IMPORTANT: Impact Hub Multi-factor Authentication Mandatory Setup

Overview

Multi-factor authentication has been available in the Impact Hub for the last few months, and at **12pm** on **31 March 2025** setting up multi-factor authentication will be mandatory for accessing the Impact Hub to further support the cyber security of your Beneficiary data.

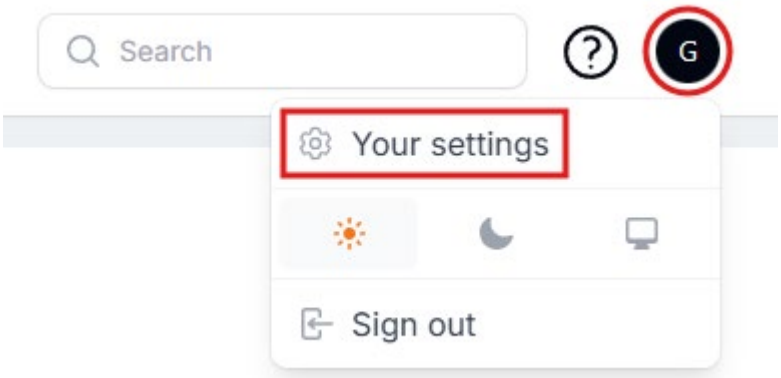
What is Multi-factor Authentication?

Multi-factor authentication (MFA) or two-factor authentication (2FA) provides a second layer of security. When logging in with multi-factor authentication, you will enter your password, followed by a six-digit code to prove it's really you.

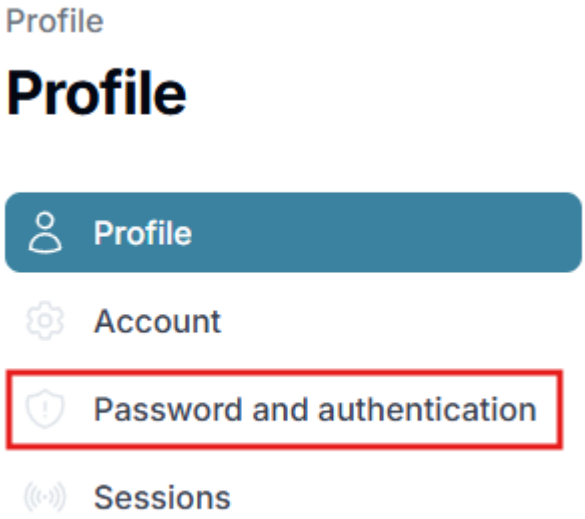
Setting up Multi-factor Authentication

We advise setting up multi-factor authentication now by following these steps:

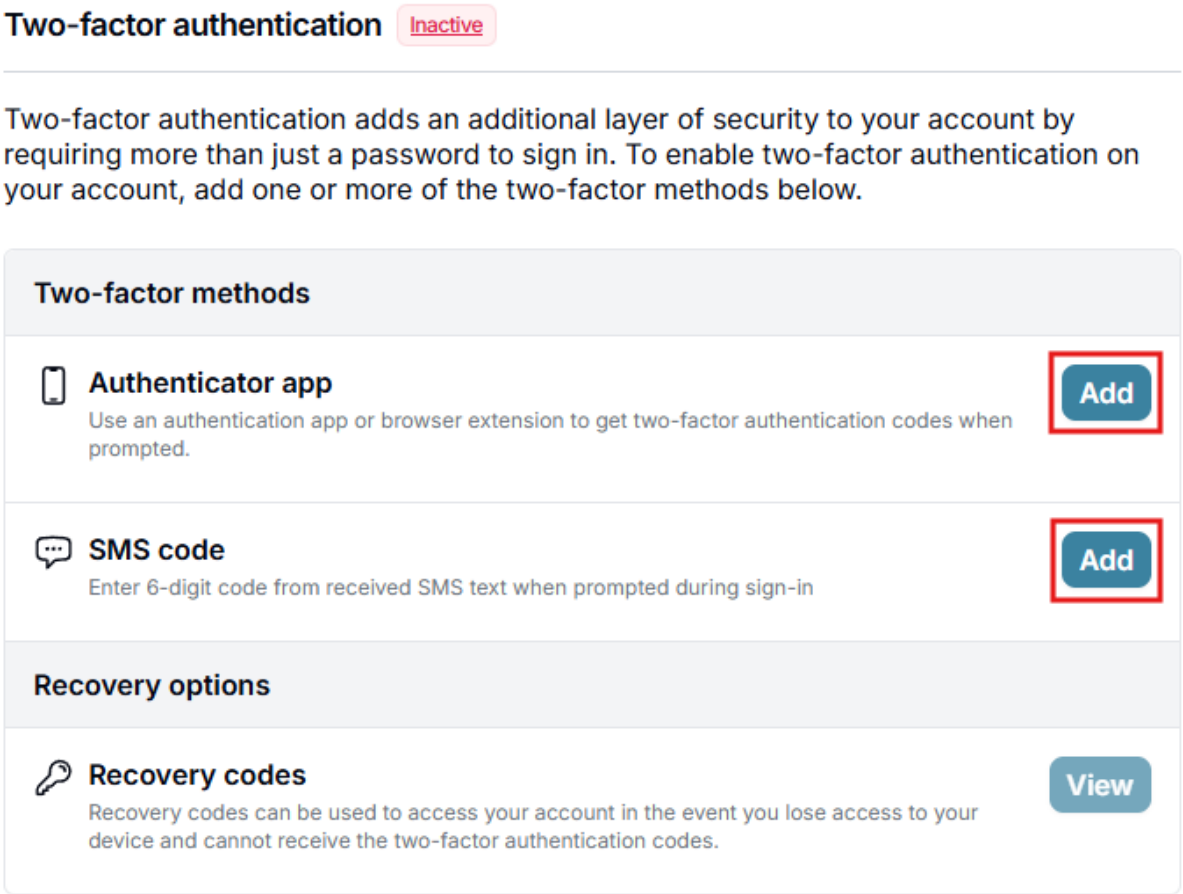
1. Login to the Impact Hub, click on the profile icon top right and click **Your settings**



2. Click **Password and authentication** on the profile menu



3. Scroll down and click either the **Add** button next to **Authenticator app** if you want to use an App on your Mobile device (Android phone/tablet, iPhone or iPad) or a browser extension (1Password), or the **Add** button next to **SMS code** if you would prefer to receive a code to your Mobile device via SMS instead. If none of these options are viable then it is possible to use a landline number to receive SMS codes, but we do not recommend this as it is less secure and less reliable.



a. If you selected the **Authenticator app** option you will be asked to re-enter your password and click a **Confirm** button.

   You will then be shown details of the supported mobile authentication Apps, we recommend using Google Authenticator (Android, iPhone & iPad) or Microsoft Authenticator (Android, iPhone & iPad) or **1Password** (paid browser extension)

   In **Google Authenticator** tap the plus icon (bottom right) and select “Scan a QR code” and scan the code on the page.

   In **Microsoft Authenticator** tap the QR code button (bottom right) and scan the code on the page.

   The two options above are free, **1Password** requires a licence, pricing starts at €2.65/month. You will need to create an account and follow the instructions on their website to install and use the browser extension to scan the QR code.

   This will add an item to the app/extension called **Armed Forces Covenant Fund Trust**, this is where you can view the six digit authentication code which changes every 30 seconds.

   On the page add a friendly name for the mobile device in **Device name** if required, then enter the six digit code in **Verify the code from the app** and click the **Save** button before it changes to a new number, if the number changes in the App the authentication will fail and the new number will need to be added.

   If the code is saved successfully you will be provided with recovery codes which can be used to recover your account should you lose access to the authenticator app on the mobile device. Please save these to a secure location.

   To change the mobile device, edit the name or remove the authenticator app click the **Edit** button.

b. If you selected the **SMS code** option you will be asked to re-enter your password and click a **Confirm** button.

   You will then be asked to enter the number you wish to use for authentication in **Phone number**, once entered click the **Verify** button.

   This will send an SMS to you the number entered, enter the six digit code in **Verify the code from received sms text** and click **Save**.

   If the code is saved successfully you will be provided with recovery codes which can be used to recover your account should you lose access to the

authenticator app on the mobile device. Please save these to a secure location.

To change or remove the number click the **Edit** button.

Help

If you need any assistance, please contact your Grant Manager and provide details of the issue(s) you are experiencing, including a screenshot if possible.