Multi-Factor Authentication (MFA) Policy

Tribe User Guides

Multi-Factor Authentication (MFA) Policy

Purpose

The purpose of this policy is to establish the requirements for Multi-Factor Authentication (MFA) to enhance security measures and protect user accounts on the Tribe platform. This policy ensures that all administrative accounts and other key accounts have access to an additional layer of security beyond just a password.

Scope

This policy applies to all users who have administrative or privileged access to the Tribe platform, as well as any other users where enhanced security measures are deemed necessary. This includes employees, contractors, and third-party partners.

Policy Statement

1. **MFA Requirements**
   a. All administrative and privileged user accounts must enable MFA.
   b. MFA is optional but recommended for standard users.
2. **MFA Implementation**
   MFA is implemented using a second factor of authentication in addition to a password. SMS-based verification: A six-digit code is sent to the user's registered phone number, which must be entered to complete the login process.
3. **User Responsibilities**
   a. Users must provide a valid phone number to enable MFA.
   b. Users are responsible for ensuring the phone number is active and can receive SMS codes.
4. **Enforcement**
   a. MFA setup for all newly created administrative accounts is recommended and where individual organisation policies dictate may be mandatory, as set by your company admin lead.
   b. In cases where MFA is not set up for existing administrative accounts, an alert will be sent to remind the user.
5. **MFA Dashboard**
   The following platforms and dashboards implement MFA:
   a. Admin User Dashboard
   b. Tribe iOS App
   c. Tribe Android App
6. **Support and Documentation**
   a. Users experiencing issues with MFA can contact the Tribe support team for assistance using either the resolution centre or by emailing support@tribeproject.org
   b. Tribe will maintain this MFA policy and review it annually.

MFA Setup steps:
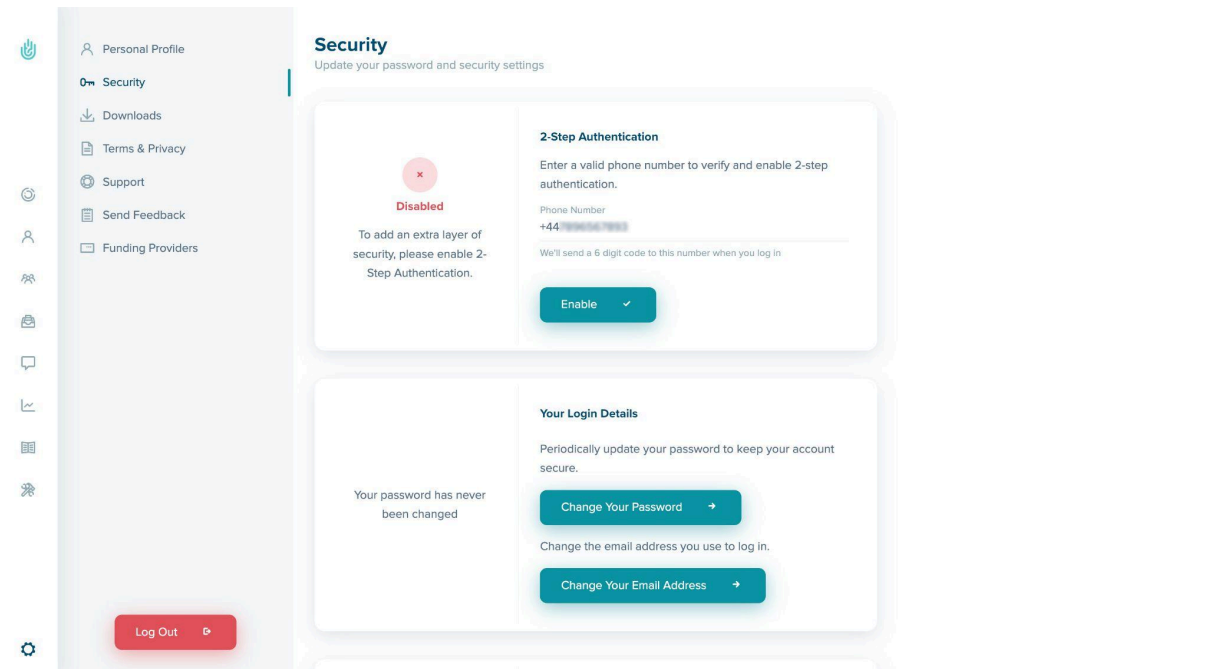
Within Profile > Settings, locate '2-Step Authentication', enter a valid and working mobile number that you have access to, and click on 'Enable'.
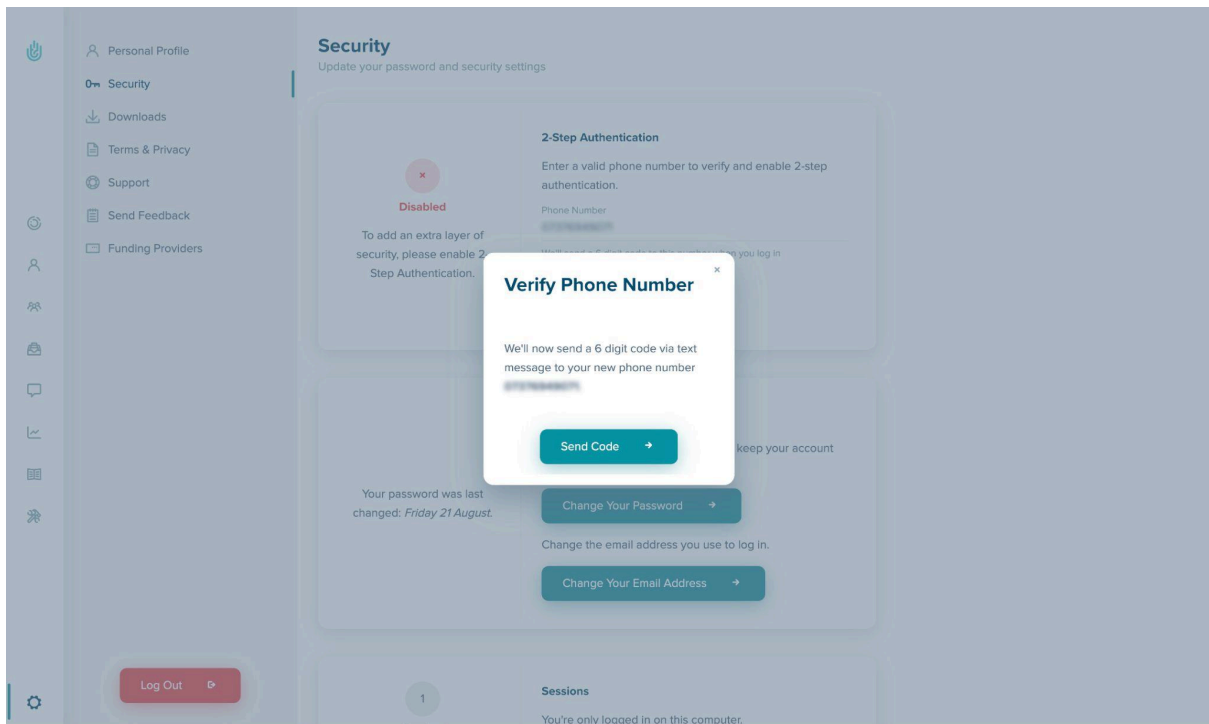

You will see a prompt confirming them number you have entered, if this is correct, please click on 'Send Code', if it is not, please close and re-enter your number again.
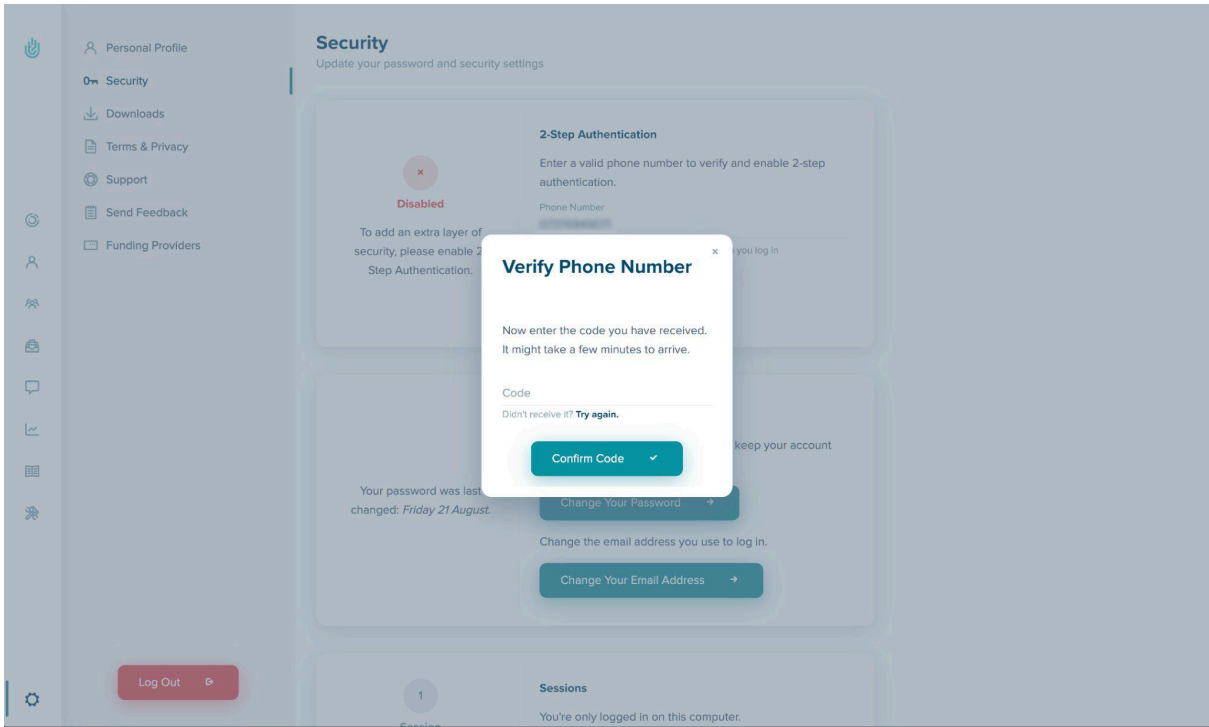
You should have received a 6 digit code via SMS text message, please enter this and click on 'Confirm Code'.
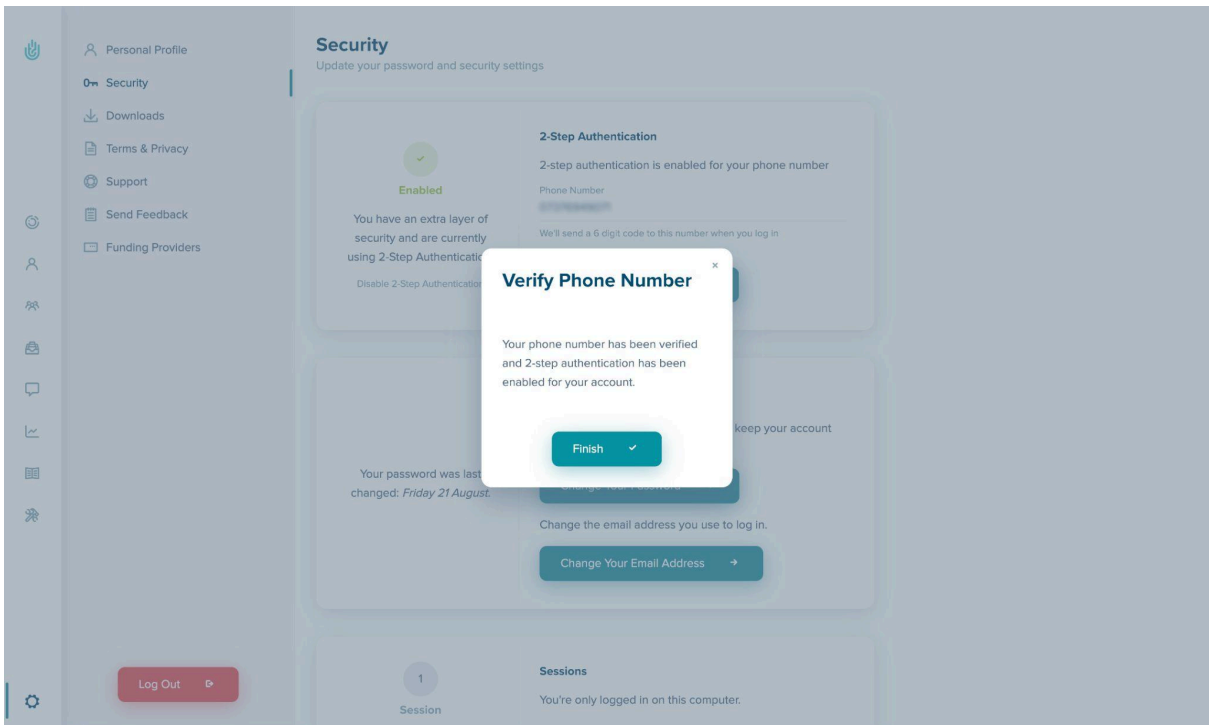
Once successful, you will receive a confirmation message, and the 2-Step Authentication panel will show as 'Enabled'.
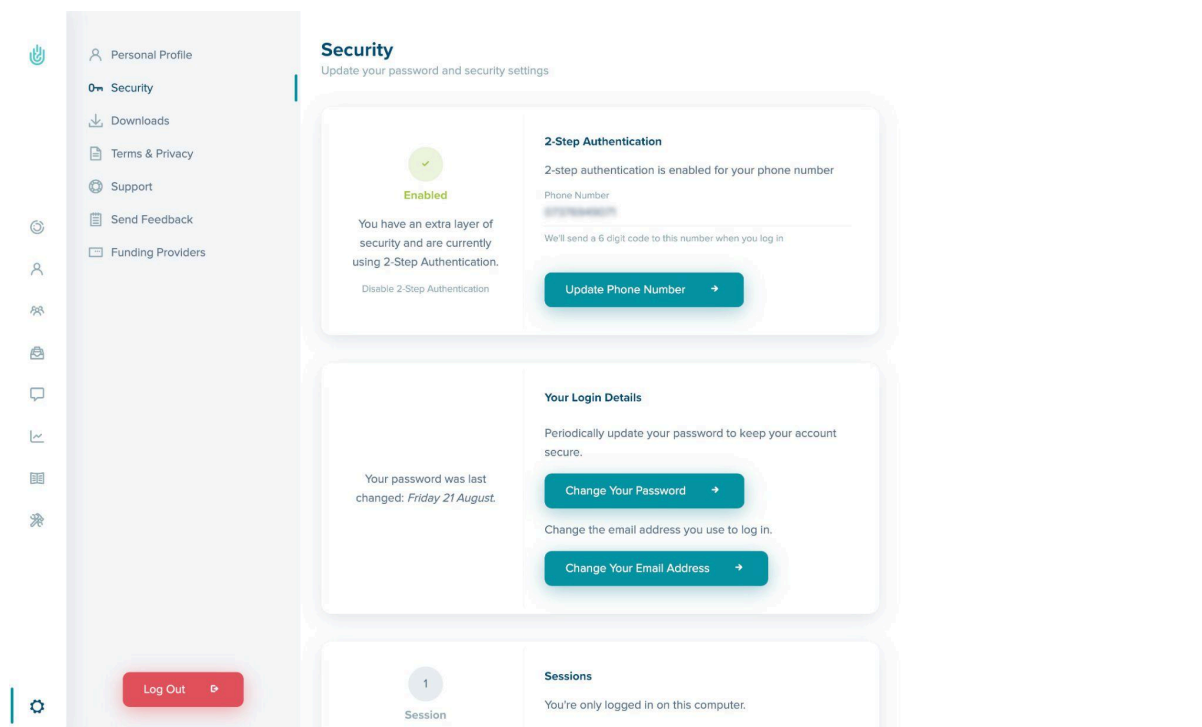
Should your phone number change at any time, you can update it in the same place, following the same steps as noted.