

# Two Factor Authentication (“2FA”)

## Contents

Cyber Security .....	1
Logging on for the first time using 2FA.....	2
Sign in to the Portal .....	2
Changing from Email to Authenticator app (preferred) .....	3
Access your User Profile .....	3
Switch to Authenticator app .....	4
Have no access to your app? .....	6
Change from Authenticator app to Email 2FA.....	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 has aligned itself with current standards and has made the use of 2FA mandatory, for all Portal Users.

When you log into the Portal, a 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 please email: [2FASupport@gfsc.gg](mailto:2FASupport@gfsc.gg)

## Logging on for the first time using 2FA

2FA will default to Email unless you change it in your User Profile.

### Sign in to the Portal

This applies to the Main, Online Submissions and PQ Portals

1. Sign in to the Portal using your registered email address and password.  
The following screen will appear:



Send Verification Code

### Send Verification Code

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

Submit

2. Click on 'Submit'.
3. 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

4. Click 'Submit' and you will be logged on to the Portal.

# Changing from Email to Authenticator app (preferred)

## Access your User Profile

When you are signed in, your profile can be accessed from any of the following screens shown below by clicking on your user details in the top right-hand corner.

1. Main log on Screen

Guernsey Financial Services Commission

test@test.gg Logout

## 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.  
[Open Online Submissions](#)

**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 PQ portal](#)

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

2. Online Submissions Portal log on Screen:

Guernsey Financial Services Commission

Test Testing

Home

My GFSC Support

## Welcome to Online Submissions

### 3. PQ Portal log on Screen:

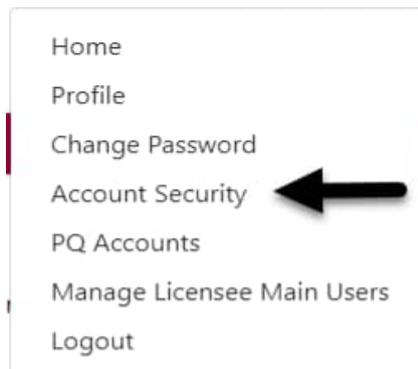


Help Online

Test Testing ▾

## Welcome to the PQ Portal

Clicking from the PQ and Online Submissions Portal screen above will give you the options shown below. Choose 'Account Security'.

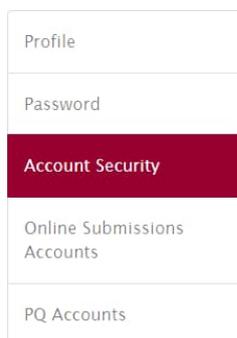


### Switch to Authenticator app

Authenticator app is recommended as the more secure option.

1. Click 'Setup authenticator app':

## Manage your account



### Account Security

Passwords can be stolen by cyber criminals, potentially giving them access to your online accounts. The Commission therefore protects 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.

### Switch to 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



2. 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



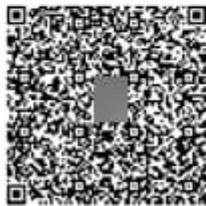
Google Authenticator



Authy



2. Scan the QR Code or enter this key `s4q2 pluc locp 7ua3 hhgw zyyj 26q1 oji1`



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**

3. Download the App and follow the instructions to use the authenticator app, that is:
  - (a) Download an Authenticator app (links are included to the three examples by clicking on the relevant black icon).
  - (b) 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'.
  - (c) 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).
  - (d) The app will generate a number.
  - (e) Enter the number in the box provided.
  - (f) Select the 'Two-step verification' button.

Enter the Verification Code generated by your Authenticator App

**Two-Step Verification**

4. 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

The screenshot shows the 'Manage your account' interface. On the left is a sidebar menu with three items: 'Profile', 'Password', and 'Account Security' (highlighted in red). The main content area is titled 'Recovery codes' and features a yellow warning box with a triangle icon that says 'Put these codes in a safe place.' Below this, a message states: 'If you lose your device and don't have the recovery codes you will lose access to your account.' To the right of the message is a vertical list of 12 recovery codes, each on a separate line: e d, 9 e, 1 0, e 5, e 7, 3 1, 0 1, e 2, e 1, 9 f.

5. Log out of your account.

## Have no access to your app?

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

The screenshot shows the 'Two-Step Verification' login screen. At the top, it says 'Two-Step Verification.' Below that, it prompts the user to 'Enter the Verification Code generated by your Authenticator App' with an input field. A red 'Submit' button is located below the input field. At the bottom of the screen, there is a link that says 'Don't have access to your authenticator device? You can log in with a recovery code.' A black arrow points to this link from the right.

2. 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.

Recovery code

Sign In

3. Click 'Sign In', you will now be logged in.

## Change from Authenticator app to Email 2FA

1. To switch from Authenticator app to email , in your user profile, under 'Account Security', click on 'Set up email':

## Manage your account

Profile
Password
<b>Account Security</b>
Online Submissions Accounts
PQ Accounts

### Account Security

Passwords can be stolen by cyber criminals, potentially giving them access to your online accounts. The Commission therefore protects 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.

Reset recovery codes

Reset authenticator app

### Switch to 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



2. The next time you log on, the following screen will be displayed. Click 'Submit'.



Send Verification Code

## Send Verification Code

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

Submit

3. 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).



Guernsey Financial  
Services Commission

## Two-Step Verification.

---

Enter the Verification Code that was emailed to you

Submit

4. Click 'Submit' and you will be logged in.