Two-factor Authentication (2FA) Quick Guide

Setting up Two-Factor Authentication for the REMAP-CAP Trial Database

We have chosen to allow users the option of utilizing any of Google Authenticator, Microsoft Authenticator, or Twilio Authy as the 2FA method for our trial database due to their reliability and ease of use. Follow the simple steps below to set up 2FA for your REMAP-CAP Trial account.

Step 1: Download a Two-Factor Authenticator app

- The following apps can be used for two-factor authentication in the REMAP-CAP database:
    - ✳ Google Authenticator (App Store for iOS | Google Play Store)
    - 🔵 Microsoft Authenticator (App Store for iOS | Google Play Store)
    - 🔴 Twilio Authy (App Store for iOS | Google Play Store)
- On your smartphone or tablet, search for your preferred application (e.g., "Google Authenticator") in your device's app store, or use the links above, and download and install the app.
- Open your authenticator application and follow the instructions to set up your account.

Step 2: Enable 2FA in your REMAP-CAP Trial Account

- Log in to your REMAP-CAP Trial account using your usual username and password.

- Until the 1st of September 2023 (UTC), the following window will display. You can choose to set up 2FA now or later.
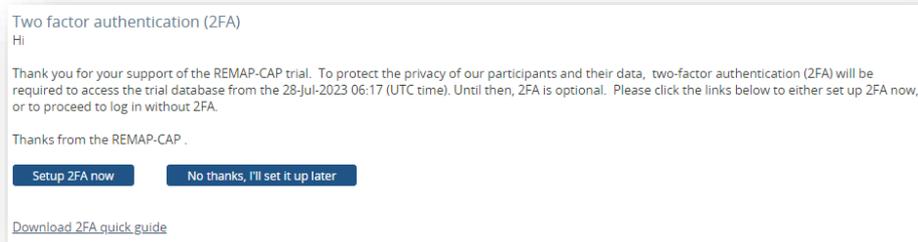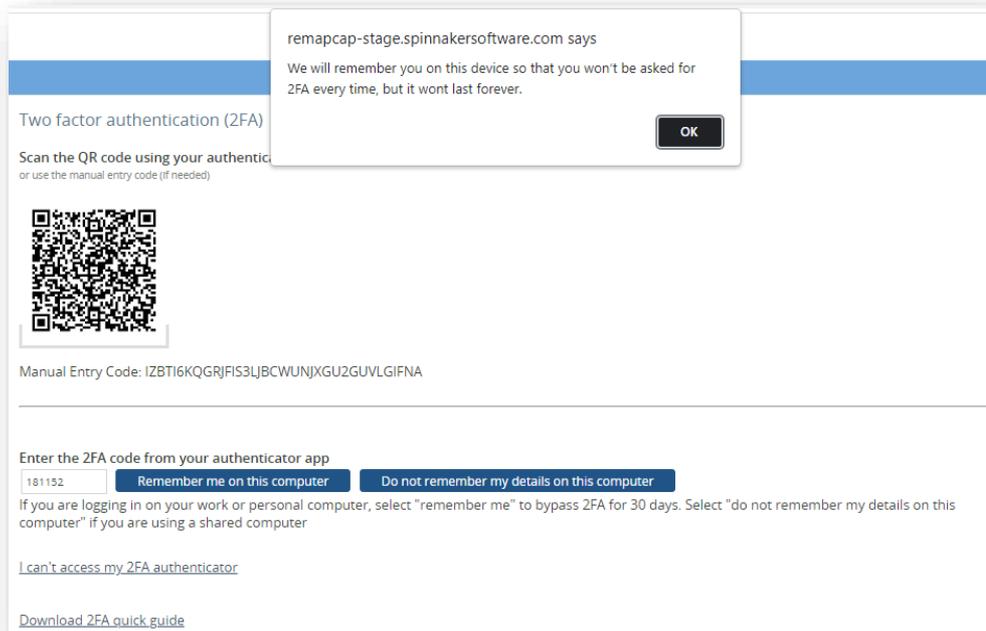

To set up 2FA:

- Open the Authenticator app on your mobile device.
- Follow the prompts to scan the QR code displayed on the REMAP-CAP Trial website or enter the provided secret key manually.
- The authenticator application will generate a unique six-digit code.
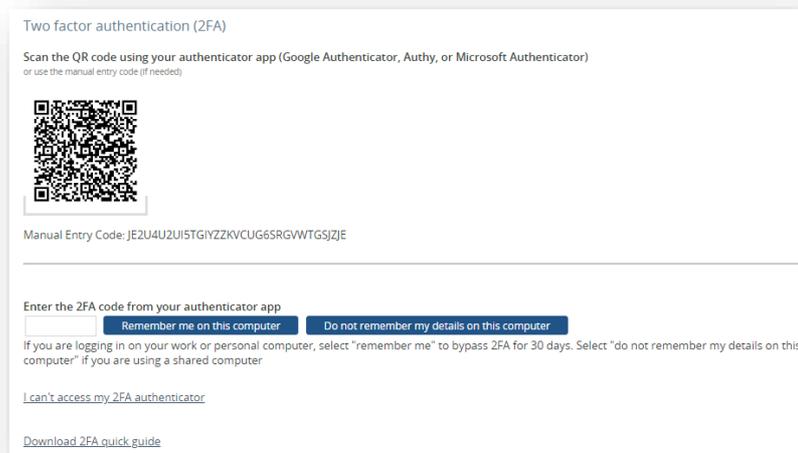
- Enter this code into the designated field on the REMAP-CAP Trial website.
- If you are logging in on a personal device, you can ask the database to remember your details and bypass 2FA for 30 days. Do not select this option when using a shared computer.

- Once you have entered the code, the REMAP-CAP Trial website will confirm successful setup.
- Your authenticator will generate a new six-digit code every 30 seconds.
- When prompted for the authentication code during future login attempts, open the authenticator app and enter the most recent code displayed.

Can't access your two-factor authenticator app or want to reset your 2FA codes?
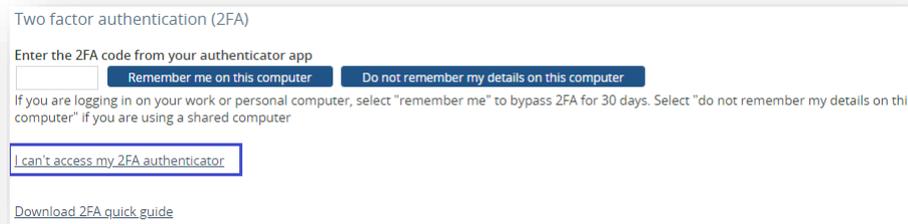
To reset your 2FA authentication keys you can call your project manager directly, send a request via the REMAP-CAP database, or reset it yourself via the 2FA authentication feature under your **'My profile'** tab.

To send a 2FA reset request via the REMAP-CAP website:

- Log in to the REMAP-CAP Trial database.

If the 'Two-factor authentication (2FA)' page displays follow the next steps:

- Click '**I can't access my 2FA authenticator'**.

- Add an entry in the available text box and click 'Send message'. A confirmation message will display.

- You will receive notification via email once your request is actioned by your regional manager.
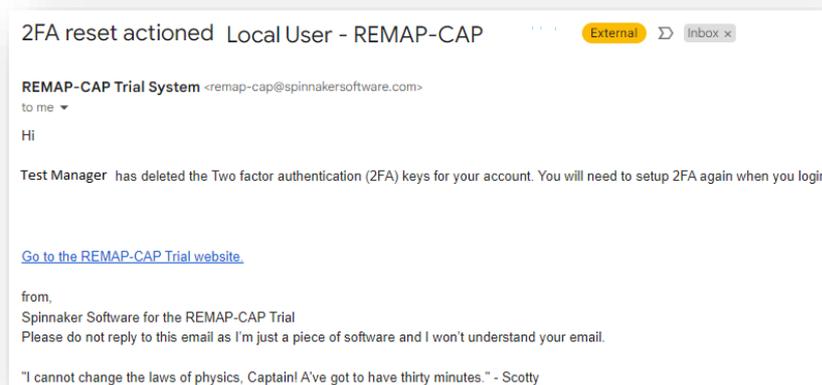
If you require 2FA reset and can bypass the 2FA follow the next steps:

- Go to your **'My Profile'** tab (top right of the menu bar)
- Click '2FA authentication' in the left panel to display the 2FA authentication options.
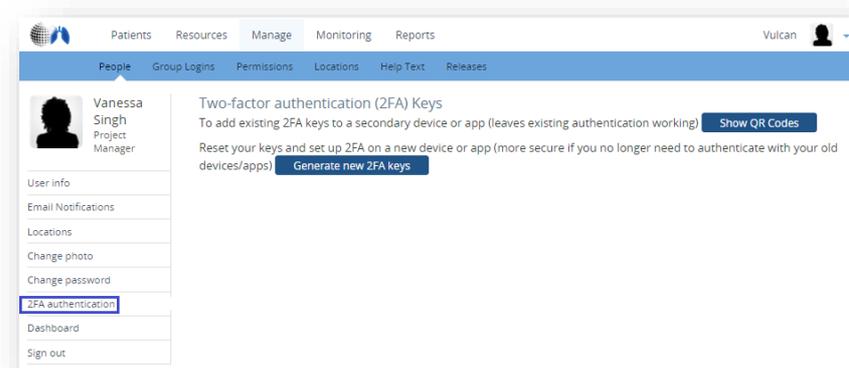
- You can choose to **'Show QR Codes'** or **'Generate new 2FA keys'**
- Select **'Show QR Codes'** to add existing 2FA codes to a secondary device. Users can scan and use the same QR code for each device and authenticator they have.
- Select **'Generate new 2FA keys'** if you would like to reset your 2FA codes. Follow the steps to scan the QR code displayed (or enter the secret key manually) and enter the new authentication code in the designated field.
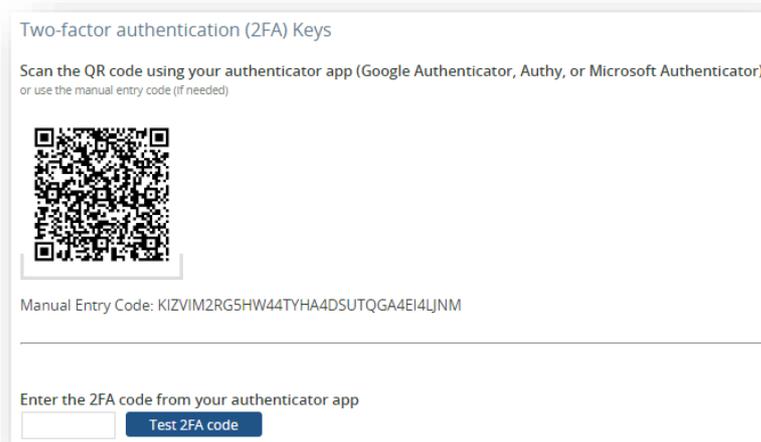
- If you have more than one REMAP-CAP database account, you can link your authenticator app to all relevant user accounts.

Contact your Regional Manager if you require any assistance in managing your database accounts.