

Oracle® Health Sciences ClearTrial Cloud Service

System Administrator User Guide

Release 4.8

E36702-01

September 2012

Copyright © 2012, Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT 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 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.

Contents

Preface	v
Audience	v
Documentation Accessibility	v
Related Documents	v
 1 Introduction to ClearTrial Terms	
1.1 ClearTrial Terms	1-1
 2 User Account Management	
2.1 ClearTrial User Roles and Descriptions.....	2-1
2.1.1 Primary Roles	2-1
2.1.2 Additional Roles and Capabilities.....	2-1
2.2 Creating User Accounts	2-2
2.3 Editing User Accounts.....	2-3
2.4 Deleting User Accounts	2-4
2.5 Restoring Deleted User Accounts.....	2-4
2.6 Clearing User Sessions	2-4
2.7 Locking and Unlocking User Accounts.....	2-4
2.7.1 Locking Accounts	2-5
2.7.2 Unlocking Accounts	2-5
2.8 Inactive Users Report	2-5
 3 Resetting a Forgotten Password	
3.1 Reset a Password.....	3-1
3.2 Resetting an Account.....	3-1
 4 Managing Deleted Items	
4.1 Purging Deleted Items.....	4-1
 5 Configurable ClearTrial Parameters	

Preface

The Oracle Health Sciences ClearTrial Cloud Service System Administrator User Guide is a reference for System Administrators who are managing user accounts for their organization.

Audience

This document is intended for System Administrators who are managing ClearTrial user accounts.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

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

Related Documents

For more information, see the following documents in the Oracle Health Sciences ClearTrial Cloud Service Release 4.8 documentation set:

- *Oracle Health Sciences ClearTrial Cloud Service v4.8 Release Notes*
- *Oracle Health Sciences ClearTrial Plan and Source Cloud Service User Guide*
- *Oracle Health Sciences ClearTrial Track Cloud Service User Guide*

Introduction to ClearTrial Terms

System Administrators should be familiar with the following ClearTrial terms.

1.1 ClearTrial Terms

- **Authentication:** The process of providing information that identifies a user to an application. A common means of authentication is to login with a user name and password.
- **Authorization:** Specific permissions, or privileges, that control what features and data are available to a user.
- **Credentials:** Information submitted to an application in order to be authenticated and/or authorized. For example, a user name and password.
- **User Account:** Each user has an account that stores their credentials, personal data, and preferences
- **Permission:** An expressed authority to use a specific feature or access certain data.
- **Role:** A group of permissions that can be granted to a user.
- **Edit Mode:** One of four levels of interaction that control which fields the user can access. Quick Mode is intended for either "ballpark" estimation or novice users, Basic Mode is for normal operation, Advanced Mode is intended for use when planning studies with unusual or specific assumptions that differ from the defaults and Expert Mode allows the user to access every field.
- **Maximum Edit Mode:** The Maximum Edit Mode is the highest edit mode users are authorized to use.
- **Preferred Edit Mode:** ClearTrial defaults users to their Preferred Edit Mode every time they create a new study or plan. Users can change their preferred edit mode by using the Edit Profile button.
- **Preferred Home Page:** ClearTrial allows users to select the preferred screen they need displayed upon logging in. Users can select the Plan List, Study List, or Portfolio List Screens to be displayed.
- **Preferred Locale:** The Preferred Locale is the geographic location of the user. System Administrators can select the Preferred Locale for a user, which will determine how dates and numbers are displayed in ClearTrial.
- **Security Question and Answer:** Upon registration, users select a security question and provide an answer. System Administrators use this information to identify a user to reset their password. Users need this information to reset their password with the "Forgot your Password?" feature.

User Account Management

Every ClearTrial user must have a corresponding user account to access the system. Users that have System Administrator permissions can manage user accounts for their organization.

2.1 ClearTrial User Roles and Descriptions

In ClearTrial, there are Primary Roles and Additonal Roles/Capabilites that can be assigned to users. To access the application, users must be assigned a Primary Role. The Additional Roles/Capabilities are not required to access ClearTrial, but they can be assigned to users to grant them permissions to access certain features or perform specific job responsibilities.

2.1.1 Primary Roles

Primary roles are assigned by the System Administrator when user accounts are created or edited. A user must be assigned one of these roles to access ClearTrial.

- **Read-Only User:** The Read-Only User role grants permission to view products, studies, plans, etc., but does not allow the user to create, edit, or delete any of these items. This role does not have permission to modify notes or export data from the application.
- **User:** The User role grants permission to view products, view studies, and to create, edit, and view plans. Users can edit plans they have created, but cannot edit plans created by other users.
- **Power User:** The Power User role grants all of the permissions of User, along with the ability to create, edit, view, and delete templates and studies. Power Users can edit plans created by other users.
- **Clinical Administrator:** The Clinical Administrator grants all of the permissions of Power User, along with the ability to create and maintain products, service providers, and billing rates.
- **System Administrator:** The System Administrator role grants permission to manage ClearTrial users.

2.1.2 Additonal Roles and Capabilities

The Additional Roles and Capabilities described below grant users additional capabilities that are not included with the Primary Roles. These roles and capabilities allow users to access various features in ClearTrial. System Administrators have the ability to grant users these roles.

- **Exchange Rates Administrator:** The Exchange Rates Administrator grants permissions required to create, edit, view, and delete shared exchange rate tables.
- **Resources Administrator:** The Resources Administrator grants permissions required to create, edit, view, and delete resources. The Resources capabilities are only available to Enterprise Licensed users.
- **Reporting Regions Administrator:** The Reporting Regions Administrator role grants permissions to create, edit, and delete reporting region names and to map countries to reporting regions. Mapping enables you to view the budget by location with the Monthly Budget by Reporting Region Report on the Reports Tab. The Reporting Regions capabilities are only available to Enterprise Licensed users.
- **Departments/GL Codes Administrator:** The Departments/GL Codes Administrator role grants permissions to create, edit, and delete departments and GL Codes. This role allows you to map labor fees and costs to departments and GL Codes by resource, location, task, or a combination of rules. Mapping allows you to view budget fees and costs by departments and GL Codes within reports on the Reports Tab.
- **WBS Editor:** The WBS Editor role grants permissions to create, edit, and delete plan-specific major tasks, tasks, and resources in the Work Breakdown Structure (WBS) in plans created by the user. This role allows the user to view and edit the Level of Effort Algorithm for a plan-specific task and resource. The WBS Editor is only available to Enterprise Licensed Users.
- **WBS Manager:** The WBS Manager role grants all of the WBS Editor permissions, with the added ability to edit and delete major tasks, tasks, and resources in the Work Breakdown Structure (WBS) of plans created by other users. This role allows the user to view and edit the Level of Effort Algorithm for a plan-specific task and resource. The WBS Manager is available to Enterprise Licensed Users.
- *Can edit notes:* This capability can be granted to Read-Only Users to allow them to edit notes associated with plans or other items for the purposes of review.
- *Can export report data:* This capability can be granted to Ready-Only Users to allow them to export reports to PDF, Excel, or CSV.
- *Can access WS-API:* For customers who have licensed the Web Services API Product, this capability can be granted to users or accounts that will interact with the applications programmatically. The users's primary role and other capabilities control what data they can view, edit, create or delete with the API.

2.2 Creating User Accounts

Users with the System Administrator role can create user accounts for their organization.

To create an account:

1. Login to the application.
2. Select Users from the Admin menu to display the User List Screen.
3. Click the New button to view the Create User Screen. The Profile Tab allows you to enter user information and the Roles Tab allows you to select user roles.
4. On the Profile Tab, enter the user's login name. This is the name or phrase he or she will type in the login field. Enter the user's first name, last name, and email address. The email address will allow the user to access the "Forgot Your Password?" feature.

5. Next, select the Maximum and Preferred Edit Modes.

The Maximum Edit Mode is the highest mode the user can access while creating plans. The Preferred Edit Mode is in effect when a plan is created by a user. Users can change this edit mode by selecting their login name in the upper right corner of the screen and clicking the Edit Profile button.

6. Next, select a Preferred Home Page and Preferred Locale for the user.

The Preferred Home Page is the screen a user will see upon logging in. Users can change this by editing their user profile. The Preferred Locale is the geographic location of the user. The selected location determines how dates and numbers are displayed.

7. Click Save and an email is sent to the user with the customer code, login name, and a link to complete the registration. Users will be prompted to create a password upon logging in. Passwords must contain the minimum number of characters specified by the system administrator. For more information about configuration settings, see Configurable ClearTrial Settings.

User passwords are required to have at least one number and one letter. Passwords must also contain a special character from the following: !\$*+-.=?@^_ | ~. Passwords cannot contain user's login name or the words: password, oracle, guest, admin, administrator, cleartrial.

Note: If your organization does not allow user account information to be sent through email, you need to communicate the customer code, login name, and temporary password to the user through a secure form of communication.

8. Upon logging in, users will be prompted to set a security question and answer. The security question and answer are used to identify a user attempting to reset his or her password.
9. Navigate to the Roles Tab.
10. On the Roles Tab, you need to assign a Primary Role for the user. Primary Roles grant the user access to ClearTrial. To assign a Primary Role, select one from the drop-down menu. The Additional Roles and Capabilities grant permissions that are not included with the Primary Roles. To assign these roles, select them from the list. Click Save.

For more information about user roles, refer to ClearTrial User Roles and Descriptions.

After an account has been created, the user receives an email with instructions on how to complete their registration.

2.3 Editing User Accounts

Users with the System Administrator role can edit user accounts for their organization.

To edit a user account:

1. Login to the application.
2. Select Users from the Admin menu to display the User List Screen. Select a user account and click the Edit button to view the Profile and Roles Tabs.
3. Edit information as needed and click Save.

2.4 Deleting User Accounts

System Administrators can delete and restore user accounts. Deleting a user account marks the user profile invalid and the user cannot login. User accounts are not immediately discarded from the system, they can be restored for up to 30 days or until the record is purged. For information on purging deleted items, see Managing Deleted Items.

To delete a user account:

1. Login to the application.
2. Select Users from the Admin menu to display the User List Screen.
3. Select one or more users and click the Delete button to remove them from the list.

2.5 Restoring Deleted User Accounts

System Administrators can restore deleted user accounts. Deleted accounts can be restored for up to 30 days. After 30 days, deleted user accounts (and other deleted items) are automatically purged from the system.

To restore a deleted user account:

1. Login to the application.
2. Select Users from the Admin menu to display the User List Screen.
3. Select show "All Users" to ensure the list includes all deleted users. Deleted users are displayed with a line through their information.
4. Select one or more users and click the Restore button. The accounts are marked as valid.

2.6 Clearing User Sessions

System Administrators can clear user sessions when they become stranded. A stranded session occurs when a user no longer has any means of connecting to that session.

If there is an urgent need to gain access to the application immediately, or clear a stranded session that is locking a plan, the user can contact a System Administrator to clear the session.

To clear a user session:

1. Login to the application.
2. Select Users from the Admin menu to display the User List Screen.
3. Click the name of the user whose session is to be cleared and select the Clear Session button. The application removes the records associated with the session and the user can establish a new session by logging in.

2.7 Locking and Unlocking User Accounts

ClearTrial accounts can be locked and unlocked in order to temporarily deactivate users. Locking accounts is not the same as deleting them; a locked account will not be purged from the system. If a user needs to be temporarily deactivated, the account can be locked. A user whose account is locked cannot gain access to the system.

2.7.1 Locking Accounts

System Administrators can lock user accounts.

To lock a user account:

1. Login to the application.
2. Select Users from the Admin menu to display the User List Screen.
3. Click a user account to lock and select the Edit button. Click Yes next to the field label, "Account Locked."
4. Click Save.

Note: If the user is currently logged in, they will remain logged in until the current session expires or is terminated. Subsequent attempts to login will be denied.

2.7.2 Unlocking Accounts

System Administrators can unlock user accounts.

To unlock a user account:

1. Login to the application.
2. Select Users from the Admin menu to display the User List Screen.
3. Select the user account to unlock and click the Edit button. Click No next to the field label, "Account Locked."
4. Click Save.

2.8 Inactive Users Report

The Inactive Users Report allows System Administrators to view information about how often users login to the system during a period of time.

To generate an Inactive Users Report:

1. Login to the application.
2. Select the Inactive Users Report from the Report menu.
3. Select the number of days since the last login you want to view and click OK.
4. After selecting the days, the application generates a report that can be printed or exported as PDF, Excel, and CSV files.

Resetting a Forgotten Password

In most cases, users are able to reset their own password via the "Forgot Your Password?" link on the login page. Users can provide their customer code, login name, and email address to receive an email with further instructions on how to reset their password.

3.1 Reset a Password

If a user does not recall his or her customer code, login name or email address, the System Administrator can resolve the issue by resetting the password.

Note: Upon resetting a user account or password, the user will receive an email notifying them of the change. By default, the email directs the user to contact ClearTrial Support for any questions or issues. If you would prefer your users contact an internal support team, please notify ClearTrial Support or your Clinical Services Manager to have the email message changed.

To reset a password:

1. Login to the application.
2. Select Users from the Admin menu to display the User List Screen. Highlight the user and click the Edit Password button.
3. Click Save to assign the user a randomly generated password or click the Set Password link to enter a password. The user will receive an email informing them of the updated password, but the email does not disclose the new password. You will have to inform the user of their temporary password.
4. Upon logging in, users will be forced to change the password.

3.2 Resetting an Account

When a user account is reset, the user will receive an email containing a link to select a security question and answer, and to enter a password.

To reset an account:

1. Login to the application.
2. Select Users from the Admin menu to display the User List Screen. Highlight the user and click the Reset Account button. A message confirming the account reset is displayed.

3. Click OK to reset the account. An email will be sent to the user informing them of the account reset and requiring them to enter a new password, and security question and answer.

Note: If your organization does not allow user account information to be sent through email, upon clicking OK in Step 3, you will be shown the user's temporary password. Please communicate this password to the user through a secure form of communication.

Managing Deleted Items

When data is deleted from ClearTrial, it is not permanently removed, but marked as deleted. Deleted items are purged after 30 days.

Before a deleted item is purged, it can be restored. If the item is deleted again at a later date, the expiration period is restarted and the item may again be restored for up to 30 days from the date it was last deleted.

System Administrators can purge deleted items prior to their expiration.

4.1 Purging Deleted Items

A scheduled "housecleaning" job runs each night and processes all items that were deleted 30+ days before the current time. No user interaction is required. The System Administrator may, however, purge items ahead of schedule.

To purge deleted items:

1. Login to the application.
2. Select Purge Deleted Items from the Maintain menu to view the Purge Options Screen.
3. Check the box next to each item you want to purge and click the Purge Selected Items button.

Configurable ClearTrial Parameters

ClearTrial offers the following configurable parameters to be set for the software to meet your organization's business needs and best practices of your users. If you would like to request to edit any of these from the ClearTrial default value stated below, please contact ClearTrial Support.

Table 5–1

Configuration Parameters	Description	Default Value
Login Attempts Limit	Number of login attempts before users are locked out of the application.	5
Password Expiration Time	User passwords to expire after a certain period of time. When enabling this, all users who have not changed their passwords within the configured interval will be forced to change their password immediately on their next login.	No Default Value
Minimum Password Length	Number of minimum characters required for user passwords. User passwords are required to have a minimum of 8 characters and have a maximum of 20 characters.	8
Session Expiration Time	User's browser session to expire after a certain period of time.	No Default Value
Hide ClearTrial Default Template	Hides the ClearTrial Default System Template (by default) in the list of Plan Templates from which to choose when creating a plan. Users can reveal and use the ClearTrial Default System Template at any time by clicking on the link to show it.	Not Hidden
Prohibit ClearTrial Default Template	Prohibits the use of the ClearTrial Default System Template by users without the ability to reveal and use it.	Not Prohibited
System Administrator Email	The System Administrator Email that users will be directed to contact for user account requests.	cleartrial-support_ww@oracle.com
System Administrator Name	The System Administrator Name that users will be directed to contact for user account requests.	ClearTrial Support
System Administrator Phone	The System Administrator phone number that users will be directed to call for user account requests.	+1 (877) 206-4846

