Oracle® Health Sciences ClearTrial Cloud Service

System Administrator User Guide

Release 5.3

E60051-01

February 2015

ORACLE®

Oracle® Health Sciences ClearTrial Cloud Service

System Administrator User Guide

Release 5.3

E60051-01

February 2015

ORACLE®

Oracle Health Sciences ClearTrial Cloud Service System Administrator User Guide, Release 5.3

E60051-01

Oracle Health Sciences ClearTrial Cloud Service System Administrator User Guide, Release 5.3

E60051-01

Contents

Preface

The Oracle Health Sciences ClearTrial System Administrator User Guide is a reference for users who are performing administration tasks for their organization.

Audience

This document is intended for Oracle Health Sciences ClearTrial Cloud Service application system administrators.

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.

Finding Oracle Documentation

The Oracle website contains links to all Oracle user and reference documentation. You can view or download a single document or an entire product library.

Finding Oracle Health Sciences Documentation

To get user documentation for Oracle Health Sciences applications, go to the Oracle Health Sciences documentation page on oracle.com at:

http://www.oracle.com/technetwork/documentation/hsgbu-154445.html

or, for the documentation for this product, to:

http://http://www.oracle.com/technetwork/documentation/hsgbu-clinical-407519.html

Note: Always check oracle.com to ensure you have the latest updates to the documentation.

Related Documents

For more information, see the following documents in the Oracle Health Sciences ClearTrial Cloud Service Release 5.3 documentation set:

- *Oracle Health Sciences ClearTrial Cloud Service 5.3 Release Notes*
- *Oracle Health Sciences ClearTrial Cloud Service 5.3 Plan and Source User Guide*
- *Oracle Health Sciences ClearTrial Cloud Service 5.2 Track User Guide*
- *Oracle Health Sciences ClearTrial Cloud Service 5.3 Third Party Licenses and Notices*
- *Oracle Health Sciences ClearTrial Cloud Service 5.3 Web Services API User Guide*
- *Oracle Health Sciences ClearTrial Cloud Service 5.3 Secure Configuration Guide*

1

Getting Started: Administration Basics and Common Tools

This chapter provides information on how to work with administration features in the Oracle Health Sciences ClearTrial Cloud Service application.

System administrators maintain user accounts for their organization. In addition, they perform other administrative tasks, such as editing customer preferences, purging deleted items, and clearing user sessions when users are locked out.

Editing Customer Preferences

System administrators manage customer preferences. Customer preferences are preconfigured settings that apply across the application and to all users, regardless of roles and statuses.

The application logs and audits all customer creation, configuration, and administration activity.

1. From the Admin menu, select **Customer Preferences**.

   The Edit Customer Preferences screen appears.

2. Edit the values as needed.
   - For more information about a field, click the field name.
   - For more information about customer preferences fields, see Edit Customer Preferences Screen Fields.

3. Click **Save**.

Requesting Changes to Non-Custom Parameters

System administrators can configure most ClearTrial parameters, as described in this chapter. However, the following parameters cannot be configured by system administrators. To request changes to these parameters, contact ClearTrial Support.

Table 1–1 Custom ClearTrial Parameters

Parameter	Description	Default value
Login Attempts Limit	Number of login attempts permitted before a user is locked out of the application.	5

Table 1–1 (Cont.) Custom ClearTrial Parameters

Parameter	Description	Default value
Password Expiration Time	Time after which user passwords expire. Users who have not changed their passwords within the configured interval are forced to change their password immediately on their next login.	No default value
Minimum Password Length	Minimum number of characters required for user passwords. User passwords are required to have a minimum of 8 characters and have a maximum of 20 characters.	8 Password length cannot be less than 8 characters.
Session Expiration Time	Period of time after which a user browser session expires.	No default value
System Administrator Email	Email address for the system administrator that users can contact for user account requests.	cleartrial-support_ww@oracle.com
System Administrator Name	Name of the system administrator that users can contact for user account requests.	ClearTrial Support
System Administrator Phone	Phone number of the system administrator that users can call for user account requests.	+1 (877) 206-4846

Purging Deleted Items

When users delete data, the application does not remove it immediately. Rather, the application marks the data as deleted, stamps the data with the date it was marked, and then purges it on a scheduled basis or when requested. This allows you to restore data that has been deleted in error.

Automatic purging, which takes place nightly or according to the number of days you specify on the Edit Custom Preferences screen, permanently removes items that were deleted more than a specified number of days prior to the current date.

For more information, see Edit Customer Preferences Screen Fields.

You can also manually purge deleted plans, studies, products, users, portfolios, exchange rate tables, RFPs, and bids prior to their scheduled removal.

1. From the **Maintain** menu, select **Purge Deleted Items**.

   The Purge Deleted Items screen appears.

2. Select the checkbox next to each item you want to purge.

   - In the **deleted at least n days ago** field, enter the number of days prior to which deleted data is to be purged.
   - To purge all deleted items of the selected type, enter 0 for the number of days.

3. Click **Purge Deleted Items**.

2

Managing Your Administrator Profile

This chapter provides information on how to view your profile and permissions, how to edit your administrator profile, and how to change your administrator password.

Viewing Your Permissions

1. From any screen of the application, click your user name or the role that appears after Welcome.

   Your user profile appears.

2. On your profile page, click the link for each primary role and additional capabilities assigned to you to view the Permissions dialog box for that role.

   By default, when you click a permissions link the application displays only permissions assigned to you.

3. To see all application permissions, on the Permissions dialog box, click the **Show All Permissions** link. Checkmarks indicate the permissions assigned to you.

   For more information on user roles, see User Roles and Capabilities.

   For more information on permissions, see User Permissions.

4. To close the Permissions dialog box, click **Done**.

Editing Your Profile

1. From any screen of the application, click your user name or the role that appears after Welcome.

   Your user profile appears.

2. Click **Edit Profile**.

   The Edit User screen appears.

3. Edit the information on the Profile tab.

   - For more information about a field, click the field name.
   - For more information about the screen, see User Profile Tab Fields.

   The Roles tab is locked when editing your own profile. You cannot change the roles assigned to you.

4. Click **Save**.

Changing Your Password

1. From any screen of the application, click your name or the role that appears after Welcome.

   Your user profile appears.

2. Click **Change Password**.

   The Change Password screen appears.

3. In the **Current Password** field, enter your password.

4. In the **New Password** field, enter your new password.

   For more information on password fields and password requirements, see Change Password Screen Fields.

5. In the **Verify New Password** field, retype your new password.

6. Click **Save**.

3

Managing Users

This chapter provides information on how to create, edit, delete, and restore user profiles, assign and change user roles, and reset user passwords and accounts.

Viewing Existing Users

To access the ClearTrial application, every user must have a user account. System administrators can manage these user accounts for their organization.

1. From the Admin menu, click **Users**.

   The Users screen appears.

2. Filter the Users list as necessary.

   Filtering allows you to specify which users to display on the Users screen. You can show all users, active users only, or users matching filters you have defined.

Filtering Users

System administrators define display criteria for users on the Users screen. By defining user filter criteria, you can limit the number of users displayed on the Users screen or you can find a specific user. If you save the filtering criteria, it is applied every time you select that filter.

1. From the Filter section of the User screen, select which users to show:
   - **All Users—**All users. No filter is applied.
   - **Active Users Only—**Users that have not been marked as deleted.
   - **Users matching filter—**Shows only users that match the criteria defined in the filter you select from the drop-down list.

Defining or Modifying a Filter

1. On the Users screen, click the **Modify** link.

   The Define User Filter dialog box appears.

2. Complete the **User Filter Criteria** and **Save Filter** sections.
   - For more information about a field, click the field name.
   - For more information about the dialog box, see Define User Filter Dialog Box Fields.

3. Click **Ok**.

Creating User Accounts

Only system administrators can create user accounts for their organizations.

1. From the Admin menu, select **Users**.

   The Users screen appears.

2. Click **New**.

   The Create User screen appears.

3. On the Profile tab, complete the **User Preferences** section:

   a. Enter a login name, the first and last names of the user, and the email address.

   b. Specify the maximum edit mode by selecting it from the **Maximum Edit Mode** drop-down list. Select the preferred edit mode from the **Preferred Edit Mode** drop-down list.

      The edit modes control the precision of the plan by determining which assumptions the user can set. The maximum edit mode is the most advanced edit mode the user can access when creating or editing plans. The preferred edit mode is the mode the application automatically applies when the user creates or edits plans.

      For more information on edit modes, see User Profile Tab Fields.

   c. The application displays a system-generated password. The user must provide this password to access the application and complete registration. To change the password, click the **Set Password** link. You can also select a random password.

   d. From the **Preferred Home Page** drop-down list, select the screen the user will see after login.

   e. From the **Preferred Locale** drop-down list, select a language.

      Locale determines how dates and numbers are displayed and interpreted.

4. Click **Save**.

   You must save these settings to make the Roles tab active.

   The application sends an email containing the customer code, login name, and link to complete the registration to the user. Upon logging in, the application prompts the user to create a password.

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

   - For more information about password length setting, see Edit Customer Preferences Screen Fields.
   - For more information about password requirements, see Change Password Screen Fields.
   - Upon logging in, users set a security question and answer that the application uses to identify users who attempt to reset their passwords.

5. On the Roles tab:

a. Assign the user a primary role.

b. Assign additional roles and capabilities.

For more information about user roles, see User Roles and Capabilities.

6. Click **Save**.

User Roles and Capabilities

You can assign primary roles and additional roles and capabilities to users.

- To access the application, users must be assigned a primary role.
- Additional roles and capabilities can be assigned to users to grant them permissions to access certain features or perform specific job responsibilities.

Depending on the primary role you set for the user, you can also assign different additional roles and capabilities.

Table 3–1 Primary Roles

Primary role	Description	Notes
Read-Only User	Can view most items in the application but cannot create, edit, or delete any of these items. This role does not give permission to modify notes or export data from the application.	
User	Can view products and studies, and can create, edit, and view plans. Users can edit the plans they create but cannot edit plans created by other users.	
Power User	Has all of the permissions of the User primary role and can also create, edit, view, and delete templates and studies. Power users can edit plans created by other users.	
Clinical Administrator	Has all of the permissions of the Power User primary role and can also create and maintain products, service providers, and billing rates.	
System Administrator	Has all of the permissions of the Clinical Administrator primary role and can manage ClearTrial users.	Includes the RFP Administrator additional capabilities.

Table 3–2 Additional Roles and Capabilities

Additional role	Description	Notes
Exchange Rates Administrator	Grants permissions to users to create, edit, view, and delete shared exchange rate tables.	
Resources Administrator	Grants permissions to users to create, edit, view, and delete resources.	Resources capabilities are only available to Enterprise Licensed users.
Reporting Regions Administrator	Grants permissions to users to create, edit, and delete reporting region names and to map countries to reporting regions. Mapping enables you to view the budgets by location.	Only available to Enterprise Licensed users.

Table 3–2 (Cont.) Additional Roles and Capabilities

Additional role	Description	Notes
RFP Administrator	Grants permissions to users to view, create, edit, and delete RFPs and bids.	System administrators have these permissions by default.
RFP Reader	Grants read-only access to RFPs and bids.	The System Administrator and RFP Administrator can grant these permissions to clinical administrators.
Department/GL Codes Administrator	Grants permissions to users to create, view, edit, and delete departments or to create, view, edit, or delete GL codes.	
WBS Editor	Grants permissions to users to create, edit, and delete plan-specific major tasks, tasks, and resources in the Work Breakdown (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.	Only available to Enterprise Licensed users.
WBS Manager	Grants all of the WBS Editor permissions plus the abilities to edit and delete major tasks, tasks, and resources in the WBS of plans created by other users.	Only available to Enterprise Licensed users
Can edit notes	Grants permission to read-only users to edit notes associated with plans or other items for review purposes.	Can be granted to read-only users.
Can export report data	Grants permission to read-only users to export reports to PDF, Excel, or CSV.	Can be granted to read-only users.
Can access WS-API	Grants permission to users, who have licensed the Web Services API product, the capability to interact with the application programmatically. The primary role and other capabilities control the data users can view, edit, create, or delete with the API.	Only available to customers who have licensed the Web Services API product.

User Permissions

Permissions enable users to access certain features or perform specific actions in the application.

Primary role permissions, granted by primary roles, are generic actions that users can perform. Additional permissions, granted by additional roles, are used for access or maintenance in certain parts of the application, such as the resources and reporting regions.

For more information on user roles, see User Roles and Capabilities.

Editing User Accounts

1. From the Admin menu, select **Users**.

   The Users screen appears.

2. Select a user checkbox and click **Edit**.

The Edit User screen appears.

3. On the Profile tab, edit the user preferences fields as necessary.
   - For more information about a field, click the field name.
   - For more information about the Profile tab fields, see User Profile Tab Fields.
4. Click **Save**.

   You must save these settings to make the Roles tab active.
5. On the Roles tab, change the primary role and select or de-select additional roles and capabilities.
   - For more information about a field, click the field name.
   - For more information about user roles, see User Roles and Capabilities.
6. Click **Save**.

Locking and Unlocking User Accounts

You can lock accounts to temporarily deactivate users. A user whose account is locked cannot log into the application. Locking an account is not the same as deleting it, as locked accounts cannot be purged.

1. From the Admin menu, select **Users**.

   The Users screen opens.
2. Select the checkbox for a user account and click **Edit**.

   The Edit User screen appears.
3. On the Profile tab:
   - To lock the account, set the **Account Locked** field to **Yes**.
   - To unlock the account, set the **Account** Locked field to **No**.
4. Click **Save**.

   If you lock an account when the user is logged in, the user remains logged in until the session expires or is terminated. The application denies subsequent log-in attempts.

Deleting User Accounts

System administrators can delete user accounts. Deleting a user account marks the user profile invalid and prevents the user from logging in.

User accounts are not immediately deleted from the system and can be restored before purging. For information on purging deleted users, see Purging Deleted Items.

1. From the Admin menu, select **Users**.

   The Users screen appears.
2. Select one or more users and click **Delete.**

   When you display all users, the deleted user is greyed out and a line appears through the information.

Restoring Deleted User Accounts

System administrators can restore deleted user accounts that have not been purged from the application.

1. From the Admin menu, select **Users**.

   The Users screen appears.

2. In the Filter section, select the **All users** option to ensure deleted users appear on the page.

   Deleted users appear in grey and have a line through their information.

3. Select one or more users to restore, and click **Restore**.

Resetting User Passwords

Users can reset their password using the **Forgot Your Password?** link on the login screen. To reset their password, users need to provide their customer code, login name, and email address.

System administrators can reset passwords for users who have forgotten their credentials.

1. From the Admin menu, select **Users**.

   The Users screen appears.

2. Select a user and click **Edit Password**.

   The Reset Password screen appears.

   A new random password is automatically generated for the user and appears on the screen.

   To manually enter a new password for the user, click the **Set password** link. Enter and confirm the new password or assign a different random password by clicking the **Use a random password** link.

3. Click **Save**.

   After you reset a password, the user receives an email stating that the password has changed. The email does not contain the new password. You must provide the user with the new password through a secure form of communication. The application prompts the user to change the password upon successfully logging in.

Clearing a Stranded Session

A stranded session occurs when a user can no longer connect to a session. Stranded users must contact a system administrator for help.

1. From the Admin menu, select **Users**.

   The Users screen appears.

2. Select a user and click **Clear Session**.

   The application removes the records associated with the session and the user can establish a new session by logging in.

Resetting User Accounts

Resetting a user account:

- Clears the security question and answer associated with the account.
- Unlocks the user account if it is locked.
- Forces the user to reset the password upon login.

1. From the Admin menu, select **Users**.

   The Users screen appears.

2. Select a user from the users list.
3. Click **Reset Account**.

   An account reset confirmation message appears.

4. Click **OK**.

   The application clears the security question and answer and sends the user an email with a link to reset the password.

Viewing Inactive Users

Use the Inactive Users Report to view users that have not logged into the application for a certain period of time. You can print or export the report as PDF, Excel, or CSV.

1. From the Report menu, select **Inactive Users Report**.

   The Inactive Users Report Options screen appears.

2. In the **Days Since Last Login** field, enter the number of days since the last login.
3. Click **Ok**.

   The application generates the report.

4

Administration Field Descriptions

Define User Filter Dialog Box Fields

Table 4–1 Define User Filter Dialog Box Fields

Field	Description	Notes
Has logged in within the last n days	Number of days since a user last logged into the application.	
Include deleted users	Includes users that have been previously deleted.	When you delete a user account, it is not immediately deleted from the application. This allows you to recover users that may have been inadvertently deleted. Deleted users are purged after a specified period. For more information, see Purging Deleted Items.
Save filter as	Filter name.	
Sort By	Sets column order on the Users screen.	
Show number of users per page	Number of users that appear on the Users screen.	

Configure List Options Dialog Box - Users Screen

Table 4–2 Configure List Options Dialog Box Fields - Users Screen

Field	Description	Notes
Configure Columns	Checked items are the columns on the Users screen.	
Sorting and Paging		

Table 4–2 (Cont.) Configure List Options Dialog Box Fields - Users Screen

Field	Description	Notes
Sort By	Orders the users based on your selections.	Change the order by clicking a column heading.
Show n users per page	Number of users displayed on each page.	Use the paging tool to move to the next or previous page or directly to a page number.

User Profile Tab Fields

Table 4–3 User Profile Tab Fields

Field	Description	Notes
Login Name	Name or phrase you use along with your password to log into the application.	
First Name	First name of the user.	
Last Name	Last name of the user.	
Email Address	Email address of the user.	To reset their passwords, users must supply this email address.
Security Question	Question the application asks you to answer for authentication purposes, such as when you try to recover a forgotten password.	
Security Answer	Answer to the security question.	
Preferred Edit Mode	The edit mode used most often by the user when creating or editing plans.	Plans automatically open in this mode.
Preferred Home Page	The page that appears when a user logs in.	If a user requests a specific screen or follows a previously bookmarked URL, that page appears after a successful login, not the Preferred Home Page.
Preferred Locale	The preferred geographical location of the user. This selection overrides the default setting.	Determines how dates and numbers are displayed and interpreted.
Account Locked	Select Yes to deactivate a user account. Select No to unlock an account.	

Edit Customer Preferences Screen Fields

Table 4–4 Edit Customer Preferences Screen Fields

Field	Description	Notes
Default Language	Language the application suggests when planning clinical trials. The application assumes that documents are created in this language and must be translated into the languages associated with the countries in which the trial will take place.	You can change document translations settings on the Locations tab.
Default Currency	Currency to use to model the trial costs.	Users can override this setting.
Number of future years users can create billing rate cards for vendors	The maximum number of rate years, from the present year, that can be selected when creating rate cards.	Must contain a value between 1 and 99.
Number of days deleted items are kept and can be restored before being purged:	Number of days deleted items remain available to be restored before being permanently deleted or purged.	Must be a value between 1 and 365.
Hide the ClearTrial Default System Template (when there are user-defined templates)	Set to True to hide the ClearTrial Default System Template (when there are user-defined templates). Users can choose to show and use a hidden template unless it is prohibited.	
Prohibit use of the ClearTrial Default System Template (when there are user-defined templates)	Set to True to prohibit use of the ClearTrial Default System Template (when there are user-defined templates).	Users can use the default template only if there are no available user-defined templates.

Change Password Screen Fields

Table 4–5 Change Password Screen Fields

Field	Description	Notes
Current Password	Your currently valid password.	Required to authorize the password change request.

Table 4–5 (Cont.) Change Password Screen Fields

Field	Description	Notes
New Password	The password to use for subsequent logins.	Passwords must be at least eight characters and contain at least one letter, one number, and one of the following special characters: !$*+-.=?@^_|~. Passwords must not contain the login name or any of the following words: password, oracle, guest, admin, administrator, or cleartrial.
Verify New Password	The new password retyped to ensure that you have not mistyped the password.	

Reset Password Screen Fields

Table 4–6 Reset Password Screen Fields

Field	Description	Notes
New Password	The password for the user to use for subsequent logins.	Passwords must be at least eight characters and contain at least one letter, one number, and one of the following special characters: $*+-.=?@^_|~. Passwords must not contain the login name or any of the following words: password, oracle, guest, admin, administrator, or cleartrial.
Verify New Password	The new password retyped to ensure that you have not mistyped the password.	
Use a random password	Use a randomly generated password instead of specifying a password.	Link appears after you have displayed the Reset Password screen.