

# Oracle® Argus Safety

Release Content Document

Release 7.0

E22764-01

April 2011

---

## Change Record

Date	Author	Version	Change Reference
10-March-2011	Kapil Kedia	A	New Document

## Disclaimer

This Release Content Document (RCD) describes product features that are proposed for the specified release of the Oracle Argus Safety. This document describes new or changed functionality only. Existing functionality from prior point releases is not described. It is intended solely to help you assess the business benefits of upgrading to Release 7.0.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Software License and Service Agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

## Introduction

### Purpose of Document

The Release Content Document (RCD), produced as part of Oracle's Applications Product Lifecycle (APL), communicates information about new or changed functionality in the specified release of the Oracle Argus Safety. Existing functionality from prior point releases is not described. However, content introduced by Family

Packs, Mini-Packs or Standalone patches since the prior point release has been included in this document and denoted accordingly.

- Oracle Argus Safety 7.0

## Release Overview

Contract Research Organizations (CROs) may offer a range of global safety and pharmacovigilance services, which span from limited case management activities to full clinical trial and post-marketing services, and anything in between.

Multi-tenancy support will increase a CRO's ability to increase their profit margin. Multi-tenancy users will be able to reduce from many databases to a single database. This will enable them to reduce the amount of hardware needed for an implementation, reduce the number of patches and dictionary upgrades periodically performed, and subsequently reduce the resource requirements to support the implementation. They will be able to leverage standard configurations, such as code lists, workflow steps and user/new Enterprise setup

## Reference Documents

Name	Location	Completion Date
Argus Safety 7.0 BRD	Caliber	
Argus Safety 7.0 FDD	Clearcase	

## Oracle Argus Safety 7.0 Product Overview

Following are the features that are new with the release of Oracle Argus Safety 7.0:

### Segregate data by Enterprise

#### Partitioned data

The option of segregating data by Enterprise profiles allows the user to maintain the data set in one database but protected across different Enterprises based on the security permissions defined to the user

#### Display Enterprise identifier

The identifier for the partitioned data set is displayed when a user is viewing or processing Enterprise cases

#### Change Enterprises within the same session

Users should only be able to create or access cases with respect to the partitioned data set being accessed. Users will not be able to have two cases from two different Enterprises open at the same time and would be able to access cases across Enterprises without the need to log off from the application whilst switching Enterprises

### **Enter a case for a Enterprise**

The user has to choose the appropriate enterprise while creating a new case

### **Intake cases for a Enterprise**

Users shall have the option to import cases in the correct enterprise via the following based on their permissions as well as the Enterprises which they have access to

- E2B Import for structured data
- Worklist Intake for Unstructured data.
- Affiliate intake

### **Receive E2B imports for a Enterprise**

The messages can be received via email, electronic media, or a gateway. Each E2B message can contain one or many cases. Each message may contain one or more reports. Standard error processing is managed on a Enterprise by Enterprise basis. Here, It is assumed that the gateway product can be configured to route E2B messages to uniquely identified folders based upon status of the combination of <messagereceiveridentifier> and the <sender ID> or the dedicated web address

Following are a few examples for E2B import:

- Manually import an E2B message
- Import an identifiable imported E2B message

### **Import or export additional data elements beyond E2B for a Enterprise**

Extended E2B elements are also supported for Export as well as Import for a Enterprise.

## **Global Work list**

### **Segregate data based upon Enterprise authorization**

CRO users will log into the safety application a single time and need to be presented with a Worklist of their cross-enterprise work, and the ability to access each project for which they are authorized. The CRO user needs to review, sort and filter a list of work across their authorized Enterprises/projects, create process, review and report cases if authorized, access the query module for each enterprise, and for administrators, manage the configuration for each enterprise

### **Process data for Enterprises a user is authorized to access**

A given user may have work that extends across several Enterprises, not a single Enterprise. Users need to see the sum of all work, so they can prioritize effectively and understand the amount of pending work assigned to them

### **Global worklist types**

Global Worklist allows the Users to view the data across multiple enterprises based on their security permissions.

Following are the sample Worklist available:

- Case-based (New, Open)

- Action items
- Contacts

## **Multi-tenancy Enterprise setup and maintenance**

### **Enable multi-tenancy usage**

When processing data for a Enterprise, a CRO user requires that Enterprise's cases and configuration be partitioned. Partitioning of data and the additional interfaces that support accessing separate Enterprises should only be available in the multi-tenancy deployment and not impact single-tenant implementations.

### **Establish Enterprises**

A "enterprise" is the highest level for which data is isolated. A Enterprise can include one or more studies/programs, one or more products, one configuration, and one set of user permissions such as unblinding access. Each Enterprise may have one or more dictionaries (i.e., dictionary by study).

### **Enterprise configuration setup wizard**

To correctly setup a new Enterprise, several sequential steps must be completed. The system administrator should be able to quickly establish a new Enterprise in the database, based upon selecting from standard libraries or by copying from an existing setup. Enterprise-specific adjustments should be able to be made during the initial setup, or alternatively at some later time when Enterprise-specific configurations are clearly identified.

- Enable the administrator to copy a setup from an existing setup. Note some Enterprise-specific data should not be included in a copy, including products, actual study information and license information.
- The wizard should include some or all the following:
  - Enterprise ID
  - Drug Dictionary (Create, Load and configure for the Enterprise)
  - Reportability rules
  - Workflow steps
  - Code list values
  - E2B settings
  - Grant user access to Enterprise
  - Screen/field modifications

### **Modify an Enterprise**

The setup of a Enterprise may need to be change. New studies or post marketing services may be added or completed to an existing Enterprise; configuration such as workflow steps, code list items, screen and field setup, and spare field use may be changed.

When an administrator modifies the Enterprise setup, he needs to clearly be presented the Enterprise's existing options. The ability to modify Enterprise configuration should be controlled by user permissions.

### **Control user access to Enterprises/Enterprise data**

Access to each Enterprise's study/project should be controlled on a user-by-user basis.

### **Migrate to multi-tenancy**

Existing CRO Enterprises must migrate from a single-tenant implementation to a multi-tenant implementation

## **Security Requirements**

A large CRO houses data for hundreds of clinical trials at a given time, and is subsequently the constant target of attacks. Since part of the safety application is exposed outside of the CRO, the application must be able to defend itself from hacking. Types of potential attacks include but are not limited to cross-site scripting, SQL injection, cross-site request forgery, and parameter tampering.

## **Tracking Items Sent to Investigators**

Queries may be sent to investigators to clarify or gather information in an adverse event case. When a query is sent to an investigator, the drug safety group needs to track that they query has been sent. When an investigator is sent a query, it should be automatically marked as being sent for tracking purposes.

## **Overdue Action Items Filtering**

During adverse event case processing, action items may be created to enable additional people not necessarily in the workflow to participate in case tasks. When a task is overdue, it should be marked as such, and the list of tasks should be able to be filtered by overdue tasks.

## **Terminology**

Term	Definition
CRO	Contract Research Organization
E2B	ICH data format for electronic ICSR exchange.
ICH	International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use
ICSR	Individual Case Summary Report
Study	Studies (or protocols) to evaluate the effectiveness and safety of medications or medical devices by monitoring their effects on large groups of people

## **Documentation Accessibility**

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive

technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

### **Accessibility of Code Examples in Documentation**

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

### **Accessibility of Links to External Web Sites in Documentation**

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

### **TTY Access to Oracle Support Services**

To reach AT&T Customer Assistants, dial 711 or 1.800.855.2880. An AT&T Customer Assistant will relay information between the customer and Oracle Support Services at 1.800.223.1711. Complete instructions for using the AT&T relay services are available at <http://www.consumer.att.com/relay/tty/standard2.html>. After the AT&T Customer Assistant contacts Oracle Support Services, an Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process.

---

Oracle Argus Safety Release Content Document, Release 7.0  
E22764-01

Copyright © 2101, 2011 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 software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

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

This software 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 which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on 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. 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.