2B R3 profile.
Encoding	Enables the user to select the character set encoding used in XML. This field is disabled for the E2B (R3), eVAERS, and eMDR profile and set to UTF-8. Populated with default values and is displayed in the read-only mode for the PMDA E2B R3 profile.
Allowed Attachment File Size (in MB)	Enables the user to specify allowed attachment file size (in MB).
Allowed Report Size (in MB)	Enables the user to specify allowed Report size (in MB).
"URL of ACK Schema"	Enables the user to enter the path where the ACK schema resides on the internet or enter the full path if it is located on the disk. This field is disabled for the E2B (R3), eVAERS, and eMDR profile.
Incoming Folder	Enter the path to the folder where incoming files are stored.
Outgoing Folder	Enter the path to the folder where outgoing files are stored.
ICSR Attachment Outgoing Folder	The path to the folder where outgoing E2B attachments are processed.
Suppress Auto-scheduling	If the checkbox for <i>Suppress Auto-scheduling</i> is marked for an Agency in the Reporting Destination codelist, the system does not schedule reports (Initial, Follow-up, Amendment, Nullification) for that specific Agency during Auto-scheduling (via AG services, Clicking on Auto-scheduling, Auto-scheduling of f/p reports for a manually submitted report). However, reports can be manually scheduled to the Agency that is set for <i>Suppress Auto-scheduling</i> .

Note: For Argus J users, an additional field called *Message Profile 2* is displayed for the configuration of the PMDA - J profile. This field is required for the PMDA agency to specify the PMDA J profile.

Use the following procedure to configure EDI:

1. Select the **Agency Name** (or row) of the reporting destination displayed under **Total Number of Rows** that needs to be modified. The **Modify** section is populated with information about the selected code list.
2. You may use the **Reporting Destination Filter** to make your search specific to an EDI. The filtering criterion is essential as it helps you to search for specific items.
3. Select the appropriate **Field** as the filtering criteria from the drop-down list.
4. Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.
5. Enter the search criteria in **Value**
6. Click **Filter** to apply the selected criteria. This displays the search results under **Total Number of Rows**.

Tip: You can alternatively click **Add New** to create a new EDI.

- Click **Copy** to make an editable copy of an existing EDI.
 - Click **Delete** to delete a selected EDI.
 - Click **Print** to print the selected information as a PDF.
7. Select the format in which the report is to be sent by selecting the **SGML** and **XML** radio buttons.
 8. Click the **Mark as Auto Submit** checkbox if you wish to mark the report for auto-submission.
 9. Select the country where the imported cases need to be assigned.
 10. Select the initial workflow state of the case.
 11. Enter the routing ID configured in Cyclone for the sender community under the **Agency Identifier** field.
 12. Enter the Agency Duns code under the **Identification Code** field.
 13. Enter the Code Qualifier under the **Code Qualifier** field.
 14. Select the message profile from the **Message Profile** drop-down list.
 15. Select the acknowledgement profile from the **ACK Profile** drop-down list.
 16. Enter the Agency Duns Code in the **Identification Code** field.
 17. Enter the Company Identifier in the **Company Identifier** field.
 18. Enter the Code Qualifier in the **Code Qualifier** field.
 19. Enter the name of the file in the **File Name** field.
 20. When a case is accepted as an initial or follow-up case, the system attaches the source XML and the Initial Selection PDF to the case on the Additional Info tab.
 21. Select the SGML file in the **SGML Declaration File** drop-down list.
 22. Enter the maximum number of reports that need to be included in the message under the **Maximum # of reports to include in the msg** field.
 23. Select the method from the **Method** drop-down list. This list contains options like **E2B - Gateway**, **Physical Media** and **XML Transmission**.
 24. Click the **EDI Header** checkbox to generate an EDI Header.
 25. Enter the version of XML in which it is coded in the **XML Version** field.
 26. Enter the path where the message DTD resides on the internet or enter full path if it is located on the disk under the "**URL of Message DTD**" field.
 27. Select the character set encoding used in XML in the **Encoding** drop-down list.
 28. Enter the path where the ACK DTD resides on the internet or enter the full path if it is located on the disk in the "**URL of ACK DTD**".
 29. Click **Auto Accept ICSR's** to auto accept ICSR's.

Note: When the **Auto Accept ICSR's** checkbox is checked and the value **All** or **Initial** is selected from the drop-down list, you must select valid values from the drop-down lists for both **Imported Case are assigned to** and **Initial Workflow State**.

30. Click **Transmit E2B Attachments** to transmit E2B attachments.

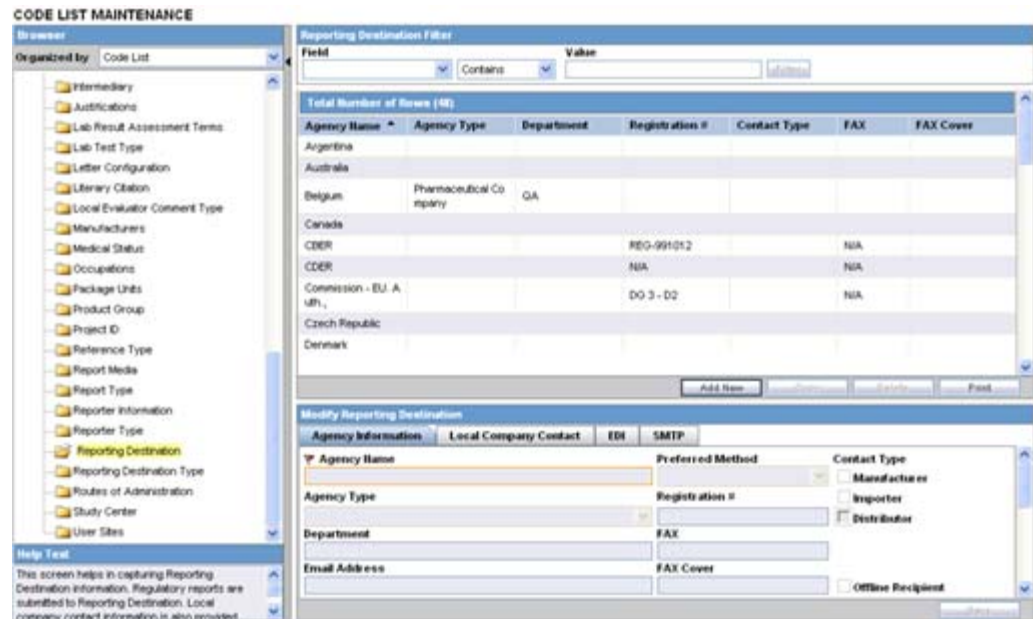
31. Click **Save** to save the changes made.

Use the following procedure to configure reporting destination.

1. Select Code Lists -> Argus to view the Code List Maintenance screen.

Tip: The code list items are displayed in the left-panel. Click on the required Code List folder to be configured. The details of this code list item appear in the right panel.

2. Select **Reporting Destination**. The screen appears as shown below.



Configuring the Base Directory Path

A new database only (not shown in the UI) global level common profile switch `BASE_DIR_PATH_FOR_GATEWAY_FOLDERS` is available for providing the base path for all incoming, outgoing and E2B attachments folders.

Users can configure the base directory path of a machine or network shared path through this switch. This path is suffixed with values provided in new configurations and all incoming, outgoing and E2B attachment folders are created under base directory only. This profile switch is mandatory for the Oracle cloud customers whereas it is optional for the on-premise customers. With this optional set up, on-premise customers can retain their existing folder structure when upgrading from older version of Argus Safety. Cloud customers would need to reconfigure their gateway folders based on the new architecture. When the `BASE_DIR_PATH_FOR_GATEWAY_FOLDERS` is set, make sure to create the base directory path along with the enterprise name.

For example,

If `BASE_DIR_PATH_FOR_GATEWAY_FOLDERS` is set to `C:\BASE_DIR` for the enterprise `ENT_DEFAULT`, then the folder `C:\BASE_DIR\ENT_DEFAULT` is created. IF the Incoming Folder is set to `AGECNCY\Incoming`, Outgoing Folder to `AGECNCY\Outgoing` and ISCR Outgoing Attachment Folder to `AGECNCY\OutAttachment`, the actual incoming folder path would be `C:\BASE_`

DIR\ENT_DEFAULT\AGECNCY\Incoming. The same standard applies for the outgoing and attachment folder too.

If the BASE_DIR_PATH_FOR_GATEWAY_FOLDERS is not set, the Incoming, Outgoing and Attachment folders could have the complete directory path.

SMTP

This section lists the Field Descriptions and configuration steps for the **SMTP** tab.

The screenshot displays the 'CODE LIST MAINTENANCE' window with the 'SMTP' tab selected. The 'Email SMTP Configuration' section is visible, containing fields for 'From', 'CC', and 'BCC', along with checkboxes for 'Delivery Receipt' and 'Read Receipt'. The 'Modify Reporting Destination' section above shows a table of reporting destinations, with the 'Belgian Pharmaceutical Company' row highlighted.

Agency Name	Agency Type	Department	Registration #	Contact Type	FAX	FAX Cover
Argentina						
Australia						
Belgian Pharmaceutical Company	Pharmaceutical Company	GA				
Canada						
CDER			REG-991012		N/A	
CDER			N/A		N/A	
Commission - EU - Auth.			DO 3 - D2		N/A	
Czech Republic						
Denmark						
EMEA XML 2.1						
ESM FDA 0						

Field Descriptions

The following tables lists and describes the fields on the **SMTP** tab.

Field/Control Name	Description
From	Enables the user to enter the email address of the sender.
CC	Enables the user to enter the email addresses to send email as CC.
BCC	Enables the user to enter the email addresses to send email as BCC.
Delivery Receipt	Enables the user to check this box to receive a delivery receipt.
Read Receipt	Enables the user to check this box to receive a read receipt.

Use the following procedure to configure SMTP.

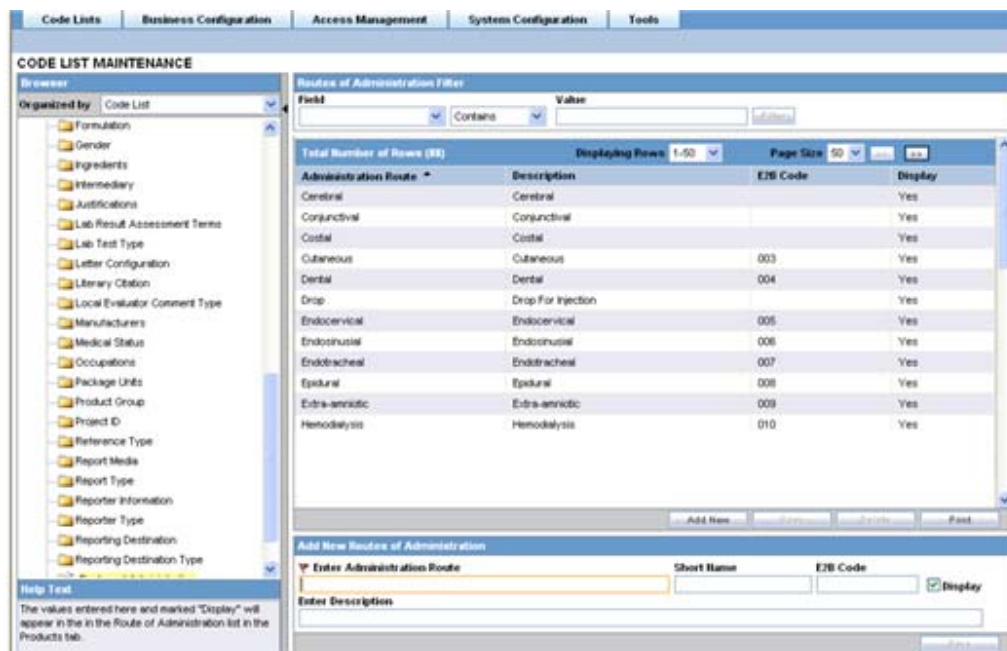
1. Select the **Agency Name** (or row) of the reporting destination displayed under **Total Number of Rows** that needs to be modified. The **Modify** section is populated with information about the selected code list.
2. You may use the **Reporting Destination Filter** to make your search specific to an SMTP. The filtering criterion is essential as it helps you to search for specific items.
3. Select the appropriate **Field** as the filtering criteria from the drop-down list.
4. Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.

5. Enter the search criteria in **Value**
6. Click **Filter** to apply the selected criteria. This displays the search results under **Total Number of Rows**.
 - Tip:** You can alternatively click **Add New** to create a new SMTP.
 - Click **Copy** to make an editable copy of an existing SMTP.
 - Click **Delete** to delete a selected SMTP.
 - Click **Print** to print the selected information as a PDF.
7. Enter the email address of the sender under the **From** field.
8. Enter the email addresses to send email as CC under the **To** field. Multiple e-mail addresses must be separated by a comma (,), and not by a semi-colon (;). If you separate the email addresses by a semi-colon, the transmission service will fail.
9. Enter the email addresses to send email as BCC under the **BCC** field. Multiple e-mail addresses must be separated by a comma (,), and not by a semi-colon (;). If you separate the email addresses by a semi-colon, the transmission service will fail.
10. Click the **Delivery Receipt** checkbox to receive a delivery receipt.
11. Click the **Read Receipt** checkbox to receive a read receipt.
12. Click **Save** to save the changes made.
13. Click **Save** to save the changes made.

Configuring Routes of Administration

This screen enables you to configure the Route of Administration information. This describes the route of drug administered to the patient. This data is reflected in Expedited and Periodic regulatory reports.

- The values entered here and marked under **Display** appear in the in the **Route of Administration** list on the **Products** tab.
- Select Code Lists -> Argus to view the Code List Maintenance screen.



Tip: The code list items are displayed in the left-panel. Click on the required Code List folder to be configured. The details of this code list item appear in the right panel.

Click on the **Routes of Administration** folder in the left panel. The associated data appears in the **Total Number of Rows** section in the right panel.

Field Descriptions

The following table describes the fields associated with this section.

Field/Control Name	Description
Administration Route	Displays information about the route of administration. It displays information about how the drug was administered. This is a required field.
Short Name	Displays the short name of the administrator route.
Description	Displays a description of the administrator route.
E2B Code	Displays the E2B Code of the administrator route.
Display	Enables the user to display the record in the Administrator Route in the Products screen.

Use the following procedure to configure routes of administration.

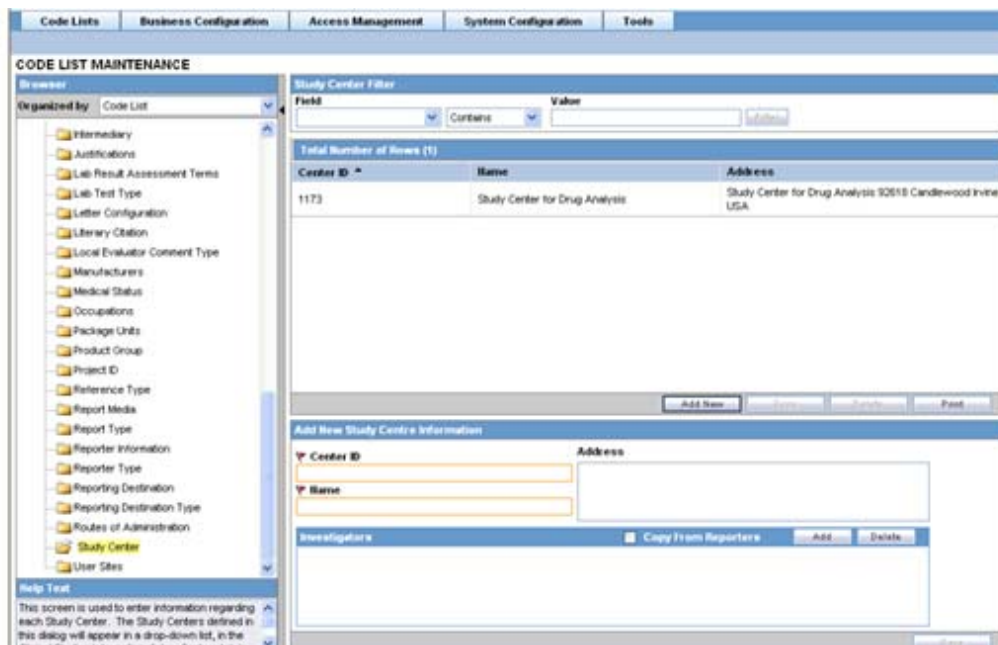
1. Click the **Administration Route** (or row) to view the details associated with the administration route. The details appear in the **Modify Administration Route** section.
2. You may use the **Routes of Administration Filter** to make your search specific to a route. The filtering criterion is essential as it helps you to search for specific items.
3. Select the appropriate **Field** as the filtering criteria from the drop-down list.

4. Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.
5. Enter the search criteria in **Value**.
6. Click **Filter** to apply the selected criteria. This displays the search results under **Total Number of Rows**.
 - Tip:** You can alternatively click **Add New** to create a new route.
 - Click **Copy** to make an editable copy of an existing route.
 - Click **Delete** to delete a selected route.
 - Click **Print** to print the selected information as a PDF.
7. Enter information about the administration route in the **Enter Administration Route** field.
8. Enter a short name about the administration route in the **Short Name** field.
9. Enter the E2B Code of the administration route in the **E2B** field.
10. Select the **Display** checkbox to display the record in the Add field in the Products screen.
11. Enter the description about the administration route in the **Enter Description** field.
12. Click **Save** to save the changes made.

Configuring Study Center

This screen enables you to configure the Study Center information. This screen is used to enter information regarding each Study Center. The Study Centers defined in this dialog appear on a drop-down list in the **Clinical Studies Information** dialog under the **Centers** tab in **List Maintenance**. You can create a Study Center with the same Center ID but with a different name and address. When you select the studies in the Study Look and Center Lookup in the Console, the system concatenates the Center Name (Center ID) in the look-up dialog.

- Investigators for each Center can also be added via this dialog.
- Select Code Lists -> Argus to view the Code List Maintenance screen.
- Click on the **Study Center** folder in the left panel. The associated data appears in the **Total Number of Rows** section in the right panel.



Tip: The code list items are displayed in the left-panel. Click on the required Code List folder to be configured. The details of this code list item appear in the right panel.

Field Descriptions

The following table lists and describes the fields associated with this section.

Field/Control Name	Description
Center ID	Enables the user to enter the Center ID.
Name	Enables the user to enter the name of the center.
Address	Enables the user to enter the address of the center.
Copy from Reporters	Enables the user to copy the information from Reporters.
#	Displays the row count of the number of investigators.
Investigator	Enables the user to enter the name of the investigator.
Phone	Enables the user to enter the phone number of the investigator.
Fax	Enables the user to enter the fax number of the investigator.
Notes	Enables the user to enter comments or remarks.

Use the following procedure to configure study center.

1. Click the **Center ID** (or row) to view the details associated with the administration route. The details appear in the **Modify Study Center** section.
2. You may use the **Study Center Filter** to make your search specific to a center. The filtering criterion is essential as it helps you to search for specific items.
3. Select the appropriate **Field** as the filtering criteria from the drop-down list.
4. Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.

5. Enter the search criteria in **Value**.
6. Click **Filter** to apply the selected criteria. This displays the search results under **Total Number of Rows**.
 - Tip:** You can alternatively click **Add New** to create a new center.
 - Click **Copy** to make an editable copy of an existing center.
 - Click **Delete** to delete a selected center.
 - Click **Print** to print the selected information as a PDF.
7. Enter the ID of the center in the **Center ID** field.
8. Enter the name of the center in the **Name** field.
9. Enter the address of the center in the **Address** field.
10. Select the **Copy from Reporters** checkbox to copy the information from Reporters.
11. Enter the name of the investigator in the **Investigators** field.

Tip: Click **Add** to add a new investigator. Click **Delete** to delete a selected investigator record.

12. Enter the phone number of the investigator in the **Phone** field.
13. Enter the fax number of the investigator in the **Fax** field.
14. Enter comments, if any, under the **Notes** field.
15. Click **Save**.

Configuring Holiday Calendar

This screen enables you to configure the Holiday Calendar information. The Code List allows the user to define holidays at country level.

The screenshot shows the 'CODE LIST MAINTENANCE' application window. At the top, there are tabs for 'Code Lists', 'Business Configuration', 'Access Management', 'System Configuration', and 'Tools'. The main area is titled 'CODE LIST MAINTENANCE' and contains a 'Browser' pane on the left with a tree view of code lists. The 'Holiday Calendar' folder is selected. To the right of the browser is a 'Holiday Calendar Filter' section with a 'Field' dropdown, a 'Value' input field, and a 'Filter' button. Below the filter is a table header for 'Total Number of Rows (0)' with columns: 'Holiday Name', 'Date', 'Description', and 'Country'. The table body is empty, showing 'No records to display.'. At the bottom of the filter section are buttons for 'Add New', 'Copy', 'Delete', and 'Print'. Below the table is the 'Add New Holiday Calendar' form, which includes a 'Holiday Name' field, a 'Date' field, and a 'Country' field with 'Add' and 'Delete' buttons. A 'Description' text area is also present. At the bottom right of the form is a 'Save' button. A 'Help Text' box at the bottom left of the browser pane states: 'The values entered here will be used for the report due date adjustment in the Reporting Destination.'

The Country of Reporting Destination will be matched with the Country in the Holiday Calendar to identify the holidays to be adjusted for the Reporting Destination.

Go to Code Lists > Argus to view the Code Lists page and click the Holiday Calendar folder in the left panel.

The associated report appears in the Total Number of Rows section in the right panel.

Tip: The code list items are displayed in the left-panel. Click on the required Code List folder to be configured. The details of this code list item appear in the right panel.

Field Descriptions

The following table describes the fields associated with this section.

Field/Control Name	Description
Holiday Name	This field displays the unique name for the holiday name.
Date	This field displays the date on which the holiday has been scheduled.
Description	This field displays a description of the holiday.
Country	This field displays the name of the country (or countries) with which the holiday is associated.

Use the following procedure to configure study center.

1. Click the **Holiday Name** (or row) to view the details associated with that Holiday Calendar. The details appear in the **Modify Holiday Calendar** section.
2. You may use the **Holiday Calendar Filter** to make your search specific to a Holiday Calendar record. The filtering criterion is essential as it helps you to search for specific items.
3. Select the appropriate **Field** as the filtering criteria from the drop-down list.
4. Once you have selected the **Field**, you can specify whether your search should **contain** or **start with** specific alphabets.
5. Enter the search criteria in **Value**.
6. Click **Filter** to apply the selected criteria. This displays the search results under **Total Number of Rows**.

Tip: You can alternatively click **Add New** to create a new Holiday Calendar record.

- Click **Copy** to make an editable copy of an existing Holiday Calendar record.
 - Click **Delete** to delete an existing Holiday Calendar record.
7. Enter the Holiday Name for the Holiday Calendar.
 8. Enter the Date for the record.
 9. Enter the Country (or countries) with which the holiday must be associated.
 10. Enter the Description for the Holiday Calendar record.
 11. Click **Save**.

Other Code List Items

The following table lists and describes additional code list items that you should be aware of.

Code List Item	Description
Accidental Exposure	Enables you to capture Accidental Exposure information. Accidental Exposure is in the Dosage regimen section of the Products tab as a drop-down list.
Action Taken	Enables you to capture Action Taken information. Action Taken information is required to capture information about steps taken when an adverse drug event occurs. The values that you enter in this field are read-only, and appear in the Dosage Regimen section on the Action Taken drop-down in Case Form > Products tab.
Action Type	Enables you to capture Action Type information that describes the action type required for the case. Values entered in this field are read-only, and appear in the Code/Description list of the Activities tab. Go to Code List Maintenance > Code List > Argus and click Action Type in the browser tree.
Age Group	Enables you to capture Age Group information. An Age Group is the range of lower and upper age limits. Patients are categorized in different age groups. This data appears in Expedited and Periodic regulatory reports. The values that you enter in this field appear on the Patient Information Screen, and in the Age Group drop-down list. The Range values that you specify for new age groups must not contain numbering gaps or overlapping values.
Age Unit	Enables you to capture Age Unit information. An Age Unit displays time in periods such as Year, Month, Day, Hours, and so on. This data appears in the Expedited and Periodic regulatory reports. It also appears in the Age Unit drop-down, Gestation Period unit, and Device Age unit fields on the Patient Information screen, as per the settings made to the Age unit, Gestation Period unit, and Device Age unit flags in the Age unit codelist.
Always Serious Term List	Enables you to select the report types you would like the always serious to run against. You can select specific Product Families to have the always serious terms run against.
Anatomical Location	Enables you to capture information about the location where vaccinations are given. This data appears in the expedited and periodic regulatory reports. The values that you enter in these fields appear on the Anatomical Location drop-down list on the Vaccine screen.
Attachment Classifications	Enables you to capture the attachment classification that is used to describe attachment types. The values that you enter in these fields appear in the Attachment Classification section on the Additional Information screen. Attachment Classification that are marked as 'E2B Additional Doc' can be configured to be sent as attachments while transmitting E2B (R2) and E2B (R3) reports.
Attachment Keywords	Enables you to capture information about the attachment keywords that are used to define an attachment type. The values appear in the Attachment Keywords section on the Additional Information screen.
Birth Type	Enables you to capture birth type information when capturing pregnancy information. This data appears in multiple regulatory reports and in the Birth Type drop-down list on the Pregnancy information screen.

Code List Item	Description
Case Classifications	Enables you to capture Case Classification to help categorize cases. This information does not impact any report or screen, but is used during case searches to narrow the results set.
Causality Category	Enables you to capture information about the causality type. This data appears in expedited and periodic regulatory reports and on the Event Causality drop-down list in the Event Assessment section on the Event screen.
Causality Method	Enables you to capture Causality Method information. It appears on the Case Form Event Assessment tab. The E2B report uses this information to determine the drug assessment method.
Causality Source	Enables you to capture Causality Source information. It appears on the Case Form Event Assessment tab. The E2B report uses this information to determine the drug assessment source.
Clinical Reference Type	Enables you to capture information about the clinical reference type. The Clinical Reference Type appears as a drop-down list in Study Configuration.
Condition Type	Enables you to capture information about the condition of the patient such as historical condition, current condition, historical drug, illness at the time of vaccination etc.. This data appears in expedited and periodic regulatory reports and in the Condition Type drop-down list on the Other Relevant History screen.
Contact Type	Enables you to capture information about the type of contact (such as Follow-up, Investigator). The values appear in the Contact Type drop-down list in the Contact Log section of the Activity Tab.
Countries	<p>Enables you to capture information about the country where the adverse event occurred. If you enter A2, A3, or the numeric country code, the system automatically populates the Country field with the name of the country.</p> <p>The 'Countries Grouping' field enables you to create a group of countries. For example, to group all European Union member countries, you first create a country called 'EUROPEAN UNION'. You then select a European Union member country in the countries table, type 'EUROPEAN UNION' in its Countries Grouping field, and then click Save. Repeat the process for all European Union member countries. On screens where you need to enter a list of all European Union members, you can type European Union, and all countries in this group will be entered automatically.</p> <p>The 'Group 2 Country' checkbox enables you to add a Group 2 Country. This is required when the Due Date for expedited reports differs from country to country, as per their regulations.</p> <p>For Group 1 countries, the Due Date is based on the Aware Date received globally for the case. For Group 2 countries, the Due Date is based on the aware date when the affiliate or a company representative of that country received information about the case.</p>

Code List Item	Description
Date Ranges	<p>Enables you to capture date range information as follows:</p> <ul style="list-style-type: none"> ■ Description -- Enables you to enter a description of the date range. ■ Duration -- Enables you to specify the exact duration as opposed to a range of dates. Must be used in conjunction with Amount and Units. When you select "Duration," the system disables the "Range" radio button. ■ Amount -- The numeric value that specifies the length of the time period when combined with a value selected from the Units drop-down list (such as days, weeks, months, years, etc.) ■ Units -- The unit of the duration (such as days, months, years) ■ Range -- Enables you to select a specific range of dates. Must be used in conjunction with the Start and End fields. When you select "Range," the system disables the "Duration" radio button. ■ Start -- The initial date of the date range. ■ End -- The last date of the date range.
Delivery Types	<p>Enables you to capture information about the type of delivery that occurred during pregnancy. This data appears in expedited and periodic regulatory reports and on the Delivery Types drop-down list on the Pregnancy Information screen.</p>
Device Preliminary Comments	<p>Enables you to capture comments about medical devices. Device Preliminary Comments appear on the Product screen when the user selects the Device option.</p>
Device Subcomponents	<p>Enables you to capture information about subcomponents that are part of a medical device. This information appears on the Product screen when the user selects the Device option.</p>
Device Type	<p>Enables you to capture information about patient device types. This data appears in expedited and periodic regulatory reports.</p>
Dosage Frequency	<p>Enables you to capture information about how often medication is given (such as daily, bid, weekly, etc.) This information appears on the frequency drop-down list on the Products screen.</p> <ul style="list-style-type: none"> ■ Frequency -- Enables the user to specify how often the dose is given. ■ Number of doses per day -- Enables the user to specify the number of doses administered each day. ■ Number of separate dosage -- Enables the user to define the dosage verbatim. ■ Number of units in the interval -- Enables the user to define the dosage verbatim. ■ Definition of Interval -- The length of time between doses such as year, month, day, week (default), hour, minute.

Code List Item	Description
Dosage Unit	<p>Enables you to capture dosage units information. This information is required when capturing the quantity of drug on sale and also appears in expedited and periodic reports.</p> <ul style="list-style-type: none"> ■ Unit Name -- The name of the dosage unit. ■ E2B Code -- The E2B code associated with the Dosage Unit. ■ Dosage Unit -- When checked, it indicates that the current item is the dosage unit. ■ Lab Test Unit -- When checked, it indicates that this is a lab test unit. ■ Display -- When checked, it indicates that the Unit Name is displayed in the application. <p>A new <i>Strength Unit</i> column has been introduced. Check the Strength Unit checkbox to capture strength unit information about the Dosage unit.</p> <p>For more information on the Factory data for Dosage Units codelist, see the <i>Argus_Safety_8.1.2_CaseForm_Console_Updates_Summary.xls</i>.</p>
Ethnicity	Enables you to capture Race information of the patients. This information appears in periodic regulatory reports and eVAERS reports.
Evaluation Reason	Enables you to capture information about why the product is being evaluated. This information appears in the Evaluation Reason list on the Case Form > Products tab.
Event Frequency	Enables you to capture information about the frequency of the event. It includes categories such as intermittent, continuous, and single episode. The values entered in this field appear in the Event Frequency drop-down list on the Event Information screen.
Event Intensity	Enables you to capture information about the intensity of the adverse event and includes categories such as mild, moderate, and severe. The values that you enter on this screen appear on the Event Intensity drop-down list on the Event Information screen.
Event Outcome	Enables you to capture event outcome information such as Fatal, Abortion due to AE/Infection, and Recovered. This data appears in expedited and periodic regulatory reports and on the Event Outcome drop-down list on the Event Information screen.
Fetal Outcome	Enables you to capture information about fetal outcome and includes information such as abnormal development or pre-natal complications. This data appears in expedited and periodic regulatory reports. The values entered here appear on the Fetal Outcomes drop-down list on the Pregnancy Information screen.
Formulation	Enables you to capture information about the formulations (cream, drop, capsule, etc.) available for a product. The values that you enter here, appear on the Formulation drop-down list on the Product screen.
Gender	Enables you to capture gender information. This information appears in expedited and periodic regulatory reports.
Ingredients	Enables you to capture information about the ingredients in the product. This includes the ingredient, the concentration, and the units of ingredients used to make the product. This information appears in expedited and periodic regulatory reports.
Intermediary	Enables you to capture information about intermediaries such as sales representative, licensee, regulatory authority or local affiliate. The values that you enter here, appear on the Intermediary drop-down list on the Reporters screen.

Code List Item	Description
Interval Units	This codelist is used to maintain the interval units that are used as units for Age, Duration, etc.
Justifications	Enables you to capture justification information. You can enter reasons for overriding system determinations in the Justifications dialog box. The values that you enter here, appear in the Action Justification dialog.
Lab Assessment Terms	Enables you to capture the lab result assessment terms that define the terms that describe the patient's results on various lab tests (such as elevated, depressed, etc). This data is reflected in expedited and periodic regulatory reports. The values that you enter here, appear on the Lab Result Assessment Terms drop-down list on the Laboratory Data screen.
Lab Test Type	Enables you to capture the lab test type. This defines test type and whether it has normal, high, or low values. It can be coded as defined in the MedDRA dictionary. The values that you enter here, appear on the Lab Test drop-down on the Patient screen.
Lab Test Units	This codelist is used to maintain the units of measures used in Lab test.
Languages	This codelist is used to maintain the ISO codes of the languages in which text data entry can be made.
Literary Citations	Enables you to enter information about literary citations.
Local Evaluation Comment Type	Enables you to capture the category of a local comment such as French, German, English, etc. The values that you enter here, appear in the Analysis, Local Comment type.
Location	This codelist is used to maintain the Anatomical locations in which Vaccines are administered.
Manufacturer	Enables you to capture information about the product manufacturer. Manufacturer is required while capturing, adding, or modifying information on manufacturer sites. This data appears in expedited and periodic regulatory reports and on the Manufacturer drop-down list on the Product Configuration screen.
Medical Status	Enables you to capture medical information about patient status. This data appears in both the expedited and periodic regulatory reports. The values that you enter here appear on the Medical Status drop-down list.
Message Type	Enables you to enter information about each E2B message type. The system uses the defined message types when it creates an E2B file.
Nature of Event	Enables you to capture information about the type of adverse event that occurred.
Occupations	Enables you to capture information about patient and reporter occupations such as physician, regulatory agent, and journalist. This data appears in both expedited and periodic regulatory reports. The values that you enter here, are marked as ICH Occupation, and appear in the Reporter's Occupation drop-down list on the General Screen.
Package Units	Enables you to capture information about product packaging. The package units define the number of units in a package.
Product Group	Enables you to capture information about a specific Product Group. Users can use the Product group field to categorize Product Families based on therapeutic area. The values that you enter here appear in the drop-down list associated with the Project Group field of the Product Family.

Code List Item	Description
Project ID	Enables you to capture project ID information used to group similar studies under a single project. The values that you enter in this field appear on the Project ID field drop-down on the Study Configuration.
Purchased With	This code list is used to maintain the Funds from which Vaccine was purchased.
Reference Types	Enables you to capture reference type information and defines a list a reference types such as Parent-Child Link, Patient ID, etc. The values that you enter here, appear in the Type drop-down in the References section on the Additional Information tab.
Relation	This codelist is used to maintain the Reporter relation to the Patient.
Report Media	Enables you to capture Report Media information. The values that you enter appear on a drop-down field in the Reporter Information section.
Report Types	<p>Enables you to capture information about report types. The report type describes the type of report and the abbreviation associated with the specific type. This data appears in expedited and periodic regulatory reports. The values that you enter here, appear on the Report Type drop-down list on the General Screen.</p> <p>The <i>Considered cases for report type</i> drop-down list determines whether a case is considered marketed or investigational for a given reporting destination. When creating a new case report type, the selected value is Marketed by default.</p>
Reporter Information	Enables you to capture reporter information such as First Name, Last Name, Occupation, and so on.
Reporter Type	Enables you to capture information about the person reporting the adverse event and includes categories such as lawyer, nurse, doctor, etc. The values that you enter here, appear on the Reporter Type drop-down list on the Product screen.
Reporting Destination Type	Enables you to capture information about the reporting destination. The values that you enter here, appear on the Reporting Destination configuration.
Routes of Administration	Enables you to capture information about how a drug is administered to a patient such as auricular, cutaneous, dental, and so on.
Study Center	<p>Enables you to capture information about the study centers. Values entered here appear on a drop-down in the Clinical Studies Information dialog and on the Centers tab in List Maintenances. You can also add investigators for each center.</p> <p>You can create a study center with the same center ID but with a different name and address.</p>
Vaccinated At	This code list is used to maintain the Vaccination Facility Type information.

Formulation Factory Data

The following table provides information about the Formulation Factory Data:

Formulation ID	Formulation	Formulation Name	Formulation Symbol
38	Aerosol (Spray and Inhalation)	Aerosols	AER

Formulation ID	Formulation	Formulation Name	Formulation Symbol
13	Alternative Form		
23	Cachet (including wafer)	Cachet	CTS
2	Capsule	Capsules	CAP
24	Chewable Tablet	Chewing Tablet	CTB
25	Drop	Drops	DRO
32	Dusting Powder	Dusting Powders	DPO
39	Ear Drops	Ear Drops	EDR
8	Effervescent Tablet		
47	Enema	Enemas	ENM
21	Enteric Table	Enteric-coated dosage forms	ENT
49	External Use		
12	Extra Formulation	External Preparations of Uncertain Dosage Form	EXT
40	Eye Drops	Eye Drops	EED
41	Eye Ointment	Eye Ointments	EOI
20	Grain	Granules	GRA
18	Granule	Fine Granules	FGR
46	Implantation	Inserting Preparations	IMP
43	Inhalation Gas	Gas Inhalant	INS
6	Infusion	Infusing Preparations	INF
9	Inhaler	Inhalants	INH
5	Injection	Injections	INJ
48	Jelly	Jellies	JEL
11	Liquid	External Liquids	LIQ
33	Lotion (except lotion for eye)	Lotions	LOT
28	Lozenge (troche and candy too)	Lozenges	LOZ
45	Mouthwash	Throat Washings	MWH
17	N/A		
42	Nasal Drops/Spray	Nose Drops	NDF
34	Ointment/Cream	Ointments/Creams	OIT
31	Oral Drug Unspecified Form	Oral Preparations of Uncertain Dosage Form	POR
4	Patch		
26	Pill (except tablets)	Pills	PIL
19	Powder (except DPO)	Powders	POW
35	Shampoo	Shampoos	SHP
22	Slow Release Capsules	Slow-release Capsules	SRC

Formulation ID	Formulation	Formulation Name	Formulation Symbol
30	Slow Release Granule	Slow-release Granules	SRG
29	Slow Release Tablet	Slow-release Tablets	SRT
27	Solution (except Syrup)	Solutions for Oral Use	SOL
44	Spin Cap	Spin Cap	SPC
36	Spray (except Inhalation)	Sprays	SPR
3	Suppository	Rectal Suppositories	SUP
7	Syrup	Syrups	SYR
1	Tablet	Tablets	TAB
37	Tape (including Poultice)	Tapes	TAP
16	Unknown	Uncertain	XXX

Configuring Code Lists > Flexible Data Re-Categorization

The Flexible data re-categorization feature allows Argus Safety and its associated applications such as Argus Mart and Argus Insight to handle the code list values in a much more flexible manner, as compared to the previously existing Argus Safety Code List database design.

Working with Flexible Data Re-Categorization

The Flexible Data Re-Categorization feature allows applications and customers to store and maintain all types of code list values in a single flat database table structure which shall be easier to maintain. This code list data storage design can be leveraged to easily add new and custom code lists or values by applications as well as customers without adding new database tables and columns. This database structure was added in previous release of Argus Safety.

Argus Console provides a user interface that displays values for different code list languages for the flexible data re-categorization code list feature. This user interface helps add and remove custom languages for an existing code list, present in the flexible data re-categorization code list tables and also the flexibility of adding new code list items through this User Interface (UI).

However, this UI does not allow users to perform any modification for the languages which are maintained via the Console Code List feature. Any changes done to the values through this user interface are audit logged.

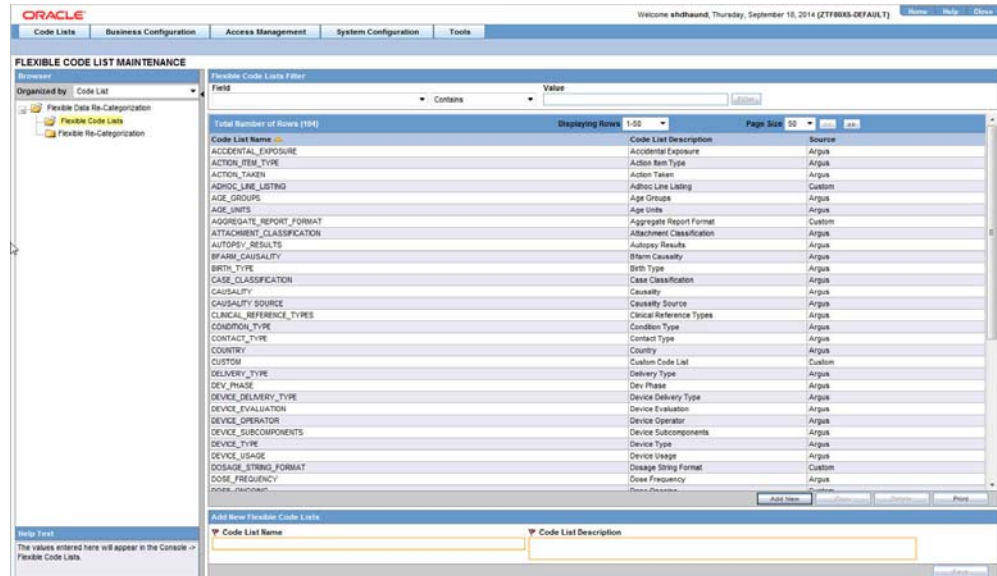
The Flexible Data Re-Categorization feature allows administrators to manage and display the existing and new code list items.

Flexible Code Lists

To access Flexible Data Re-Categorization:

1. Go to Argus Console > Code Lists > Argus > Flexible Data Re-Categorization.

The following screen is displayed:



The following table describes the fields associated with this section:

Field Name	Description
Code List Name	This is the unique name of code list which can be used in the application and reporting for fetching the values of a code lists. This is mostly derived from the source Argus Safety code list names. However, it can be different in some scenarios as per the customer need.
Code List Description	This is the description of code list which can be used to define the purpose of this code list.
Source	Argus: All the code lists which are part of Argus Safety factory configuration and can be edited using standard Argus console code list UI show the source as 'Argus'. Custom: Any code lists added as part of factory data which cannot be modified from Argus console standard code list UI are considered as custom. Any code list added by customers has source as 'Custom'.

2. This page is used to add new values or view existing code list values in the code lists.

Click **Add New** to add a new flexible code list item.

To make any changes, users can select a code list, modify values in the given text boxes, and save those changes for modification.

Click **Delete** to delete an existing flexible list item.

Click **Copy** to copy an existing flexible list item.

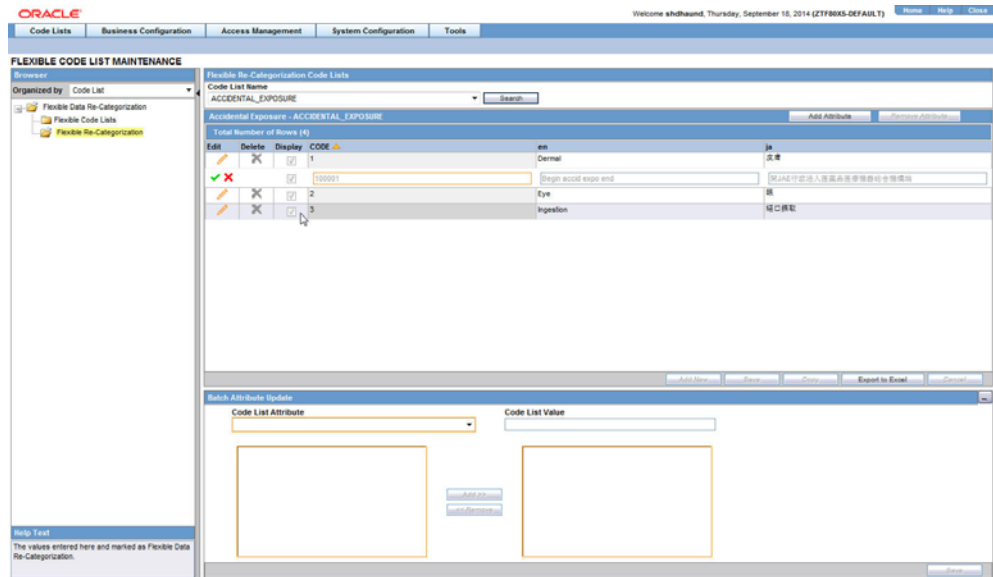
3. Click **Save** to save the new or existing flexible code list item information.

Flexible Re-Categorization

To access Flexible Re-Categorization:

1. Go to Argus Console > Code Lists > Argus > Flexible Re-Categorization.

The following screen is displayed:



The following table describes the fields associated with this section.

Field Name	Description
Code List Name	This is a drop-down list that displays all the available flexible code lists for selection.
Attribute Name	<p>This is the language Decode context for selected code list which can have language code and other properties of code lists.</p> <p>The following are possible values for this field for the factory data rows which will be populated based on the current code list factory data. Customer can add more language/type values for the new code list items that they create from flexible re-categorization screen, based on their usage:</p> <ul style="list-style-type: none"> i. en: English display value for a code list item ii. jp: Japanese display value for a code list item iii. E2B: E2B code value for this code list item iv. RPT: Display value for Reports v. ISOA2: A2 country code for the country code list items vi. ISOA3: A3 country code for the country code list items vii. EN_ABBRV: This is used for defining abbreviation values. viii. SM: This decode context is used by Argus Mart while populating data into the SM tables. ix. UCUM_CODE: UCUM code value for this code list item. This is used in E2B (R3) and eVAERS reports. x. E2B_R3: E2B (R3) value for this code list item. This is used in E2B (R3) and eVAERS reports. xi. VAERS_CODE: VAERS Code value for this code list item. This is used in eVAERS and VAERS report mapping. xii. NCI_CODE: NCI code value for this code list item. This is used in eVAERS reports.
Code List Display Value	This the re-categorized display value for the code. This display value shall be based on a code list, code, and language combination.

Field Name	Description
Add Attribute	Enables you to add a language attribute.
Remove Attribute	Enables you to remove a language attribute.
Attribute Name	This is the language Decode context for selected code list which can have language code and other properties of code lists.
Code	This is the first column in the grid for all flexible code lists. This column displays the internal id for the existing 'Code' list value. For custom code list, the application always populates the code columns with system generated unique sequence value for the selected code list. It is possible for customers to provide a custom 'Code' value for any of the new rows. This value is always unique for a code list.
<All Language Attributes>	All the language attributes are displayed as a new column in the grid with Primary attribute being the first one after the Code column.
Right-click > Make Primary	Allows you to make the selected language attribute as the primary attribute. The primary attribute column is moved as the first attribute in the grid after the 'Code' column. This configuration is available every time the user opens the same flexible code list.
Right-click > Make Preferred	Allows you to mark the selected cell values corresponding to selected language attribute as Preferred in the database. Preferred values are displayed with an asterisk (*) in the grid for easy identification. At any given time, only one value can be marked as preferred within matching values for a language attribute.
Export to Excel	Enables you to export all the values of selected code list into an excel file.
Batch Attribute Update	A collapsible interface, this option displays the list of all attributes available for the selected code list in Flexible re-categorization screen. It also provides a text box called Code List Value, where users can enter the required display value of the code list for the selected attribute.

- This page is used to add new values or view existing code list values in the code lists.
- Click **Edit**. The grid cells of corresponding row become editable for all the attributes added in that code list by the user.

On clicking **Edit**, a green tick mark is displayed, along with a red colored, cross icon.

Click the green tick mark to temporarily save the grid values (until saved into database by clicking Save button). The selected row comes out of Edit mode.

Click the red colored cross icon to discard any changes made to the selected row. The selected row comes out of Edit mode.

On changing the value of a preferred cell, its preferred status is removed upon saving the grid values.

- Click **Delete** to allow the users to delete an entry from the flexible code lists. The Delete icon is enabled for only custom code lists, for which protected flag is set to 0 in CODE_LIST_CODE_ATTRIBUTES table. Click this icon to delete all the attribute values corresponding to the selected row from the database.
- The **Display** checkbox is checked by default (except for hidden entries), for a new row added into the flexible code list.

6. Click **Save** to save all the changes made on flexible code list screen.

The following Code Lists are used/provided for BIP Aggregate Reports:

1. **REPORT_TEMPLATE**: This code list is used for managing various BIP report templates available in the system (OOB + Custom) and assign an Argus periodic configuration (ICH PSUR or CTPR) using which user want to execute this report template. Whenever a new report template is added in BIP, this code list should be modified for providing report template name, its path and corresponding Argus configuration.
2. **ADHOC_LINE_LISTING**: All the LISTNAME added in adhoc_line_listing code list are available in the UD Summaries tab of periodic reports configuration for attaching the memorized reports to a particular line listing section of periodic report. User can renames these using flexible re-categorization user interface. System provides four adhoc line listings by default which can be increased using this code list if you have more adhoc line listing sections in your report. Once configured, use Argus UI for attaching the UD summaries with line listings of your custom report.
3. **SOC_DISPLAY_ORDER**: Use this code list to reorder the printing of SOC in various tabulations.
4. **AGGREGATE_REPORT_FORMAT**: Use this code list to define the report formats which you want to use with BIP reports execution. Make sure to use only those formats which are supported by BI Publisher.
5. **DOSAGE_STRING_FORMAT**: This code list can used to restrict/add the dosage string formats which should be available while BIP report execution. More dosage string formats can be added with the help of custom code. The following dosage string formats are provided out of box which print values for dosage string as mentioned in the EN attribute.

Code	EN
Do	Dose
DoFo	Dose, Formulation
DoFoFr	Dose, Formulation, Frequency
DoFoFrRt	Dose, Formulation, Frequency, Route
DoFoRt	Dose, Formulation, Route
DoFr	Dose, Frequency
DoRt	Dose, Route

6. **UNIQUE_PATIENT_ID_FORMAT**: This code list is used to restrict/add the dosage string formats which should be available while BIP report execution. More dosage string formats can be added with the help of custom code. The following dosage string formats are provided out of box which print values for dosage string as mentioned in the EN attribute.

Code	EN
CePt	Center, Patient
InPt	Investigator, Patient
Pt	Patient

Code	EN
StCeInPt	Study, Center, Investigator, Patient
StCePt	Study, Center, Patient
StCnCeInPt	Study, Country Name, Center, Investigator, Patient
StCnCePt	Study, Country Name, Center, Patient
StCoCeInPt	Study, Country ISO Code, Center, Investigator, Patient
StCoCePt	Study, Country ISO Code, Center, Patient
StInPt	Study, Investigator, Patient

7. LABELING_ALGORITHM: Use this code list to define new labeling algorithm with the help of custom code. Please see labeling algorithms for more information on out of the box algorithms.
8. EVENTSERIOUSNESS: This code list is provided as part of factory data and is used for printing the actual value of seriousness defined against a serious event.
9. ORGAN_IMPAIRED_HLT: This code list is added for defining the high level terms which needs to be scanned through to find out if event reported falls under organ impairment section or not. This can be used in custom reports.
10. BIP_DFLT_VALUES: This code list used for configuring the default values for some of the important fields which are used in various grouping and tabulations. For example, how to handle/print an event without and SOC. Value configured in this code list corresponding to SOC will be used in PBRER/DSUR tabulation for events with undefined SOC.

The following Code Lists are used in reports, such as E2B(R3), eVAERS, VAERS, and eMDR reports:

Code List	Description
AGE_UNIT	This code list enables you to capture Age Unit information. An Age Unit displays time in periods such as Year, Month, Day, Hours, and so on with E2B and UCUM code information.
CAUSALITY_SOURCE	This code list lets you capture the source from which the causality information was derived, along with the EU_CODE attribute. For each custom value that you add, you must enter the value of the associated EU_CODE attribute in order to populate this info in the EMA E2B report. The values that can be entered for the EU_CODE attribute need to be in the range 1-6, as permissible values for EVCTM are 1-3, and permissible values for EVHUMAN are 3-6
CAUSALITY_CATEGORY	This code list lets you capture the category of the causality information with the EU_CODE attribute.
CAUSALITY_METHOD	This code list lets you capture the method by which the causality information was derived.
* CODE_SYSTEM	For the current release, this codelist is not used in the application (Case Form, Reports).
COUNTRY	This code list maintains the list of Countries with the ISO A2, ISO A3, and EEA attributes.
DEVICE_AGE_UNIT	This code list enables you to capture Device Age Unit information. Device Age Unit displays time in periods such as Year, Month, Day, and Hours with eMDR code information.

Code List	Description
DOSE_UNITS	This code list is used to maintain the units of measures used in Dose with E2B and UCUM code information.
ETHNIC_GROUP	This code list is used to maintain information about Ethnicity data of Patient or Parent such as Hispanic or Latino, Not Hispanic or Latino with NCI Codes information.
ETHNICITY	This code list is used to maintain Race information along with NCI Codes information.
EVALUATION_REASON	This code list is used to maintain the List of reasons for not evaluating devices with NCI Codes information.
FORMULATION	This code list enables you to capture information about the formulations (cream, drop, capsule, and so on) available for a product with NCI Codes information.
GENDER	This code list is used to maintain the Gender with E2B and NCI Codes information.
INTERVAL_UNITS	This code list is used to maintain the interval units that are used as units for Age, Duration, and so on.
LAB_TEST_UNITS	This code list is used to maintain the units of measures used in Lab test.
LANGUAGES	This code list is used to maintain the ISO codes of the languages in which text data entry can be made.
LOCATION	This code list is used to maintain the Anatomical locations in which Vaccines are administered.
LOCATION_EVENT_OCCURRED	This code list is used to maintain the locations where the events occurred. This data is used in the eMDR and the MedWatch Device report.
MEDIA_TYPE	This code list maintains the file types that can be sent as attachments in E2B(R3) reports with the ICH, FDA, EMA, and PMDA attributes to indicate if attachment types are allowed for these agencies.
MILITARY_STATUS	This code list is used to maintain the details of the Military status of the Patient such as Active Duty, Reserve, National Guard, TRICARE Beneficiary, and Other with NCI Codes information.
NULL_FLAVOR	This code list stores the different null flavors such as UNK, NA NASK, and ASKU. Null flavor sets are attributes in the Null Flavor codelist which are used to create sets with various combinations of Null Flavors. The Null flavor set can be assigned to Case Form fields in Field Properties Configuration and users can select the Null flavors associated with a Null Flavor set as a part of Case Form data.
PRODUCT_IDENTIFIER_TYPE	This code list identifies the type of Product name being used such as Medicinal Product Identifier (MPID), Pharmaceutical Product Identifier (PhPID).
PRODUCT_NAME_PARTS	This code list specifies the name of a product as a separated component such as container name, form name, device name, invented name, scientific name, trademark name, intended use name, scientific name and so on.
PURCHASED_WITH	This code list is used to maintain the Funds from which Vaccine was purchased.
RELATION	This code list is used to maintain the Reporter relation to Patient.
REPORTER_INFORMATION	This code list is used to maintain the Reporter information such as First Name, Last Name, and so on.

Code List	Description
REPORTER_OCCUPATION	This code list is used to maintain the Occupation with NCI Codes and Device Operator information.
ROUTE	This code list enables you to capture information about how a drug is administered to a patient such as auricular, cutaneous, dental and so on with E2B and NCI Codes information.
SPANISH_STATES	This code list lets you capture the states of Spain with the STATE_CODE attribute.
SPECIALIZED_PROD_CATEGORY	This code list is used to maintain details of the Product category details as per FDA specifications such as Convenience Kit of Co-Package, Prefilled Drug Delivery Device/System, Drug/Biologic Combination, and so on with NCI Codes information.
US_STATES	This code list lets you capture the states of USA with the STATE_CODE attribute.
VACCINATED_AT	This code list is used to maintain the Vaccination Facility Type information.

Add custom values to a flexible code list

1. Click **Argus Console**.
2. From **Code Lists**, select **Flexible Data Re-Categorization**.
3. On the **FLEXIBLE CODE LIST MAINTENANCE** page on the right, in the **Flexible Re-Categorization Code Lists** section, select the flexible code list that you want to add custom values to.
4. To avoid the creation of a duplicate custom value, verify that the value doesn't already appear in the **Total Number of Rows** section.

Tip: The number that appears in parentheses is the number of existing custom values for the flexible code list.

5. Click **Add New**.
6. In the **Total Number of Rows** section, enter information as necessary for the new custom value.
7. Click the green check mark (✓).
8. To add additional custom values, repeat steps 4 to 6.

Accessing Tools

Accessing Tools

This section explains the report (features and purpose) generated when **Tools -> ICSR Length Check** is accessed.

When Argus Code List item length is greater than the E2B field length, the data is truncated when maximum length is entered and an E2b report is generated.

Report Features

The report prints the code list items that exceed E2B (R2) length specifications and also lists code list data that has codes not matching with codes required for the E2B (R2) report.

This report does not provide the length check and Code check validations pertaining to E2B (R3), eVAERS, and eMDR reports.

The report contains the following as illustrated:

ORACLE HEALTH SCIENCES	ICSR Reports 13-SEP-2017 17:38 GMT +5.5
----------------------------------	---

ICSR Report Data Check Errors & Warnings

As of 13 September 2017

List Maintenance	
1.	ICH-ICSR V2.1 MESSAGE TEMPLATE
2.	ICH-ICSR V2.1 MESSAGE TEMPLATE - EMA
3.	ICH-ICSR V2.1 MESSAGE TEMPLATE - FDA
4.	ICH-ICSR V2.1 MESSAGE TEMPLATE - FDA PIP

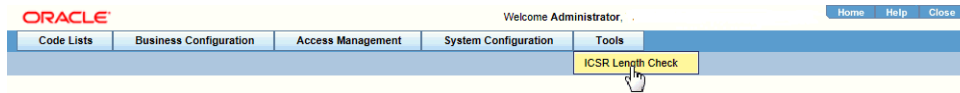
Validation Type	Data Element	DTD Element	Case Form Field	Actual Error Message	Profiles	LM Data
Length Check Validation	A.2.3.1	STUDYNAME	List Maintenance / Clinical Studies / Description	Field value exceeds the ICSR item's maximum field length. Actual Data Entered = 259, DTD Length = 100, Data Truncated = 159	1, 3	CEL-234-002
	A.2.3.1	STUDYNAME	List Maintenance / Clinical Studies / Description	Field value exceeds the ICSR item's maximum field length. Actual Data Entered = 449, DTD Length = 100, Data Truncated = 349	2	CEL-234-001
	A.2.3.1	STUDYNAME	List Maintenance / Clinical Studies / Description	Field value exceeds the ICSR item's maximum field length. Actual Data Entered = 274, DTD Length = 100, Data Truncated = 174	2	CEL-234-002
	A.2.3.1	STUDYNAME	List Maintenance / Clinical Studies / Description	Field value exceeds the ICSR item's maximum field length. Actual Data Entered = 434, DTD Length = 100, Data Truncated = 334	1, 3	CEL-234-001
Other Validation	A.1.2	OCCURCOUNTRY	General Information / Country of Incidence	Invalid E2B Code - WW	1, 2, 3, 4	WORLD
	A.1.2	OCCURCOUNTRY	General Information / Country of Incidence	Invalid E2B Code - EU	1, 2, 3, 4	EUROPEAN UNION
	A.1.2	OCCURCOUNTRY	General Information / Country of Incidence	Invalid E2B Code - RA	1, 2, 3, 4	ASIA

Viewing the ICSR Length Check Report

This section enables you to view the ICSR Length Check Report.

Use the following procedure to view the ICSR length report.

1. Select Tools > ICSR Length Check.



2. The ICSR Length Check PDF report opens in a separate window.

ICSR Report Data Check Errors & Warnings

As of

List Maintenance	
1.	EMA-21-DP
2.	ICH-ICSR V2.1 MESSAGE TEMPLATE
3.	ICH-ICSR V2.1 MESSAGE TEMPLATE - EMA
4.	ICH-ICSR V2.1 MESSAGE TEMPLATE - FDA
5.	ICH-ICSR V2.1 MESSAGE TEMPLATE - FDA PIP

Validation Type	Data Element	DTD Element	Case Form Field	Actual Error Message	Profiles	LM Data
Length Check Validation	A.2.3.1	STUDYNAME	List Maintenance / Clinical Studies / Description	Field value exceeds the ICSR item's maximum field length. Actual Data Entered = 2000, DTD Length = 100, Data Truncated = 1900	1, 2, 3, 4	BEGINTHISSTUID END
	A.3.1.3b	SENDERTITLE	List Maintenance / Regulatory Authority / Local Company Contact / Title	Field value exceeds the ICSR item's maximum field length. Actual Data Entered = 27, DTD Length = 10, Data Truncated = 17	1, 2, 3, 4	EMA_R2
	A.3.1.3b	SENDERTITLE	List Maintenance / Regulatory Authority / Local Company Contact / Title	Field value exceeds the ICSR item's maximum field length. Actual Data Entered = 27, DTD Length = 10, Data Truncated = 17	1, 2, 3, 4	ESM FDA 1
	A.3.1.3b	SENDERTITLE	List Maintenance / Regulatory Authority / Local Company Contact / Title	Field value exceeds the ICSR item's maximum field length. Actual Data Entered = 27, DTD Length = 10, Data Truncated = 17	1, 2, 3, 4	ICH_R3
	A.3.1.3b	SENDERTITLE	List Maintenance / Regulatory Authority / Local Company Contact / Title	Field value exceeds the ICSR item's maximum field length. Actual Data Entered = 27, DTD Length = 10, Data Truncated = 17	1, 2, 3, 4	FDA_PIP

Administrator



Page 1 of 11

Tip: This report compares the lengths of the code list elements with the maximum ICSR length allowed for each of the DTD profiles (ICH, FDA, EMA).

It also displays the elements where the length of the code-list element is greater than the allowed ICSR length.

Using Advanced Conditions

Using Advanced Conditions

This section discusses how to create and use Advanced Conditions. If you **do not** have access to the advanced conditions on certain screens, the system displays only the **Advanced Condition Names** you can access (instead of displaying a blank) and **does not** permit you to modify or view the advanced condition details. The system displays a warning message stating that you **do not** have permissions to update the advanced conditions. The following screens are affected by this change:

- Expedited Reporting Rules
- Auto Signals
- Batch Reports
- Letters
- Studies
- Case Priority
- Field Validation
- Narrative Templates
- Profile Switches | Auto Archiving

This option is available from the Advanced Conditions icon.

Argus Safety provides a powerful search tool that enables complex queries to be built in order to retrieve data from the system. Detailed knowledge of the database schema is not required.

Complex or non-standard queries are constructed by means of the Advanced Conditions dialog, that enable users to define field level search criteria.

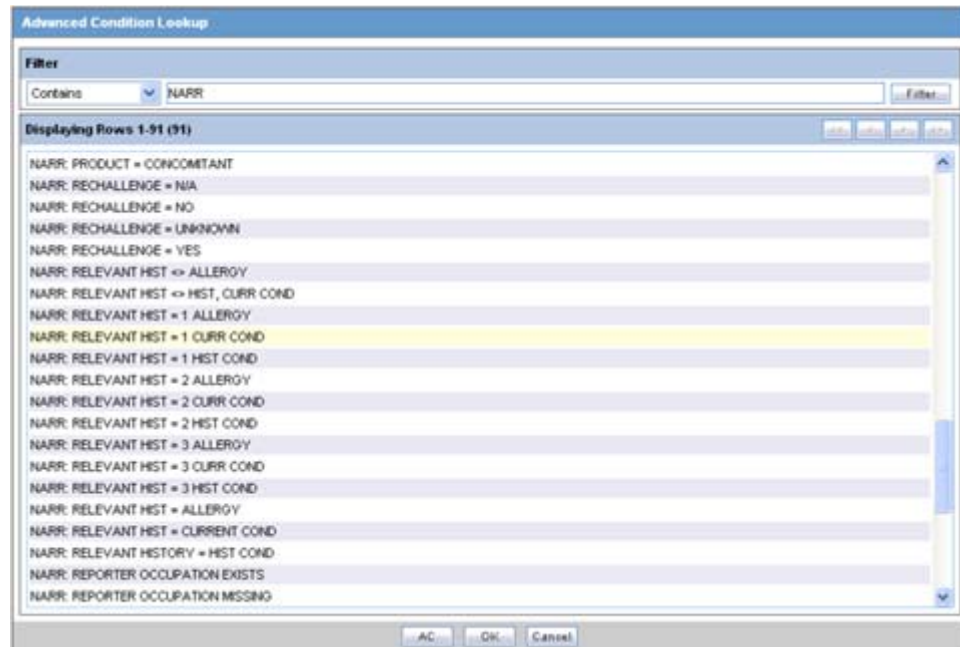
Sets of search criteria (advanced conditions) can be saved and retrieved from the Advanced Conditions dialog. These conditions may then be added, edited, or deleted.

Access rights and permissions can be assigned to individual advanced conditions. You can execute and modify rights to one or more groups on a per-advanced condition basis.

Features within Advanced Conditions

By default, the Advanced Conditions drop-down list enables you to view only the **New**, **None** and already selected Advanced Conditions.

1. Select **New** or **None** from the drop-down list and click the AC button to create a new advanced condition.
2. Click the lookup icon to filter for existing advanced conditions.
3. Execute the steps below to filter for existing Advanced Conditions:
4. Click **Lookup** in the **Case Search Criteria** section. The **Advanced Conditions Lookup** dialog is displayed.



5. Select one of the following options from the drop-down list under **Filter**.
 - **Contains** - Enables you to filter for advanced conditions that contain the entered criteria.
 - **Starts With** - Enables you to filter for all advanced conditions that start with the entered criteria.
6. Enter the search criteria for the advanced conditions in the text box, as applicable.
7. Click **Filter**.
The advanced conditions matching the specified filtering criteria are displayed.
8. Select an advanced condition from the list, as per your search requirements.
9. Execute any of the actions below, as applicable:
 - Click **OK**. The selected advanced condition is listed in the **Advanced Condition** drop-down list.
 - Click **AC**. The details of the selected advanced condition are displayed in the **Advanced Conditions** dialog.
 - Click **Cancel**. The **Advanced Condition Lookup** dialog is closed without saving any changes.

- Select a previously selected advanced condition from the drop-down list to apply the search criteria for that condition.

Using Advanced Conditions

Use the following procedure when using advanced conditions.

1. Click the **Select** lookup to view/edit/create the Advanced Condition in the Advanced Condition dialog.

Note: Only trusted users should be given access to the Advanced Condition, as users with this access will have complete access to the information in the Argus schema.

2. To use advanced conditions, the following options are available, depending on how the set of criteria is to be used:
 - To use a set of previously saved criteria, select the appropriate set of criteria from the **Advanced Condition** list
 - To add a new condition to a set of criteria, select the set of criteria from the **Advanced** list and click the adjoining Advanced Condition icon.
 - To enable the creation of new advanced conditions by associating logical operators (like AND, OR) with items from the Case Form, refer to [Creating Advanced Conditions](#).
 - To create an advanced condition query set from existing advanced condition search criteria, refer to [Creating a Query Set of Advanced Conditions](#).

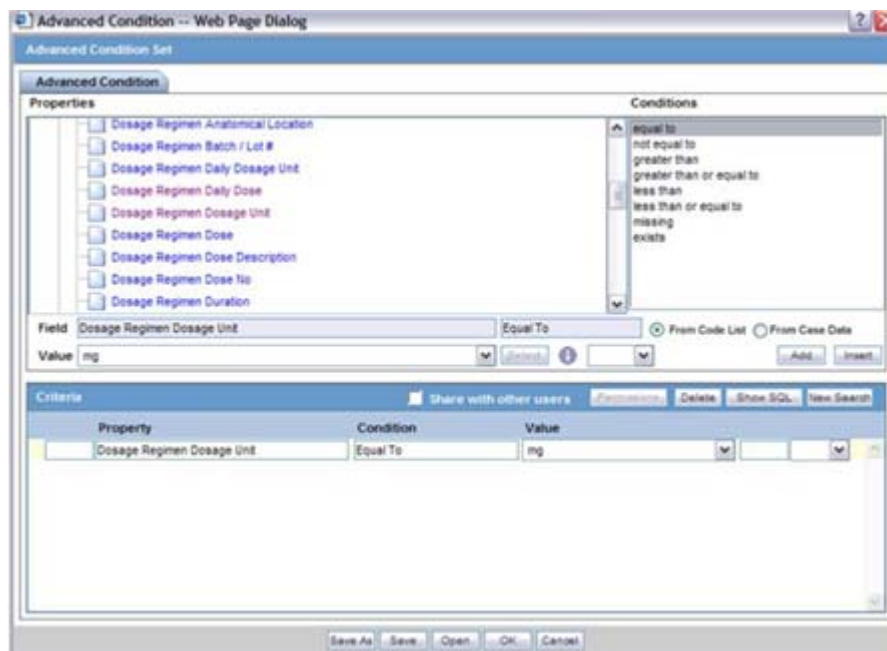
Creating Advanced Conditions

Use the following procedure to create advanced conditions.

1. Select **New** from the **Advanced Conditions** drop-down list or click the **Advanced Conditions** icon.
2. This displays a confirmation dialog.



3. Select whether you wish to create a query set by using previous advanced condition query sets or by creating one through logical operators.
 - Click **Yes** to create a new advanced condition query set.
 - Click **No** to create a new advanced condition by associating logical operators (like AND, OR) with items from the Case Form.
4. If you select **No**, an **Advanced Condition Set** dialog is displayed.



Note: The **Advanced Condition Set** dialog enables you to search for those entities under the **Properties** tree-list, which are from either the case data or from the code list. For this, the dialog provides two radio buttons - **From Code List** and **From Case Data**.

- Select the relevant entity and one of the radio buttons, as applicable.
 - This searches the entity based from the code list or case data, as specified.
 - The radio buttons are displayed only if the selected entity belongs to a code list.
 - If the selected entity is part of the code list, and the user selects:
 - **From Code List** - If this option is selected, the **Value** drop-down list displays the list of all values configured in the Code List.
 - **From Case Data** - If this option is selected, the **Value** drop-down list displays the list of only those values, which are actually present in the cases.
-

5. Select a property type from the **Properties** tree list.

The items available under the folders in the **Properties** list represent those fields on the Case Form that can be used to perform the search in the advanced conditions.

Note: When a Property for which terms can be encoded is selected, the **Select** button is enabled. You can use the MedDRA Browser to select (possibly) multiple terms for the property.

An SMQ icon is enabled when the SMQ-related properties are selected from the Properties tree-list. Click this icon to view the SMQ Info dialog. The SMQ Info dialog contains details about the selected SMQ.

6. In the **Conditions** list, select a condition that must apply to the item selected above.

The available conditions are "equal to", "contains", "less than", "greater than", "not equal to", "missing", "greater than or equal to", "less than or equal to", "exists", "does not contain" or "begins with".

7. Under **Value**, enter the value which will apply to the property, or select an appropriate value from the list, as applicable.
8. If the condition created in steps 4 through 6 above is to be linked with another condition, select the appropriate logical operator in the list adjoining **Value**.

Tip: The logical operators that can be used to link the existing condition to a new condition are *AND/OR*.

9. Click **Add** to add the newly created condition to the advanced condition.
10. Repeat steps 3 through 7 to add more conditions to the advanced condition.
11. When each of the required conditions for the advanced condition is entered, click **Save**.
12. Enter a name for the advanced condition and click **OK**.

Note: To enable other users to use the advanced condition, the **Share with other users** check box should be selected. More about sharing advanced conditions

- If an Advanced Condition is not shared with other users, it does not appear in the Advanced Condition list for any user except the Administrator and the user that created it.
- If the Advanced Condition is shared, all users can view the advanced condition, but they cannot modify it.
 - Not allowed if the Advanced Condition is in use in the system.
 - The Console manages access to the **Advanced Condition Library** screen.
 - The **Advanced Condition Library** option has been added to enable or disable (default) access to the following screen:

Access Management -> Argus -> Groups>
Menus> Utilities (subarea) section

IMPORTANT! Customers should cleanup the aggregate case series data (such as `cfg_adv_cond_hitlist` and related tables) from the **Advanced Condition Library** which are no longer used or are not likely to be required in future.

With each periodic execution, the number of aggregate case series can keep growing in the system and it is up to the customers to manage these case series either by deleting them manually or by deploying an Oracle job.

Tip: To enter a customized date range, select Custom Date Range from the list. Enter an appropriate date range in the custom date range dialog and click **OK**.

Creating a Query Set of Advanced Conditions

The user can configure the Action Items type to be scheduled based on the Advanced Conditions rules as shown in the following.

New Action Type Fields and Field Description

Field/Control Name	Description	Property
Query Action	Defines the Action Item as a Query Action used to generate the letter and used as a placeholder.	Checkbox
Advanced Conditions	Enables the user to configure an Advanced Conditions Rule for creating the Query Type Action Item in the case.	User Selectable
User Group	Enables the user to define a User group (undeleted user groups in Access Management) for the Action Item created in the case.	Type Ahead
Letter Placeholder Content	Enables the user to enter Letter Text that prints in the letter using the Open Query placeholder.	Text (1000 characters)

Due In (days)	When the action item is created on the Case form, this option enables the user to define the number of days until the Action Item is due..
---------------	--

Be aware of the following:

- The Advanced Conditions, User Group, Letter Placeholder Content, and Due In fields are enabled only if Query Action is checked.
- The system tracks any changes made to the profile switch in the audit log.
- The **Action Type** report prints any additional fields.
- The system has a profile switch to enable the user to generate open queries when he/she saves the case.
 - **No (Default)** - When the user clicks **No**, the system **does not** generate open queries in the case when the user saves the case.
 - **Yes** - When the user clicks **Yes**, the system generates **all** action items with a query action type based on the advanced conditions defined for the Action Taken due in *xxx* days for User group *yyy*

where:

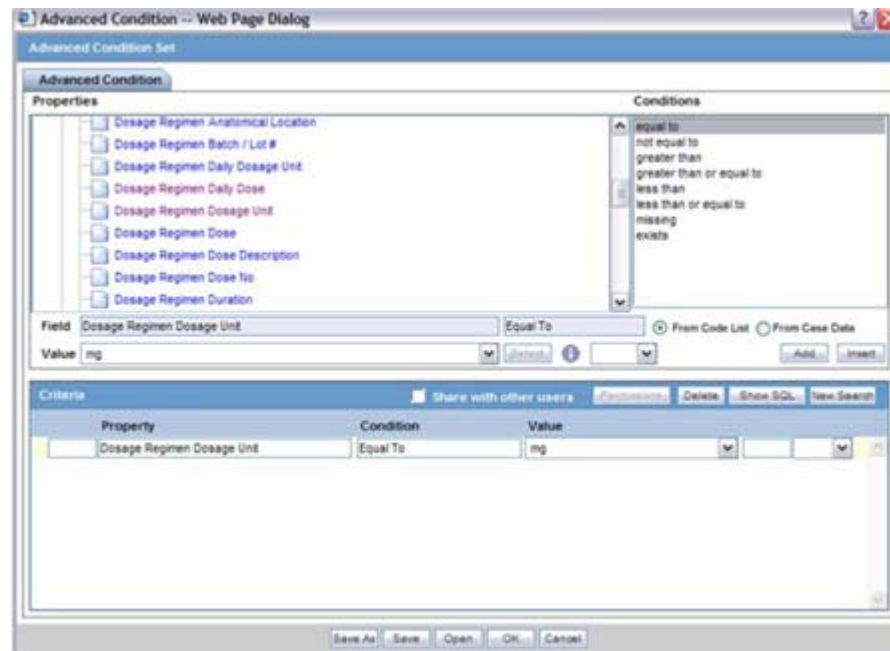
xxx is the number of action items defined + the System Date for the defined user group

yyy is the user group
- The system tracks changes made to the **Profile Switch** in the audit log.

Use the following procedure to create a query set of advanced conditions.

1. Select **New** from the **Advanced Conditions** drop-down list or click the Advanced Conditions icon
2. A dialog that prompts for the creation of an advanced condition query set opens.
3. Click **Yes** to create a set of advanced conditions by linking together those advanced conditions that have been defined previously.
4. The Advanced Condition Set dialog opens.

In this dialog, previously-created advanced conditions can be linked together using set operators like UNION, MINUS, and INTERSECT.



5. Click **Add** to add an advanced condition to the query set. A new row opens in the advanced condition selection area. In this row, select an appropriate advanced condition from the **Advanced Condition** list.

Tip: To modify, open, or delete advanced conditions, click **Open** in the Advanced Conditions dialog. A list of all the advanced conditions will be displayed. In this list, select the appropriate advanced condition and click **Open** to open or modify it, or **Delete** to delete it.

To view or modify the SQL statement associated with an advanced condition, click **Show SQL**. Make the required modifications to the SQL statement, if necessary. The SQL supports the list of parameters as defined in the profile switch *Comma separated list of allowable parameters for custom advanced conditions*.

6. Select an appropriate set operator from the **Set Operator** list. This set operator will link this advanced condition to the next advanced condition.
7. To add the next advanced condition to the query set, click **Add**.
8. Repeat steps 5 through 7 for each advanced condition that must be entered in the query set.

Tip: If the required advanced condition is not already present in the list, it can be created by selecting (New) from the list.

- If an existing advanced condition requires modification, select it and click Edit.
 - The advanced condition can be edited by a user only if it was created by that user.
9. When each of the advanced conditions for the query set is entered, click **Save**.
 10. Enter a name for the advanced condition and click **OK**.

Tip: To view or modify the SQL statement associated with an advanced condition, click **Show SQL**. Make the required modifications to the SQL statement, if necessary.

Rename Query Sets

You can save and retrieve sets of search criteria (advanced conditions), and add, edit, or delete them.

You can select and rename a query set on the **Advanced Condition** screen based on the permissions to modify the advanced condition. When you open an advanced condition or query set, the query name is displayed in the **Name** field.

- To enable the **Save** button, in the **Name** field, enter an advanced condition name.
- To record changes to the advanced condition name, click **Save**.

The query set is saved with the new name and description, and the Query Set drop-down list is refreshed.

- To update the changes to the query set name, click **Save**.
- When you click **New**, all the values in the **Name**, **Description**, and **Query Set** fields are cleared.

Use the Advanced Conditions from the Case Selection Dialog Box

Users can view a list of Cases that satisfies an Advanced conditions from the Case Open screen.

1. Select **Case Actions > Open**.
2. You can do the following:
 - Use a set of previously saved criteria.
 - Select the appropriate set of criteria from the **Advanced Condition** list.
 - Select the set of criteria from the **Advanced** list, and click the adjoining Advanced Condition icon.
 - Add a new condition to a set of criteria.
 - Create a new advanced condition by associating logical operators (like AND, OR) with items from the Case Form.

Use the Advanced Conditions Library

From the Utilities drop-down menu, select **Advanced Conditions Library**.

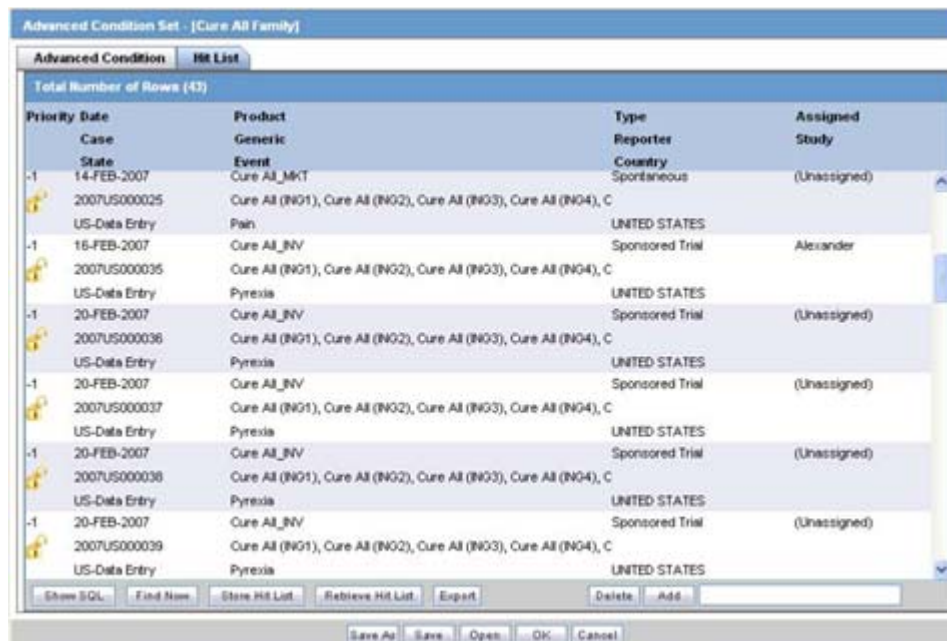
From this screen, you can:

- Create a new advanced condition
- Reassign an advanced condition
- Set advanced condition permission levels
- Modify an existing advanced condition
- Delete an advanced condition
- Print a list of advanced conditions

To search for an existing query sets or advanced conditions, enter the search criteria, and click **Search**.

Case Series (former Hit List) Tab

The **Case Series** (former **Hit List**) tab in the Advanced Condition Set dialog can be used to search for cases that match the query set criteria.



1. Click **Find Now** in the **Case Series** (former **Hit List**) tab of the Advance Conditions dialog.

This runs a search based on the selected query set criteria and displays a list of cases (if any) that satisfy the advanced condition query set.

2. Perform these operations to do the following:

To...	Click...
Manually add an existing case to the case series (former Hit List)	Add and enter the Case ID
Remove a case from the Case Series (former Hit List)	Remove
Save the Case Series (former Hit List) result for future use	Store Advanced Condition (former Hit List)
Retrieve results of the saved Case Series (former Hit List)	Retrieve Advanced Condition (former Hit List)
Save the Case Series (former Hit List) as a text file	Export
View SQL for Query	Show SQL
Run a Query	Find Now

Data Privacy

The Argus application provides various methodologies to protect data between different sites, user groups, and users. This chapter discusses personally identifiable information (PII) and the methods to protect it.

Personally Identifiable Information

PII (personally identifiable information) or SPI (sensitive personal information), as used in information security and privacy laws, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. PII is any data that could potentially identify a specific individual. Any information that can distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII. The application protects the sensitive PII data as per user access.

Note: All PII is personal data, but not all personal data is PII.

In Argus, the following data is considered as PII:

- Patient Initials
- Patient Date of Birth
- Parent Initials
- Parent Date of Birth

The PII Data can be controlled via user group accesses and common profile switches. The user group accesses that can be used to control the PII data fields are:

- Case Patient - Patient Information
- Case Patient - Patient Details
- Case Patient - Parent Information
- Case Patient - Parent Details

These user groups accesses are found under **Argus Console > Access Management > Groups**.

In the Case Form, the patient and parent fields are grouped under the Information/Details sections as shown below.

Patient Information and Details Sections

Parent Information and Details Sections

The fields are controlled through the user groups as shown in the table below.

Group Access Name	Value	Case Form Behavior	Impacted Case Form Fields
Case Patient - Patient Information	Modify	User can add/modify all the fields	<ul style="list-style-type: none"> ■ Patient Information
	View	User can only view the fields	<ul style="list-style-type: none"> ■ Title ■ First Name ■ Middle Name ■ Last Name ■ Address 1 ■ Address 2 ■ City ■ State ■ Postal Code ■ Country ■ Email Address ■ Protect Confidentiality
	No Access	The fields are hidden and inaccessible	

Group Access Name	Value	Case Form Behavior	Impacted Case Form Fields
Case Patient - Patient Details	Modify	User can add/modify all the fields	Patient Information <ul style="list-style-type: none"> Initials
	View	User can only view the fields	Patient Details <ul style="list-style-type: none"> Date of Birth Age and Age Units Age Group Weight and Units Height and Units Gender Pregnant Date of LMP Breastfeeding BMI Body Area Occupation Age At Vaccination and Units Ethnic Group Military Status Country
	No Access	The fields are hidden and inaccessible	
Case Patient - Parent Information	Modify	User can add/modify all the fields	Parent Information <ul style="list-style-type: none"> Title
	View	User can only view the fields	<ul style="list-style-type: none"> First Name Middle Name Last Name
	No Access	The fields are hidden and inaccessible	
Case Patient - Parent Details	Modify	User can add/modify all the fields	Parent Information <ul style="list-style-type: none"> Initials
	View	User can only view the fields	Parent Details <ul style="list-style-type: none"> Date of Birth Age and Age Units Weight and Units Height and Units Gender Date of LMP Parent Breastfeeding Age At Vaccination and Units Ethnic Group Medical History
	No Access	The fields are hidden and inaccessible	

Note: The initials field is located under the *Information* sections, but still controlled through the *Details* access group.

This default behavior can be overridden using a set of common profile switches. The switches located at **Argus Console > System Configuration > System Management (Common Profile Switches) > Case Processing > Group Data Access** are used for this purpose. These switches help the *Initials* and *Date of Birth* fields to be controlled via the alternate user groups as shown below.

Switch Name	Use	Default Value
Access on Patient Initials	Sets the <i>Patient Initials</i> either to be part of Patient Information or Details Group	Initials part of Patient Details Access Group
Access on Patient Date of Birth	Sets the <i>Patient Date of Birth</i> either to be part of Patient Information or Details Group	Date of Birth part of Patient Details Access Group
Access on Parent Initials	Sets the <i>Parent Initials</i> either to be part of Parent Information or Details Group	Initials part of Parent Details Access Group
Access on Parent Date of Birth	Sets the <i>Parent Date of Birth</i> either to be part of Parent Information or Details Group	Date of Birth part of Parent Details Access Group

Personally Identifiable Information and Application Behavior

This section provides details about the impacted areas and their behavior.

Case Form Print, Case Summary and Medical Summary Reports

The Case Form Print, and the Case and Medical Summary reports display PII data fields only based on the user group access and common profile switches setup.

Case Form Title Bar

For certain report types, the case form title bar displays the Patient initials. These will now be visible based on user group access and common profile switches.

Case Revision

Case Revisions display PII data based on the user group access and common profile switches.

Audit Log Report

The Audit Log reports displays the PII data based on the user group access and common profile switches. If the main user group (Argus Console > Access Management > Groups > Patient Information) is restricted, the new user group access and common profile switches will be ineffective.

System Reports

Both the Patient and Parent PII data in the system reports are controlled only through Argus Console > Access Management > Groups > Patient Information. The sub-level user group access and common profile settings do not have any effect.

Duplicate Search (Book-in, Local Affiliate and ICSR Pending)

The Duplicate search result displays the PII data based on the user group access and common profile switches.

Case Copy and Audit Logging

Case Copy and the Audit Log continue to handle PII data even when the fields are hidden or read-only.

Copy Patient Information from Reporter

Patient initials are copied from the reporter only when the Patient initials field is visible and editable.

Patient/Parent Initials Automatic Calculation

The Patient or Parent Initials are automatically calculated when the Patient or Parent initials field is visible and editable.

Accept ICSR/Affiliate Acceptance (Interchange and LAM)

The Accept ICSR/Affiliate Acceptance dialogs and reports work as in the existing version of Argus Safety. These modules do not follow the PII restrictions levied by user group access setting and common profile switches.

The following sections provides a sample of the Case Form behavior between two users who have been set up for PII Data Privacy.

User Details	Access Settings
User 1	User ID: usr_pat_info Group: Patient_info_group Access Setting: Case Patient - Patient Information: No Access Case Patient - Patient Details: Modify
User 2	User ID: usr_pat_det Group: Patient_det_group Access Setting: Case Patient - Patient Information: Modify Case Patient - Patient Details: No Access

No changes to the common profile set up from the default values.

With the above set up when user 1 and user 2 logs into the application, the application behaves as following:

Logged in User	usr_pat_info
Application Behavior	In the case patient tab, all the fields under Patient-Information group are hidden except Initials, Child Only case and Country fields.
Logged in User	usr_pat_det
Application Behavior	In the case patient tab, all the fields under Patient-Details group are hidden. Patient Initials, Child only Case and Country fields are hidden too.

- [Configuring Argus Safety for ICSR Reports \(HL7\)](#)
- [Attachments in HL7 Reports](#)
- [Creating and Managing Amendments for eVAERS and E2B \(R3\) report](#)
- [Null Flavor Handling in HL7 Reports](#)
- [Best Practices in a Multi-Tenant Environment](#)

Configuring Argus Safety for ICSR Reports (HL7)

HL7 reports include the ICH E2B(R3), eVAERS, eMDR, EMA E2B(R3), and PMDA E2B(R3) reports built using HL7 v.3.0. This section contains the following topics:

- [Configuring Reporting Destination for HL7 ICSR Reports](#)
- [Customizing Profiles](#)
- [Configuring ICSR Validation using the New Framework](#)
- [Configuring Codelists](#)
- [PMDA E2B \(R3\) Flex Codelist](#)
- [Business Configuration Updates](#)
- [System Configuration Updates](#)
- [Optional Upgrade Scripts for Data Migration to New Fields](#)

Configuring Reporting Destination for HL7 ICSR Reports

The Reporting Destination must be configured with the appropriate profile based on the report type to be sent to the Agency:

1. Configuring Profiles for Message and Acknowledgement

Message and Acknowledge profile must be selected as follows for different report types:

Agency	Message Profile	Acknowledgement Profile
CBER	CBER eVAERS V1.0 MESSAGE TEMPLATE	-
CDRH	CDRH EMDR V1.0 MESSAGE TEMPLATE	Disabled for eMDR Profile

Agency	Message Profile	Acknowledgement Profile
PMDA	ICH-ICSR V3.0 MESSAGE TEMPLATE - PMDA	PMDA E2B(R2) Acknowledgement Profile
ICH	ICH-ICSR V3.0 MESSAGE TEMPLATE	E2B(R2) Acknowledgement Profile
EMA	ICH-ICSR V3.0 MESSAGE TEMPLATE	E2B(R3) Acknowledgement Profile

2. Path for Incoming and Outgoing Messages

The Path for Incoming and Outgoing Messages or Acknowledgements must be specified in:

Codelist -> Reporting Destination -> EDI tab -> Incoming folder

Codelist -> Reporting Destination -> EDI tab -> Outgoing folder

3. Attachment and Report File Size Configuration

The attachment file and overall file size of the reports are checked for HL7 reports during report generation or transmission. The file size and attachment size limit can be configured using the parameters in the Reporting Destination Code list.

The recommended size for various report types are:

Report Type	Allowed attachment file size (in MB)	Allowed report size (in MB)
eVAERS	15 MB	20 MB
eMDR	15 MB	50 MB
ICH E2B R3	15 MB	20 MB
PMDA R3	N.A.	AS1: 10 MB AS2: 50 MB
EMA	15 MB	20 MB

For more information on changes required in the file types, refer to the Console guide for the Common profile switch for the file types allowed for the report forms.

4. ICSR Report Submission Date Configurations

The existing profile switch based system level ICSR submission date options have now been moved to reporting destination level for all ICSR submissions. Hence, set the appropriate value for the respective destinations for both R2 and R3 reports.

-
- Note:** 1. When any of these profiles are selected, message type is automatically set as XML, and *Maximum # of reports to include in the msg* is set to 1. This is because report batching in an xml is not supported.
2. Refer to Attachments in HL7 reports for settings to be made in Reporting Destination.
 3. Oracle recommends that you configure the existing Reporting Destination that was used for sending MedWatch/VAERS with the eMDR/eVAERS profile.
 4. When reporting is switched from the current PMDA E2B (R2) to PMDA E2B (R3), the follow-up report numbering sequence remains intact (including downgrade and nullification report over the previous PMDA E2B R2). The same is applicable when reports are switched from EMA E2B(R2) to EMA E2B(R3).
-

Customizing Profiles

Perform the following steps to customize profiles:

1. Creating a Custom Profile:

Standard profiles must be copied to modify mappings or add new elements. You can copy a profile using the Copy button in Interchange Mapping.
2. Adding extension elements:

If a new element is required in a profile due to a change in regulations, the extension element can be added to the Custom Profile. The extension element is created using the Insert statement in the CFG_E2B table.
3. Providing custom export logic for the required data element:

SQL for the required data element can be modified in the custom profile using the Interchange Mapping.
4. Updating XSL files

If the xpath of the element must be changed due to a change in regulations, the corresponding XSL must be altered. The location of XSL files is:

```
{ArgusInstallPath(FromArgus.ini)} \ Argus.NET\CommonWebUIComponent
\HL7\XSLT\AS\
```

Refer E2B(R3) Extensibility guide for guidelines on updating XSL files.
5. Configuring a Reporting Destination with the Custom profile:

The custom profile created in step1 must be specified to the required Reporting Destination.

Configuring ICSR Validation using the New Framework

A new ICSR validation framework has been implemented for E2B (R3) based ICSR reports. This provides a robust framework to enhance the ICSR generation validation capabilities to reflect the process by which they are executed by the regulatory authorities.

Currently, only PMDA E2B (R3) is using the new framework for validations by default. All required factory data validation have been provided for PMDA E2B R3 template profile only.

If you want to enable the new framework for other R3 based ICSR profiles (ICH and eVAERS), load/add the required validations using the UI and update the back-end profile level flag (CFG_PROFILE.APPLY_CONF_RULE=1).

Configuring Codelists

Oracle recommends you configure Codelist data using the Flexible Data Re-categorization codelist to ensure legacy Vaccine data is properly represented in reports.

eMDR Specific Codelist Updates

Occupation

The Occupation codelist is provided with Factory data along with NCI_Codes. If Companies already have entered data in this codelist and if this data has been used in the Device cases prior to upgrading to the 8.x release, Oracle recommends you do the following:

- Update the NCI codes for the existing data in Occupation codelist using Flexible Data Re-categorization codelist.
- Set *Display* to No, for the new factory data provided in Occupation codelist using Standard Codelist .

eVAERS Specific Codelist Updates

Since the values allowed for few fields in eVAERS are different from VAERS report, Oracle recommends you configure the existing codelist values with appropriate NCI_CODE in the Flexible Data Re-categorization Codelist so that appropriate data is sent in eVAERS reports.

Relation to Patient

Relation codelist is now provided with additional Factory data along with NCI_Codes as per CBER guidelines on eVAERS. If there are legacy cases with data that is similar to the values provided in the table, Oracle recommends you update the NCI codes for these codelist values as per NCI_CODE column.

Codelist List Value	NCI_CODE
Vaccine Provider	C102430
Patient/Parent	C16960 or C42709

Anatomical Location

Anatomical Locations codelist is now provided with Factory data along with NCI_Codes. If Companies already have entered data in this codelist and if this data has been used in the Vaccine cases prior to upgrading to the 8.0 release, Oracle recommends you do the following:

- Update the NCI codes for the existing data in Anatomical Location codelist using Flexible Data Re-categorization codelist.
- Set *Display* to No, for the new factory data provided in Codelist -> Anatomical Location.

Ethnicity

Ethnicity codelist is now provided with Factory data along with NCI_Codes. If Companies already have entered data in this codelist and if this data has been used in

the Vaccine cases prior to upgrading to the 8.0 release, Oracle recommends you do the following:

- Update the NCI codes for the existing data in Ethnicity codelist using Flexible Data Re-categorization codelist.
- Set *Display* to No, for the new factory data provided in codelist -> Ethnicity.

Vaccination Facility

Vaccination Facility codelist provides distinct options for facility types. However prior version of application had factory data as follows in **LM_VACCINATED_AT** table. If there are legacy cases with any data same as the value provided in the below table, Oracle recommends you update the NCI codes for these codelist values as per NCI_CODE column.

Codelist List Value	NCI_CODE
Private Doctor's Office/Hospital	C16988 or C16696
Public Health Clinic/Hospital	C51282 or C16696
Military Clinic/Hospital	C51282 or C114861 or C16696 or any other appropriate NCI_CODE

PMDA E2B (R3) Flex Codelist

License Category

Data for the License category codelist has been synchronized as per the PMDA E2B (R3) regulation. The E2B (R2) codes have been mapped to the appropriate values with the following exceptions:

CATEGORY	CATEGORY_J	E2B_R3
During the re-review period (medicines that require pharmacist intervention)	再審査期間中 (要指導)	6
During the PMS period (medicines that require pharmacist intervention)	PMS 期間中 (要指導)	7

Update the appropriate E2B (R2) codes for the newly added items to the codelist.

Study Development Phase (Development Phase)

Data for Study Development Phase codelist has been synchronized as per the PMDA E2B (R3) regulation. The E2B (R2) codes have been mapped to the appropriate values with the following exceptions:

DEV_PHASE	DEV_PHASE_J	E2B_R3
Microdose tests, etc.	マイクロドーズ試験等	0
Phase I/II Trial	第 I / II 相	4
Phase II/III Trial	第 II / III 相	5

Update the appropriate E2B (R2) codes for the newly added items to the codelist.

Business Configuration Updates

Setting up the Application Type in Business Configuration -> Products and Licenses (eVAERS specific)

FDA requires the use of a prefix to determine the application type associated with suspect products. For licensed vaccines, you must include the appropriate acronym *BLA*, *STN*, or *PLA* followed by the primary six-digit number. Therefore, Oracle recommends you update the newly added column in **Business Configuration-> Products and Licenses-> License-> Application Type** with appropriate license types.

Configuring PMDA Specific License Parameters

Configure the following License level parameters that will be used to auto-populate the respective configured values in the Case Form:

Status category of new drug: Use this drop-down list to set the status category of the new drug as per the allowed values from the License category codelist. This configured value is used to auto populate the Case Form -> Analysis -> PMDA -> General -> Category of New Drug. The user can modify the auto populated value in the Case Form.

Risk category of OTC drug: Use this drop-down list to set the Risk category of OTC Drug as per the allowed values from newly added Risk category codelist depending on the value for OTC Product checkbox. This configured value auto populates the Case Form -> Analysis -> PMDA -> General -> Route of acquiring OTC drugs. The user can modify the auto populated value in the Case Form.

Configuring PMDA E2B (R3) Specific Study Parameter

Configure the appropriate Notification number for existing studies in the Study Configuration J pop-up. The value configured here is expected to be transmitted in J2.13.r.1 (Notification Number) tag of PMDA E2B (R3) report.

System Configuration Updates

PMDA E2B (R3) Specific Switches

Some switch based application behaviors may impact the PMDA E2B (R3) report directly or indirectly. Oracle recommends you configure the appropriate switch value as per company specific business needs:

- Profile Switch under *Common Profile -> Argus J*
 - a. On Adding/Updating the Case form -> Events -> Description as Reported by an English user, auto populate *Description as Reported* on the Japanese side with:

Option 1: English Verbatim (Default)

Option 2: Japanese PT (From Meddra J)

Based on the value configured for the above switch, the application auto populates the user entered English verbatim or the Japanese PT in the Japanese verbatim.

- b. Allow user to update the *Reason for Downgrade/Nullification report* and *Comments for start date of reporting timeframe* after the case is locked (globally and locally locked):
 - Option 1: Yes (default)
 - Option 2: No

Based on the value configured for the above profile switch, *Reason for Downgrade/Nullification report* and *Comments for start date of reporting timeframe* text areas are made available for edit even after the case lock.
- c. Default viewing format of the PMDA E2B R3 report (used with Interchange-J)
 - Option 1: XML
 - Option 2: Decoded (Default)
 - Option 3: HL7

The default view for E2B Viewer for PMDA E2B R3 report can be configured using the above profile switch.
- Profile Switch under *Common Profile -> Case Processing -> Dictionary Browser*
 - a. Allow User to Add Non-Current Meddra Terms for:
 - Option 1: Case irrespective of Country of Incidence
 - Option 2: Case where Country of Incidence is other than Japan (Default)

This profile switch value is used to control the application behavior to allow the user to add the Non-current LLT (J) term to Case Forms.
 - b. On change of LLT Term Sync English and Japan LLTs, irrespective of the currency:
 - Option 1: Yes
 - Option 2: No (Default)

This profile switch value is used to set the application behavior to synchronize the LLT term when the user updates the LLT.

Optional Upgrade Scripts for Data Migration to New Fields

eVAERS specific

Illness at the time of Vaccination

Illness at the time of Vaccination data is used in the eVAERS report and this data is captured in Case Form -> Patient -> Other Relevant History -> Condition Type = *Illness at Vac*. LLT code and MedDRA version of the ORH record with Condition Type as *Illness at Vac* is transmitted in data elements *illnessatvaccination* and *illnessatvaccinationmeddraversion* respectively.

The VAERS report continues to map Illness at the time of Vaccination with the corresponding field in Vaccine tab.

If Illness at time of Vaccination in Vaccine tab has data in legacy cases, this data can be copied to Case Form -> Patient -> Other Relevant History by executing the optional upgrade scripts providing along with this release. Oracle recommends you keep this data in ORH and Vaccine tab in sync so that same data is presented in VAERS and eVAERS report.

Emergency Room visit

Emergency Room Visit data is used in the eVAERS report and this data is captured in Case Form -> Event -> Emergency Room Visit (checkbox). If this checkbox is checked, then *seriousnesservisit* data element is transmitted as true. If this checkbox is unchecked, then null flavor NI is transmitted.

The VAERS report continues to map Emergency Room visit data with the field **Required ER visit** in Vaccine tab.

If **Required ER visit** checkbox is ticked in Vaccine tab in legacy cases, this data can be copied to Case Form -> Event-> Emergency Room visit by executing the optional upgrade scripts providing along with this release. Oracle recommends you keep this data in Event tab and Vaccine tab in sync so that same data is presented in VAERS and eVAERS report.

Prior Adverse Event

The VAERS report transmits LLT code and MedDRA version data from Case Form-> Patient -> Other Relevant History. Upgrade scripts are provided to copy data from Case Form -> Product -> Vaccine -> Prior Adverse Event (where Person type=Patient) to Case Form-> Patient -> Other Relevant History.

The VAERS report continues to print the verbatim text entered for Adverse Event in box 21 from Case Form -> Product -> Vaccine -> Prior Adverse Event as per existing functionality.

Oracle recommends that customers enter Prior Adverse Event experience by Patient in Case Form -> Patient -> Other Relevant History so that required information is populated in the eVAERS report and if the VAERS report must be sent, the same data can be entered in Case Form -> Product -> Vaccine -> Prior Adverse Event.

Admin By and Responsible Physician

The Vaccine Administration Section in Products > Vaccine has been re-organized and several new fields have been included to be compliant with CBER eVAERS Guidance.

Upgrade scripts are provided to copy data from *Admin By* (CASE_VACC_VAERS.ADMIN_BY) to Best Doctor Physician Last Name (), if *Admin By* is blank, the data from Responsible Physician CASE_VACC_VAERS.PHYSICIAN is copied.

Based on company requirements, the upgrade logic can be altered to consider *Responsible Physician* data first instead of *Admin By*.

eMDR Specific

Device Age and Unit

The Device Age and Unit fields are provided in Products -> Device tab. Upgrade scripts are provided to copy data from Device Age (approx) to Device Age and Unit fields by using the following logic. Oracle recommends customers review this logic and make necessary changes based on the format in which Device Age was entered in Device Age (approx) field.

1. Device Age is derived from CASE_PROD_DEVICES.DEVICE_AGE by considering the initial numeric value of the Device Age field value.
2. Unit is derived from CASE_PROD_DEVICES.DEVICE_AGE by considering later portion of Device Age field value.
 - a. Unit is populated as Hours, if the later portion of CASE_PROD_DEVICES.DEVICE_AGE text is Hour or Hours or Hr irrespective of upper/lower case used.

b. Unit is populated as Days, if the later portion of CASE_PROD_DEVICES.DEVICE_AGE is Day or Days or Da irrespective of the upper/lower case used.

c. Unit is populated as Month, if the later portion of CASE_PROD_DEVICES.DEVICE_AGE is Month or Months or Mo irrespective of the upper/lower case used.

d. Unit is populated as Year, if the later portion of CASE_PROD_DEVICES.DEVICE_AGE is Year or Years or Yr irrespective of the upper/lower case used.

Location where Event Occurred

The Location where event occurred field is changed to a type ahead field in Case Form -> Analysis -> MedWatch Info tab.

Previously, *Location Where Event Occurred* was captured using multiple checkboxes representing different locations. As per typical business use case, the event occurrence is likely to happen only in one location.

Upgrade scripts are provided to copy data from the following fields with matching Codelist ID from the Location event occurred codelist. If data is present in more than 1 field, the data is not copied in the upgraded database and the upgrade log indicates that **users need to manually** select appropriate data for this field as the prior version had multiple options marked.

- CASE_MEDWATCH_DATA.LOC_HOSP
- CASE_MEDWATCH_DATA.LOC_HOME
- CASE_MEDWATCH_DATA.LOC_NH
- CASE_MEDWATCH_DATA.LOC_OTF
- CASE_MEDWATCH_DATA.LOC_ODF
- CASE_MEDWATCH_DATA.LOC_ASF
- CASE_MEDWATCH_DATA.LOC_OTHER

Attachments in HL7 Reports

ICSR Attachments can be sent in ICH E2B (R3), eVAERS, eMDR, and PMDA E2B(R3) reports. The Reporting Destination must be configured for sending attachments by marking *Transmit E2B Attachments* and selecting the *Attachment classification* that is required to be sent as an inline attachments in these reports.

Attachments are encoded using the B64 format.

Compression Format

For ICH E2B (R3), EMA E2B(R3), and PMDA E2B(R3) reports, attachments are compressed in the format as specified in the l Common Internal Profile switch.

- ICH E2B (R3) and EMA E2B(R3) reports use the internal common profile switch *ZIPSTREAM_COMPRESSION_ALGORITHM*. DF (Deflate) is the default compression algorithm used for compressing attachments; other options supported are GZ and ZL.
- PMDA E2B(R3) reports uses the common Profile switch *Compression algorithm for file attachments in PMDA E2B R3*. DF (Deflate) is the default compression algorithm used for compressing attachments; the other option supported is GZ IP.

eMDR and eVAERS profiles do not require compression as per guidelines from CDRH and CBER respectively.

File Formats

For more information on file formats supported for Attachments, refer to the following sections.

Configuring Common Profile Switches -> For configuring file types for the Report Types.

Attachment Size

For more information on Attachment size validation, refer to the following sections.

Attachment and report file size configuration: Configuring Reporting Destination for ICH E2B(R3), EMA E2B(R3), eVAERS, eMDR, and PMDA(R3) profiles.

Creating and Managing Amendments for eVAERS and E2B (R3) report

When to create Amendments?

If Initial / Follow-up eVAERS / E2B (R3) reports are submitted to a Reporting Destination/Agency and then there is a request from the Agency to send attachments, amendments can be created by unlocking the case as significant follow-up and ticking the **Amendment** checkbox in Case Form -> General Tab -> Follow-up section and providing the reason for creating Amendments.

Users can include Attachments and provide the details of the attachments in the Case Summary.

Auto-scheduling of Amendment Report

Amendment reports are auto-scheduled for cases with Significant Amendments only for the Reporting Destination configured with an eVAERS / E2B (R3) Profile.

Follow-up reports are auto-scheduled for cases with Significant Amendments for the Reporting Destinations that are configured with Non E2B and E2B (R2) reports.

Manual Scheduling of Amendment Reports

Amendment reports for eVAERS / E2B (R3) can be manually scheduled for Significant Amendments or Non Significant Amendments using the Scheduling New Expedited Report dialog. Users can select the Aware date pertaining to the Amendment and schedule an eVAERS / E2B (R3) report. Aware date pertaining to an Amendment can be identified by text (A) appended to the Aware date. Oracle recommends you have only one amendment for an Aware date, else it may be difficult to identify the latest amendment from the Aware date drop-down list in the *Scheduling New Expedited Report* dialog.

If User manually schedules Non E2B or E2B (R2) reports for an Amendment Aware date, then system schedules follow-up report if there is a previously submitted report of the same report type to the same agency, else will schedule an Initial report.

Other Recommendations

Amendments can be created only when there exists a previously submitted eVAERS / E2B (R3) report.

Null Flavor Handling in HL7 Reports

Null flavor data is not sent in eMDR in absence of clear guidance on the exact null flavor allowed for the individual data elements.

Null Flavor can be entered for Date and Text fields as per the ICH E2B(R3) Implementation Guidelines.

EMA, CBER, PMDA have minor differences in the allowed Null Flavors for various data elements.

Oracle recommends you customize the fields with appropriate Null Flavor sets based on reporting needs.

New Null Flavor sets can be created using Flexible data re-categorization.

For text fields, Null Flavors must be entered for English and Japanese fields separately by manually selecting them from the NF drop-down list.

Null flavors can be selected for Codelist fields by selecting key values such as *MASKED*, *UNKNOWN* and so on from the typeahead/drop-down fields.

During Report generation, mapping logic for the data elements (that support Null flavors) identifies these keywords as Null flavors and populates required information in the HL7 report.

Validation is done to check for only allowed Null flavor if Case data is missing. Error messages are displayed if incorrect Null flavors are used for a data element or when both Case Form data and Null flavors do not have the mandatory data elements.

Best Practices in a Multi-Tenant Environment

This section lists the best practices to follow in a multi-tenant environment.

Single Sign-on

Single Sign-on needs to be enabled to have the capability to switch client context and to open the Argus Safety application from the Global Worklists/Application Access Portlet. If SSO is enabled, then it becomes mandatory for a user to be configured as an LDAP user in all the enterprises where the data displays on the screen/portlet.

Accessing Argus Safety Directly via URL

It is expected that you will pass the internal Enterprise ID as a URL parameter for the Argus Safety application to open with the appropriate Enterprise context. If Enterprise ID is not passed, the user is validated against the default enterprise.

Because the EOSU Tool is a client-server application and does not have a mechanism to specify the Enterprise ID, it will always validate users against the default enterprise. Hence, users that are expected to login into these applications are configured with appropriate access/roles within default enterprise. For this reason, "Active" checkbox for the default enterprise is always marked checked and disabled in Global Enterprise Management screen.

Global Homepage and Portlets

Set up appropriate Portal user and user group privileges to restrict access to Portlets and the Global Homepage. It is recommended that you configure the out-of-the-box Portlets so these (specified below) are accessible to all multi-tenant users who need to access data across multiple enterprises, except the ones specifically recommended for administrators.

- Global Worklist - New
- Global Worklist - Open

- Global Worklist - Action Items
- Global Worklist - Contacts
- Global Enterprise Management: Recommended for Administrators
- Global User Management: Recommended for Administrators
- Application Access Portlet

Global Worklists Columns

The system allows flexibility to hide some of the fields/columns in the Global Worklist Portlets through the Global Worklist grid/menu XML(s) which resides on the Web Server(s). It is advisable to hide only those fields/columns which are not updated nor referred by any Worklist context menu actions.

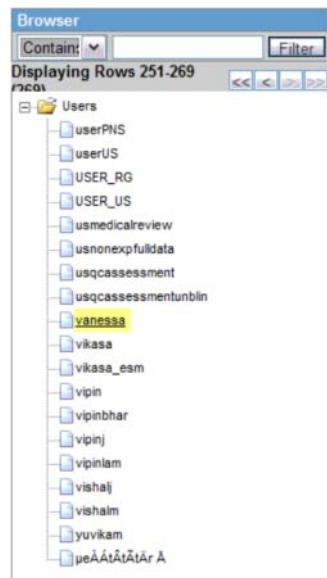
Global User Management

Global User Management is intended to configure users across multiple enterprises. When user configuration changes need to affect only a specific enterprise, it needs to be done from the Argus Safety Console > User Management screen for that enterprise.

Note: Your access is restricted depending on your access to this Portlet at the Portal server level.

The Browser displays a left hand pane that lists the existing users (distinct users based on Login User ID) in the system, in a tree view. The tree displays users from the enterprise partitions for which the user has access.

Figure 10–1 Argus Safety Console Browser



Local users can locally lock a case for which local Japan data entry/assessment is complete, triggering the scheduling and/or generation of the applicable local reports. Similarly, they can locally unlock the case after a local lock is applied and modify the data. To grant the privilege to locally lock or unlock a case to a local user, you can use the **Allow Local Locking** option from the Argus Console > Access Management > Users section. The checkbox is unchecked by default.

Global Enterprises

From the Global Enterprise Management tab, you can:

- Add a new enterprise.
- Define new enterprise attributes.
- Copy configuration from an existing enterprise.
- Associate users to the new enterprise.

User-Enterprise Association

To associate existing users from one enterprise to other enterprises:

1. Select an enterprise from **Copy User Attributes From**.

Note: The selected enterprise is used to set the attribute values for the user in the new enterprise to which the user is being associated. The attribute values for the already associated enterprises remain the same.

2. Add an **Available Enterprise** or **Add All** available enterprises.
3. Select **Save**.

Note: During Save, all the user attributes are copied from the Enterprise selected in the **Copy User Attributes From** to all the newly associated Enterprises.

4. To print the user details of the current user or all the users, select **Current User** or **All Users** and click **Print**.

When a user is copied from one enterprise to another, it is expected that you have set up the appropriate site and the user groups in the target enterprise. Otherwise the user-association will fail with the appropriate error message.

New User Creation/Association

Argus Console allows same UserID to be used to create different users across multiple enterprises. It is recommended that this feature is only be used if users are not expected to be shared across enterprises. Otherwise, if users are expected to be shared across multiple enterprises, then same UserID will not be used to create different users across different enterprises. Instead of that, a user created in one enterprise is associated to other enterprises through Global User Management.

Synchronizable User Attributes

The purpose of the Synchronizable User Attributes section is to allow you to apply updates to user attributes displayed in this section, and keep them in sync across all enterprises.

The users that are listed to be administered in this screen are restricted by the following rules:

- Admin users, System users and users for which the Service User is checked in Console are not listed.

- Only the users from the enterprises for which you have access to the Console User management screen, i.e. you should have access to all of the following in those enterprises:
 - Console User Management screen ' Application Access field ' Console checkbox is checked.
 - Console Group Management screen ' Menus section ' Console, Access Management and User radio options are set to enabled at least for one user group in the respective enterprise partition.
 - Is not marked as "Account Disabled".

When you select the Synchronize User Attributes tab, the left hand pane displays a list of enterprises to which the user being administered belongs to. The right hand pane displays a list of Synchronizable user attributes in a grid.

vanessa

▼ UserID
vanessa

Synchronize User Attributes Associate Enterprises

Enterprises

DFLT
DOC1
ENT1
ENT2

Use the following section to synchronize the selected user attributes for all above enterprises.

<input type="checkbox"/>	Synchronizable Attribute	Synchronized Value	Current
<input type="checkbox"/>	User Name	vanessa	
<input type="checkbox"/>	Email Address		
<input type="checkbox"/>	Enable LDAP Login	Yes	
<input type="checkbox"/>	LDAP Server Alias	LDAP	
<input type="checkbox"/>	Application Access	<input checked="" type="checkbox"/> Argus <input type="checkbox"/> Insight <input checked="" type="checkbox"/> Console	Disolav
<input type="checkbox"/>	Default Application	Argus	
<input type="checkbox"/>	Account Disabled	No	
<input type="checkbox"/>	Worklist to display at Login	-None-	
<input type="checkbox"/>	User Roles	<input checked="" type="checkbox"/> AC Library Admin <input checked="" type="checkbox"/> Copy Configuration <input checked="" type="checkbox"/> Enterprise User <input checked="" type="checkbox"/> ESM Admin	
<input type="checkbox"/>	Allow unblinding of cases	Yes	
<input type="checkbox"/>	Protect from unblinded information	No	

Save Print

The value of the Synchronizable fields can be modified for a specific enterprise so that these attributes can be different for that enterprise as compared other enterprises.

Note: If **User Name** and **Email address** fields are updated in Argus Safety Console for a user which belongs to multiple enterprises, an error displays.

If you make changes to the data on one of these tabs and attempts to move away from this current tab without saving the changes, then the warning message "You have made changes to the existing item, if you press **OK**, changes will be lost." displays. Click **OK** to ignore changes. Click **Cancel** to stay on the current tab.

Inactivating an Enterprise

It is recommended that you first archive all the cases belonging to the Enterprise before inactivating the Enterprise.

Add a New Enterprise

1. Click **Add New Enterprise**.
2. Enter information about your Enterprise in the required fields.
3. Click **Next**.
4. From **Copy Configuration Data Source**, select an Enterprise to use as a template for your new Enterprise.

Tip: You can make changes to the configuration once the enterprise has been set up.

5. Click **Setup**.
6. Click **Finish**.

New Enterprise Setup

It is expected that you create and choose the appropriate Enterprises with generic configuration data which can be used as source for copying the configuration data for creation of a new enterprises. Following is a list of items that are recommended to ensure that the values being copied from the source enterprise are appropriate for the newly created enterprise:

- Advanced Conditions used within any configuration item
- Reporting Destination Code List ' Company identifier field values
- System Numbering and LAM System Numbering Formats
- ESM Mapping Utility ' Setup INI File Setup ' Service DB Setup ' Outgoing and Incoming folders for each Agency.

Common Profile Switches

- MedWatch Configuration
- Documentum configuration
- Lot Number Web Service Configuration
- Case Processing - Default Network Directory for Scanned Images

Note: The Default Network Directory for Scanned Images is partitioned by enterprise/client. You can define separate image folders to accept company-specific image files for the New Case from Image functionality.

Data Segregation

Multi-tenancy allows an organization to use a single database for many clients, which reduces the amount of hardware needed for an implementation. Fewer patches and dictionary upgrades are required, which decreases the resources necessary to support an implementation. This also allows administrators to use standard configurations, such as code lists, workflow steps and user/new client setup.

The entire Argus Safety application and all of its components and data are partitioned by Enterprise ID. The Enterprise ID is a unique identifier for a customer's client and contract. The appropriate context of the Enterprise ID selected by the user that the user has access to, is set by the system and operates within the partition of this context.

Data Segregation by Module

The following table describes how each module in the Oracle Health Sciences Safety suite provides data segregation in a multi-tenant environment.

Note: It is not recommended that you open the Argus Safety application for multiple enterprises at the same time. Close the Argus Safety application for the previous enterprise before opening it for the next enterprise to avoid data issues.

It is recommended that you use the Application Access portlet to open the Argus Safety application for different enterprises, as it takes care of closing the previous enterprise before opening the new one.

Module	Cross Enterprise	Accessed Via Portal	Notes
Global Worklists	Yes	Yes	Displays data from across multiple enterprises.
Global User Management	Yes	Yes	Displays data from across multiple enterprises.
Global Enterprise Management.	Yes	Yes	Displays data from across multiple enterprises.
Applications Access	Yes	Yes	Displays Application Access options from across multiple enterprises.
Argus Safety	No	No	Displays data for one enterprise at a time to the logged-in user based on the selected enterprise.

Module	Cross Enterprise	Accessed Via Portal	Notes
Argus Console	No	No	Displays data only for the enterprise for which Argus Safety was opened by the user.
Argus Affiliate	No	No	Displays data for one enterprise at a time to the logged-in user, based on the selected enterprise.
Argus Unblinding	No	No	Displays data for one enterprise at a time to the logged-in user, based on the selected enterprise.
ESM Mapping Utility	No	No	Displays data for one enterprise at a time to the logged-in user, based on the selected enterprise. However, the screens related to ESM Service Configuration display data related to all the active enterprises, irrespective of the user access rights to those enterprises.
Argus Interchange Service	Yes	No	ESM Service process data from all the enterprises, as it is a background service.
ESM Service Configuration	Yes	No	As ESM Service is common across all the enterprises, hence its configuration tool is also common.
Argus Safety Service	Yes	No	Argus Safety Service processes data from all the enterprises as it is a background service.
AG Service Configuration Tool	Yes	No	As AG Service is common across all the enterprises, hence its configuration tool is also common.
MedDRA Re-code Tool	Yes	No	Allows the option to perform recoding of MedDRA terms across the enterprises.

Module	Cross Enterprise	Accessed Via Portal	Notes
MedDRA Dictionary Load	Yes	No	Single instance/version of the loaded MedDRA dictionary is available for all the enterprises.
MedDRA/WHO Web Services	Yes	No	These web services remain common to be used across all the enterprises. Their configuration is maintained in a common XML file on the web server(s).
J Drug Dictionary	Yes	No	Single instance/version of the loaded J Drug dictionary are available for all enterprises.
Case Intake	No	No	Case Intake messages for separate enterprises are segregated and loaded into appropriate enterprise partitions.
Literature Intake	No	No	Literature Case Intake data for separate enterprises are segregated and loaded into appropriate enterprise partitions.
New Case from Image	No	No	Scanned Image folder paths for separate enterprises are segregated and loaded into correct enterprise partitions.
PSL	No	No	The PSL interface segregates the incoming requests for each enterprise partition.
DLP	No	No	Partitions the case revisions by enterprises.
TMS Integration	No	No	TMS integration for single-pharma installations only.
Argus Dossier	No	No	As this module is linked to Periodic Reports, hence it partitions the periodic reports data by enterprise.

Module	Cross Enterprise	Accessed Via Portal	Notes
Global Worklists	Yes	Yes	Displays data from across multiple enterprises.
Global User Management	Yes	Yes	Displays data from across multiple enterprises.
Global Enterprise Management.	Yes	Yes	Displays data from across multiple enterprises.
Applications Access	Yes	Yes	Displays Application Access options from across multiple enterprises.

Data Segregation by Enterprise

Following is the list of items that are segregated by enterprises. It is recommended that you configure distinct values across enterprises to ensure proper data segregation across enterprises.

- Literature Intake folder: Argus Console ' Common Profile Switches ' Argus J ' Shared Path for the Literature Intake
- Case Intake folder: Argus Console ' Code List ' User Sites ' Intake File Path
- E2B Incoming Folder: ESM Mapping Utility ' Setup INI File Setup ' Service DB Setup ' Incoming Folder
- Site Printers: Argus Console ' Code List ' User Sites ' Site Printers ' Path

Maintaining Consistency Across Enterprises The following is the list of items that are segregated by enterprises but the CRO is recommended to maintain consistent across all enterprises:

- Common Profile Switches ' Argus Insight URL
- Common Profile Switches ' Argus Safety Load Balancer Server
- System Configuration ' Enabled Modules

In order to apply updates to the "Synchronizable" fields to all the enterprises in the system, you should maintain some administrative users with the Console'Access Management 'Groups' Menus 'Console: Access Management: User menu access enabled for all enterprises in the system.

Data Segregation impact on system-level configuration items

The following table specifies some specific system-level configuration items which are configured through Argus Console. It specifies the impact on these configuration items due to data segregation design for multi-tenant installations and also specifies the recommendations for customers on these items.

Configuration Item	Application Design	Recommendation for Customers	Configuration Item
Enable/Disable MedDRA/WHO Web Service Encoding	System keeps it segregated for each enterprise. However, the underlying web service used for MedDRA/WHO is common for all the enterprises as their configurations are maintained in common XML file on the web server(s).	None	Enable/Disable MedDRA/WHO Web Service Encoding
Lot Number Web Service configuration	System keeps it segregated for each enterprise.	As this is related to the product, Oracle recommends you keep it specific for each enterprise.	Lot Number Web Service configuration
Documentum Configuration	System keeps it segregated for each enterprise.	All parameters except for Cabinet Name are expected to be maintained as same for different enterprises.	Documentum Configuration
Enable/disable LDAP & LDAP Server configuration	This will be maintained by application as common for all enterprises.	None	Enable/disable LDAP & LDAP Server configuration
Enabled Modules	The system keeps it segregated for each enterprise.	None	Enabled Modules
Enable/disable SSO & SSO Header Configuration	This will be maintained by application as common for all enterprises.	None	Enable/disable SSO & SSO Header Configuration
Argus Insight URL	System keeps it segregated for each enterprise.	It is expected to be maintained same for across all enterprises by the customer.	Argus Insight URL
Argus Safety Load Balancer Server	System keeps it segregated for each enterprise.	It is expected to be maintained same for across all enterprises by the customer.	Argus Safety Load Balancer Server

Configuration Item	Application Design	Recommendation for Customers	Configuration Item
User Information	System keeps it segregated for each enterprise.	For multi-tenant installations, user attributes can be synchronized for all the enterprises through Global User Management. However, user attributes can also be updated for a specific enterprise through Console as well.	User Information
Default Enterprise	System keeps it segregated for each enterprise.	This is a new internal common profile switch that marks an enterprise as the Default enterprise. This is set during the time of install. Default enterprise once created during database creation is fixed. This is required to avoid the data synchronization issues that may occur for AG Service users in different enterprises.	Default Enterprise
SMTP Configuration	System keeps it segregated for each enterprise.	None	SMTP Configuration
Enable/Disable MedDRA/WHO Web Service Encoding	System keeps it segregated for each enterprise. However, the underlying web service used for MedDRA/WHO is common for all the enterprises as their configurations are maintained in common XML file on the web server(s).	None	Enable/Disable MedDRA/WHO Web Service Encoding
Lot Number Web Service configuration	System keeps it segregated for each enterprise.	As this is related to the product, Oracle recommends you keep it specific for each enterprise.	Lot Number Web Service configuration
Documentum Configuration	System keeps it segregated for each enterprise.	All parameters except for Cabinet Name are expected to be maintained as same for different enterprises.	Documentum Configuration

Configuration Item	Application Design	Recommendation for Customers	Configuration Item
Enable/disable LDAP & LDAP Server configuration	This will be maintained by application as common for all enterprises.	None	Enable/disable LDAP & LDAP Server configuration
Enabled Modules	The system keeps it segregated for each enterprise.	None	Enabled Modules
Enable/disable SSO & SSO Header Configuration	This will be maintained by application as common for all enterprises.	None	Enable/disable SSO & SSO Header Configuration
Argus Insight URL	System keeps it segregated for each enterprise.	It is expected to be maintained same for across all enterprises by the customer.	Argus Insight URL
Argus Safety Load Balancer Server	System keeps it segregated for each enterprise.	It is expected to be maintained same for across all enterprises by the customer.	Argus Safety Load Balancer Server
User Information	System keeps it segregated for each enterprise.	For multi-tenant installations, user attributes can be synchronized for all the enterprises through Global User Management. However, user attributes can also be updated for a specific enterprise through Console as well.	User Information
Default Enterprise	System keeps it segregated for each enterprise.	This is a new internal common profile switch that marks an enterprise as the Default enterprise. This is set during the time of install. Default enterprise once created during database creation is fixed. This is required to avoid the data synchronization issues that may occur for AG Service users in different enterprises.	Default Enterprise
SMTP Configuration	System keeps it segregated for each enterprise.	None	SMTP Configuration

Configuration Item	Application Design	Recommendation for Customers	Configuration Item
Enable/Disable MedDRA/WHO Web Service Encoding	System keeps it segregated for each enterprise. However, the underlying web service used for MedDRA/WHO is common for all the enterprises as their configurations are maintained in common XML file on the web server(s).	None	Enable/Disable MedDRA/WHO Web Service Encoding
Lot Number Web Service configuration	System keeps it segregated for each enterprise.	As this is related to the product, Oracle recommends you keep it specific for each enterprise.	Lot Number Web Service configuration
Documentum Configuration	System keeps it segregated for each enterprise.	All parameters except for Cabinet Name are expected to be maintained as same for different enterprises.	Documentum Configuration
Enable/disable LDAP & LDAP Server configuration	This will be maintained by application as common for all enterprises.	None	Enable/disable LDAP & LDAP Server configuration
Enabled Modules	The system keeps it segregated for each enterprise.	None	Enabled Modules
Enable/disable SSO & SSO Header Configuration	This will be maintained by application as common for all enterprises.	None	Enable/disable SSO & SSO Header Configuration

Data Shared Across Enterprises

Following is the list of items that are common for all enterprises

- MedDRA and WHO Web Services
- Common Profile Switches ' Security ' LDAP ' Enable/disable LDAP
- Common Profile Switches ' Security ' LDAP ' LDAP Server configuration
- Common Profile Switches ' Security ' Enable/disable SSO
- Common Profile Switches ' Security ' SSO Header Configuration
- Common Profile Switches ' Case Processing ' Where to store temporary case information during data entry
- Common Profile Switches ' Case Processing ' Auto Archiving ' The database job and its frequency - "Execution Period (in Days)"

- Default Enterprise

The common profile switches (related to SSO, LDAP, Auto Archiving job & frequency and Temporary Case Data Storage) which are common for all enterprises will only be displayed, updated and audit logged in DEFAULT enterprise. This is because any update to global level profile switches impacts all enterprises and is controlled. Also, such an update will also require propagation of the audit log to all other enterprises where the current user may not even exist or may not have proper access.

Applications Access

You can define which applications are enabled for a selected enterprise from the Argus Safety Console >User Management > Application Access.

Pre-upgrade Considerations for Existing Databases

Make sure that all the AG Service users (login user id) in all the databases that are to be merged into single database are in sync with the DEFAULT ENTERPRISE. If there are AG Service users in other enterprises which do not exist in the DEFAULT ENTERPRISE, then you can either rename their login user IDs to map them to existing AG Service users in the DEFAULT ENTERPRISE or delete them. If extra users are found in other enterprises during multi-tenant database migration, then they will be marked disabled and you will not be able to enable them later.

Make sure that all the event & indication and who-drug encoding dictionaries used in Argus Console ' System Configuration 'Common Profile Switches 'Case Form Configuration 'Auto Encoding, Dictionary and Central Encoding section and Argus Console ' Business Configuration 'Studies 'Enable Study Specific Encoding 'Auto Encoding dialog, in all databases that are to be merged into single database are already loaded in the target database with the same name. This is required to enable the automatic linking of dictionaries configured in the separate databases to the already existing dictionaries present in the target database during the database merge script/process.

Post-upgrade Considerations for Existing Databases

E2B Outgoing and Incoming folders is configured again in ESM Mapping Utility because various folders for different transmission methods are now merged as one pair of folders for all transmission methods. Now these are saved into database rather than the ESM Service INI file.

Document Type field value from ESM Service configuration and AG Service configuration tool is now be configured again into Argus Console ' Common Profile Switches ' Documentum configuration as these fields are now moved to Argus Console.

Make sure that all the event & indication and who-drug encoding dictionaries used in Argus Console ' System Configuration 'Common Profile Switches 'Case Form Configuration 'Auto Encoding, Dictionary and Central Encoding section and Argus Console ' Business Configuration 'Studies 'Enable Study Specific Encoding 'Auto Encoding dialog, in the newly migrated enterprises are linked properly to the global dictionaries already present in the target database. This is required to correct any dictionary configuration linking that could not be done automatically by the database merge script due to mismatch in dictionary names in the source and target databases.

Documentum Migration

Existing single-tenant as well as multi-tenant Documentum users upgrading to AS 7.0 release, and are migrating/keeping all the documents in the Documentum server, is also add additional attributes- "enterprise_id" and "enterprise_short_name" and populate these appropriately for all their documents that are to be accessed by Argus Safety in Documentum server.

Existing single-tenant as well as multi-tenant users which are upgrading to AS 7.0 release, and have configured "Use Logged in User's Username/Password" for Argus Console ' System Configuration ' Common Profile Switches ' Document Management for Case Attachments will switch to Common Username/Password for Documentum login if not already configured for E2B, Expedited and Periodic Reports.

MedDRA and WHO Webservices: As MedDRA and WHO webservice is common for each enterprise, it will use only single version for encoding events and drugs. However, as these web services use the dictionaries configured in Argus Console ' System Configuration 'Common Profile Switches 'Case Form Configuration 'Auto Encoding, Dictionary and Central Encoding section for the respective enterprises for populating dictionary id and dictionary version information for the encoded items, configure these dictionaries as same across all enterprises.