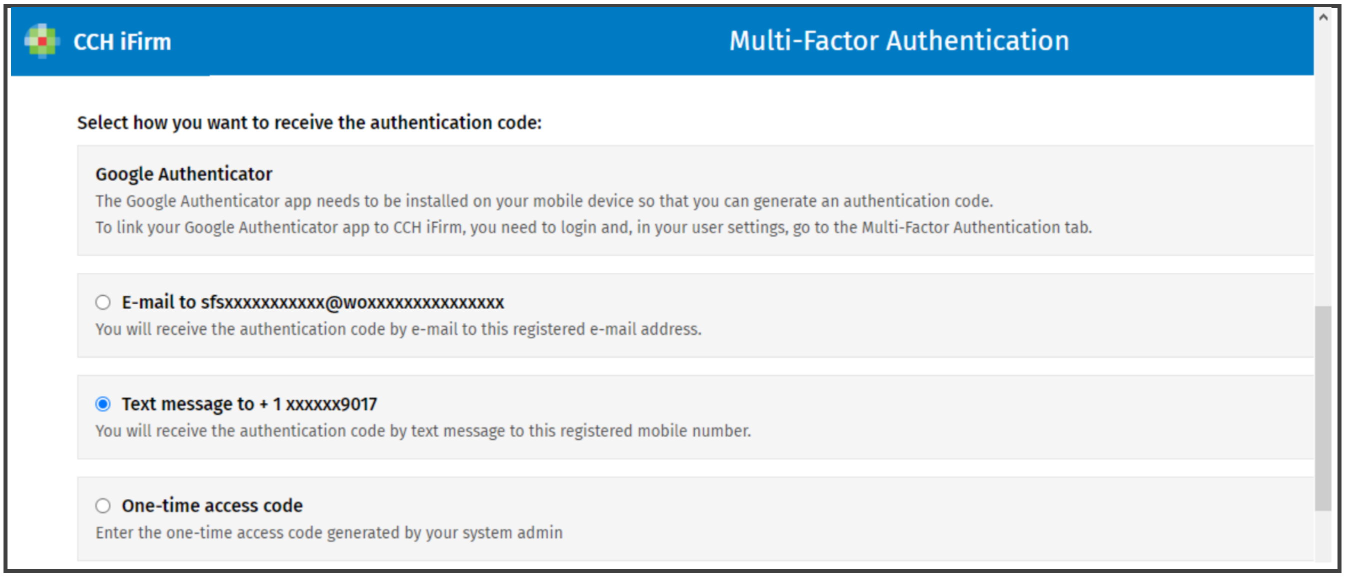
Setting up Google Authenticator

Multi-Factor Authentication provides an enhanced security to your iFirm account. When a user logs in they have four options for Multi-Factor Authentication. These include:

- **Google Authenticator** – The Google Authenticator app needs to be installed on your mobile device so that you can generate an authentication code. To link your Google Authenticator app to CCH iFirm , you need to Login and in your user settings, go to the Multi-Factor Authentication tab.
- **Email to** – You will receive the authentication code by e-mail to this registered e-mail address.
- **Text message** – You will receive the authentication code by text message to this registered mobile number. This option will only work if your mobile number was entered as part of your User Profile.
- **One-Time access code** – Enter the one-time access code generated by your system admin.



Multi-Factor Authentication

Select how you want to receive the authentication code:

Google Authenticator
The Google Authenticator app needs to be installed on your mobile device so that you can generate an authentication code.
To link your Google Authenticator app to CCH iFirm, you need to login and, in your user settings, go to the Multi-Factor Authentication tab.

○ **E-mail to sfsxxxxxxxxxxx@woxxxxxxxxxxxxxxx**
You will receive the authentication code by e-mail to this registered e-mail address.

● **Text message to + 1 xxxxxx9017**
You will receive the authentication code by text message to this registered mobile number.

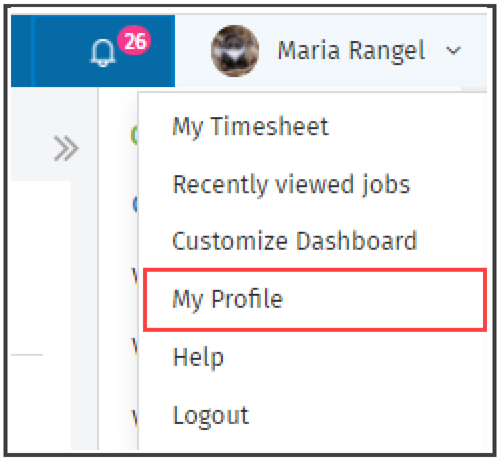
○ **One-time access code**
Enter the one-time access code generated by your system admin

Here we will cover how to setup Google Authenticator for use with CCH iFirm. To do this, you must login for the first time and authenticate using a code sent to you via email or provided to you by your admin user.

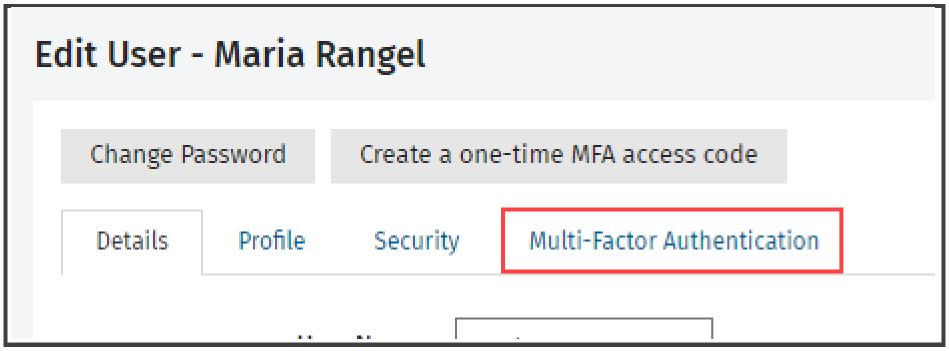
Prior to setting up Google Authenticator, it will be required that you install the Google Authenticator App to your mobile phone to generate the authentication code.

To setup Google Authenticator:

1. In the right-hand corner of CCH iFirm, click the user drop-down menu, and select **My Profile**.



2. From the Edit User page, select the **Multi-Factor Authentication** tab.

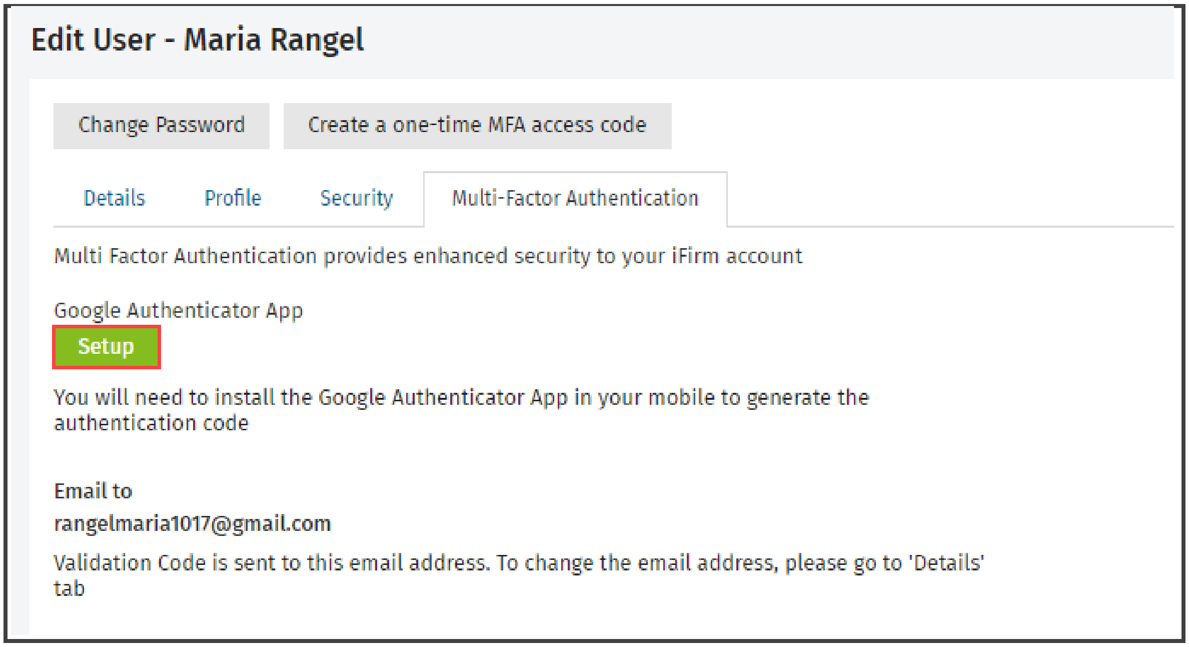


Edit User - Maria Rangel

Change Password
Create a one-time MFA access code
Details
Profile
Security
Multi-Factor Authentication

Note that the Multi-Factor Authentication tab is not visible on sites with MFA disabled, or on users that have not completed authentication via another method.

3. From the Multi-Factor Authentication tab , click the **Setup** button.



Edit User - Maria Rangel

Change Password
Create a one-time MFA access code
Details
Profile
Security
Multi-Factor Authentication

Multi Factor Authentication provides enhanced security to your iFirm account

Google Authenticator App

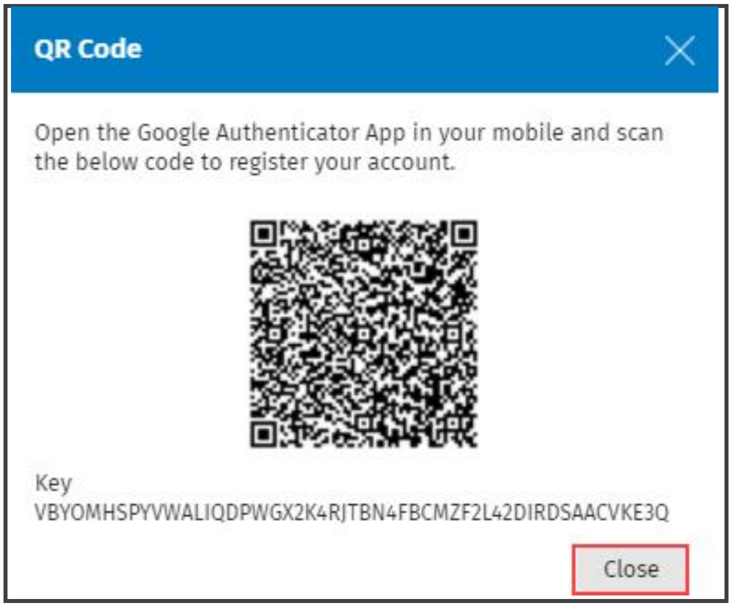
You will need to install the Google Authenticator App in your mobile to generate the authentication code

Email to

rangelmaria1017@gmail.com

Validation Code is sent to this email address. To change the email address, please go to 'Details' tab

4. CCH iFirm displays the QR Code. Open the Google Authenticator App on your mobile device and scan the code to register your account. Once scanned, click **Close**.

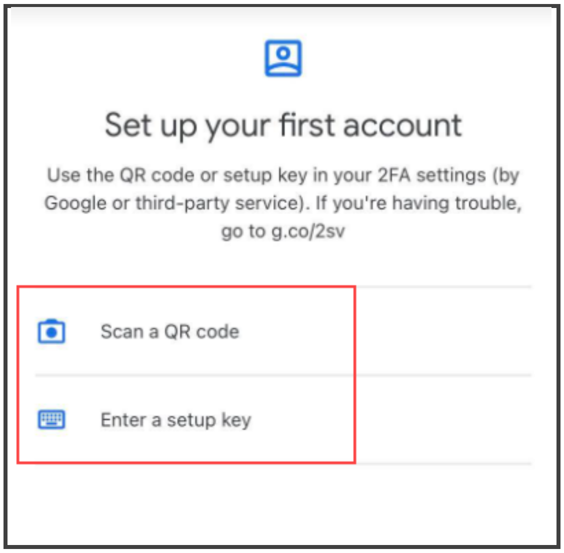


QR Code

Open the Google Authenticator App in your mobile and scan the below code to register your account.

Key
VBYOMHSPYVWALIQDPWGX2K4RJTBN4FBCMZF2L42DIRDSAACVKE3Q

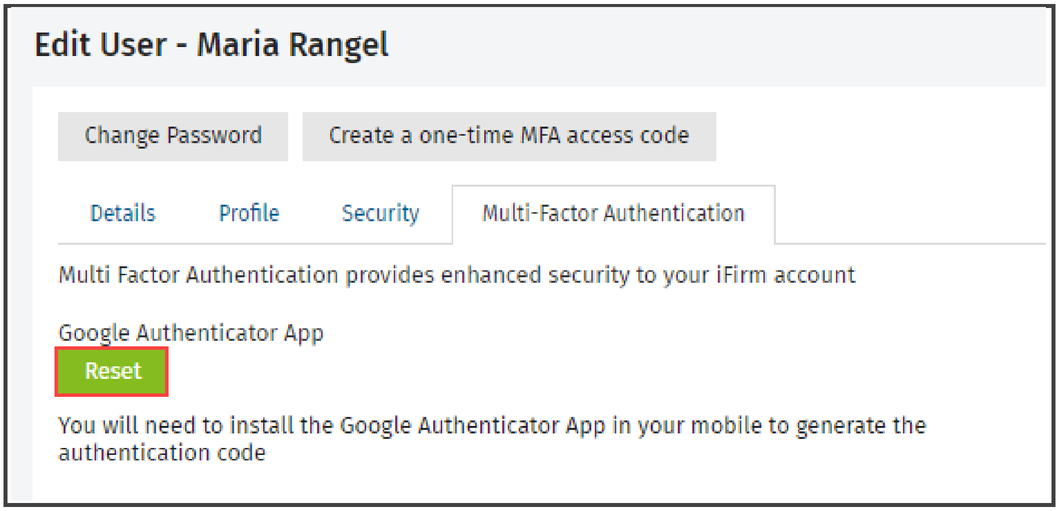
When you initiate Google Authenticator, you will be prompted to scan a QR code or enter a setup key.



Set up your first account

Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to g.co/2sv

5. Once your scan the QR Code, CCH iFIrm updates the button to Reset.



Edit User - Maria Rangel

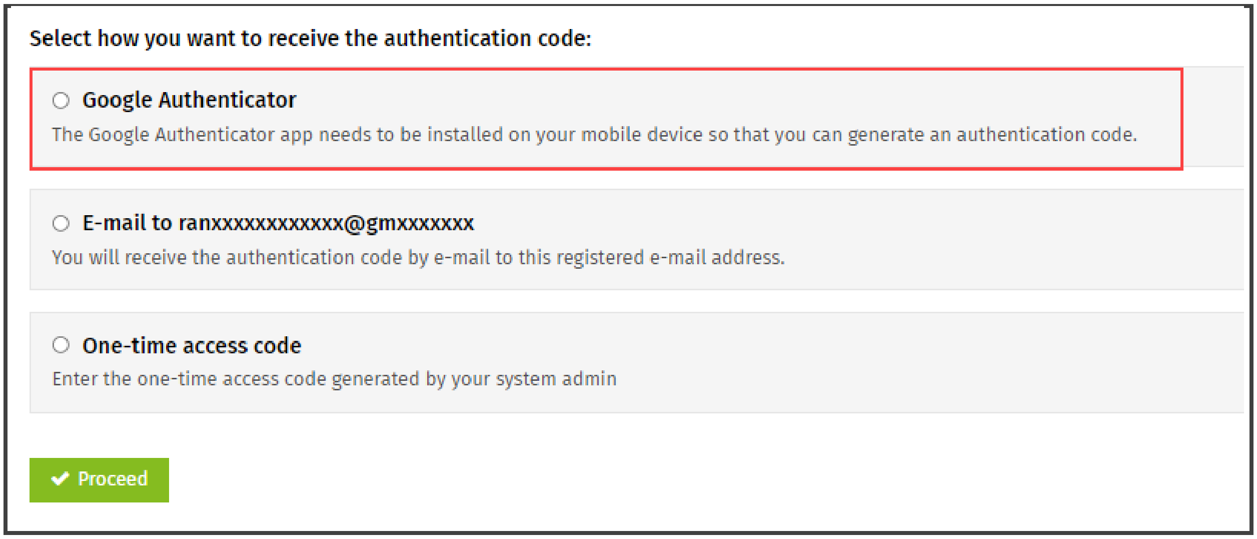
Change Password
Create a one-time MFA access code
Details
Profile
Security
Multi-Factor Authentication

Multi Factor Authentication provides enhanced security to your iFirm account

Google Authenticator App

You will need to install the Google Authenticator App in your mobile to generate the authentication code

The next time the user needs to authenticate, they will then have the option authenticate using Google Authenticator.



Select how you want to receive the authentication code:

○ **Google Authenticator**
The Google Authenticator app needs to be installed on your mobile device so that you can generate an authentication code.

○ **E-mail to ranxxxxxxxxxxxx@gmxxxxxxx**
You will receive the authentication code by e-mail to this registered e-mail address.

○ **One-time access code**
Enter the one-time access code generated by your system admin