Changing mobile device with the Authenticator App

This guide is for staff and students.

This guide details how to change mobile devices, when using the Microsoft Authenticator app to authenticate to UEA services, such as Microsoft Office (Word, Excel, etc), Teams and the My.UEA website, as well as University systems such as Blackboard.

If you no longer have access to your device, in that is lost, stolen, or broken then please contact the IT Service Desk who can help you. They will need to unregister the device at Microsoft, so that prompts are no longer sent to that device https://www.uea.ac.uk/itsupport

Before you start

- You will need your current device
- You will need your new device, ready to add the app
- Access to a laptop or desktop
- We do advise that you **read through the guidance** before starting as the Microsoft set-up process is designed to **time out** after a few minutes. The guided process will be clear on screen.
- The phone icon shown below appears when you need to use your **mobile device** and the computer icon show below appears when you need to use your **desktop or laptop**.

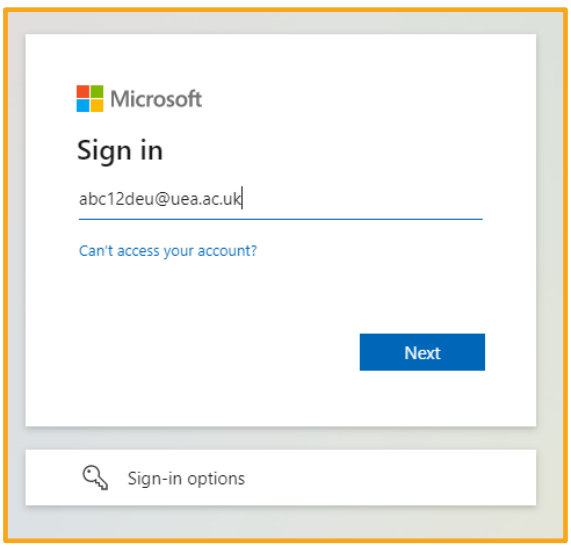
Remove your current device for authentication

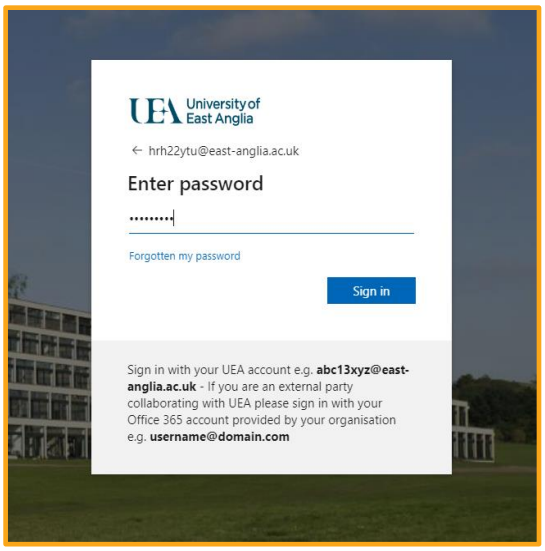
For security reasons, you will need to remove your old phone as an authentication method and to prevent authentication prompts being sent to your old device.

To do this go to https://mysignins.microsoft.com/security-info

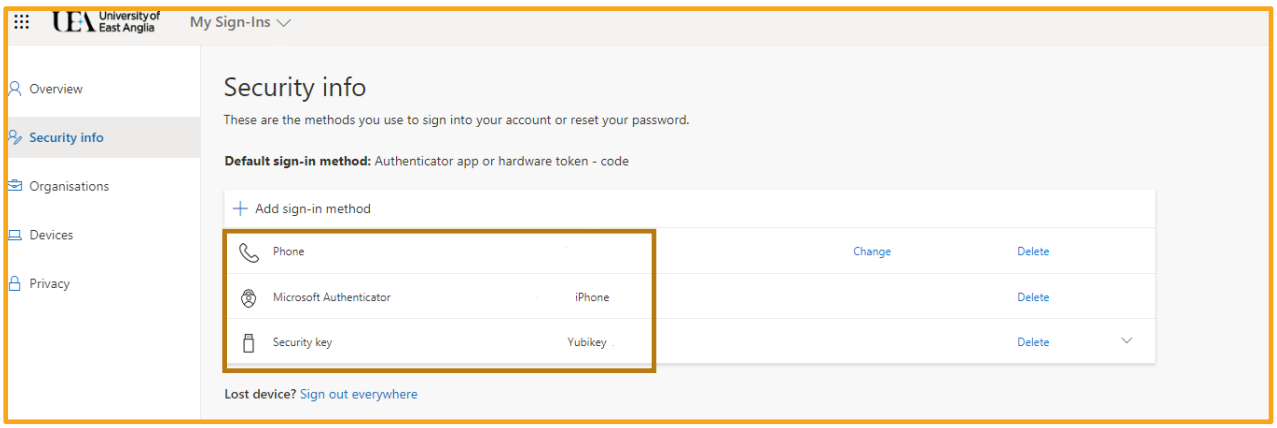
When asked to **Sign in** enter your UEA email address in the format abc12deu@uea.ac.uk and then **Enter password** and click on **Sign in**

If you are already signed into your account, you may not see these screens.

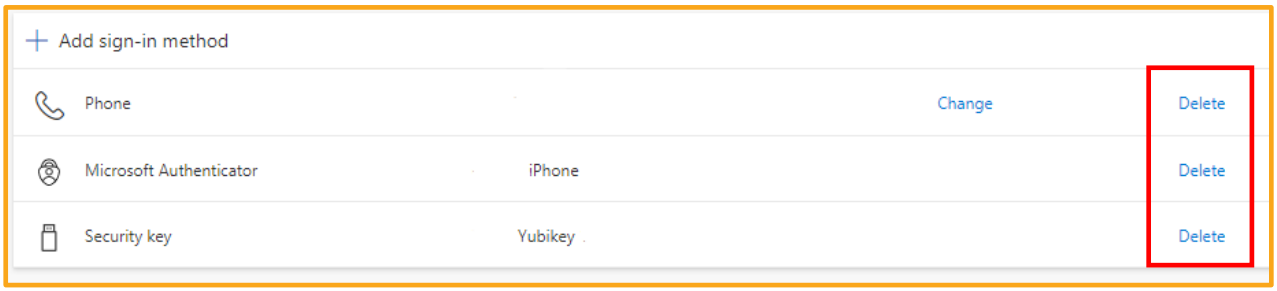




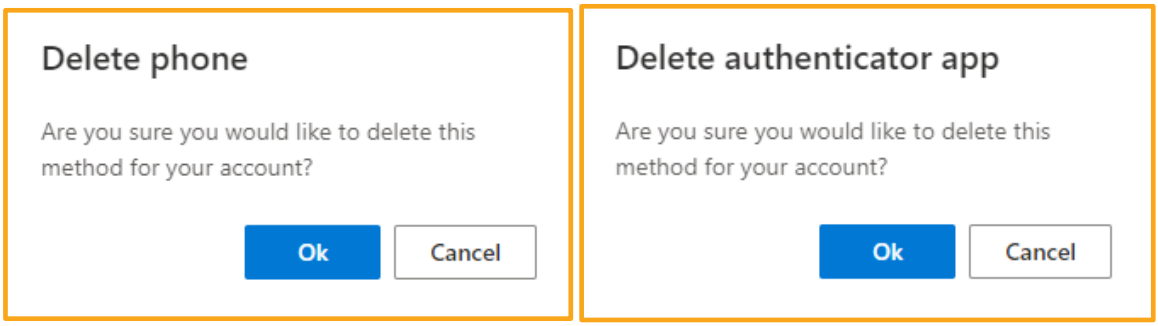
You will see a screen which shows the methods you have set up to authenticate.



Find the device you wish to remove, and the click on the **delete** link.

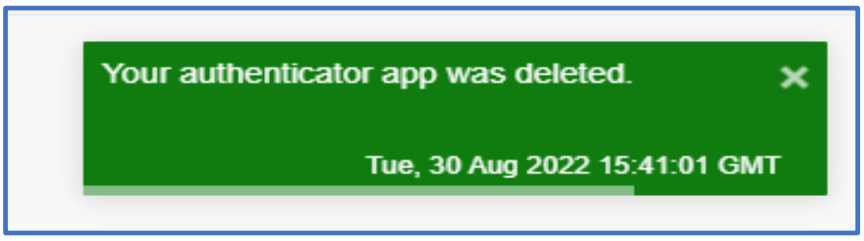


You will see a warning message, based on the option you are removing. Phone indicates that you have set up SMS and Microsoft Authenticator indicates that you have set up the app, on your phone or other device. **You may not see all methods above showing on your screen.**



Click on **Ok** to go ahead and delete the method.

Once this has been deleted, your device will no longer show as an authentication method, and a green box will appear in the top right-hand corner of the screen.

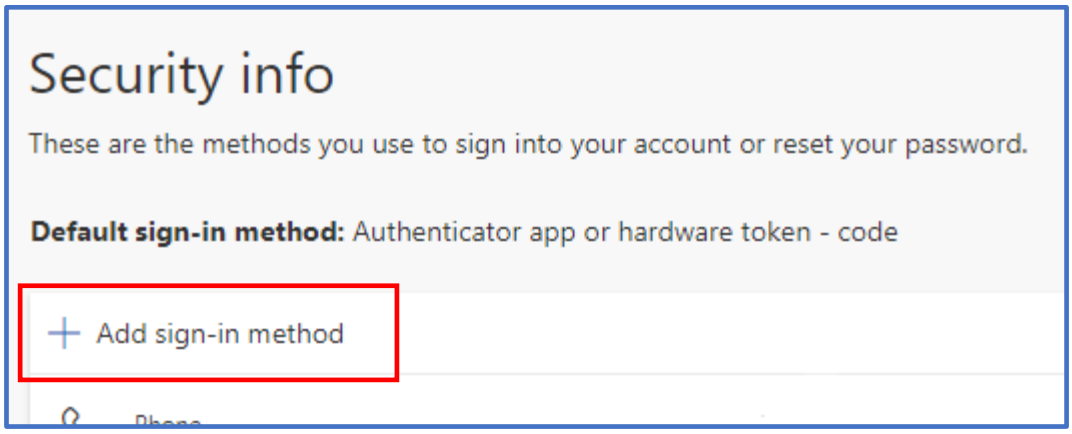


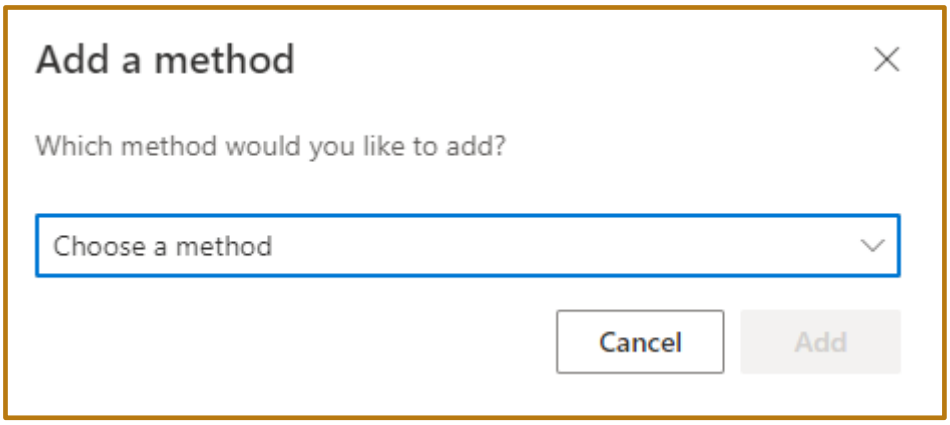
At this point you should delete the app from your old device.

Register your new device

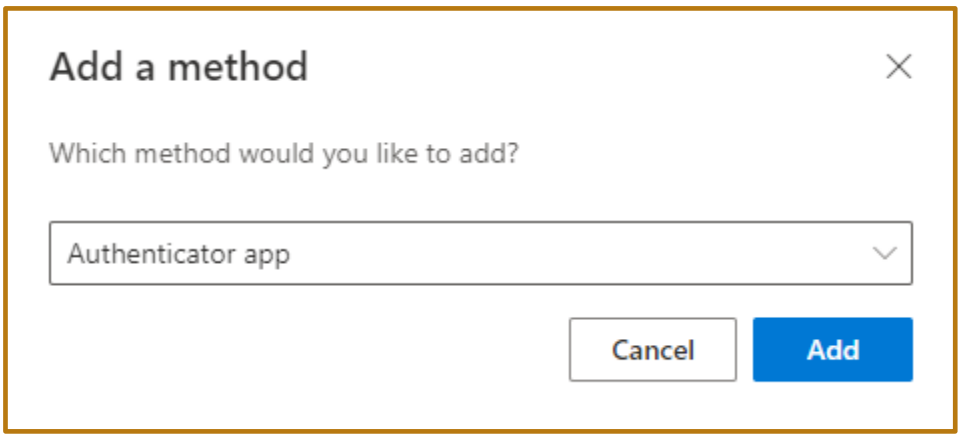
From the same screen, you can now add your new device.

Click on **Add sign-in method**

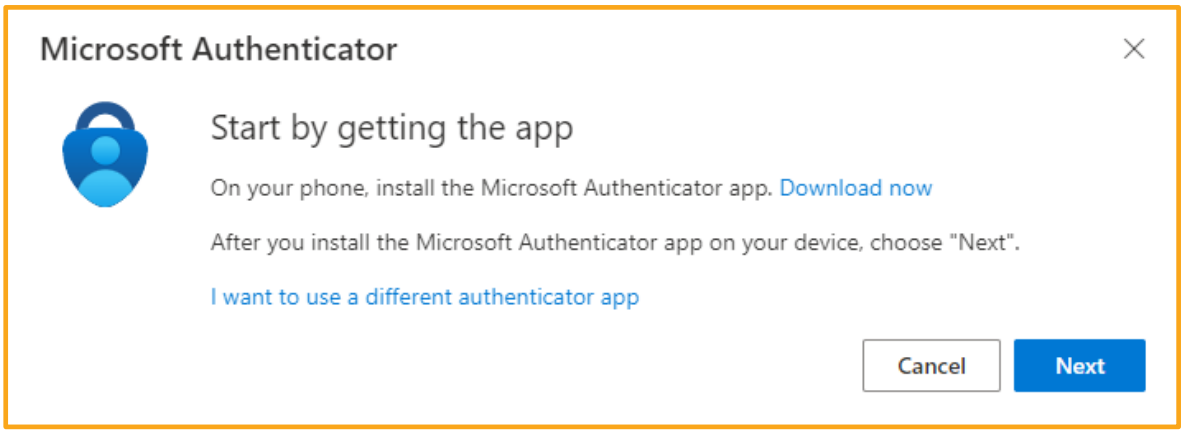




From the drop-down list, choose **Authenticator app** and click **Add.**



It will now ask you download authenticator App to your mobile device. Click **Next.**



If you have not downloaded the app on your new device, please follow the instructions below.

Download the Microsoft Authenticator App onto your new device

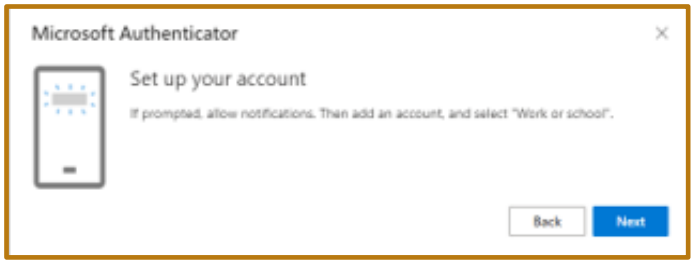
The Authenticator app is free and UEA will not have any access to the data you provide. You can use the app for any personal accounts you may have, which require authentication. MFA is becoming more common, with services such as banks, social media, like Facebook and shopping apps such as Amazon.

- Download the app from the **Google Play Store** if you have an **Android** device
- Download the app from the **iOS App Store** if you have an **Apple** device

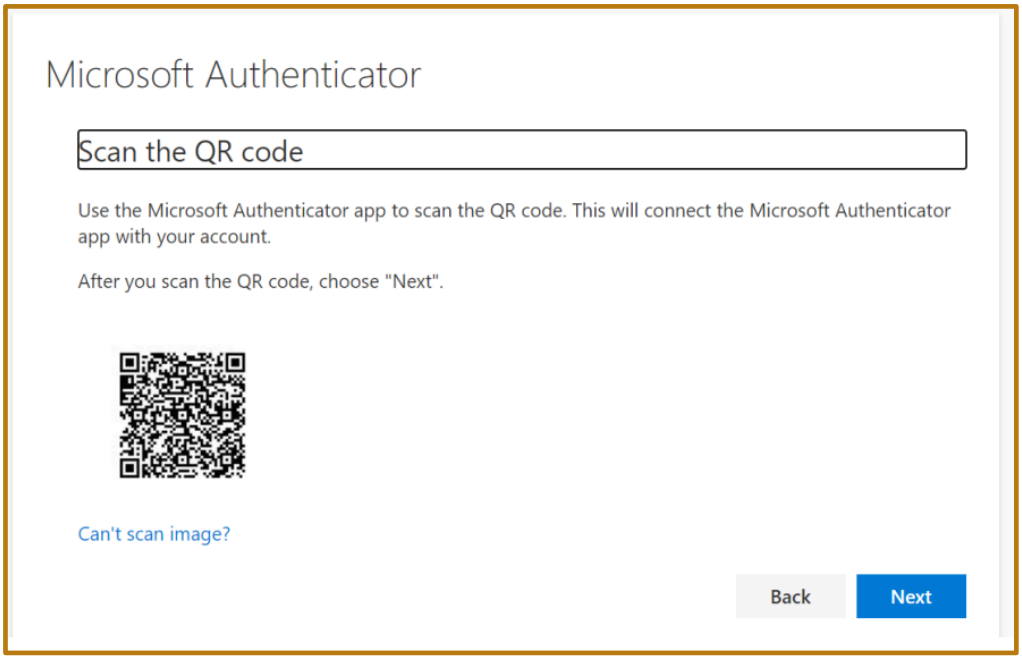
The app uses this logo

The Microsoft Authenticator can receive notifications both over mobile and Wi-Fi connections. In addition, the mobile app can generate verification codes even when the device has no signal at all.

Once the app is downloaded, click on **Next** on your laptop or desktop and you will be asked to **Set up your account**

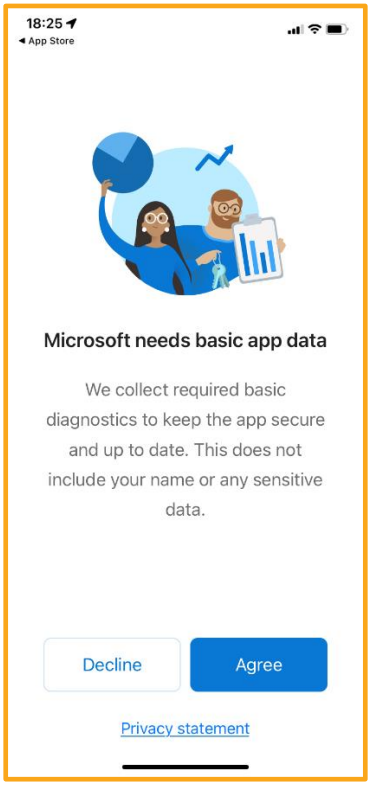


You will now see a **QR Code** on screen.



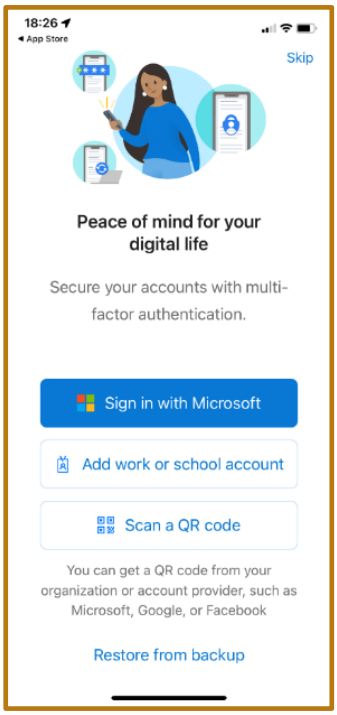
Open the Authenticator app on your phone.

It will display a screen relating to gathering basic app data. You will need to click on **Agree** to move forward.

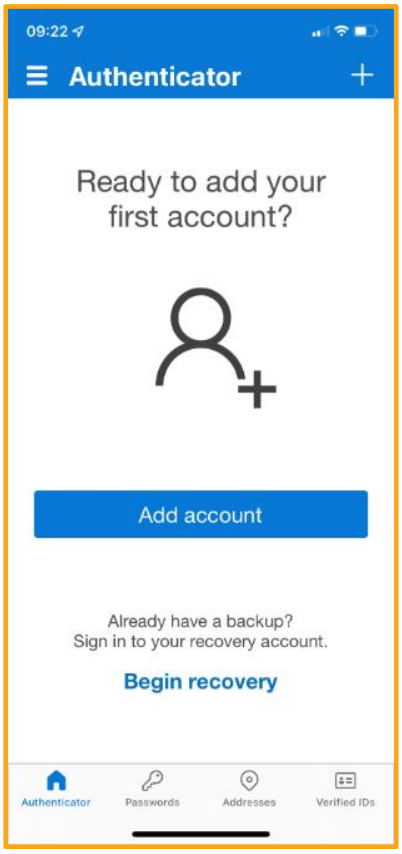


On this page, there is a link to the Microsoft **Privacy statement**.

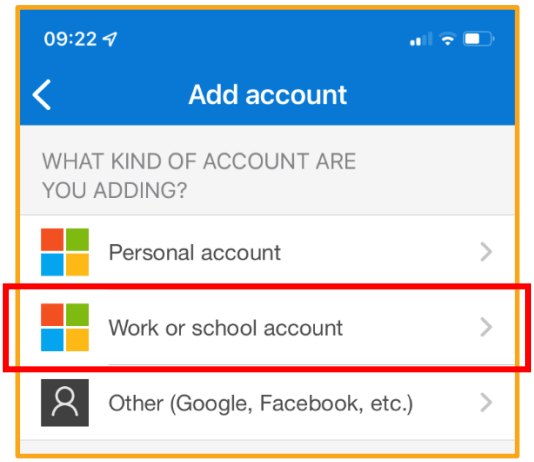
On the next screen tap on **Add work or school account.**



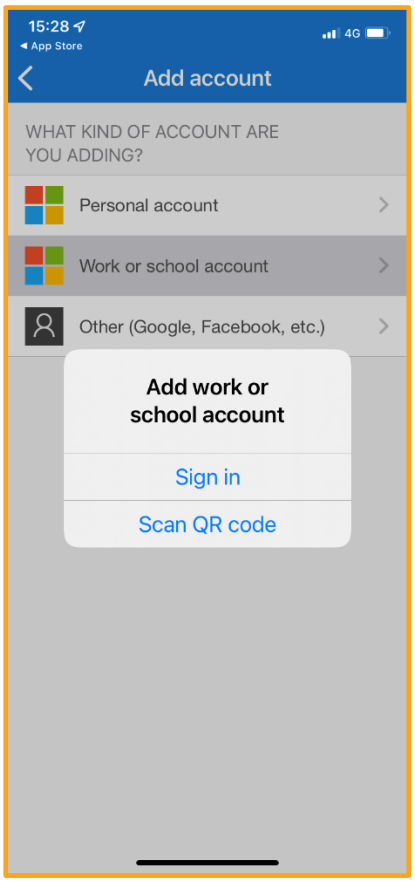
And then, **Add account** on the next screen



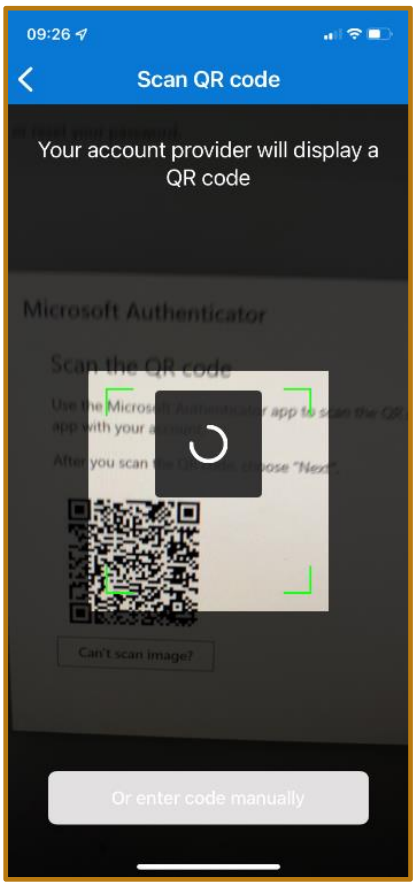
Tap on **Work or school account** on the next screen.



The box shown below will appear on screen. Tap on **Scan QR code** to open your camera. You may be asked to give permission to access your camera.

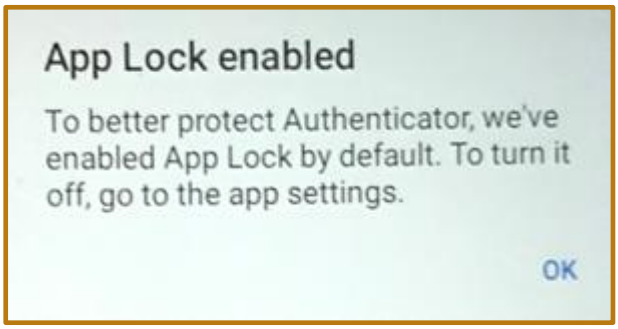


The camera will open to scan the **QR code**. Position your phone so that the **QR code** is in view and the phone will pick it up automatically.



You may see a message about **App Lock enabled**, if you have that setting on your phone.

This means you will need to unlock the app, with the same method you unlock your phone e.g., code, face ID or fingerprint ID.

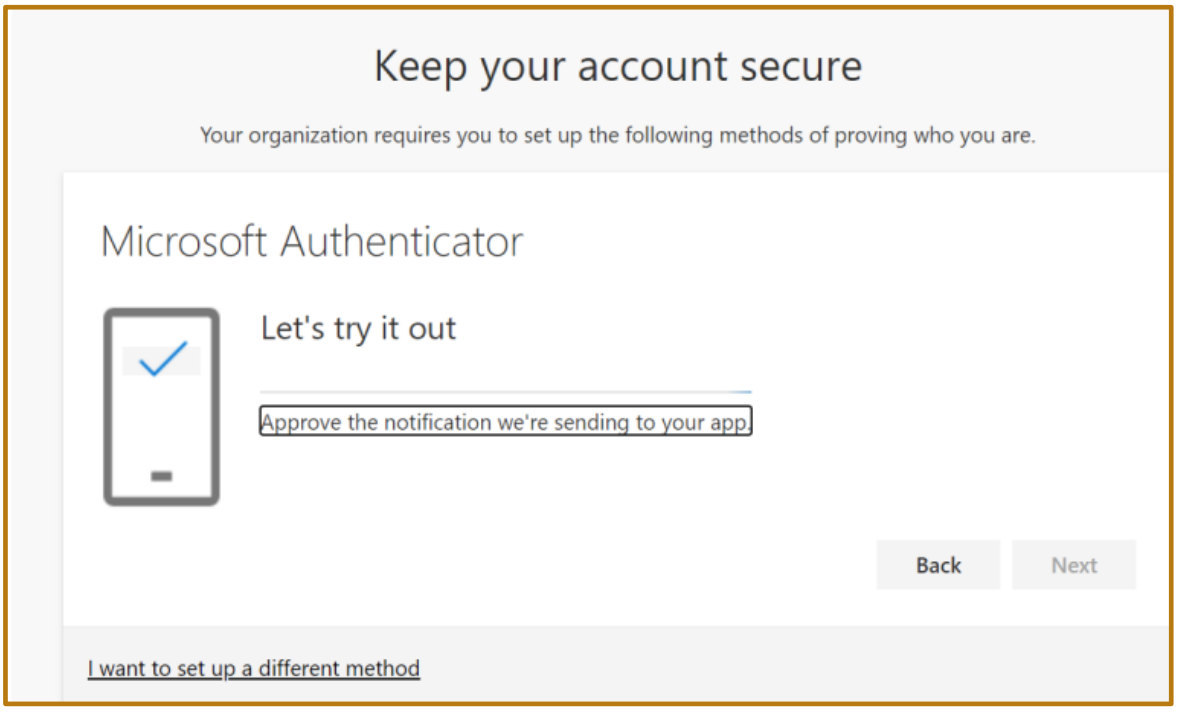


This can be turned off in the app, if needed.

Now that you have scanned the QR code, go back to your ***laptop or desktop device.***

Click **Next** on the screen.

You will now be prompted for your first MFA approval at UEA.



On your mobile device within the **Authenticator app,** you will receive a prompt. Tap on **Approve**. Any future MFA notifications will look like this)

Any future MFA notifications may look like this, or you may have to enter a code.

Once approved on your device, you will get a message on your laptop or desktop stating **Notification approved**. Click on Next.

You have successfully set up MFA on your account. Please remember that you will need your mobile device or access to the Authenticator app, for any future prompts.

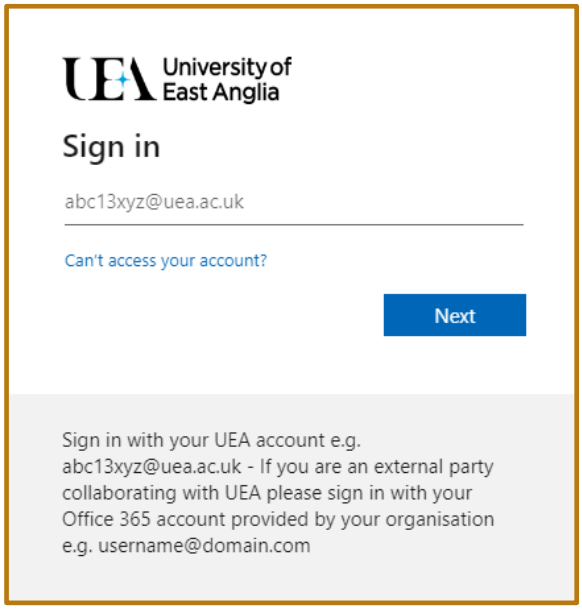
How often you see these prompts will depend on the device and applications you are using. MFA has been implemented to be as user friendly as possible, whilst still maintaining a high level of security around your account.

What will I see if I'm prompted?

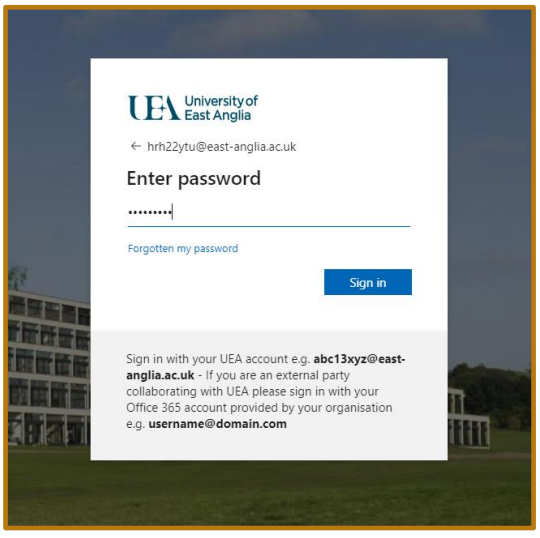
When you receive a prompt to complete MFA, you will see a box come up on screen to indicate that More information is required. Follow the instructions on screen and you can use the method you have set up to authenticate.

You will be asked to log into your account if you access any services that MFA has been applied on. For example, if you log into My UEA, you may be prompted.

Enter your **username** in the format of abc123xyz@uea.ac.uk and click on **Next.**



Enter your **password** and click on **Sign in**



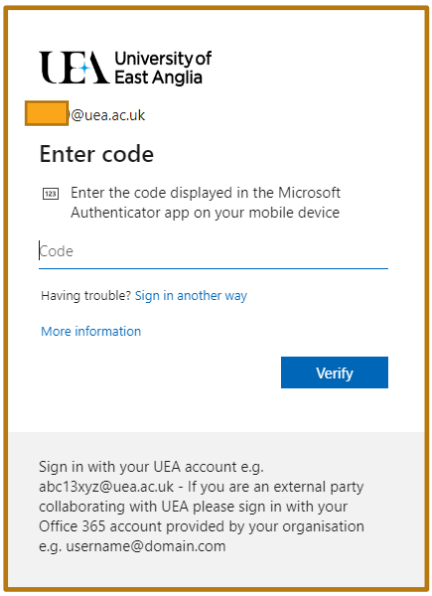
You will then be asked to **verify your identity**, with either of the methods below, based on your set up:

- a **one-time passcode** which you can find on the Authenticator App.

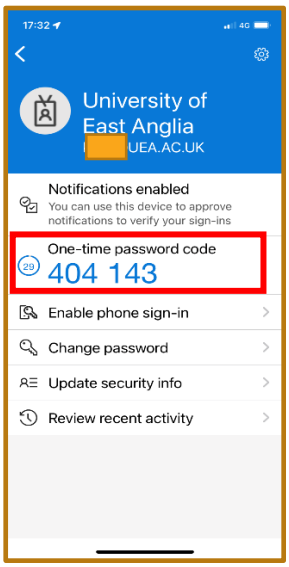
OR

- Alternatively, you could also receive an **Approve/Deny** notification on the Authenticator app.

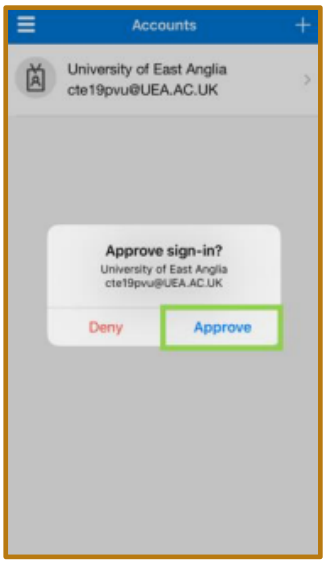
Desktop Enter code screen



Passcode option



Notification option



Enter the **code** and click on **Verify** or click on **Approve** on the app. You should now be able to access the UEA services.

More information about MFA can be found on My.UEA: https://my.uea.ac.uk/newlogin

For support, please contact the IT Service Desk visit: https://www.uea.ac.uk/itsupport (you do not require your UEA login to access this page).