Multi-factor Authentication (MFA): Microsoft Authenticator App

What is Multi-factor Authentication?

Multi-factor Authentication (MFA) is an approach to online security that requires you to provide more than one type of authentication for a login or other transaction.

Also known as 'Two-step Verification', MFA adds an extra layer of protection to your account and is used on a regular basis for many online transactions such as banking, shopping, or PayPal.

MFA requires you to authenticate using:

1. **Something you know:** your username and password
2. **Something you have**: a trusted device, such as your mobile phone, on which to receive and respond to verification requests

You must complete both authentication steps in order to access your University Microsoft account when off campus or on eduroam.

Setting up Multi-factor Authentication

Multi-factor Authentication is fast becoming essential to secure cloud-based services. For this reason, you are required set up MFA on your University Microsoft Office 365 account.

You can set up one or more of these authentication methods:

- Use the Microsoft Authenticator app on a smartphone or tablet (recommended)
- Receive a code by text[1]
- Receive a call by phone

This user guide steps you through setting up **Microsoft Authenticator app** as your authentication method.

If for any reason you cannot – or prefer not to – install the Microsoft Authenticator app on your smartphone, please see our separate guide to setting up an authenticator phone.

Set up the Microsoft Authenticator app

We recommend you use the Microsoft Authenticator app on your smartphone. You can set this up yourself, but you must follow the step-by-step instructions below carefully.

Before you start, you will need:

- a smartphone on which to download the app
- a PC, Mac or Tablet, open at a web browser
- a reliable internet connection

[1] Some services such as SSH gateway will not accept the entry of a code. If you use these services, please make sure you set up the Authenticator app and/or phone call as methods of authentication and set one of these as your default.

Set aside 10 minutes of uninterrupted time to work through this process.
If at any point the process stops working, close the app and the web browser and start again.

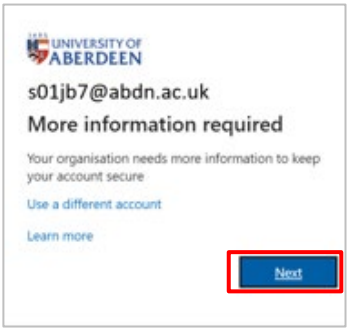
On your smartphone

1. Download the **Microsoft Authenticator App** from your App store.
2. Open the app, and if prompted, **Allow** Authenticator to send you **notifications**.
3. **LEAVING THE APP OPEN, go to the browser on your PC, Mac or Tablet.**

On your PC, Mac or Tablet

4. Open a browser and go to: https://aka.ms/setupsecurityinfo
5. If prompted, **sign in** with *your* University **username@abdn.ac.uk**, e.g. s01jb7@abdn.ac.uk
6. Enter your University **password** at the prompt

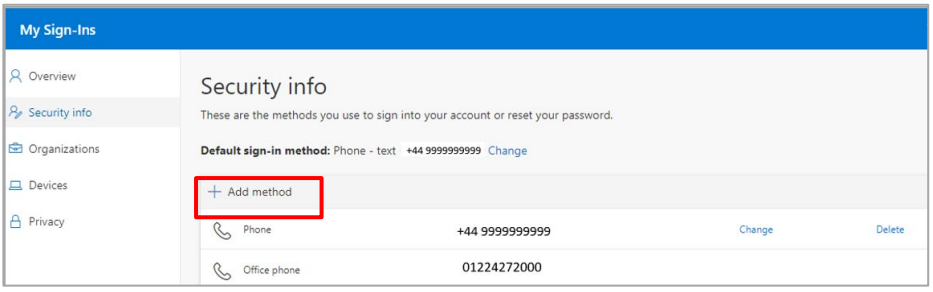
7. ***If*** you are prompted that *Your organisation needs more information to keep your account secure* click **Next** and **skip to step 9**



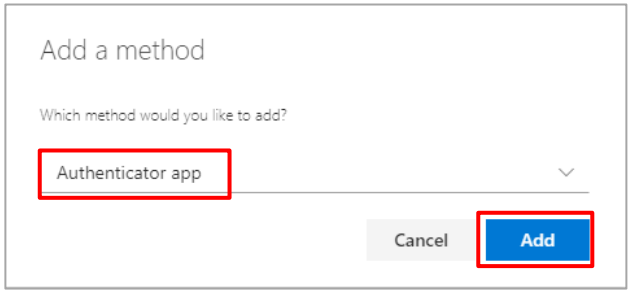
8. ***Otherwise*** the **My Sign-Ins** window will open.

   Note: If you have registered for SSPR (Self Service Password Reset), this window will already be populated with some details.

   Click **+ Add method**

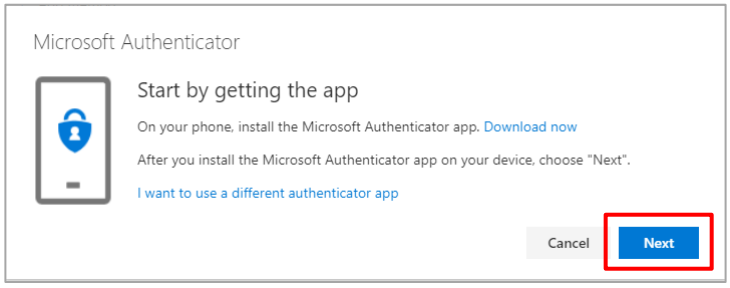


Choose **Authenticator app** as your method, and click **Add**

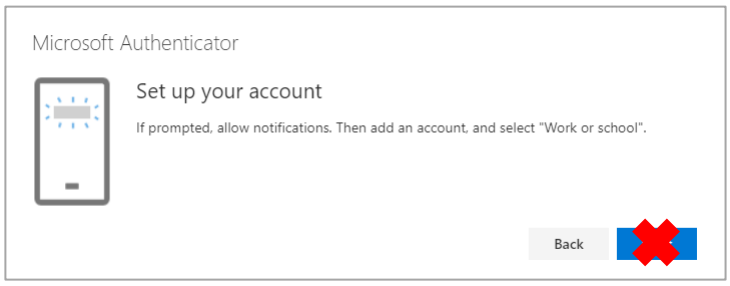


9. The following instruction window opens.

   As you have already downloaded the app, click **Next**



10. You will see the following message:



DO NOT CLICK ANYTHING! Instead, leave this message open, and go to your smartphone to set up your account.

On your smartphone

11. To **set up your account**

Android:

- Skip “one tap to verify” prompt and then click **OK**.
- Click to Add Account and choose **Work or school account** from the list.
- **Allow** Authenticator to take pictures and record video.

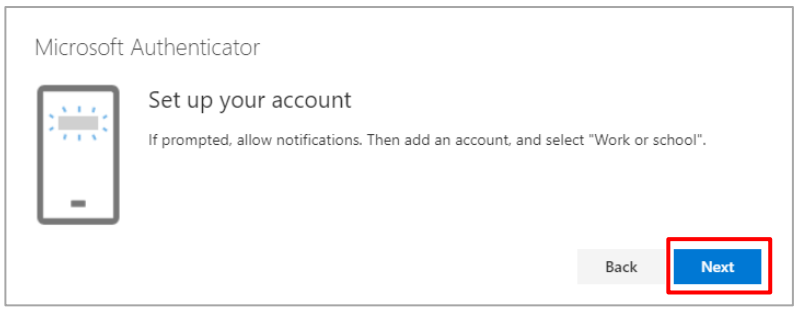
iPhone:

- If prompted, **Skip** through Add personal account and Add non-Microsoft account
- Click **Add Work Account**
- Click **OK** to allow Authenticator to access your camera

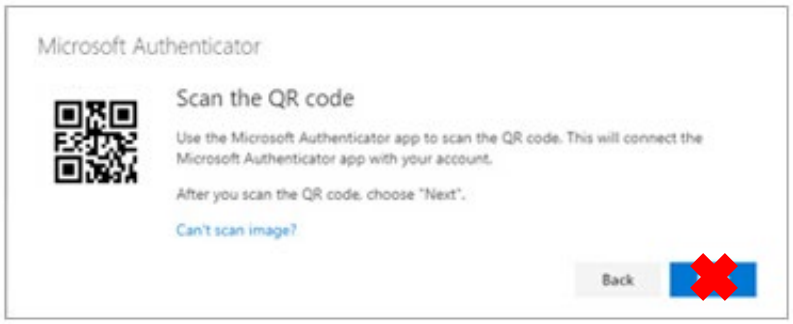
12. When prompted **Tap Scan a QR code**
    Your camera will open, ready to scan a QR code.
13. **LEAVING THE QR SCAN CODE WINDOW OPEN, return to the browser on your PC, Mac or Tablet.**

On you PC, Mac or Tablet

14. Click **Next** in the Microsoft Authenticator window.



15. A QR code will appear on screen.



DO NOT CLICK ANYTHING! Instead, leave this message open and return to your smartphone, ready to scan the QR code.

(**Note**: If for some reason it is not possible to use your camera, click **Can't scan image?** instead. You will be provided with a code and url to enter in the app.)

On your smartphone

16. Point the scan frame on your smartphone camera window at the QR code.
17. You will briefly see an **Activating** message on your smartphone.

    The Microsoft Authenticator App will generate codes as it finalises the set up of your Work Account on your smartphone:

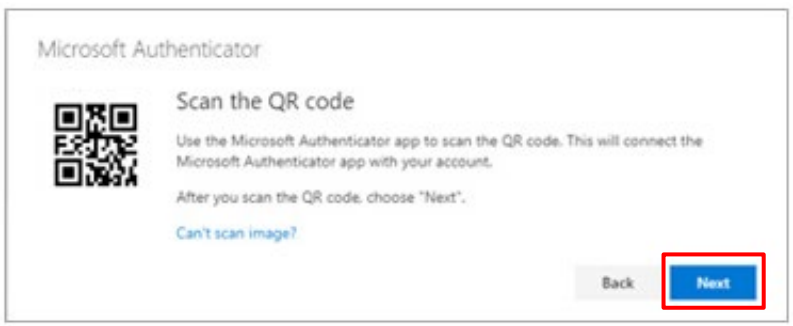
    You won't need this code just now.

    [Once your account is set up, you can authenticate using a code as an alternative to approving a notification.]

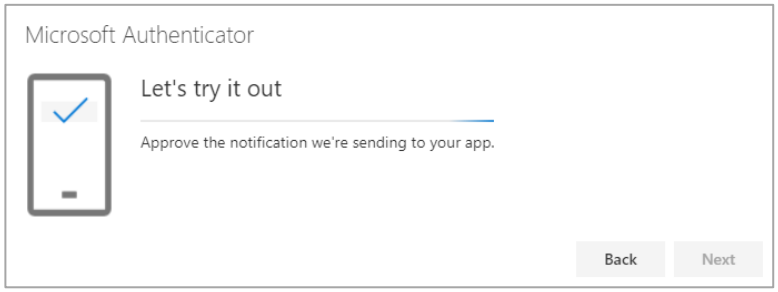
18. **Now, return to the browser on your PC, Mac or Tablet.**

On your PC, Mac or Tablet

19. Click **Next** in the Microsoft Authenticator window.



20. You will see a **Let's try it out** message and a **notification** will be sent to your smartphone.



21. **Return to your smartphone.**

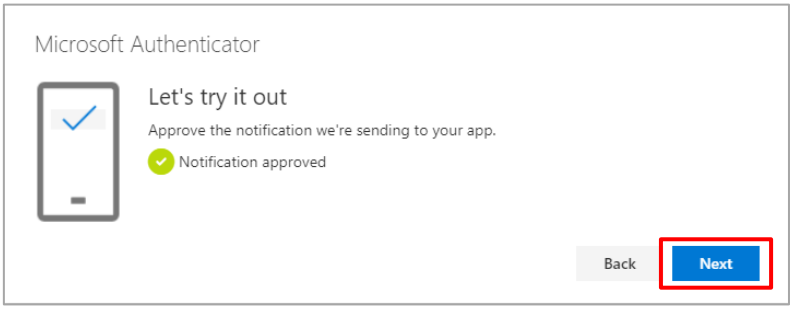
On your smartphone

22. Click **Approve**

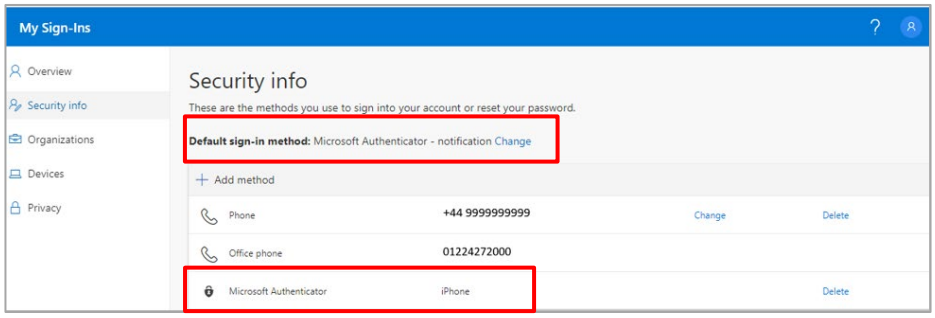
23. **Return to the browser on your PC, Mac or Tablet.**

On your PC, Mac or Tablet

24. You will see confirmation that the notification is **approved**.
Click **Next**.



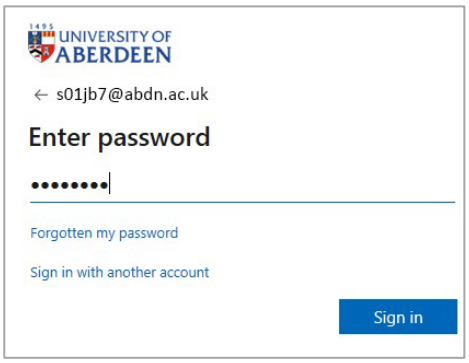
25. Microsoft Authenticator is now listed as a method of notification alongside details of your device.
We recommend you set Microsoft Authenticator app to be the **Default sign-in method**.



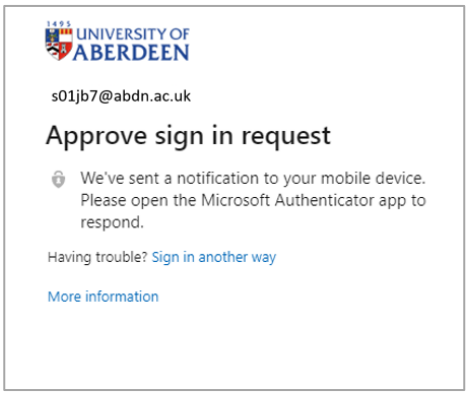
26. Go to the profile icon at top right and choose **Sign out**.

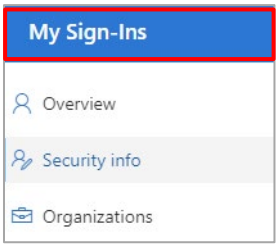
Testing authentication

1. In a browser on your PC, Mac or Tablet, go to https://aka.ms/setupsecurityinfo
2. If you are already signed in, go to your Profile picture and choose **Sign out**.
3. **Sign in** with *your* University **username@abdn.ac.uk**, e.g. s01jb7@abdn.ac.uk
4. Enter your University **password** at the prompt



5. If prompted to stay signed in, click **No**.
6. From the menu on the left, click **Security Info**.
7. You will see an action briefly on screen followed by this dialog box:





8. A **notification** will be sent to your smartphone.
9. Click **Approve** on your smartphone.
10. The sign-in to your account is complete.

If you don't receive the prompt to Approve on your smartphone app, perhaps due to loss of signal, choose **Sign in another way** and then enter the six-digit verification code from the app.

Note: This code changes periodically.

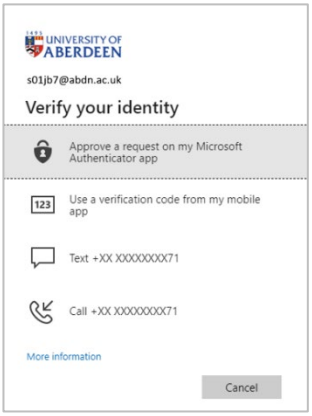
Note: You will need to use the Microsoft Authenticator app whenever you are asked to authenticate so ***keep* the app** on your smartphone - ***don't delete*** it.

If your response is slow

Don't worry if your response is slow and you see a dialog indicating **We didn't hear from you**.

You can choose to:

- Have another request sent to Microsoft Authenticator app,
- Enter a security code from the app, or
- Get a code a different way.



Text and call authentication options will only appear if you have added these as methods for sign-in. For more information see our separate guide on setting up an authenticator phone.

After you have set up Multi-factor Authentication…

What to expect on campus

You will see no difference when using the Outlook desktop client, OWA, SharePoint or Office 365 online on your desktop computer or on a University laptop when connected via direct access or uoa-corporate.

However, a device connected using *eduroam* is regarded as 'off campus'.

What to expect at home or off campus

If you were already signed into Office 365 apps – e.g. Outlook or OneDrive – on a smartphone or tablet, or the Outlook desktop client on a personal PC, you will be required to sign in again with the extra step of authenticating, approving the notification.

When you sign in to OWA, SharePoint, or Office 365 online you will be asked to authenticate, i.e. you will be prompted to:

- Enter *your* University **username@abdn.ac.uk**, e.g. s01jb7@abdn.ac.uk
- Enter your University **password**
- Approve the notification on the Microsoft Authenticator App on your smartphone

Be cautious of choosing **Approve** every time you are notified in the Microsoft Authenticator app!

Was it you that was trying to sign into your University office 365 account? If not, then **Deny**!

We recommend that you use the Outlook app to access University email.
Other email apps may not work with Multi-factor Authentication (MFA).

Further information and help

If you have any questions or concerns contact the Service Desk: https://myit.abdn.ac.uk