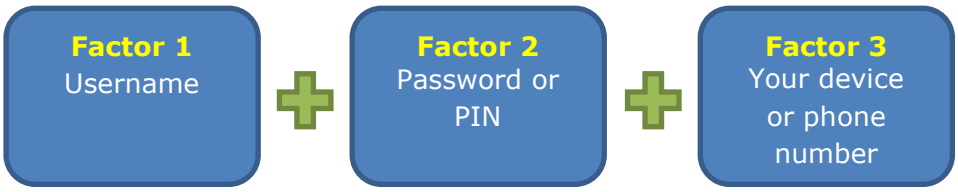
# Multi-Factor Authentication (MFA)

## What is MFA?

Multi Factor Authentication pairs your University password with an additional form of security, this could be an app on your smartphone, a phone call, or a text message (these are known as **Factors**). You are probably already using this system to login to things like online banking, so that your bank can be sure it is you.



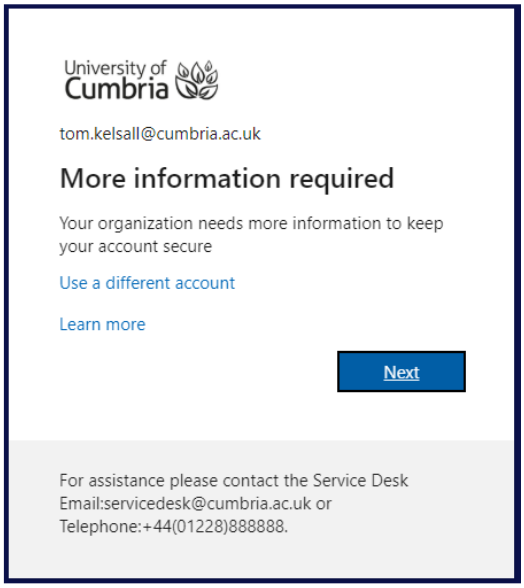

MFA is used when you login to university systems on your own device or when away from campus.

Before you can use MFA you will need to sign up to the service and choose your additional factor(s). The use of MFA is mandatory for you to access university systems and will also allow you to reset your university password whenever you like.

## Register for MFA

### 1. More information required

When you first try to login to any of the university systems (Student Hub, Blackboard, Email, StaffHub, etc.) you will receive a prompt that asks you to provide more information before you can access your account.

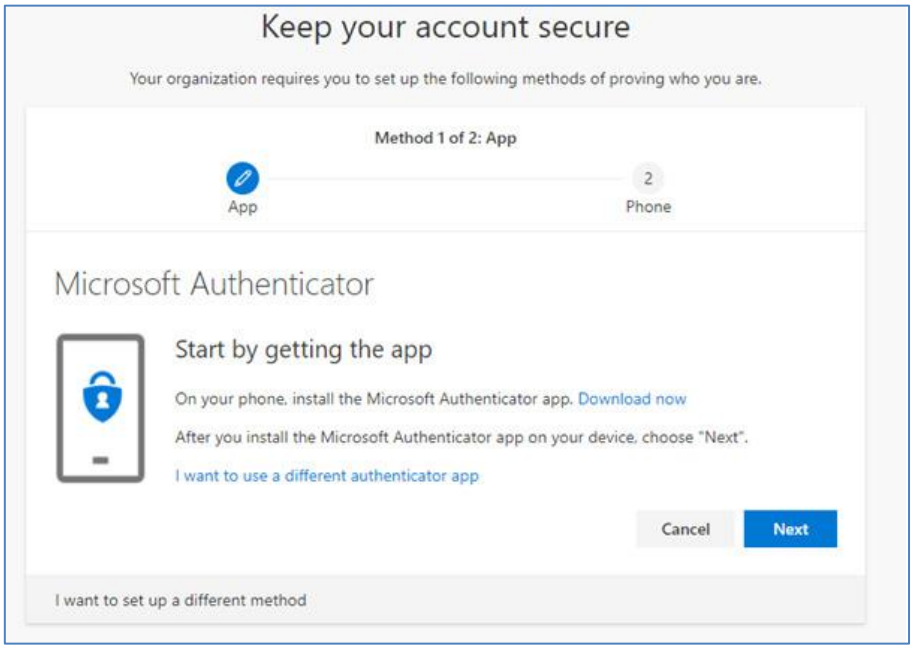



Check that your university email address is displayed correctly and click **Next**.

## 2. Keep your account secure – Install the Authenticator App

You will now see the start of the **Keep your account secure** wizard.

You are prompted to download the **Microsoft Authenticator** app onto a smartphone (Staff: this can your own phone or a work phone) which is used to send you an authentication code whenever you attempt to login to your account. You will then need this mobile device with you whenever you login to your account off campus.




There is a ***Download now*** link on the page, but you may want to open your iPhone or Android app store and search for **Microsoft Authenticator** (provided by Microsoft Corporation) of scan one of the following codes:

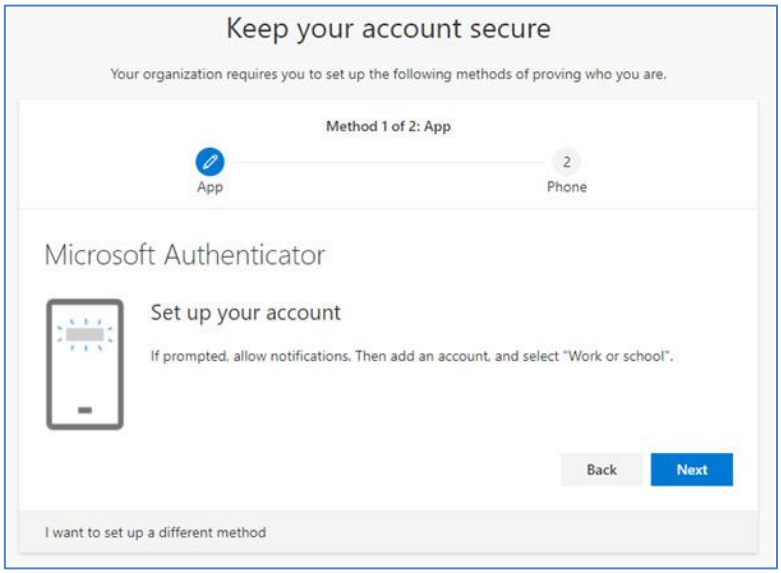
| **Microsoft Authenticator app - Android** | **Microsoft Authenticator app - iPhone** |
|---|---|
| | |

Additional information about downloading and installing the Microsoft Authenticator app is available here if required: Download and install information

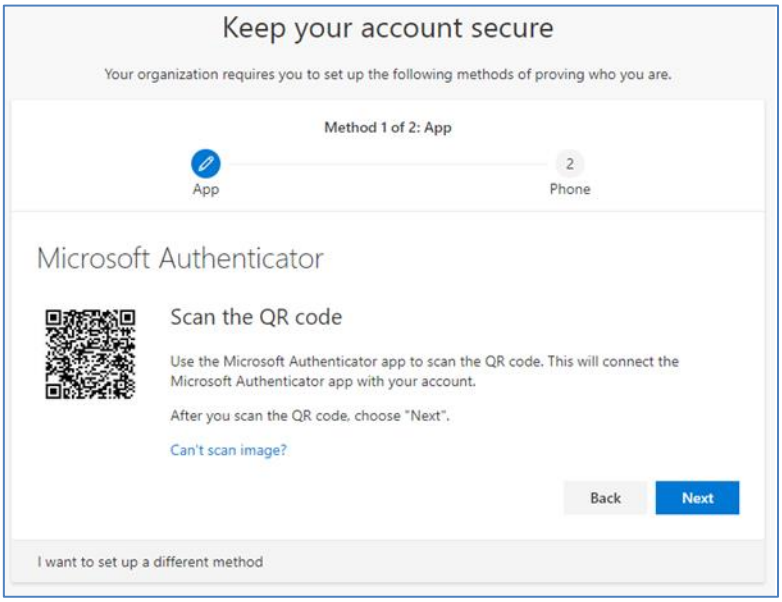
When you have installed the Microsoft Authenticator app on your device, return to the "Keep your account secure" wizard and click **Next**.

## 3. Keep your account secure – Connect the Authenticator App

Now you need to add your university account to the Authenticator app on your mobile device. You can click **Next** on this following screen:

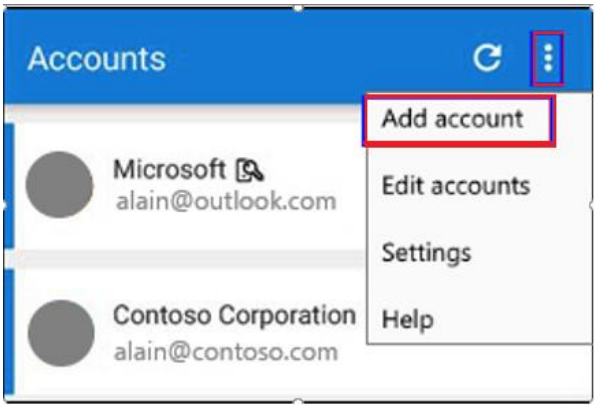



The **Keep your account secure** page should now display a QR code that will help to connect to your account.

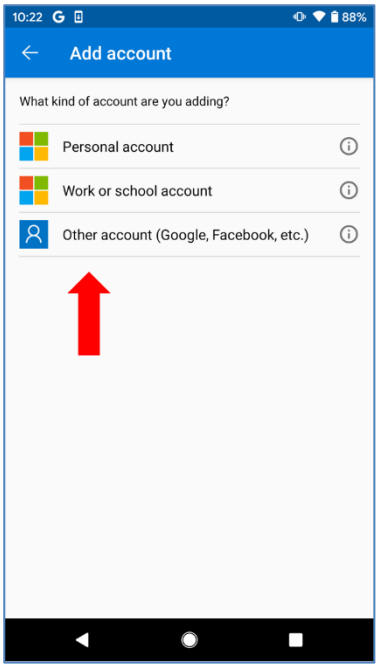


**Open the Microsoft Authenticator app on your phone**:

a. Allow notifications (if prompted)
b. Allow the app to access your camera (if prompted)
c. Allow the app to access storage (if prompted)
d. Select to **Add your first account** on the opening screen
e. Or click on the Menu button (top right) to choose to **Add account**.




f. Choose to add **Work or school account**
g. You will then have the option to **scan the QR code** (from the "Keep your account secure" page) or to manually add your University of Cumbria login. The QR code is quicker and easier.

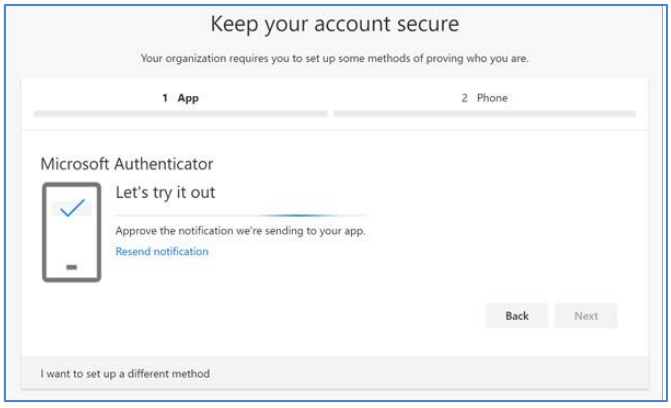



**The Authenticator app should have successfully added your university account without any additional information from you.**

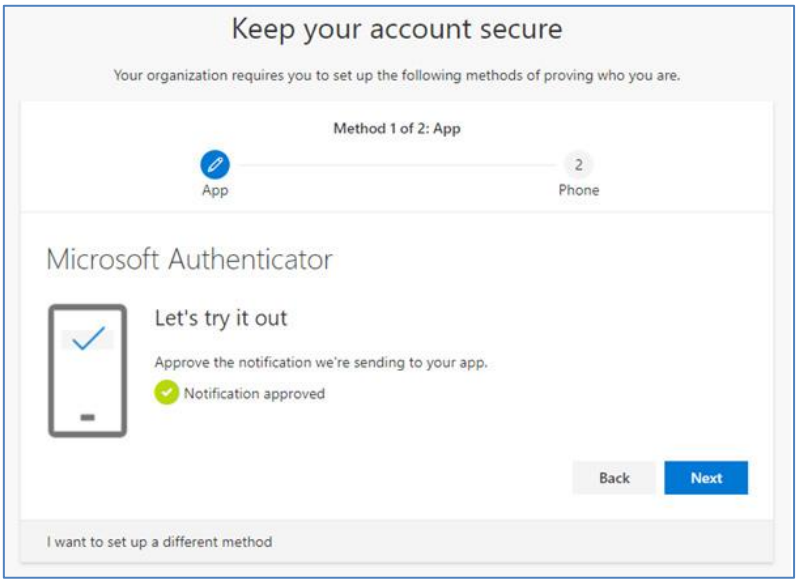
If there is a problem reading the QR code or another error, please close the Authenticator app and try again or you can choose the **Can't scan image** option on the "Keep your account secure" webpage. You will then be presented with some information and a code to enter manually into the app.

## 4. Keep your account secure – Test the connection

The "Keep your account secure" page will now send a test notification to the Authenticator app.



When you accept the notification on your phone, the webpage should change to confirm that you have approved it.




You can click on **Next** to confirm everything. MFA is now setup for you to use.

## Using MFA with the Microsoft Authenticator App

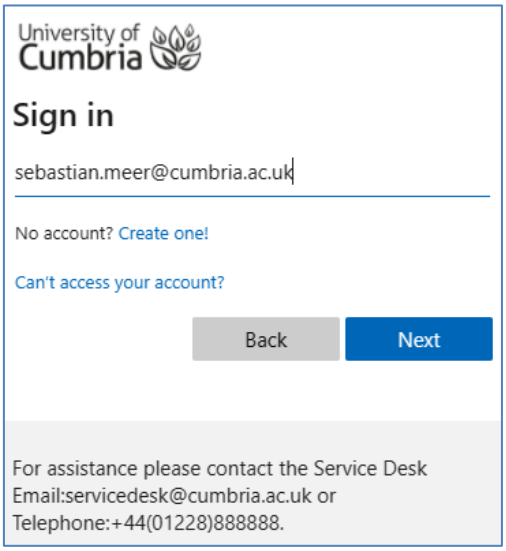
Whenever you try to login to one of our systems (on your own device or off campus) you will usually complete this action through three screens:

### 1. Username screen

The first screen will ask for your username which is your university email address.

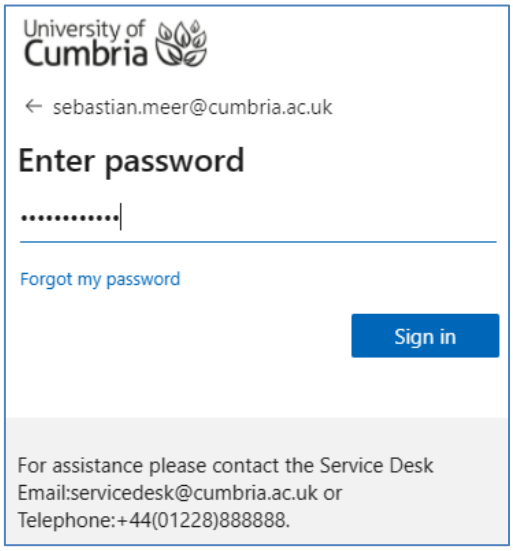
**Students**: s**0000000**@uni.cumbria.ac.uk (where "0000000" is your student number)

**Staff**: firstname.lastname@cumbria.ac.uk



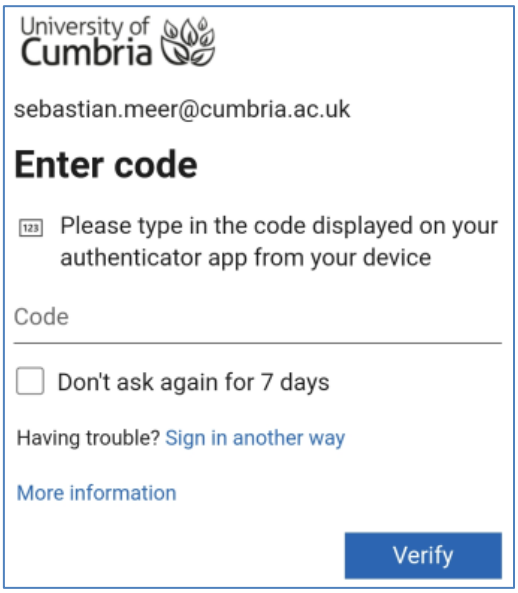
## 2. Password screen

The second screen needs your University of Cumbria password.

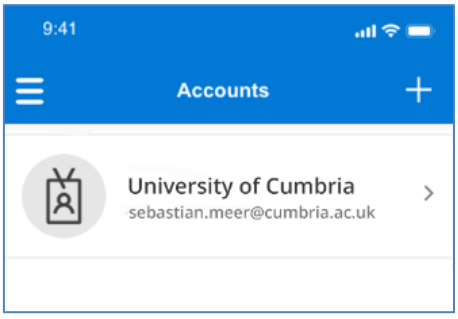



## 3. MFA screen

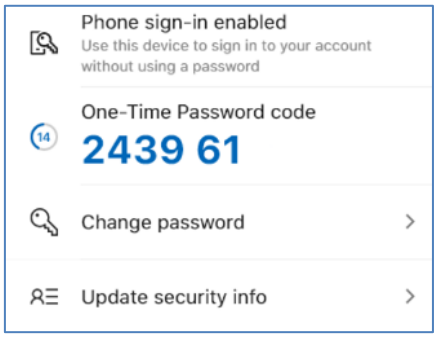
The third screen wants you to confirm your identity using MFA.



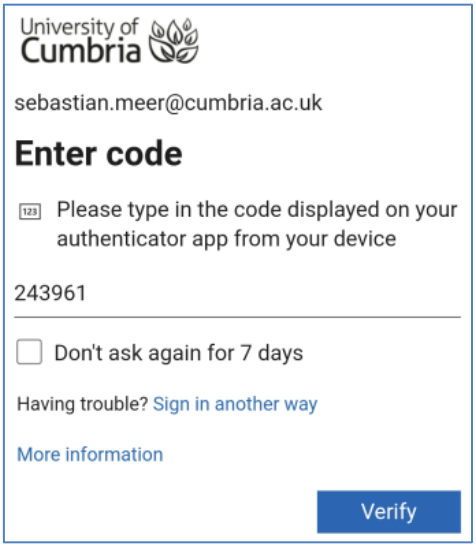

You will need to open the Microsoft Authenticator app and **select** your **University of Cumbria** account:



The screen in the authenticator app will change to present you with a 6-digit code.




In the **Enter Code** section of the system you are trying to access – type in the code shown in the app:




Hit Verify and you should be logged into the system you are trying to access.

**Please note:** The Microsoft Authenticator app automatically generates a new code every 30 seconds. If you do not use the code before it expires, you will need to use the app to get a new code.

Every 180 days you will be asked to check all your information is still current.