Oracle® Health Sciences ClearTrial Cloud Service

System Administrator User Guide

Release 5.6

E86237-01

June 2017

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

Contents

Administration basics and common tools

This section 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**.
2. Edit the values as needed. For more information about a field, click the field name to display online help.
3. Click **Save**.

Requesting changes to non-custom parameters

System administrators can configure most ClearTrial parameters. However, to change the following parameters, contact ClearTrial Support.

Table 1 Custom ClearTrial Parameters

Primary role	Description	Notes
Login Attempts Limit	Number of login attempts permitted before a user is locked out of the application.	5
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.	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 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

Deleted data is not remove immediately. Rather, ClearTrial marks the data as deleted, stamps it with the date, and 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, permanently removes items that were deleted more than a specified number of days prior to the current date.

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**.
2. Select the items 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**.

Managing your administrative profile

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

Viewing your permissions

1. Click your **user name** in the upper right corner of the screen.
2. On the **Profile** page, click the link for each primary role and additional capabilities assigned to you.
   - By default, ClearTrial displays only permissions assigned to you.

- To see all permissions, click the **Show All Permissions** link. Xs indicate the permissions assigned to you.

3. Click **Done**.

Editing your profile

1. Click your **user name** in the upper right corner of the screen.
2. Click **Edit Profile**.
3. Edit the information on the **Profile** tab. For more information about a field, click the field name to display online help.

   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. Click your **user name** in the upper right corner of the screen.
2. Click **Change Password**.
3. In the **Current Password** field, enter your password.
4. In the **New Password** field, enter your new password.
5. In the **Verify New Password** field, retype your new password.
6. Click **Save**.

Managing users

This section 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 ClearTrial, every user must have a user account. System administrators manage these user accounts for their organization.

1. From the **Admin** menu, click **Users**.
2. Filter the **Users** list as necessary.

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

Creating user accounts

Only system administrators can create user accounts for their organizations.

1. From the **Admin** menu, select **Users**.
2. On the **Users** screen, click **New**.
3. On the **Profile** tab on the **Create User** screen, enter a login name, the first and last names of the user, and the email address.

4. 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.

5. In the **Password** and **Confirm Password** fields, enter and confirm a password for the user.

   - 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.
   - The user must provide this password to access ClearTrial and complete registration.

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

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

   Locale determines how dates and numbers are displayed and interpreted.

8. Click **Save**.

   - You must save these settings to make the Roles tab active.
   - ClearTrial sends an email containing the customer code, login name, and link to complete the registration to the user. Upon logging in, ClearTrial prompts the user to create a password.
   - Upon logging in, users set a security question and answer that the application uses to identify users who attempt to reset their passwords.

   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.

9. 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.

10. Click **Save**.

User permissions

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

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.

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 2 Primary Roles

Primary role	Description	Notes
Read-Only User	Can view most items in ClearTrial but cannot create, edit, or delete any of these items. This role does not give permission to modify notes or export data.	There are no notes.
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.	There are no notes.
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.	There are no notes.
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.	There are no notes.
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 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.	There are no notes.
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 (Cont.) Additional Roles and Capabilities

Additional role	Description	Notes
Department/GL Codes Administrator	Grants permissions to users to create, view, edit, and delete departments or to create, view, edit, or delete GL codes.	There are no notes.
RFP/Bid 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.
Custom Fields Designer	Grants permissions to users to create, view, edit, and delete custom fields and to publish custom field models for use in plans.	Only available to Enterprise licensed users. The System Administrator can grant these permissions to users that are assigned a primary role of Clinical Administrator or System Administrator.
Advanced Algorithm Editor	Grants permissions to create or edit cost or resource algorithms with multiple expressions.	Only available to Enterprise licensed users. The System Administrator can grant these permissions to users that are assigned a primary role of Power User, Clinical Administrator, or System Administrator.
Expert Algorithm Editor	Grants permissions to users to create or edit scripted algorithms for costs or task resources.	Only available to Enterprise licensed users. The System Administrator can grant these permissions to users that are assigned a primary role of Power User, Clinical Administrator, or System Administrator.

Table 3 (Cont.) Additional Roles and Capabilities

Additional role	Description	Notes
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.

Editing user accounts

1. From the **Admin** menu, select **Users**.
2. Select a **user** and click **Edit**.
3. On the **Profile** tab, edit the user preferences fields as necessary. For more information about a field, click the field name to display online help.
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 to display online help.
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 ClearTrial. Locking an account is not the same as deleting it, as locked accounts cannot be purged.

1. From the **Admin** menu, select **Users**.
2. Select the **user account**, and click **Edit**.
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. ClearTrial 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 and can be restored before purging. For information on purging deleted users, see Purging deleted items.

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

   Restore a deleted user account by selecting the user and clicking **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**.
2. Select a user and click **Edit Password**.
3. In the **New Password** and **Verify New Password** fields, enter and confirm a new password for the user.
4. Click **Save**.

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

   ClearTrial 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**.
2. Select a user and click Reset Account.

   An account reset confirmation message appears.
3. Click **OK**.

   ClearTrial 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 ClearTrial 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**.
2. On the **Inactive Report Options** screen, in the **Days Since Last Login** field, enter the number of days since the last login.
3. Click **Ok**.

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.

ClearTrial Cloud Service System Administrator User Guide, Release 5.6
E86237-01

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.