OpenClinica

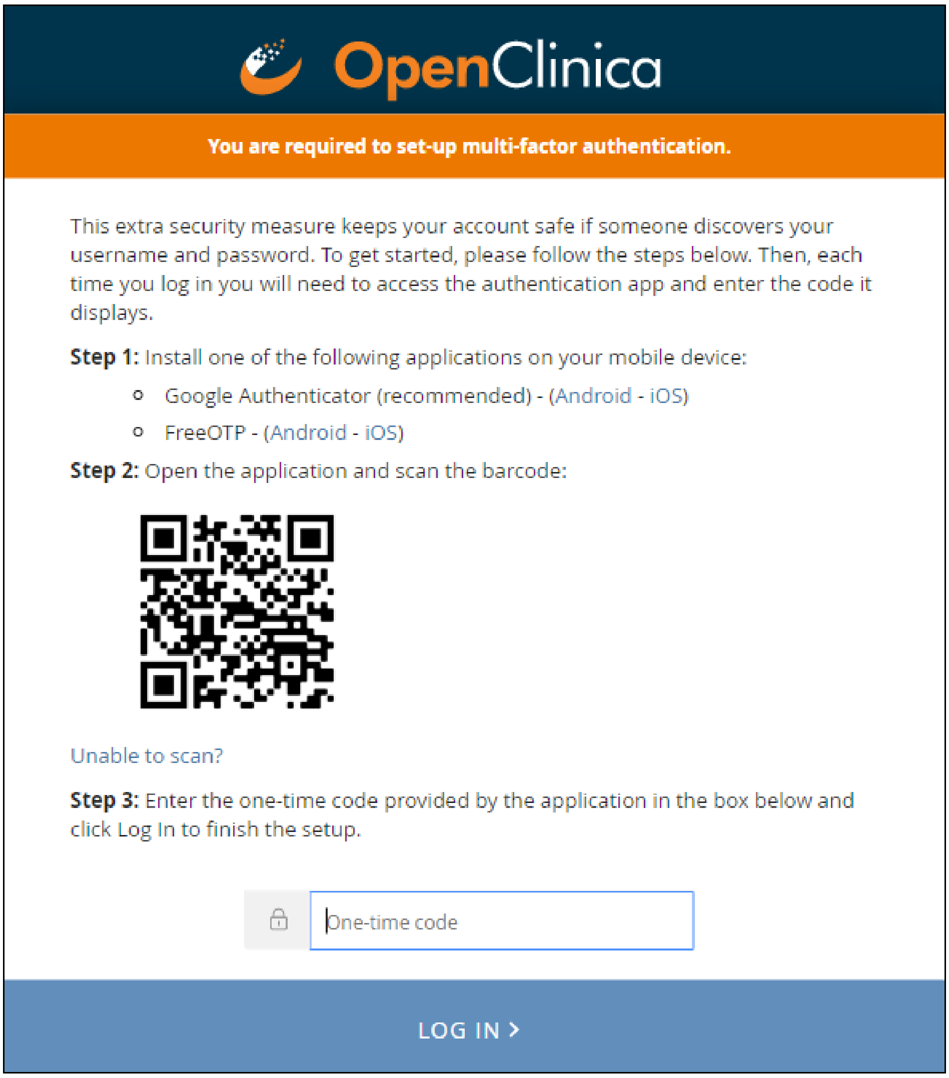
# 5.2.6 Using Multifactor Authentication

You can enable multi-factor authentication (MFA) for your OpenClinica domain with an API or contact the **OpenClinica Customer Service** team.

When you enable multi-factor authentication, users are prompted to:

1. Download either the **FreeOTP** app or the **Google Authenticator** app to your smartphone.
2. Scan a barcode.
3. Enter the access code from their device.

**Initial User Sign-up:**



OpenClinica

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:

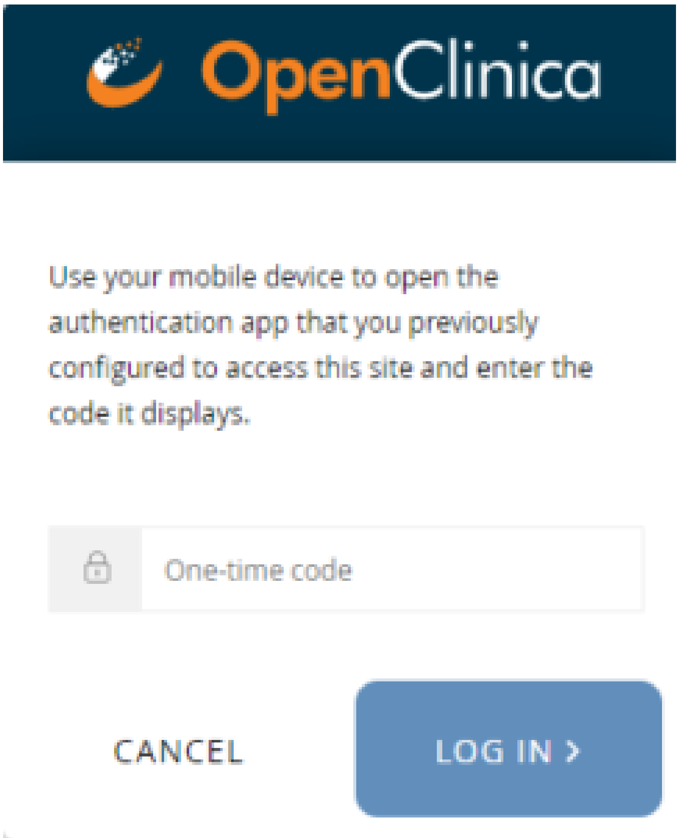
- Google Authenticator (recommended) - (Android - iOS)
- FreeOTP - (Android - iOS)

**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.

**Subsequent Logins:**



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

***Note:*** *Once you have enabled multi-factor authentication, you no longer need to scan a barcode. Only username, password, and an access code are required to sign in. The barcode should be treated as your password and should not be shared with anyone (including via screenshare).*

## If This Feature is Enabled:

- All Study and Site Users are required to login with username, password, and an additional code.
- **Data Specialists** and **Investigators** will still sign participant records with only their username and password.
- Participant users logging into **Participate** are still only required to enter access codes.
- You cannot enable multi-factor authentication for a specific study, site, or user. It must be enabled per OpenClinica domain.

## Additional Information:

**There is no link between a user's authenticator app/device and the authentication server:** Authenticator apps do not communicate with a server in any capacity. If a user deletes an MFA entry in their app, the server is not informed in any way and the user will still be expected to enter their One Time Password (OTP) upon login.

**Troubleshoot syncing the device clock to the server time:** We suggest the user compare their MFA device time to something official (e.g. https://www.time.gov/) - ensure that the users understand that MFA is sensitive down to the second. Some mobile devices fetch the time from their local Wi-Fi device and may be inaccurate.

**If a user loses their MFA device or authenticator entries:** they will have to make a request to the support team to reset their MFA credentials, which will prompt them to re-configure MFA and give them a new QR code to scan.

**Note:** Our current implementation of MFA/OTP requires a second device such as a phone or tablet running iOS or Android and using one of the apps listed above.

Functional approval by Riley Bianchi. Signed on 2021-12-17 10:27AM

Approved for publication by Paul Bowen. Signed on 2021-12-17 3:24PM

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