Oracle® Health Sciences ClearTrial Cloud Service

System Administrator User Guide

Release 5.2

E51826-01

April 2014

ORACLE

Oracle Health Sciences ClearTrial Cloud Service System Administrator User Guide, Release 5.2

E51826-01

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 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 5.2 documentation set:

- *Oracle Health Sciences ClearTrial Cloud Service 5.2 Release Notes*
- *Oracle Health Sciences ClearTrial Cloud Service 5.2 Plan and Source User Guide*
- *Oracle Health Sciences ClearTrial Cloud Service 5.2 Track User Guide*
- *Oracle Health Sciences ClearTrial Cloud Service 5.2 Third Party Licenses and Notices*
- *Oracle Health Sciences ClearTrial Cloud Service 5.2 Web Services API User 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 primarily maintain user accounts for their organization. In addition, they can perform other administrative tasks, such as editing customer preferences, purging deleted items, and clearing user stranded sessions.

Editing Customer Preferences

System administrators manage customer preferences. These 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 Customizable Parameters

System administrators can configure most Oracle Health Sciences ClearTrial Cloud Service 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 Customizable ClearTrial Parameters

Parameter	Description	Default value
Login Attempts Limit	Number of allowed login attempts before users are locked out of the application.	5

Table 1–1 (Cont.) Customizable 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	User's browser session to expire after a certain period of time.	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

Deleted data is not removed immediately. Rather, the application marks the data as deleted and then purges it on a scheduled basis.

Automatic purging, which takes place nightly, permanently removes items that have been deleted more than a specified number of days prior to the current date. You can specify the number of days items are kept before being permanently removed.

For more information, see Edit Customer Preferences Screen Fields.

You can manually purge deleted plans, studies, products, users, portfolios, and exchange rate tables, 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**.

Filtering Users

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.

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

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

   The Define User Filter dialog box appears.

2. Complete the Filter Criteria, Save Filter, and Sorting and Paging 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**.

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.

   Your user profile appears.

2. On your profile page, click the link for each role assigned to you to view your permissions for that role.

   By default, only permissions assigned to you are displayed when you click a permissions link.

3. To see all application permissions, click the **Show All Permissions** link on the Permissions dialog box. 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.

Editing Your Profile

1. From any screen of the application, click your user name.

   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.

   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 Oracle Health Sciences ClearTrial Cloud Service, every user must have a user account. System administrators can manage these user accounts for their organization.

To view existing user accounts, from the Admin Menu, click **Users**.

For more information on displaying and filtering users, see Filtering Users.

Creating User Profiles

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

   The Users screen appears.

2. Click **New**.

   The Create User screen appears.

3. On the Profile tab, enter the user preferences:

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

   b. Select the Maximum and Preferred Edit Modes.

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

   c. Select a Preferred Home Page and Preferred Locale for the user.

      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.

   An email containing the customer code, login name, and link to complete the registration is sent to the user. The user is prompted to create a password upon logging in.

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.

- For more information about password length setting, see Editing Customer Preferences.
- For more information about password requirements, see Change Password Screen Fields.
- Upon logging in, users set a security question and answer that are used to identify users attempting 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 permissions 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.	

Table 3–2 Additional Roles and Capabilities

Additional role	Description	Notes
Exchange Rates Administrator	Can create, edit, view, and delete shared exchange rate tables.	

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

Additional role	Description	Notes
Resources Administrator	Can create, edit, view, and delete resources.	Resources capabilities are only available to Enterprise Licensed users.
Reporting Regions Administrator	Can create, edit, and delete reporting region names, and can map countries to reporting regions. Mapping enables you to view the budget by location.	The Reporting Regions capabilities are only available to Enterprise Licensed users.
Can edit notes	Allows users to edit notes associated with plans or other items for review purposes.	Can be granted to Read-Only users.
Can export report data	Allows users to export reports to PDF, Excel, or CSV.	Can be granted to Read-Only users.
Can access WS-API	For users or accounts that interact with the application programmatically. The user's primary role and other capabilities control the data they 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.**

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.

3. Click **Save**.

   After resetting their password, the user receives an email informing them that their password has changed. The email does not contain the new password. You must provide the user with their new password through a secure form of communication. Users are prompted to change their password upon successfully logging in.

Removing the Lock for a Stranded Session

A stranded session occurs when a user can no longer connect to a session. Users who need to clear stranded sessions 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

You can reset a user's account to:

- Clear the account's security question and answer.
- Unlock a locked user account.
- Reset the password and prompt the user to change 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 user's new password appears.

   After an account reset, the user receives an email informing them that their password has changed. The email does not contain the new password. You must provide the user with their new password through a secure form of

communication. Users are prompted to change their password upon successfully logging in.

Viewing Inactive Users

System administrators can use the Inactive Users Report to view users that have not logged in 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**.
2. Enter the number of days you want to display the report for, and click **Ok**.

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.	
Filter name	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.	

User Profile Tab Fields

Table 4–2 User profile fields

Field	Description	Notes
Login Name	Name or phrase the user uses to log in.	
First Name	User’s first name.	
Last Name	User's last name.	

Table 4–2 (Cont.) User profile fields

Field	Description	Notes
Email Address	User's email address.	This email address allows users to use the Forgot Your Password? feature. If users forget their password, they need to supply this email address to reset their password.
Security Question	Security question used for authentication purposes.	
Security Answer	Security answer used for authentication purposes.	
Preferred Edit Mode	User's preferred edit mode, used for 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	User's preferred geographical location.	Determines how dates and numbers are displayed and interpreted.

Edit Customer Preferences Screen Fields

Table 4–3 Edit Customer Preferences screen fields

Field	Description	Notes
Default Language	Language into which study documents are translated.	You can change document translations settings on the Locations tab.
Default Currency	Currency in which studies are planned.	
Allow users to create rate cards for this many future years	Number of years through which users can create billing rate cards on the Billing Rates screen.	
Number of days to keep deleted items before removing them permanently	Number of days to keep deleted items before purging them from the application.	

Table 4–3 (Cont.) Edit Customer Preferences screen fields

Field	Description	Notes
Hide the ClearTrial Default System Template when users create new plans	Determines if the application includes the ClearTrial Default System Template in the list of available templates when users create new plans.	If False, the application includes the default template in the list of available templates. If True, users can select the default template from a link above the list of available templates.
Prevent users from creating plans from the ClearTrial Default System Template	Determines if users can use the ClearTrial Default System Template when creating plans.	If False, the application includes the default template in the list of available templates. If True, users can select the default template from a link above the list of available templates.

Change Password Screen Fields

Table 4–4 Change Password screen fields

Field	Description	Notes
Current Password	Your current password.	
New Password	Your new password.	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 your login name or any of the following words: password, oracle, guest, admin, administrator, or cleartrial. Do not use easily guessed passwords such as a pet's name; your own name, address, or phone number; or any easily identifiable personal information.
Verify New Password	Your new password.	