

You're required to set up a minimum of one authentication method in addition to your existing password and email.

Go to [GCU Identity Portal](#), enter your GCU email address ([****@caledonian.ac.uk](#)) and press next.



Sign In

 Your username (GCU domain name) _____

Next

Enter your GCU password and select email as the second authentication method.



[< Start over](#)

Authenticate to Glasgow Caledonian University

dmu13studtest@caledonian.ac.uk

 Password

Choose authentication method

Email - ***@caledonian.ac.uk

☒ Keep me signed in

[Forgot your password?](#)

Send me an email

An eight-digit code will be sent to your GCU email address, retrieve the code from your emails and press authenticate once you have entered it in the “Enter code” field.



[Start over](#)

Email sent!

dmu13studtest@caledonian.ac.uk

Email sent to ***@caledonian.ac.uk. Click the link or manually enter the code to authenticate.

Return to this app to continue.

[Enter code](#)



Authenticate



Hello dmu13Studtest@caledonian.ac.uk,

Please find your one-time authentication link or code below.

Continue with Authentication

or

Enter the following code where prompted: **95718077**

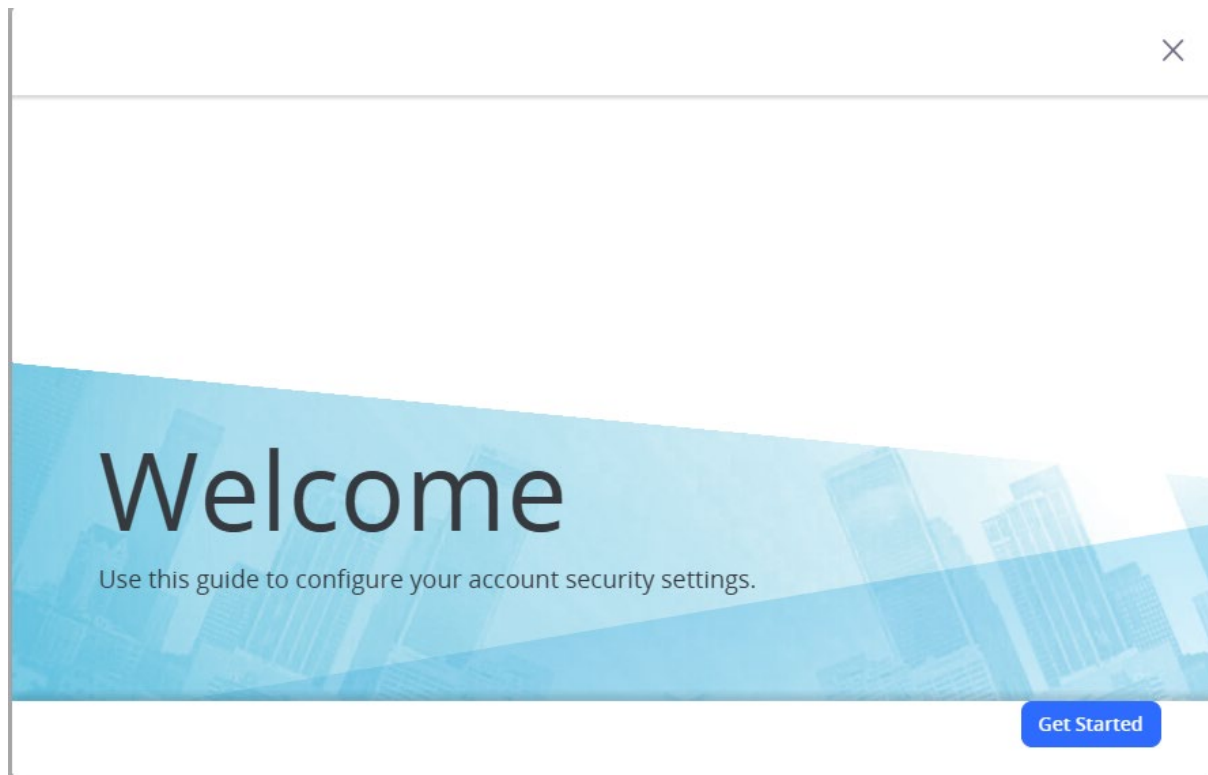
Don't Know The Sender?

You are receiving this email because you are attempting to login and authenticate your connection with GCU. If you did not initiate this process, please delete this email.

Information Services

Please do not reply directly to this mail as your response will not be received.

Once logged in you will see the below welcome message, please click “Get Started”
(You may see a different pop-up box please close this which should then take you to the welcome banner)



As we are moving to the Microsoft Authenticator application, we recommend that you set up the Third-Party Authenticator App and link it to the Microsoft Authenticator application.

✕

Authentication Setup

Welcome to the User Portal. Before we get started, please set up 1 or more mechanisms for Multi-factor Authentication. Multi-factor Authentication may be required when you sign in to the user portal or an application from the user portal.

☒ **Text Message**
Configured

☒ **Third Party Authenticator App**
Configured

☐ **Mobile Device**
Pending

1. Install your 3rd party authenticator app.
2. Launch your authenticator app and tap the "+" icon or the "Add Account" button to add a new account.
3. Select "Scan Barcode" or "Scan QR Code" and use your phone's camera to scan this code:
4. Once you have scanned the code, enter the 6-digit verification code generated by the authenticator app and click verify.

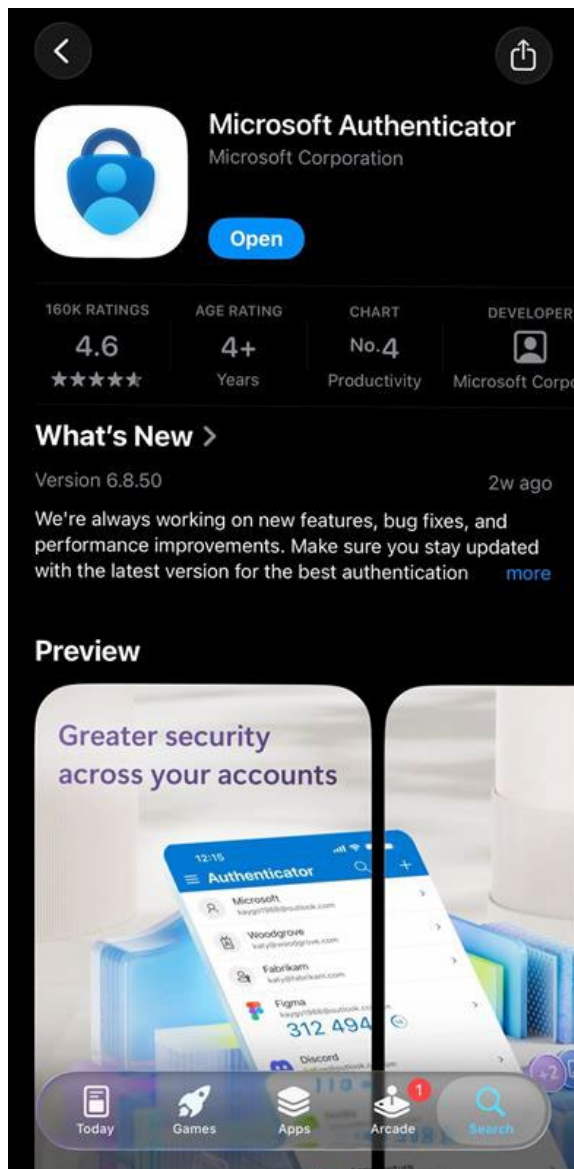
Code

Verify

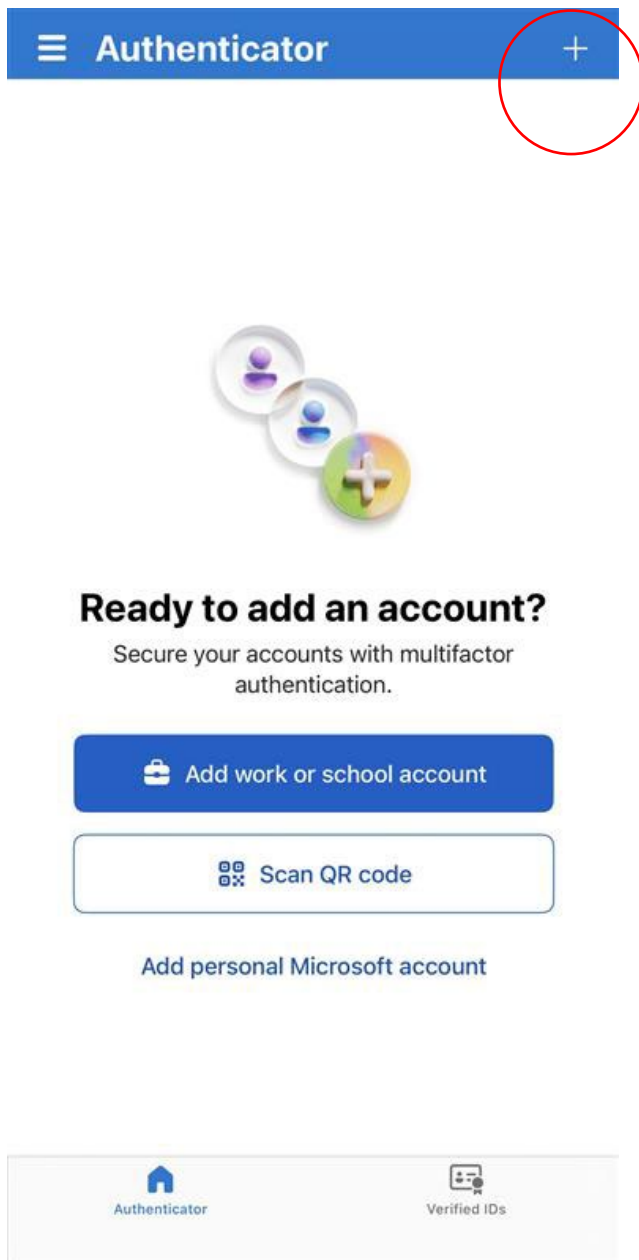
2 of 1 required mechanisms configured

Done

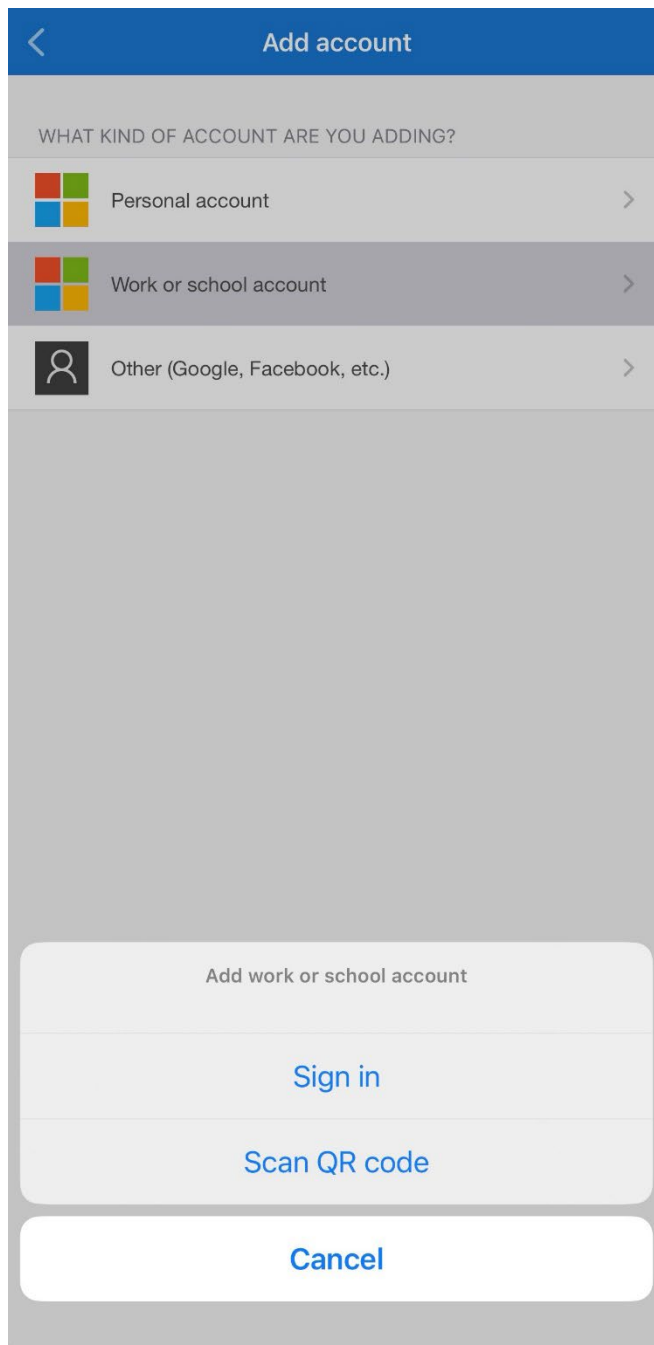
Install the Microsoft Authenticator app via the app store on your mobile phone. If you already have the application installed go to the next step.



Open the Microsoft Authenticator application and click the plus sign at the top right of the screen.



Select “Work or school account” and then “Scan QR code”



Return to the CyberArk portal and scan the QR code provided for Third Party Authenticator. Once paired you will be provided with a code on the Microsoft Authenticator application, enter this code into the CyberArk portal and click “Verify”. You have now successfully set up CyberArk MFA within the Microsoft Authenticator.