Setting up your account

Welcome

Welcome to UHI! The guide below will help you log in for the first time and set up your UHI account.

When you join us at UHI, we will issue you with a username. We refer to this as your student or staff ID and it is usually in a format ending '@uhi.ac.uk'. We will also give you a temporary password.

Your security is important to us

The first step is to set up Multi Factor Authentication (MFA). This is needed to keep everyone at UHI safe whilst using our systems.

Our guidance is focused on setting you up with the Microsoft Authenticator App, as this is one of the most reliable and secure method for accessing your account. It is worth noting that there are many authenticator apps, so you are not restricted to using Microsoft's.

If you do not have access to a smart phone, please speak with the UHI ServiceDesk either on Live Chat or by emailing on servicedesk@uhi.ac.uk. Alternatively, your local ICT support team is also on hand to provide assistance with authentication methods.

Staff should discuss any issues with their Line Managers in the first instance.

You can link to the app by scanning the QR codes or by clicking the link above.

Google Play

App Store

Setting up your account

Initial log in

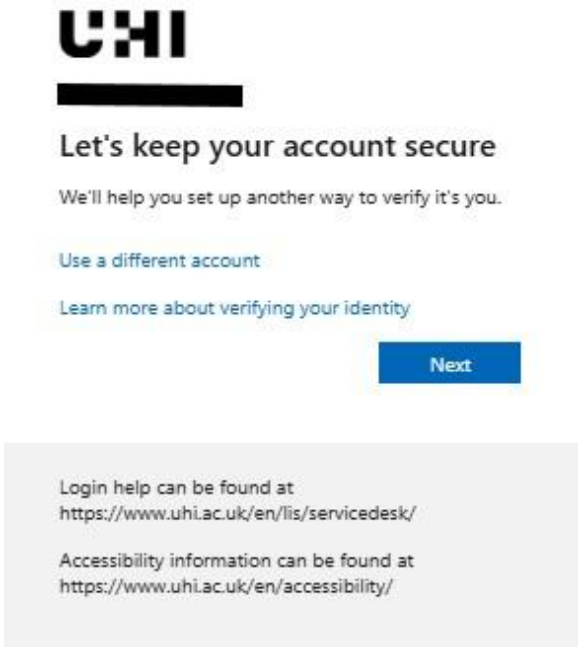
Please make sure you have these things ready:

- Your Smartphone with the Microsoft Authenticator App (or alternative) installed.
- Ideally a laptop/computer/tablet to login to your Student Account.
- Your student or Staff ID.
- Your temporary password.

Please follow the step-by-step actions below on what to do to set up your MFA.

On your Laptop/Computer/Tablet:

- Go to Outlook.com or www.studentjourney.uhi.ac.uk and login with your ID ending '@uhi.ac.uk' (e.g. 123456@uhi.ac.uk) and use your password you have been given.
- After you have successfully inputted your password, you will be presented with a prompt stating, 'Let's keep your account secure'.

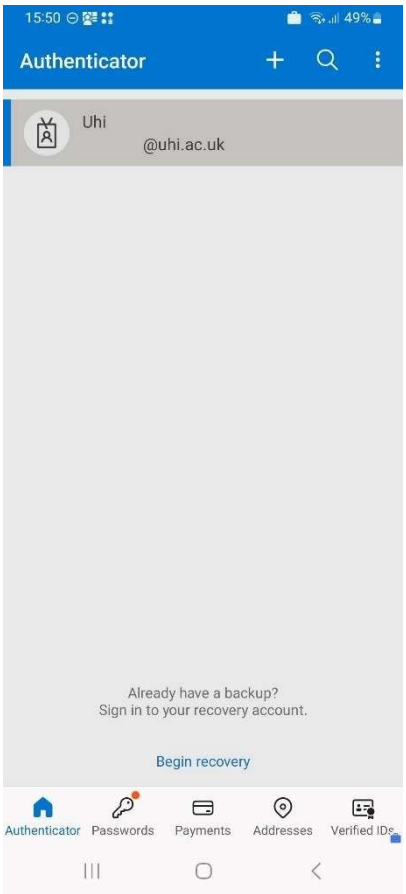


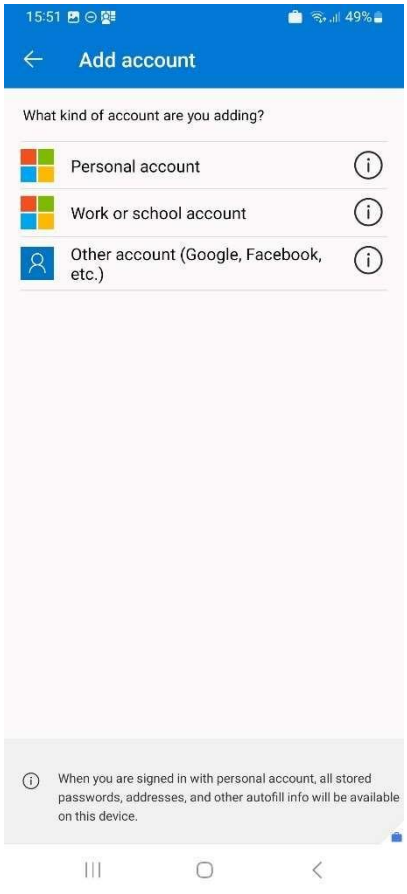
- At this point, it is recommended to pause and go to your smartphone and start/download the Microsoft Authenticator App.

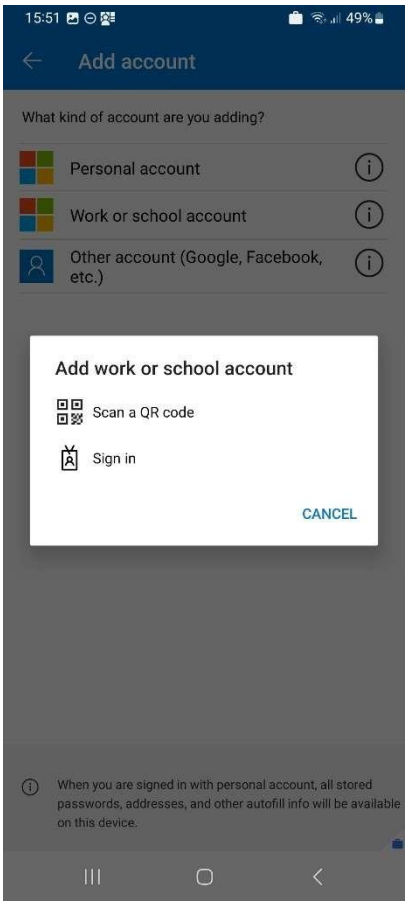
On your Smartphone:

Setting up your account

- Open the Microsoft Authenticator App o The App will default to using the same security you use to unlock your smartphone, so you may get asked to enter a PIN, Passcode, Biometrics (Face or Fingerprint recognition) etc. o You may be asked to sign in with a Microsoft account, this can be ignored.
- Select, either the '+'icon, or 'Add a work or school account'.
    - o If you must select the '+' icon, do this first then select 'Work or school account'.
- You will be given the options to 'Scan a QR Code' or to 'Sign in'.







At this point, do not select anything, and place your smartphone to the side.

<u>On your Laptop/Computer/Tablet:</u>

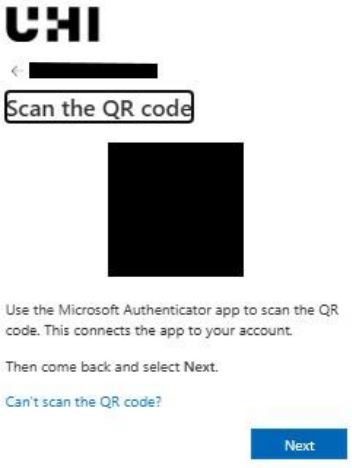
Setting up your account

- Continue by selecting ‘Next’ on each prompt.





- You should eventually reach a single QR code as shown below.



- At this point, use your phone, and Select ‘Scan a QR Code’ from your options.

- Your camera should activate.
    - You may get asked to allow access to the camera, select Yes.
- Scan the QR code on your laptop/computer/tablet screen.
- If you do not receive and error, select 'Next'.
- You will be asked to try the process has worked.
- You will then be sent a notification through your app.
- There will be a number on your computer/laptop/tablet screen.
- You will need to enter this on your phone when prompted.
- Select yes and then you will be asked to unlock your phone if you have a lock set up.

Once you have set up your MFA method, you will then be asked to change your password. When you do this, please take note of the following criteria:

- Your password MUST be at least 8 characters long.
- Your password MUST have at least 1 upper case letter. • Your password MUST have at least 1 lower case letter.
- Your password MUST have at least 1 number.

You can find more information about the Microsoft Authenticator App on their website at www.microsoft.com.