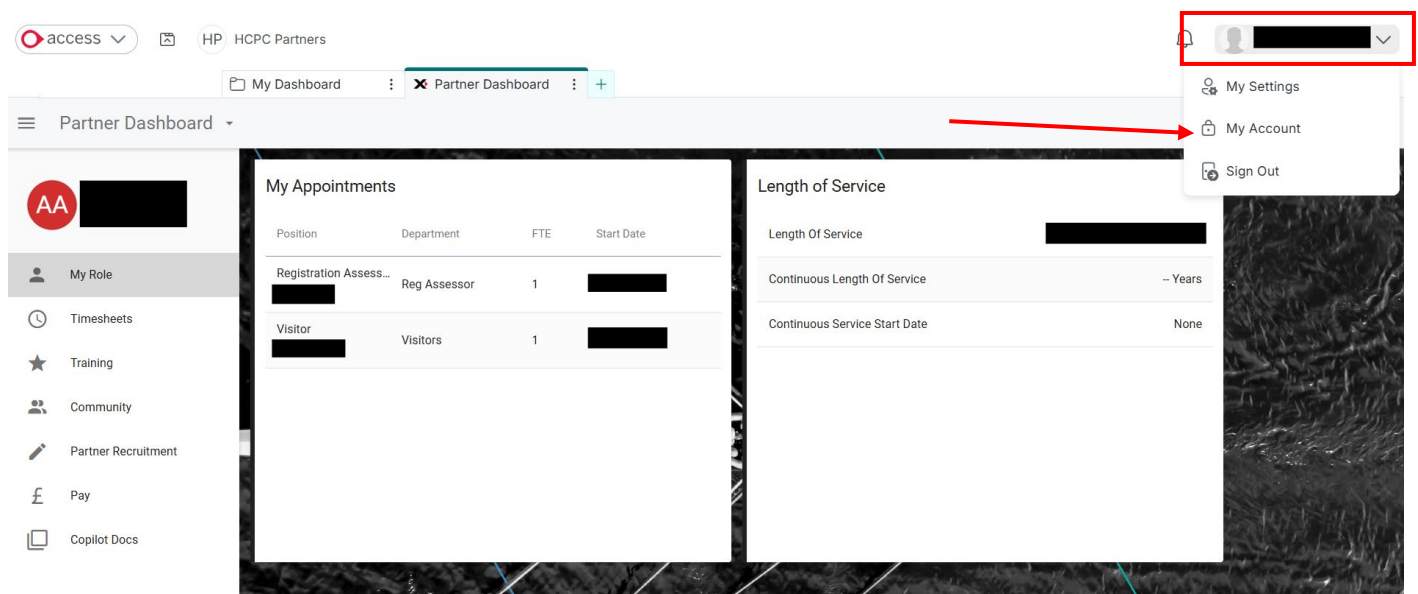


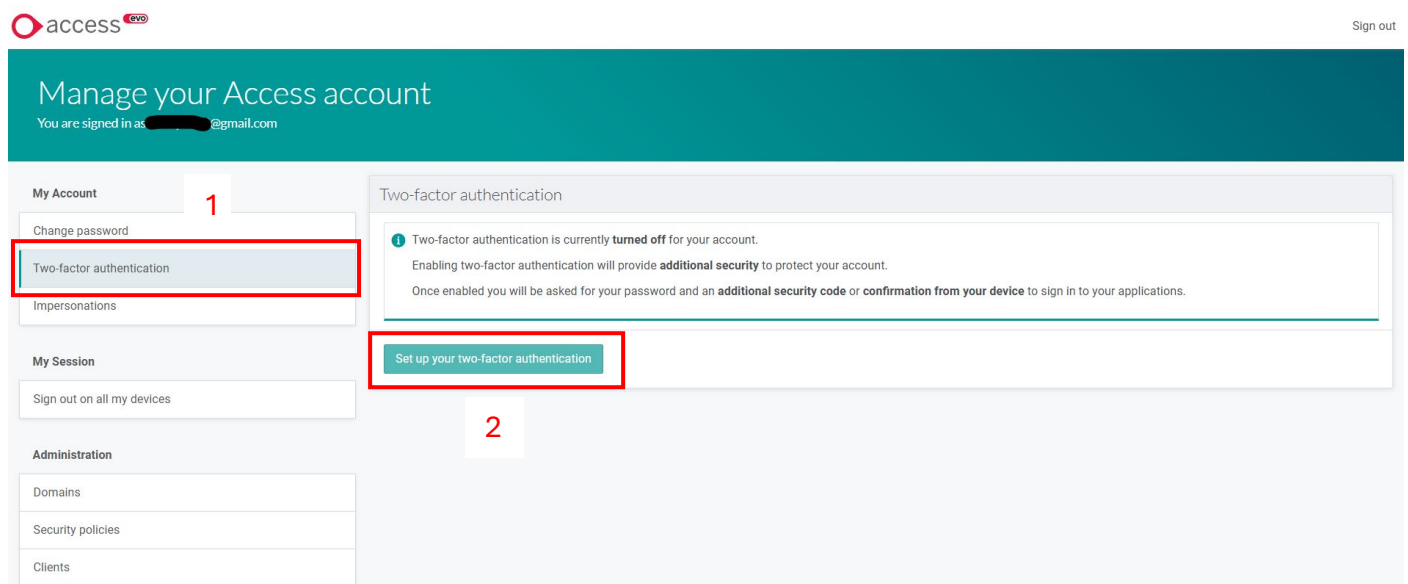
## How to: Enable two-factor authentication (2FA) for your Partner Portal Account

You now have the option of enabling two-factor authentication (2FA) for your Partner Portal account. This means, that like many other accounts you have with service providers you use personally, your login process will involve an additional step for added security. We highly encourage you to enable this additional layer of security given that your banking details and remittance information will now be available in the Partner Portal. To enable 2FA, follow the steps below. If anything is unclear, or you have any queries, please contact us at [partners@hcpc-uk.org](mailto:partners@hcpc-uk.org).

1. To enable 2FA, click on your name in the top right corner of the screen (red box in image below) and select “My Account” from the drop-down menu. Note that this can be done from any screen while logged into your Partner Portal account.



2. Another tab will open in your web browser showing the page below. In the list on the left side of the page, click the “Two-factor authentication” option, then click the “Set up your two-factor authentication” button in the middle of the page.



3. Here you will be presented with 3 options. We recommend against using the 3<sup>rd</sup> option to use your mobile phone number and will, therefore, explain the process for the other 2 options (shown in the red box).

The screenshot shows the 'Manage your Access account' interface. On the left, there's a sidebar with 'My Account' (Change password, Two-factor authentication, Impersonations), 'My Session' (Sign out on all my devices), and 'Administration' (Domains, Security policies, Clients). The main content area is titled 'Two-factor authentication' and 'Set up your two-factor authentication'. It features three options: 'Use a FIDO2 or U2F authenticator' (highlighted with a red box), 'Use an authenticator app', and 'Receive a text message'. Each option has a description and a corresponding button ('Add authenticator', 'Add authenticator app', 'Add mobile phone'). A 'Back' button is at the bottom left.

- a. First, we will look at the “FIDO2 or U2F authenticator”. Click on the “Add authenticator” button. This option is best if you wish to sign in using tools on your device, such as a fingerprint scanner or your web browsers passkey functionality.

This screenshot is similar to the previous one, showing the 'Manage your Access account' page. The 'Two-factor authentication' section is visible, with the 'Add authenticator' button under the 'Use a FIDO2 or U2F authenticator' option highlighted with a red box. The rest of the interface, including the sidebar and other options, remains the same.

- i. Next, you will be asked to give your authenticator a name. Enter whatever text you like. You will also have a list of available authenticator types in a drop-down list, depending on your device and web browser.

access 2020

Sign out

## Manage your Access account

You are signed in as [redacted]@gmail.com

**My Account**

- Change password
- Two-factor authentication
- My FIDO2 authenticators
- Impersonations

**My Session**

- Sign out on all my devices

**Administration**

- Domains
- Security policies
- Clients

My FIDO2 authenticators

To continue please register at least one authenticator device.

Add an authenticator

Name

Give your authenticator a name

Add

Authenticator type

- Built-in - e.g. a fingerprint scanner or PIN on your device
- External - e.g. a USB, Bluetooth or NFC security key
- Built-in - e.g. a fingerprint scanner or PIN on your device

Back

- ii. In this example, the name “HCPC Partner” has been used and the authenticator typer selected is “fingerprint scanner or pin on your device”. Click the “Add” button.

access 2020

Sign out

## Manage your Access account

You are signed in as [redacted]@hotmail.com

**My Account**

- Change password
- Two-factor authentication
- My FIDO2 authenticators
- Impersonations

**My Session**

- Sign out on all my devices

**Administration**

- Domains
- Security policies
- Clients

My FIDO2 authenticators

To continue please register at least one authenticator device.

Add an authenticator

Name

HCPC Partner

Add

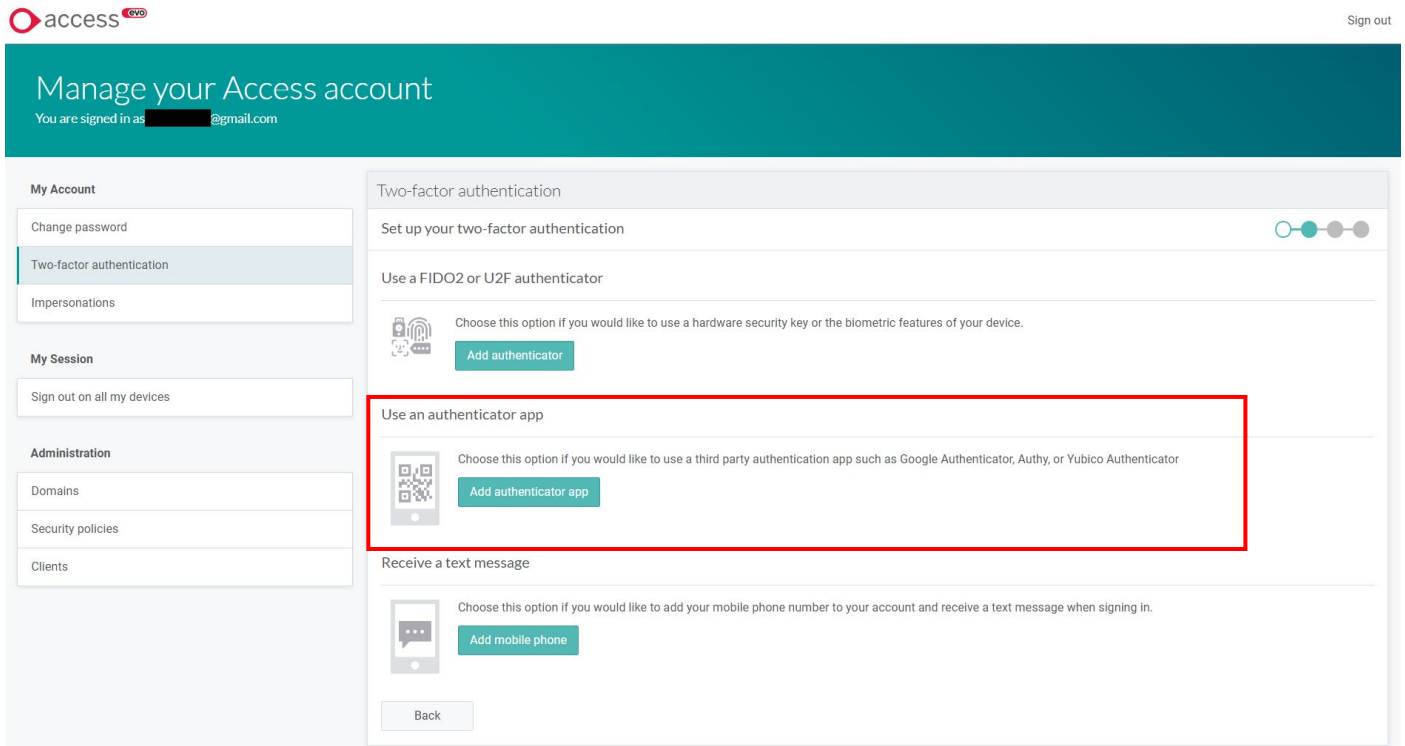
Authenticator type

- Built-in - e.g. a fingerprint scanner or PIN on your device

Back

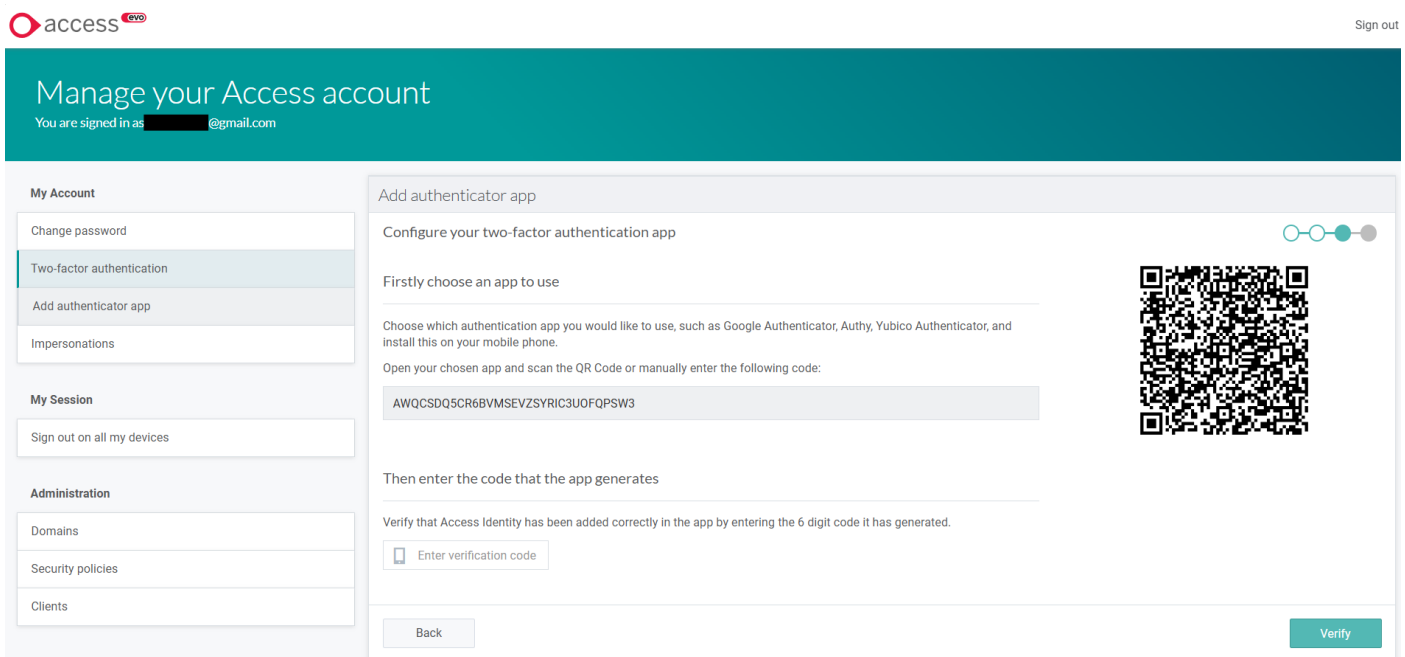
iii. From this point, the remaining steps will vary depending on your device. Follow the prompts as directed to complete setting up this form of authentication.

b. The second option is to “Use an authenticator app”. This method involves downloading a third-party app, which you will use to complete the login process. To use this method, click on the “Add authenticator app” button.



The screenshot shows the 'Manage your Access account' interface. On the left, there's a sidebar with 'My Account', 'My Session', and 'Administration' sections. The main content area is titled 'Two-factor authentication' and 'Set up your two-factor authentication'. It offers three options: 'Use a FIDO2 or U2F authenticator', 'Use an authenticator app' (highlighted with a red box), and 'Receive a text message'. Each option has a corresponding icon and a description. The 'Add authenticator app' button is a green button located next to the 'Use an authenticator app' option.

i. You will then be redirected to the page shown below, which includes further instructions to complete setting up this option. If you do not already have an authenticator app installed, you will need to choose one and download it onto your device. Some suggestions are provided in the instructions.



The screenshot shows the 'Add authenticator app' page. It has a sidebar on the left with 'My Account', 'My Session', and 'Administration' sections. The main content area is titled 'Add authenticator app' and 'Configure your two-factor authentication app'. It instructs the user to 'Firstly choose an app to use' and provides a QR code to scan. Below the QR code, it shows a verification code 'AWQCSDQ5CR6BVMSEVZSYRIC3U0FQPSW3' and a text input field for the user to enter the code generated by the app. A 'Verify' button is at the bottom right.

- ii. Once you have received an access code from your authenticator app, enter it into the field shown in the image below and then click the “Verify” button to complete the process.

Add authenticator app

Configure your two-factor authentication app

Firstly choose an app to use

Choose which authentication app you would like to use, such as Google Authenticator, Authy, Yubico Authenticator, and install this on your mobile phone.

Open your chosen app and scan the QR Code or manually enter the following code:

AWQCSDQ5CR6BVMSEVZSYRIC3U0FQPSW3

Then enter the code that the app generates

Verify that Access Identity has been added correctly in the app by entering the 6 digit code it has generated.

XYC467

Back

Verify

4. From now on, you will be able to login to your account using only your email, password and, if you have enabled it, your chosen method of authentication.