

Setting up multi-factor authentication (MFA) using GCU MFA

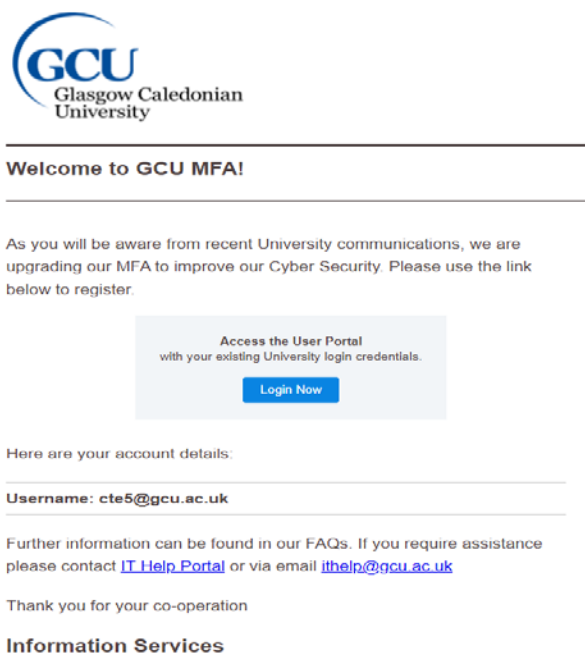
The University is upgrading our MFA to a new platform, GCU MFA, for a much-improved defence against cyber threats.

All staff with systems access must register on the GCU MFA system by Friday, August 23, and either download the app to a smartphone or set up SMS text verification.

New members of staff will need to register for both PingID and GCU MFA. [Follow the instructions for PingID here.](#)

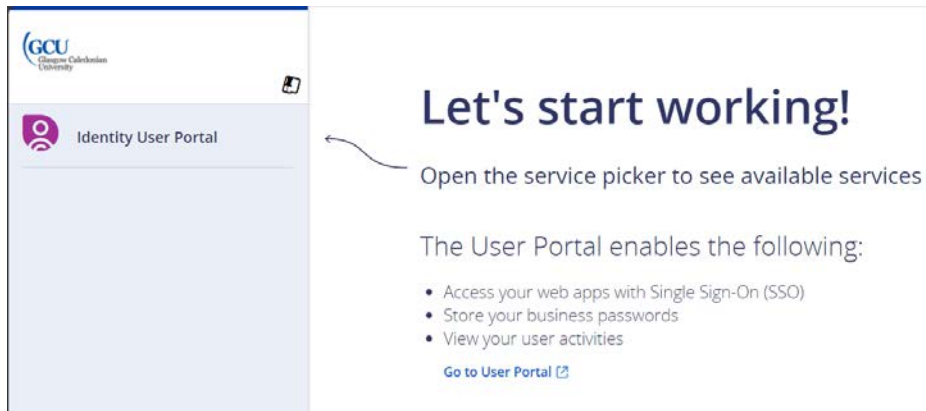
How to register for GCU MFA

You will receive the following email from GCU MFA in your University mailbox inviting you to register with the platform:



:

- Click on 'Login Now' and use the username outlined in the email
- Insert your University email password and follow the instructions on the screen to help you verify your account
 - If you select email verification, a one-time passcode (OTP) consisting of eight digits will be sent to your mailbox
 - If you select SMS verification, the OTP will be sent to you via a text message from CyberArk
- Once your account has been verified, click on 'Go to User Portal' then click on 'Get Started' in the subsequent pop up (see images below)



The screenshot shows the top part of the Identity User Portal. At the top left is the GCU logo (GCU College of Education University). Below it is the 'Identity User Portal' header with a circular icon. A callout box with an arrow points to the header area.

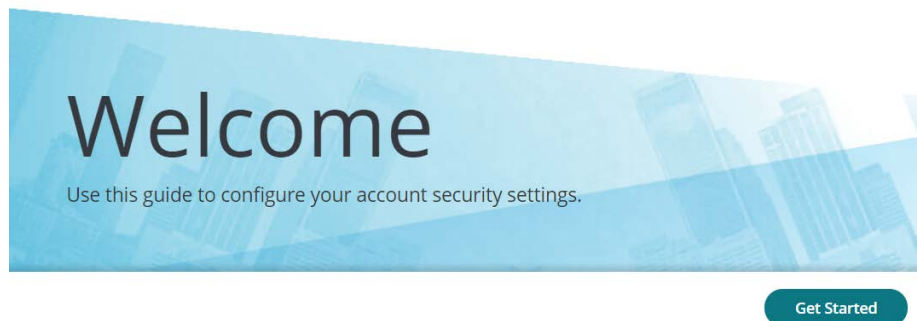
Let's start working!

Open the service picker to see available services

The User Portal enables the following:

- Access your web apps with Single Sign-On (SSO)
- Store your business passwords
- View your user activities

[Go to User Portal](#)



Welcome

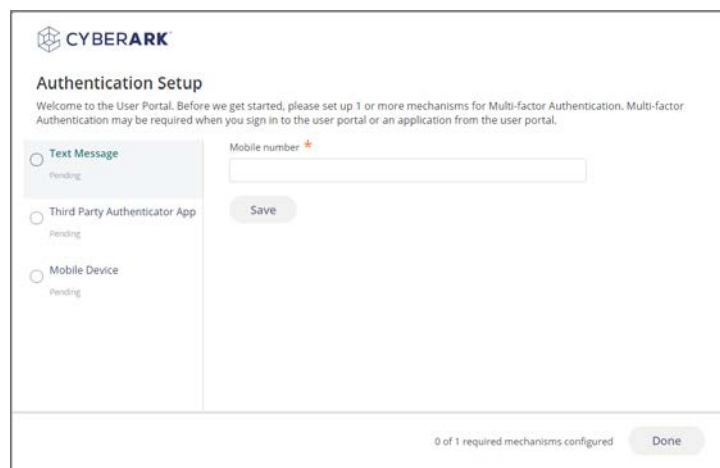
Use this guide to configure your account security settings.

[Get Started](#)

You will then need to set up at least one of the three mechanisms for MFA with your account:

1. SMS text message
2. Third party authenticator app
3. Mobile device

1. SMS text message



CYBERARK

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
Pending

Third Party Authenticator App
Pending

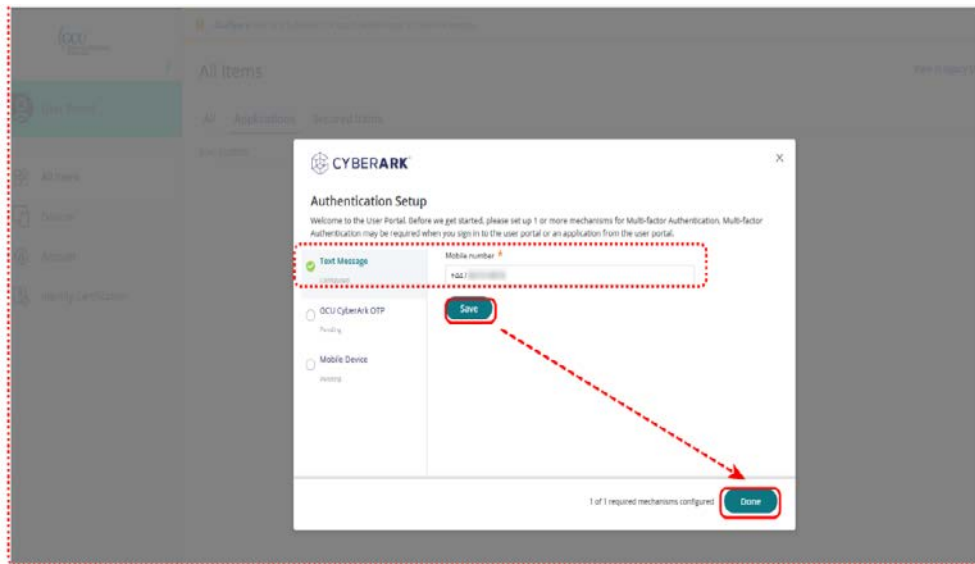
Mobile Device
Pending

Mobile number ^{*}

[Save](#)

0 of 1 required mechanisms configured [Done](#)

- Click on 'Test message' on the left-hand side menu
- Your mobile number may be pre-populated based on the information the University has on our directory.
- Click on 'Done' if your mobile number is pre-populated and is correct
- Change/add your mobile number if it is incorrect or blank. Please you start your number with the country code i.e. +44. Then click on "Save" then "Done" when complete.



2. Third party authenticator app (e.g. Microsoft Authenticator App)

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
Pending

Third Party Authenticator App
Pending

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

0 of 1 required mechanisms configured
Done

- Click on 'Third party authenticator app' on the left-hand side menu
- Install your third party authenticator app
- Launch your authenticator app and tap the '+' icon or 'Add account' button to add a new account
- Select 'Scan barcode' or 'Scan QR code' and use your phone's camera to scan the QR code on the screen
- Once you have scanned the code, enter the six-digit verification code generated by the authenticator app and click 'Verify'

3. Mobile device (i.e. CyberArk app)

CYBERARK

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.

Choose an option below to enroll your iOS or Android device.
[Privacy Policy](#)

Text Message
 Pending

Third Party Authenticator App
 Pending

Mobile Device
 Pending

Send enrollment link via:

SMS ⓘ

Email ⓘ

Scan QR code:

0 of 1 required mechanisms configured

- Click on 'Mobile device on the left-hand side menu
- Enter your mobile number or email address, or scan the QR code to be taken to your app store, where you can download the CyberArk Identity app
- Once downloaded, either log in with your University credentials or click on the 'Enrol with QR' feature to register your mobile device.



Sign In

 Your username (user@domain)

Next

If you know your organization's tenant,
[click here](#)

© 2024 CyberArk Software Ltd.
[Terms of Use](#) [Privacy Policy](#)

 Settings  Enroll with QR

- Follow the instructions as per the app to complete the device registration.

Once you have finished setting up one or more factors of authentication, you will see a link to take you to the Caledonian Connected homepage or you can close the portal.

