

# Two Factor Authentication (“2FA”)

## Contents

Cyber Security .....	1
Enable Portal 2FA.....	1
Accessing your account.....	1
Main log on Screen: .....	2
Online Submissions Portal log on Screen:.....	3
PQ Portal log on Screen: .....	3
Using Email 2FA.....	4
Using Authenticator App 2FA (preferred).....	5
Logging on for the first time with 2FA .....	7
Have no access to your app? .....	7

## Cyber Security

2FA is an additional layer of security used to ensure only authenticated users gain access to an online account and is recommended by the National Cyber Security Centre.

The Commission wishes to align itself with current standards and make the use of 2FA mandatory, for all Portal Users.

When you log into the Portal, an additional prompt will display asking you to enter a security code. This code is sent to you via your registered e-mail address or an authentication app.

The Commission wishes to impress on firms the need to ensure they take their responsibilities in respect of cyber security seriously. User accounts should be uniquely owned and generic user accounts should not be permitted.

If you have any queries regarding 2FA set up please email: [2FASupport@gfsc.gg](mailto:2FASupport@gfsc.gg)

## Enable Portal 2FA

### Accessing your account

1. Access your User Profile.

This can be accessed from any of the following screens shown below by clicking on your user details in the top right-hand corner:

Main log on Screen:



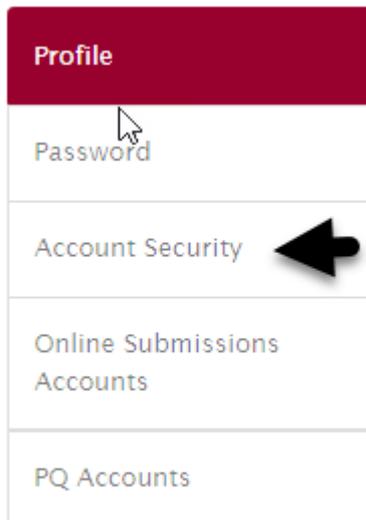
**Guernsey Financial Services Commission**

**Online Submissions**  
This Portal allows licensees and individuals to submit the most common firm applications, notifications and returns to the Commission electronically.

**Personal Questionnaire (PQ)**  
This Portal allows individuals to submit Personal Questionnaires (PQs) and Online Appointments for prescribed positions or supervised roles to the Commission electronically.

[Open Online Submissions](#) [Open PQ portal](#)

(a) Clicking from the above screen will take you directly to your Profile. Choose Account Security from the below:



**Profile**

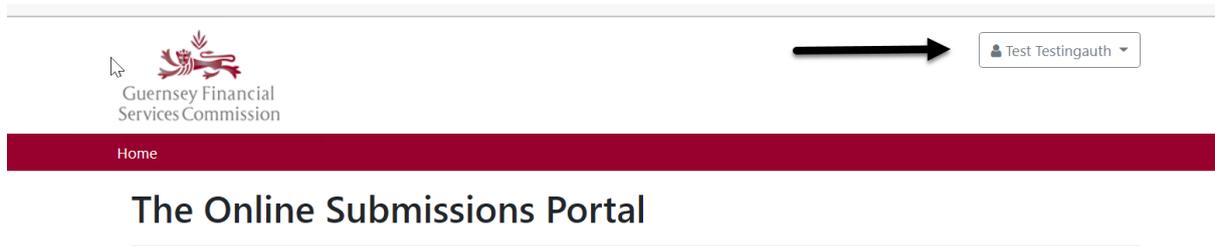
Password

Account Security

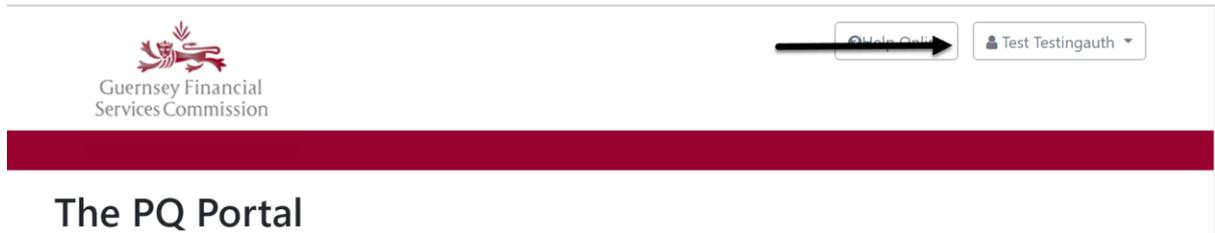
Online Submissions  
Accounts

PQ Accounts

Online Submissions Portal log on Screen:

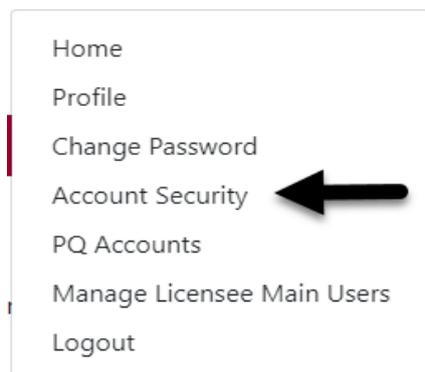


PQ Portal log on Screen:



(b) Clicking from the PQ and Online Submission Portal screens above will give you the options shown below.

Choose Account Security:



- (c) You can choose between an Email or using the Authenticator App, as outlined below (Authentication App is recommended as the more secure option):

## Account Security

Passwords can be stolen by cyber criminals, potentially giving them access to your online accounts. However, you can protect your account by requiring an extra check when you sign in, so even if a criminal knows your password, they won't be able to easily gain access to your data.

### Email

Whenever you sign in, you'll enter your password as usual. Then, a code will be sent to your email address to complete your sign in. This relies on ensuring that your email account is kept sufficiently secure from attackers.

Set up email

### Authenticator app

Whenever you sign in, you'll enter your password as usual. Then, you will be asked for a code that is generated by an app on your computer, tablet or mobile phone. This is the most secure option for protecting your account.

Setup authenticator app

## Using Email 2FA

2. If set up email is required, click on the below 'set up email' option:

Set up email

- (a) The next time you log on, the following screen will be displayed and you should choose 'Submit'

---

Send Verification Code

### Send Verification Code

You have Email Two-Factor Authentication enabled click 'Submit' to generate email with relevant code.

Submit

- (b) You will be taken to the view shown below. Check your emails and type in the code that has been emailed to you. *(If you do not receive an email please check that the email address in your 'Profile' is correct).*

# Two-Step Verification.

Enter the Verification Code that was emailed to you

Submit

(c) Click Submit and you will be logged in.

## Using Authenticator App 2FA (preferred)

3. If Setup authenticator app is required, click on 'setup authenticator app' as shown below:

Setup authenticator app

The following screen will be displayed:

### Configure authenticator app

To use an authenticator app go through the following steps:

1. Download a two-factor authenticator app

Microsoft Authenticator



Google Authenticator



Authy



2. Scan the QR Code or enter this key `s4q2 pkuc iocp 7ua3 hgw zyyj 26ql ojii`



3. Once you have scanned the QR code or input the key above, your two factor authentication app will provide you with a unique code. Enter the code in the confirmation box below.

Enter the Verification  
Code generated by your  
Authenticator App

Two-Step Verification

- (a) Download the App and follow the instructions to use the authenticator app, that is:
- (i) Download an Authenticator app- (links are included to the three examples by clicking on the relevant black icon).
  - (ii) Once you have downloaded the app on your chosen device you will be given the option to Scan a 'QR code' or 'Enter the Key'.
  - (iii) Scan the QR code (or input the key) as displayed on the Portal screen. (Please note if the key is input no spaces are required. You will also need to allocate an Account Name *e.g GFSC plus Portal user name* in the App)
  - (iv) The app will generate a number.
  - (v) Enter the number in the box provided.
  - (vi) Select the 'Two-step verification' button.

Enter the Verification  
Code generated by your  
Authenticator App

**Two-Step Verification**

- (b) You will be presented with a list of Recovery codes. This is a first time set up screen only and these codes should be kept somewhere other than your device. (If your device is lost then these codes can be used instead of your chosen App):

## Manage your account

Profile
Password
<b>Account Security</b>

### Recovery codes

**⚠ Put these codes in a safe place.**

If you lose your device and don't have the recovery codes you will lose access to your account.

e d  
9 e  
1 o  
e s  
e 7  
3 1  
0 1  
e 2  
e 1  
9 f

(c) Log out of your account.

**Congratulations your 2FA will now be active.**

## Logging on for the first time with 2FA

4. A code will be requested each time you log in:
- 5.

**Two-Step Verification.**

Enter the Verification Code generated by your Authenticator App

**Submit**

Don't have access to your authenticator device? You can [log in with a recovery code.](#)

- (a) Open the app and input the code generated into the Portal and then press submit.

**You will now be logged in.**

## Have no access to your app?

6. If you need to log in with a recovery code click 'log in with a recovery code' as per the below:

**Two-Step Verification.**

Enter the Verification Code generated by your Authenticator App

**Submit**

Don't have access to your authenticator device? You can [log in with a recovery code.](#)

- (a) One of your saved Recovery codes should then be inputted:

## Two-Step Verification Recovery code

---

You have requested to log in with a recovery code. This login will not be remembered until you provide an authenticator app code at log in or disable 2FA and log in again.

Recovery code

Sign In

**You will now be logged in.**