

1.3 Logging In

Getting Invited

You will receive an email inviting you to participate in a study.

To Accept an Invitation:

1. Open the email.
2. Click **Let's Go**.

Welcome to New Cancer Drug!

Dear Kerry,


You've been invited to join New Cancer Drug in OpenClinica. We'll get you started in a few quick steps.

[Let's Go ->](#)

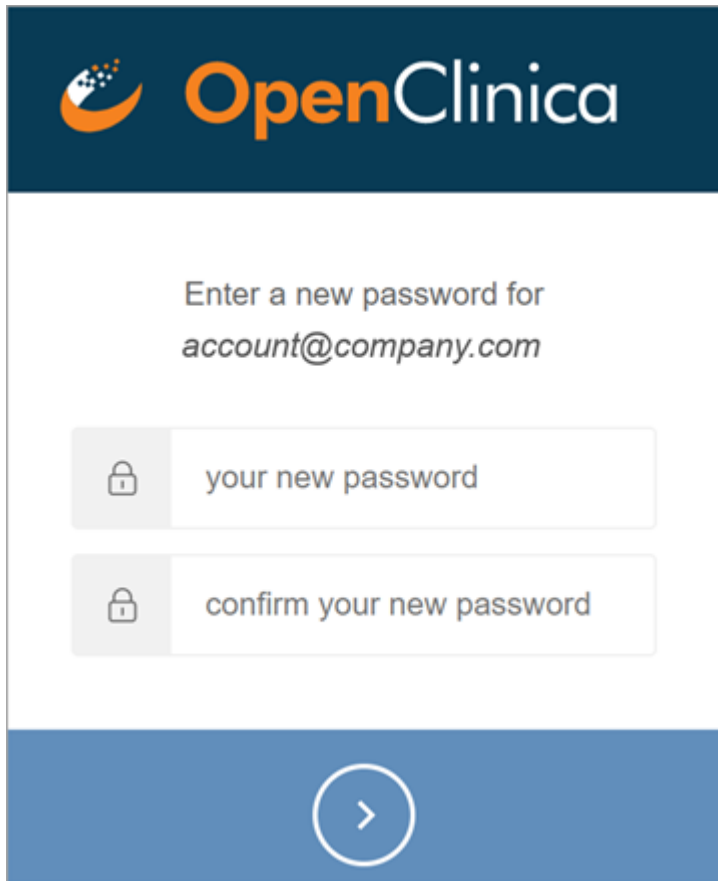
The above link will allow you to set up your login, and will only work the first time you access OpenClinica. After you've done this, you may return to OpenClinica by bookmarking the following URL: <https://cust2.openclinica-dev.io/OpenClinica/MainMenu>


OpenClinica is a simple and powerful tool for capturing and organizing your research data. It's trusted in more than 10,000 studies around the world.

Thanks!
The New Cancer Drug Team





After clicking **Let's Go**, you will be redirected to a screen asking you to set your password.




 **OpenClinica**

Enter a new password for
account@company.com

 your new password

 confirm your new password



Your Password Must:

- Be at least **8** characters in length
- Contain at least one of each of the following types of characters:
 - Lower case letters (**a-z**)
 - Upper case letters (**A-Z**)
 - Numbers (**0-9**)
 - Special characters (**!@#\$%^&***)

In Addition:

- Passwords expire every **180 days**, and users are automatically prompted to create a new password.
- User accounts are locked after **ten failed login attempts** from the same IP address.
 - The lockout resets after **15 minutes**. The login failure count resets every **24 hours**.
 - When a user tries to login after their account has been locked, it is included in the **User Audit Log** as a failed login attempt.
- If a user resets a password, it cannot be the same as the previous password.
- The password reset link is available for **24 hours**, after which, if a user has not reset the password, they must request a password reset again.
 - All reset requests are logged in the **User Audit Log**.
- Users are automatically logged out of OpenClinica after **one hour** of inactivity.
- Invitations to studies expire in **14 days** if they have not been accessed.

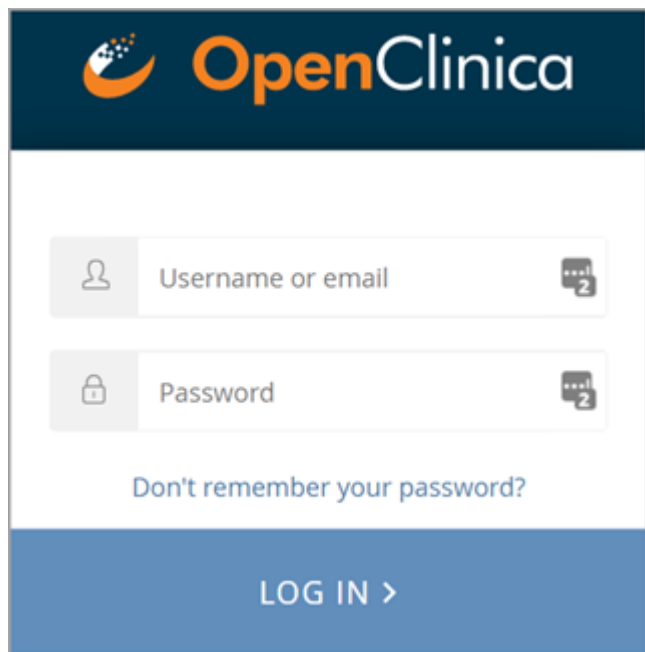
Once you have entered a password that meets the requirements, you will be prompted to log into OpenClinica.

If you want to create an OpenClinica bookmark, make sure to bookmark the **Home** screen after you login instead of bookmarking the **Login** screen.

After you log in for the first time, you can no longer click the **Let's Go** button on the invitation.

To Log into OpenClinica After Your First Login:

1. Enter the URL for OpenClinica into the search bar at the top of your browser. You can find the URL on your invitation to the study. Or if you have bookmarked the **Home** screen, click on the bookmark.
2. Enter your username.
3. Enter your password.

The image shows a screenshot of the OpenClinica login interface. At the top, there is a dark blue header with the OpenClinica logo on the left and the text "OpenClinica" in white. Below the header is a white login form. The form contains two input fields: "Username or email" and "Password". Each field has a small icon on the left (a person for the username field and a lock for the password field) and a "show/hide" icon on the right. Below the password field, there is a link that says "Don't remember your password?". At the bottom of the form is a blue button with the text "LOG IN >".

If the environment you're working with requires multi-factor authentication, the login process has an additional step.

Multi-factor Log In

In addition to entering your **username** and **password**, you must scan a barcode and enter an access code generated by the **FreeOTP** or **Google Authenticator** app on your smartphone.

To Log In with Multi-factor Authentication:

1. Download either the **FreeOTP** ([iOS](#) or [Android](#)) app or the **Google Authenticator** ([iOS](#) or [Android](#)) app to your smartphone.
2. Scan the barcode.

You are required to set-up multi-factor authentication.

This extra security measure keeps your account safe if someone discovers your username and password. To get started, please follow the steps below. Then, each time you log in you will need to access the authentication app and enter the code it displays.

Step 1: Install one of the following applications on your mobile device:

- Google Authenticator (recommended) - (Android - iOS)
- FreeOTP - (Android - iOS)

Step 2: Open the application and scan the barcode:



Unable to scan?

Step 3: Enter the one-time code provided by the application in the box below and click Log In to finish the setup.

[LOG IN >](#)

3. Enter an access code.



Use your mobile device to open the authentication app that you previously configured to access this site and enter the code it displays.

CANCEL

LOG IN >

Whenever prompted in the future, use the same mobile device you previously set up to receive the one-time passcode from either **Google Authenticator** or **FreeOTP**.

Functional approval by Ray Eichler. Signed on 2021-05-10 3:55PM

Approved for publication by Ben Baumann. Signed on 2021-05-11 10:29AM

Not valid unless obtained from the OpenClinica document management system on the day of use.