CCWS HOW TO GUIDE USING PASSKEY MFA

UNIVERSITY OF CAMBRIDGE
Information Services

DASHBOARD TECHNOLOGY

CAMBRIDGE CASUAL WORKER SYSTEM GUIDE

USING PASSKEY MULTI-FACTOR AUTHENTICATION (MFA) ON APPLE iPHONE

Introduction

We have strengthened security across Cambridge Casual Worker System (CCWS) by introducing Passkey Multi Factor Authentication (MFA); a more secure and convenient way for you to verify your identity.

Multi-factor authentication (MFA) adds an extra layer of security to your account by requiring more than just a password to sign in. With Passkey MFA you can use a secure passkey to authenticate your account.

How It Works

- One half of the key is securely stored on your device or password manager.
- The other half is stored in CCWS.
- When logging in, the system verifies that the keys match. If they do, access is granted, without requiring a separate password or an authentication code.

Where Can You Store a Passkey?

When registering a passkey, you will be given the option to store it in one of the following locations:

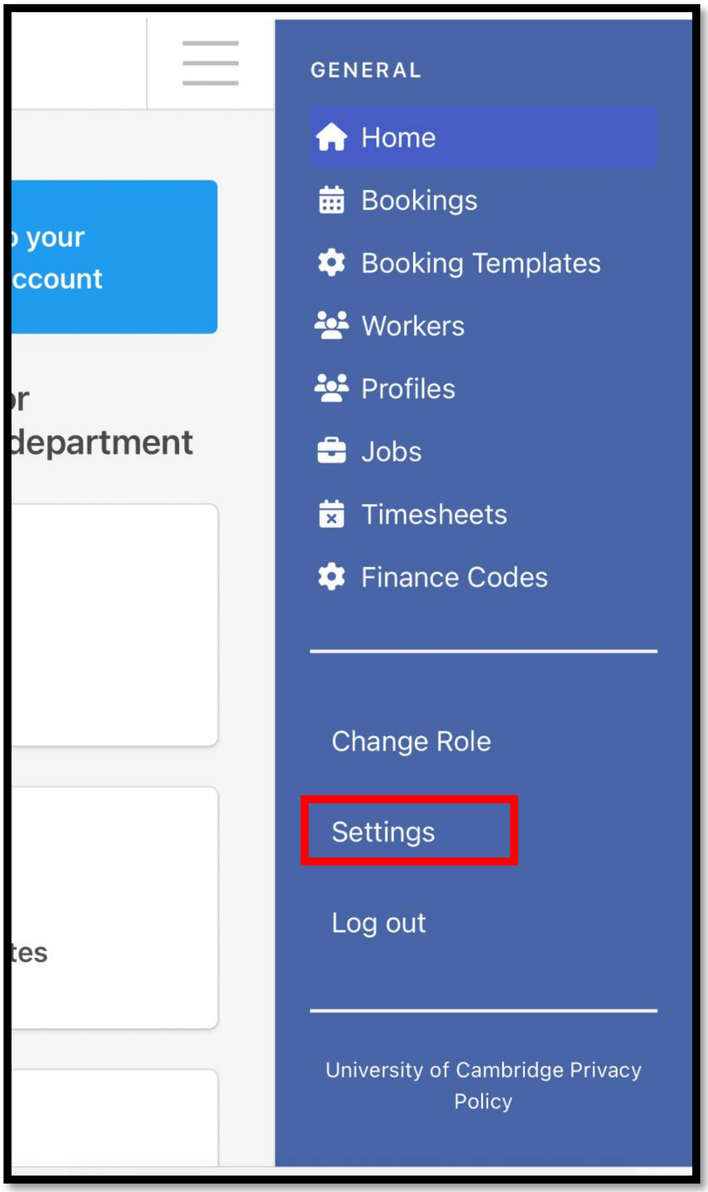
- **Password Manager** – this is recommended if you need access to the passkey across multiple devices securely.
- **Local Device** – this will store the passkey on a specific PC, laptop, or mobile phone for quick and easy login.
- **External Security Key** – this is a portable authentication method, such as a USB or NFC security key, recommended if you need an additional layer of security.

How to Enable Passkey MFA on an Apple iPhone

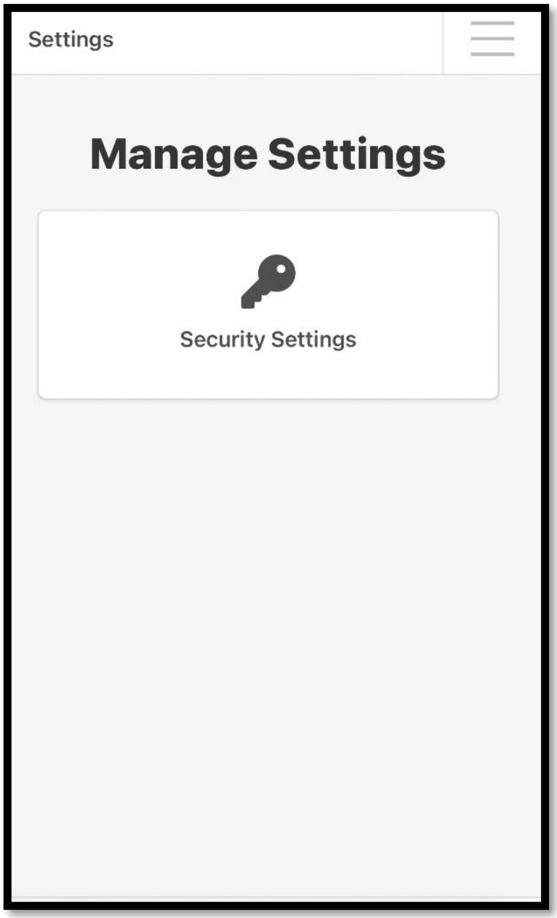
CCWS has a new **Security Settings** page where you can manage your MFA settings, which include enabling (or disabling) MFA, generating recovery codes and registering your passkeys.

Step 1: Access Security Settings

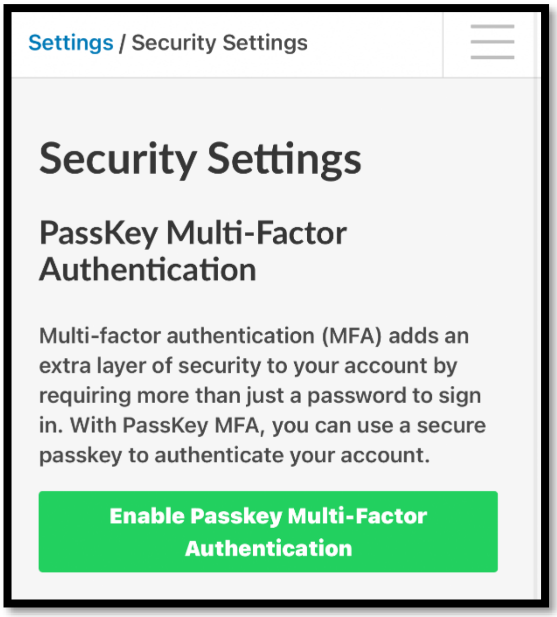
Navigate to **Settings** via the top-right dropdown menu as shown below:



Then click on **Security Settings:**



The following page will be displayed:


Settings / Security Settings

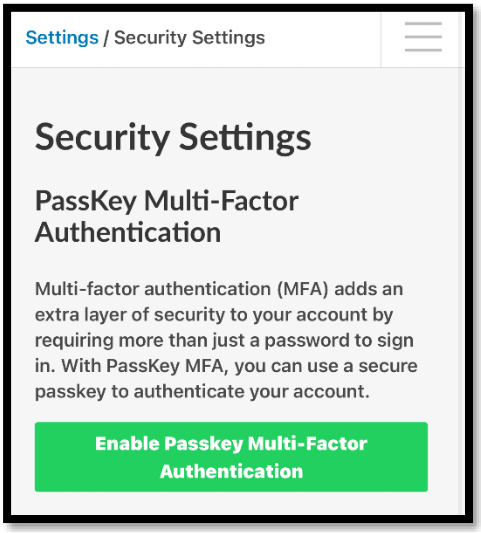
Security Settings

PassKey Multi-Factor Authentication

Multi-factor authentication (MFA) adds an extra layer of security to your account by requiring more than just a password to sign in. With PassKey MFA, you can use a secure passkey to authenticate your account.

Step 2: Enable Multi-Factor Authentication

The first step is to click the **Enable Passkey Multi-Factor Authentication** (green) button, as shown below:



Settings / Security Settings

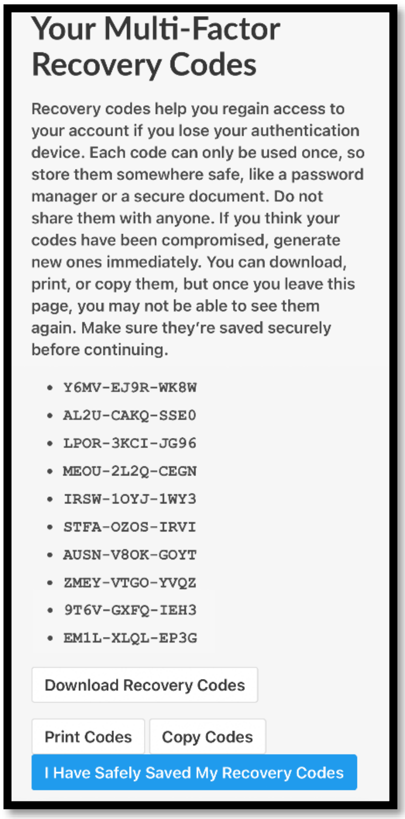
Security Settings

PassKey Multi-Factor Authentication

Multi-factor authentication (MFA) adds an extra layer of security to your account by requiring more than just a password to sign in. With PassKey MFA, you can use a secure passkey to authenticate your account.

Enable Passkey Multi-Factor Authentication

When you have done that, you should see a set of Multi-Factor Recovery Codes. These are one-time use backup codes.



Your Multi-Factor Recovery Codes

Recovery codes help you regain access to your account if you lose your authentication device. Each code can only be used once, so store them somewhere safe, like a password manager or a secure document. Do not share them with anyone. If you think your codes have been compromised, generate new ones immediately. You can download, print, or copy them, but once you leave this page, you may not be able to see them again. Make sure they're saved securely before continuing.

- Y6MV-EJ9R-WK8W
- AL2U-CAKQ-SSE0
- LPOR-3KCI-JG96
- MEOU-2L2Q-CEGN
- IRSW-1OYJ-1WY3
- STFA-OZOS-IRVI
- AUSN-V8OK-GOYT
- ZMEY-VTGO-YVQZ
- 9T6V-GXFQ-IEH3
- EM1L-XLQL-EP3G

Download Recovery Codes

Print Codes Copy Codes

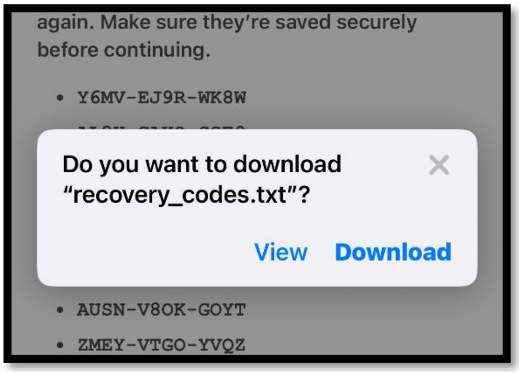
I Have Safely Saved My Recovery Codes

You will need to save these codes as they will be needed in order to log into two-factor authentication if your device is lost.

The screen will offer you 3 options for doing this:

1. **Download** as a text file
2. **Print** a PDF or physical copy
3. **Copy** them to a secure location

The screenshot below shows the process of Downloading the codes:



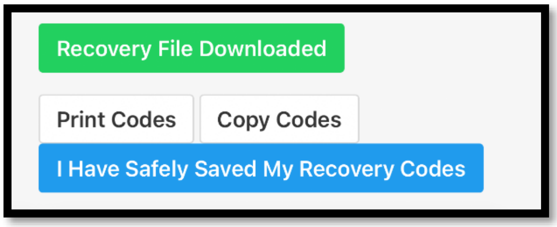
again. Make sure they're saved securely before continuing.

- Y6MV-EJ9R-WK8W

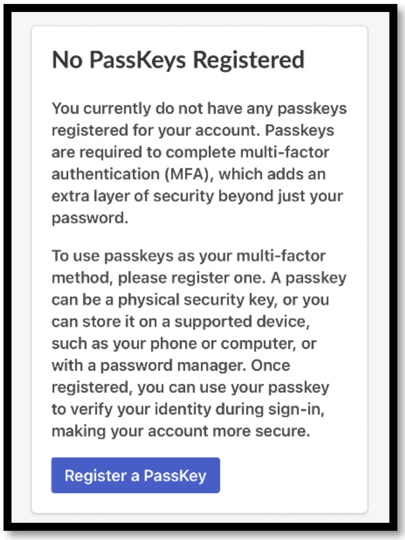
Do you want to download "recovery_codes.txt"?

- AUSN-V8OK-GOYT
- ZMEY-VTGO-YVQZ

After saving the codes, click the '**I Have Safely Saved My Recovery Codes'** button to be taken back to security settings.



You will notice that the green button has now turned red, and a message is displayed asking for Passkeys to be registered:



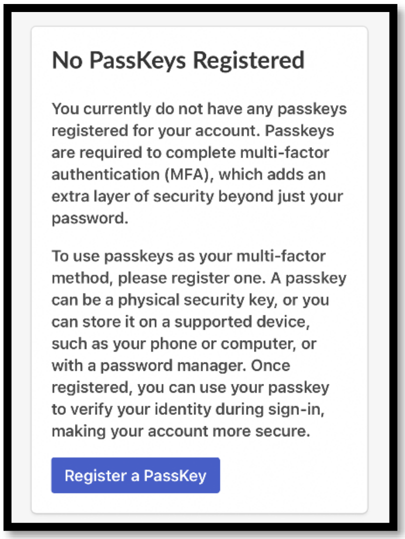
No PassKeys Registered

You currently do not have any passkeys registered for your account. Passkeys are required to complete multi-factor authentication (MFA), which adds an extra layer of security beyond just your password.

To use passkeys as your multi-factor method, please register one. A passkey can be a physical security key, or you can store it on a supported device, such as your phone or computer, or with a password manager. Once registered, you can use your passkey to verify your identity during sign-in, making your account more secure.

Step 3: Register a Passkey

The next step is to click **Register a Passkey**.

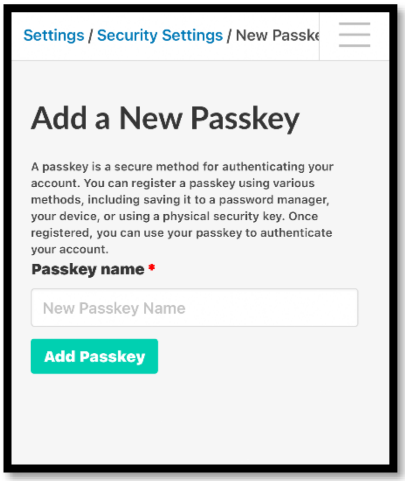


No PassKeys Registered

You currently do not have any passkeys registered for your account. Passkeys are required to complete multi-factor authentication (MFA), which adds an extra layer of security beyond just your password.

To use passkeys as your multi-factor method, please register one. A passkey can be a physical security key, or you can store it on a supported device, such as your phone or computer, or with a password manager. Once registered, you can use your passkey to verify your identity during sign-in, making your account more secure.

Please name the passkey (e.g. as per the device being used to store the passkey. For example, the brand and model of the phone that will be used to authenticate e.g. iPhone 12 and click the **Add Passkey** button.

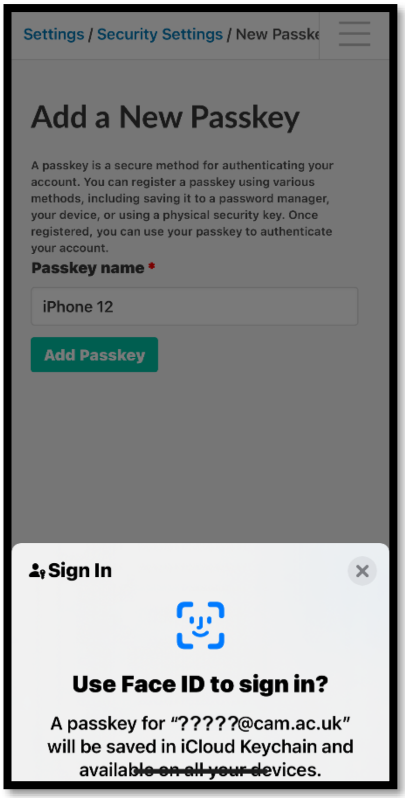


Add a New Passkey

A passkey is a secure method for authenticating your account. You can register a passkey using various methods, including saving it to a password manager, your device, or using a physical security key. Once registered, you can use your passkey to authenticate your account.

Passkey name *

On the iPhone, a message will pop up requesting that you use Face ID to sign in.



Settings / Security Settings / New Passke

Add a New Passkey

A passkey is a secure method for authenticating your account. You can register a passkey using various methods, including saving it to a password manager, your device, or using a physical security key. Once registered, you can use your passkey to authenticate your account.

Passkey name *

iPhone 12

Add Passkey

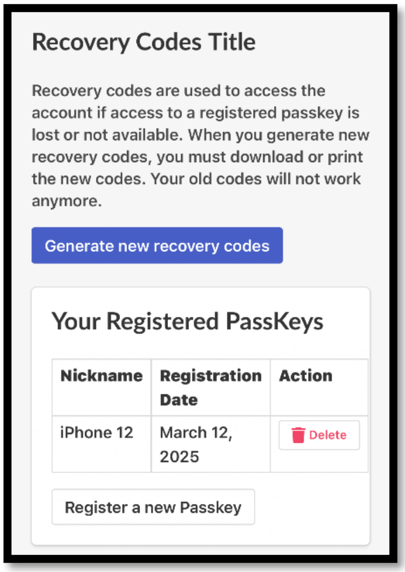
Sign In

Use Face ID to sign in?

A passkey for "?????@cam.ac.uk" will be saved in iCloud Keychain and availab~~le on all your d~~evices.

Follow the prompts to complete the registration.

When you have done this, you should be able to view your Registered Passkeys, as shown below:



Recovery Codes Title

Recovery codes are used to access the account if access to a registered passkey is lost or not available. When you generate new recovery codes, you must download or print the new codes. Your old codes will not work anymore.

Generate new recovery codes

Your Registered PassKeys

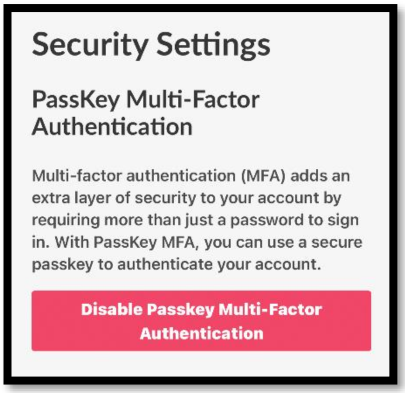
Nickname	Registration Date	Action
iPhone 12	March 12, 2025	Delete

Register a new Passkey

Managing Multi-Factor Authentication Settings

Once MFA is set up, you can manage your authentication methods at any time through the **Security Settings** page. This includes the ability to:

- **Enable or disable Passkey MFA** as needed.



Security Settings

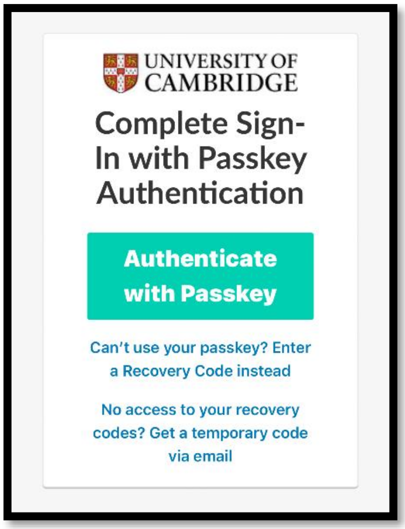
PassKey Multi-Factor Authentication

Multi-factor authentication (MFA) adds an extra layer of security to your account by requiring more than just a password to sign in. With PassKey MFA, you can use a secure passkey to authenticate your account.

- **Generate a new set of recovery codes**, which will replace any previously issued codes.
- **Register additional passkeys** to allow access from multiple devices.
- **Remove existing passkeys** if a device is lost, replaced, or no longer in use.

Step 4: Logging in for the first time after setting up a Passkey.

When you access CCWS after Registering a Passkey you will see the following screen:



UNIVERSITY OF CAMBRIDGE

Complete Sign-In with Passkey Authentication

Authenticate with Passkey
Can't use your passkey? Enter a Recovery Code instead
No access to your recovery codes? Get a temporary code via email

Click on the green button to "**Authenticate with Passkey**" and follow the instructions to use a saved passkey.

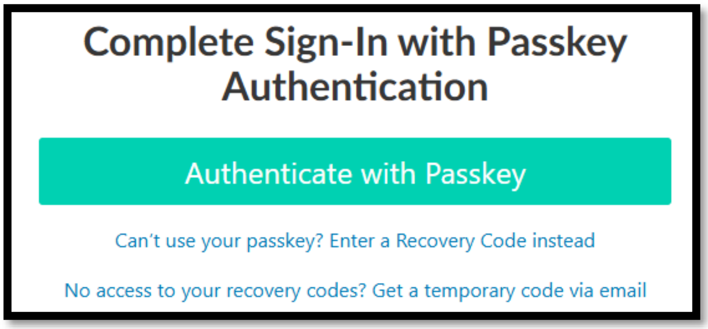
You should now be able to access your user profile in CCWS.

How to log in using a recovery code

If you can't use your Passkey, you can gain access to the system by using one of the Recovery Codes you saved when Multi-factor Authentication was set up.

Step 1: Sign into the Cambridge Casual Worker System

Sign into the Cambridge Casual Worker System as normal by using your email address and password. You will then see the screen shown below:

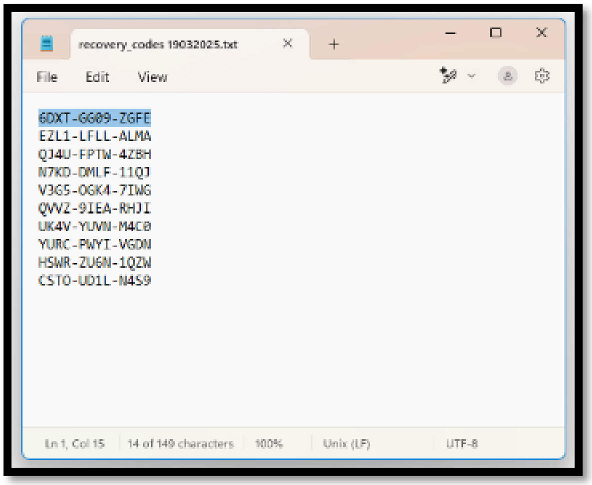


Complete Sign-In with Passkey Authentication

Authenticate with Passkey
Can't use your passkey? Enter a Recovery Code instead
No access to your recovery codes? Get a temporary code via email

Step 2: Open the list of Recovery Codes

Open the list of Recovery Codes you saved when you set up Multi-factor Authentication, and copy one of the codes.

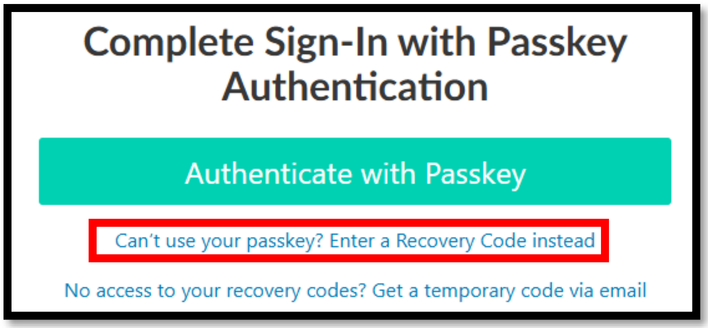


```
6DXT-GG09-ZGFE
EZL1-LFLL-ALMA
QJ4U-FPTW-4ZBH
N7KD-DMLF-11QJ
V3G5-OGK4-7IWG
QVVZ-9IEA-RHJI
UK4V-YUVN-M4C0
YURC-PWYI-VGDN
HSWR-ZU6N-1QZW
CSTO-UD1L-N4S9
```

Ln 1, Col 15 | 14 of 149 characters | 100% | Unix (LF) | UTF-8

Step 3: Enter a Recovery Code

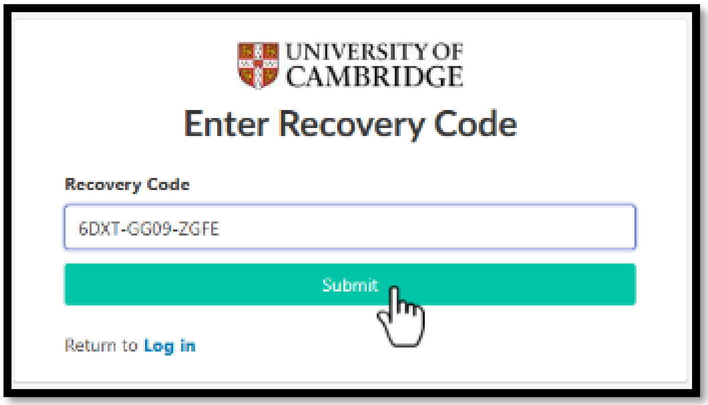
On the ‘Complete Sign-In with Passkey Authentication’ screen, select the link to ‘**Enter a Recovery Code Instead**’ as shown below:



Complete Sign-In with Passkey Authentication

Authenticate with Passkey
Can’t use your passkey? Enter a Recovery Code instead
No access to your recovery codes? Get a temporary code via email

Enter the code in the ‘**Recovery Code**’ field. Then select the ‘**Submit**’ button, as shown below:



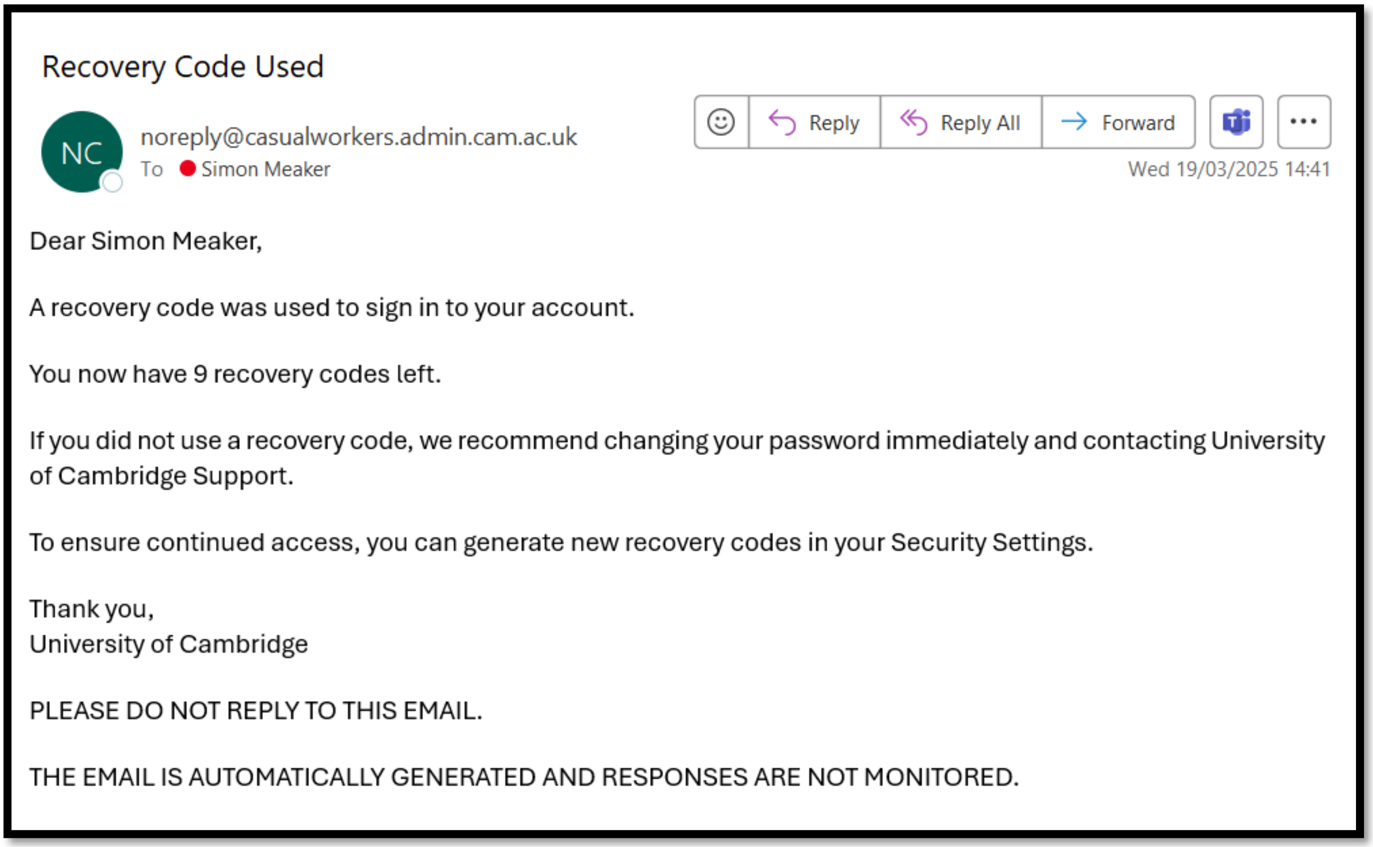
UNIVERSITY OF CAMBRIDGE

Enter Recovery Code

Recovery Code: 6DXT-GG09-ZGFE

The system will then log you into your account.

Once you have used a Recovery Code to sign into your account, you will receive a notification email informing you that '*A recovery code was used to sign into your account'*, and the number of recovery codes you have left to use.



Dear Simon Meaker,

A recovery code was used to sign in to your account.

You now have 9 recovery codes left.

If you did not use a recovery code, we recommend changing your password immediately and contacting University of Cambridge Support.

To ensure continued access, you can generate new recovery codes in your Security Settings.

Thank you,
University of Cambridge

PLEASE DO NOT REPLY TO THIS EMAIL.

THE EMAIL IS AUTOMATICALLY GENERATED AND RESPONSES ARE NOT MONITORED.

Scroll down for commonly asked questions

Common Questions

Do I have to enable Multi-Factor Authentication?

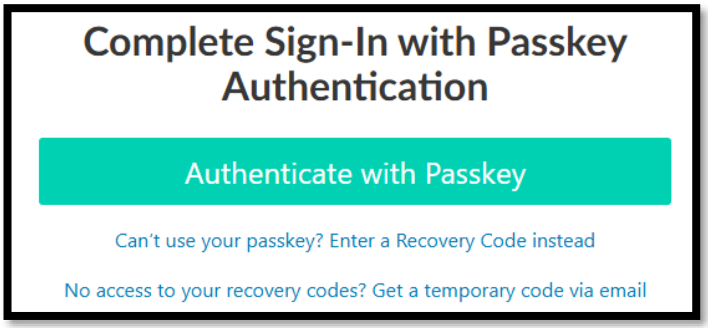
No, MFA remains **optional**. However, we **strongly recommend** enabling it for enhanced security.

Can I have multiple passkeys?

Yes, you can register multiple passkeys for different devices, but each storage location (device, password manager, or security key) can only hold one passkey per account.

What happens if I lose my passkey?

- You can use a Recovery Code to log in (please click on the 1st hyperlink to enter a recovery code instead). If you have no access to your recovery codes you can click on the 2nd hyperlink to get a temporary code via email.



Complete Sign-In with Passkey Authentication

Can't use your passkey? Enter a Recovery Code instead

No access to your recovery codes? Get a temporary code via email

- If you have no recovery codes left, please contact the CHRIS Helpdesk on CHRIS.helpdesk@admin.cam.ac.uk for further assistance.

Can I remove or replace a passkey?

Yes, you can manage passkeys via Security Settings, where you can delete or register new passkeys as needed.

Do passkeys work on shared or public devices?

No, we **do not recommend** storing passkeys on shared or public devices. Instead, you should use:

- A Recovery Code for one-time access
- An external security key for temporary authentication

What if an external security key is lost or stolen?

You should **immediately** remove it from your account via Security Settings and register a new passkey.

Do passkeys require internet access?

Yes, an internet connection is needed for the system to verify the passkey match. However, local authentication (Face ID, fingerprint, etc.) happens offline before verification.

Can I disable Multi-Factor Authentication after enabling it?

Yes, MFA can be turned off in Security Settings, though we strongly recommend keeping it enabled.

Will I still be able to use my university account for Single Sign-On?

Yes, you can still use your university account for ease of sign on and registration. The Passkey MFA implementation will ensure a greater level of security for users using email and password credentials. If you sign in with your University account you will not use MFA passkeys but will authenticate via the recognise University authentication process.

Who should I contact for help?

Please contact CHRIS.helpdesk@admin.cam.ac.uk for any issues with MFA passkeys or gaining access to CCWS.

For general queries please contact the Casual Worker HR Team at casual.workers@admin.cam.ac.uk