

# Oracle Argus Safety

## Multi-tenancy Administration Guide



Release 8.4.3

G41377-01

May 2024

ORACLE®

Copyright © 2021, 2024, Oracle and/or its affiliates.

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, software documentation, data (as defined in the Federal Acquisition Regulation), 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 embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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

---

Documentation accessibility	i
Diversity and Inclusion	i
Related resources	i
Access to Oracle Support	i

## 1 Overview

---

## 2 Global Homepage

---

Global Homepage	1
Global Worklist	1
Global Enterprise Management	2
Add a new enterprise	3
New enterprise setup	4
Inactivate an enterprise	5
Global User Management	5
Synchronizable user attributes	5
User-enterprise association	7
Application access	8

## 3 Data segregation

---

Data segregation by module	1
Data segregation by enterprise	3
Data segregation impact on system-level configuration items	4
Data shared across enterprises	5

## 4 Documentum migration

---

## 5 Pre-upgrade considerations for existing databases

---

## 6 Post-upgrade considerations for existing databases

---

# Preface

This preface contains the following sections:

- [Documentation accessibility](#)
- [Diversity and Inclusion](#)
- [Related resources](#)
- [Access to Oracle Support](#)

## 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>.

## Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

## Related resources

For information about Oracle Argus patches, see [My Oracle Support](#).

All documentation and other supporting materials are available on the [Oracle Help Center](#).

## Access to Oracle Support

To receive support assistance, determine whether your organization is a cloud or on-premises customer. If you're not sure, use Support Cloud.

### **Cloud customers receive support assistance through Support Cloud**

Oracle customers that have purchased support have access to electronic support through Support Cloud.

Contact our Oracle Customer Support Services team by logging requests in one of the following locations:

- English interface of Oracle Life Sciences Support Cloud (<https://hsgbu.custhelp.com/>)

- Japanese interface of Oracle Life Sciences Support Cloud へようこそ (<https://hsgbu-jp.custhelp.com/>)

You can also call our 24x7 help desk. For information, visit [Life Sciences Support | Oracle](#) or visit [Oracle Accessibility Learning and Support](#) if you are hearing impaired.

**On-premises customers receive support assistance through My 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.

# 1

## Overview

The multi-tenancy feature in Oracle Argus Safety enables multiple pharmaceutical clients of a CRO to reside as separate and unique tenants in a single database, with their data completely segregated and available to authorized users only.

It enables a CRO to achieve standard configuration across clients, and at the same time provides the ability to have different configurations for specific clients, as required.

It also provides the ability to a CRO to quickly set up a new client based on an existing configuration, and authorize users to the new client. It also enables CRO users who have access across multiple clients to view and understand their work across clients, and to make priority-based decisions.

# 2

## Global Homepage

Global Homepage allows Argus users to perform specific actions across multiple active enterprises and supports multi-tenant installation.

For more information, see:

- [Global Homepage](#)
- [Global Worklist](#)
- [Global Enterprise Management](#)
- [Global User Management](#)
- [Application access](#)

## Global Homepage

The following out-of-the-box Portlets are accessible to all multi-tenant users who need to access data across multiple enterprises, except the ones specifically recommended for administrators:

- Global Worklist
- Global Enterprise Management: Recommended for Administrators
- Global User Management: Recommended for Administrators
- Application Access

Global Homepage can be accessed using the SSO and the portal users who access Global Homepage need to be configured as LDAP user in all the enterprises in which the user is not a disabled user.

In multi-tenant installations, Global Homepage and Oracle Argus Safety are two different applications that are available for end-users and CRO/Hosting administrators.

Both these web applications have separate web URLs which can be accessed independently.

When you enter the URL of any of these web applications, the SSO module authenticates the user credentials and allows access to these applications without asking for any user credentials.

For Global Homepage, if the SSO authentication fails, the application displays an error message returned by SSO module.

For Oracle Argus Safety, if the SSO authentication fails, the application displays an error message returned by the SSO module.

## Global Worklist

The Global Worklist portlets allow you to access work items across authorized enterprises or clients. You can filter the Worklist for specific enterprises or clients that you can access. When you use a filter for a specific enterprise or client, any further operations on the retrieved Worklist items are restricted to that specific enterprise or client.



1. The context menu that is invoked on Global Worklist displays the action menu items based on your access rights and roles in the enterprise to which the selected records belong.
2. The user preferences of each Global Worklist are remembered for the user every time the Worklist is loaded. User preferences for Global Worklists are maintained in addition to the enterprise-specific user preferences which are applicable for the user in Argus Safety Worklists.
3. Each of these Global Worklists only displays data from the enterprises within which the user has access to that specific Worklist Menu item.

The following Global Worklist Portlets are provided in the Global Homepage:

- **Global Worklist – New:** This Worklist displays a list of cases across all enterprises and clients, or specific to one enterprise or client, according to your selection. You can only see cases that you have access to, or which have been assigned to you, but are not yet accepted.
- **Global Worklist – Open:** This Worklist displays a list of cases across all enterprises and clients, or specific to one enterprise or client, according to your selection. You can only see cases that you have access to, and were accepted by you or your user group.
- **Global Worklist – Action Items:** This Worklist displays a list of pending action items across all enterprises and clients, or specific to one enterprise or client, according to your selection. You can only see cases that you have access to.
- **Global Worklist – Contacts and Letters:** This Worklist displays a list of pending letters across all enterprises and clients, or specific to one enterprise or client, according to your selection. You can only see cases that you have access to.

### Note

The application offers the flexibility to hide some of the fields or columns in the Global Worklist portlets through the Global Worklist grid or menu XMLs, which reside on the Web Server(s). We recommend that you only hide the fields or columns which are not updated, nor referred by any Worklist context menu actions.

Global Worklist											
Global Enterprise Management				Global User Management		Application Access					
Worklist New		Worklist Open		Worklist Action Items		Worklist Contacts					
Search Case											
Filter		Value				Group Membership					
Case Number		<input type="text" value=""/>				<input type="text" value="All"/>					
<input type="checkbox"/> Only view locked Cases requiring Follow-up											
Total Number of Rows (64)											
Displaying Rows 1 to 4											
Page Size 100											
View Individual Group All											
Enterprise ID	Lock State	Priority	Receipt Date / Start Date	Days Open/ Remaining	Case Number Workflow State / Group	Product Name Generic Name	Event PT Event Validation	SUB F, L, E or H	Case Type Study ID	Reporter Type Country	Assigned To Owner
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="11-777-0000"/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="77-777-0000"/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>
DEFAULT		Initial	01-Sep-2019 01-Sep-2019	438 0	18-000009 Data Entry /	Shigeno (TRADE ASSURANCE) Shigeno-GENERIC DOB	Central Interlock Central Interlock	Y/N	Sponsored Trial Shigeno STD_048	JAPAN	(Unassigned) (Unassigned)
DEFAULT		Initial	0 13-Sep-2019	426 0	18-000009 Data Entry /	Amazac US Amazac-GENERIC DOB	Headache Headache	N/Y	Spontaneous	Physician US	(Unassigned) (Unassigned)
DEFAULT		Initial	0 13-Sep-2019	426 0	18-000009 Data Entry /	Amazac US Amazac-GENERIC DOB	Headache Headache	N/Y	Spontaneous	Physician US	(Unassigned) (Unassigned)
DEFAULT		Initial	0 27-Sep-2019	412 0	18-000009 Data Entry /	Keppa METFORMIN	Hemorrhage bleeding	Y/N	Sponsored Trial USC_UNBLIND	Hospital UNITED KINGDOM	(Unassigned) (Unassigned)
DEFAULT		Initial	0 27-Sep-2019	412 0	18-000009 Data Entry /	Keppa METFORMIN	Hemorrhage bleeding	Y/N	Sponsored Trial USC_UNBLIND	Hospital UNITED KINGDOM	(Unassigned) (Unassigned)
DEFAULT		PRQ: 3	0 08-Jul-2019	409 0	18-000009 Data Entry /	pyracic pyracic	Pyrexia fever	Y/N	Spontaneous	Hospital US	(Unassigned) (Unassigned)
DEFAULT		Initial	0 01-Nov-2019	377 0	18-000009 Data Entry /	Levetiracetam METFORMIN	Insomnia Insomnia	N/Y	Spontaneous	Physician UNITED KINGDOM	(Unassigned) (Unassigned)
DEFAULT		Initial	0 01-Dec-2019	347 0	18-000009 Data Entry /	JAMPROD1 MKT JAMPROD1	Pyrexia fever	N/Y	Spontaneous	US	(Unassigned) (Unassigned)

## Global Enterprise Management

Global Enterprise Management enables you to quickly create new enterprises or clients, and to authorize users. It also helps you quickly define enterprises based on existing configurations.

From the **Global Enterprise Management** tab, you can:

- [Add a new enterprise](#)

- [New enterprise setup](#)
- [Inactivate an 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.



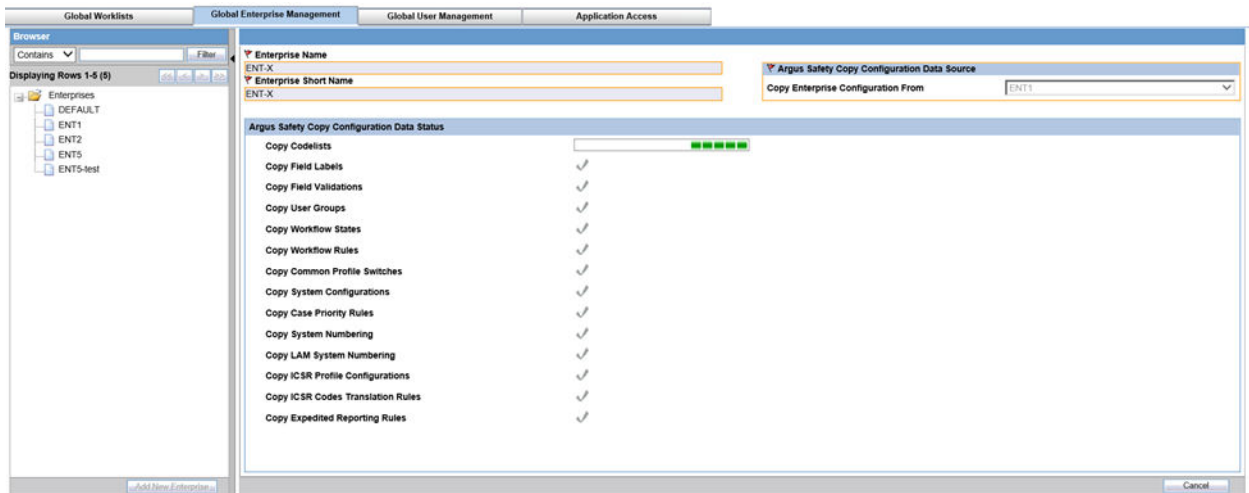
### Tip

You can make changes to the configuration once the enterprise has been set up.

5. Click **Setup**.
6. Click **Finish**.

During Copy Configuration, the system copies the configuration to the new enterprise created:

- Codelists
- Field Labels
- Field Validations
- User Groups
- Workflow States
- Workflow Rules
- Common Profile switches
- System Configuration
- Case Priority Rules
- System Numbering
- LAM System Numbering
- ICSR Profile Configurations
- ICSR Codes Translation Rules
- Expedited Report Rules



## New enterprise setup

You should create and choose enterprises with generic configuration data which can be used as a source to create new enterprises. We recommend you include the following items 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
- Reporting Destination Code List > Company identifier field values System
- Numbering and LAM System Numbering Formats
- Reporting Destination codelist > EDI Tab > Incoming / Outgoing / Attachment folders for each agency.

### Common Profile Switches

- MedWatch Configuration
- Documentum configuration
- Lot Number Web Service Configuration

### Copy Intake configuration

When you set up a new Enterprise, if the Intake module is enabled in **Argus Console > System Configuration > Enabled Modules**, then the system displays the option to setup Intake Enterprise after Argus Safety enterprise setup is complete.

If the Argus Safety Enterprise is already created and the Intake Module is enabled later, then the system checks if the enterprise setup is not already completed for Intake and then displays the **Copy Enterprise to Intake** option as enabled. If the setup is already completed for the selected enterprise, then the option is disabled.

You can select the source enterprise from which the Intake configuration is copied to the enterprise being setup for Intake. By default, the enterprise used for Argus Safety is selected in the Enterprise dropdown for Intake, but you can change it as needed.

## Inactivate an enterprise

An enterprise can be made inactive by unchecking the Active check box on the Global Enterprise Management screen.

### Note

We recommend that you first archive all the cases belonging to the enterprise before inactivating the enterprise.

## Global User Management

Global User Management allows you to associate the users to multiple enterprises, but also to keep their user attributes in sync across all enterprises.

### Note

This portlet is displayed to the user having access to the **Global Admin** role for one or more enterprises.

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. Service users are not listed in the tree view of the Global User Management screen.

### Note

Oracle Argus Safety Console allows the 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 the 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.

For more information, see:

- [Synchronizable user attributes](#)
- [User-enterprise association](#)

## 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:

1. Admin users, System users and users for which the Service User is checked in Oracle Argus Safety Console are not listed.

2. 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.
  - 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.

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.

The following the list of attributes on which synchronization can be done:

1. User Name
2. Email Address
3. Enable LDAP Login
4. LDAP Server Alias
5. Application Access
6. Default Application
7. Account Disabled
8. Worklist to display at Login
9. User Roles
10. Allow unblinding of cases
11. Protect from unblinded information
12. Protect from printing unblinded information
13. Allow closing of cases
14. Route on close case
15. Enable Checklist on Route

Global Worklists Global Enterprise Management Global User Management Application Access

LDAP1

Contains Filter

Displaying Rows 1-21 (21)

Users

- argus\_h
- boddach
- boddachdap
- dlinidap
- glady\_s\_idap
- jmorton
- jmorton2\_idap
- jmorton\_idap
- keggadi
- ldap1
- lilas\_idap
- mclark
- mclark\_idap
- shsuzuke
- shsuzuke\_idap
- shsuzukij
- shsuzukij\_idap
- shjalperm
- somarajuc
- somarajuc\_idap
- tommy

Synchronize User Attributes Associate Enterprises

Enterprises

DEFAULT

ENT-X

ENT1

ENT2

Use the following section to synchronize the selected user attributes for all above enterprises.

Synchronizable Attribute	Synchronized Value	Current Value
<input type="checkbox"/> User Name	LDAP1	
<input type="checkbox"/> Email Address		
<input type="checkbox"/> Application Access	<input checked="" type="checkbox"/> Argus <input type="checkbox"/> Insight <input checked="" type="checkbox"/> Console	Display
<input type="checkbox"/> Default Application	Argus	
<input type="checkbox"/> Account Disabled	No	
<input type="checkbox"/> User Roles	AC Library Admin	

Configure Synchronizable Attributes Save Print

### Note

If **User Name** and **Email Address** fields are updated in Oracle 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.*

### 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.

### Note

In order to apply updates to the “Synchronizable” fields to all the enterprises in the system, the customer is required to maintain some administrative users with the Console > Access Management > Groups > Menus > Console: Access Management: User menu access enabled for all enterprises in the system.

## User-enterprise association

To associate existing users from one enterprise to other enterprises:

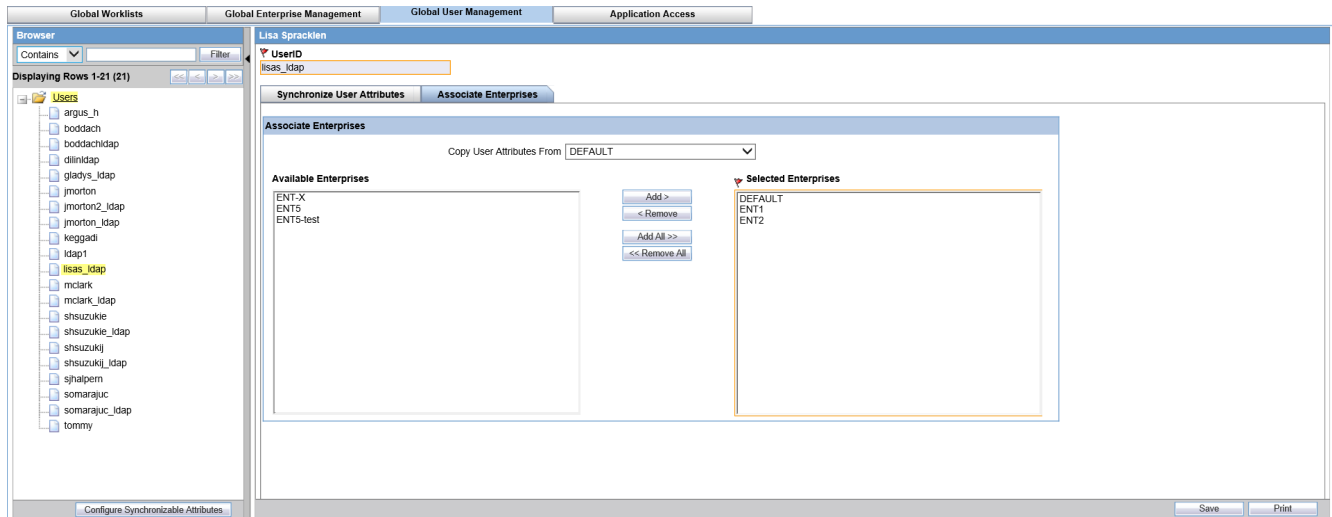
1. Select an enterprise from **Copy User Attributes From**.
2. Add an **Available Enterprise** or **Add All** available enterprises.
3. Select **Save**.

**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.

- 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.



## Application access

The Applications Access Portlet allows the users to launch the Argus applications for an enterprise that they have access to.

The following options are provided in Application access:

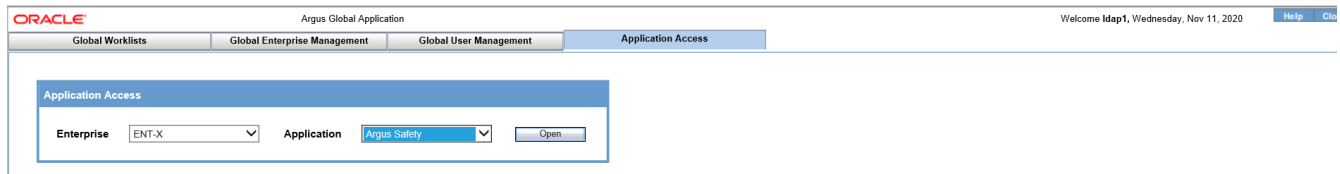
- Argus Safety
- Argus Safety Bookin
- Argus Affiliate
- Argus Affiliate Event Entry
- Argus Insight
- Safety One Intake

**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.

The Argus Safety Bookin option opens the Case Bookin screen within the Oracle Argus Safety for the selected enterprise.

The Argus Affiliate Event Entry option opens up the Local Event Entry screen within Oracle Argus Insight for the selected enterprise.



The Safety One Intake option is available only if you have the Intake Processor role assigned to you in Argus Console. This option is also available if you are assigned to a group which has access to Argus Console and System Configuration under Group Configuration in Console > Access Management > Argus > Groups > [Assigned Group] > Group Information > Menus and if you have access to Argus Console in user configuration.

**Note**

You may or may not have the Intake Processor role assigned for this condition to be valid.



# 3

## Data segregation

Multitenancy 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 codelists, workflow steps and user/new client setup.

The entire Oracle 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.

For more information, see:

- [Data segregation by module](#)
- [Data segregation by enterprise](#)
- [Data segregation impact on system-level configuration items](#)
- [Data shared across enterprises](#)

## 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 Oracle Argus Safety application for multiple enterprises at the same time. Close the Oracle 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 Oracle 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.

Module	Cross Enterprise	Accessed Via Portal	Notes
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.
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.
Argus Interchange Service	Yes	No	Argus Interchange Service processes data from all the enterprises, as it is a background service.
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.
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).

Module	Cross Enterprise	Accessed Via Portal	Notes
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.
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.

## 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: Console > Common Profile Switches > Safety Japan > Shared Path for the Literature Intake
- Case Intake folder: Console > Code List > User Sites > Intake
- Site Printers: Console > Code List > User Sites > Site Printers

### 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 > Insight URL
- Common Profile Switches > 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 Oracle Argus Safety 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
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
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.
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.
Enable/disable LDAP & LDAP Server configuration	This will be maintained by application as common for all enterprises.	None
Enabled Modules	The system keeps it segregated for each enterprise.	None
Enable/disable SSO & SSO Header Configuration	This will be maintained by application as common for all enterprises.	None
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 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.
User Information	System keeps it segregated for each enterprise.	For multitenant 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 Oracle Argus Safety Console as well.

Configuration Item	Application Design	Recommendation for Customers
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.
SMTP Configuration	System keeps it segregated for each enterprise.	None

## 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 > Auto Archiving > 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.

# 4

## Documentum migration

Existing single-tenant as well as multitenant 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 Oracle Argus Safety in Documentum server.

Existing single-tenant as well as multitenant users which are upgrading to AS 7.0 release, and have configured Use Logged in User's Username/Password for 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 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.

# 5

## 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 Console > System Configuration > Common Profile Switches > Case Form Configuration > Auto Encoding, Dictionary and Central Encoding section and 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.

# 6

## Post-upgrade considerations for existing databases

Make sure that all the event & indication and who-drug encoding dictionaries used in Console > System Configuration > Common Profile Switches > Case Form Configuration > Auto Encoding, Dictionary and Central Encoding section and 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.