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 email address 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 @aberdeen Microsoft account.

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 @aberdeen Microsoft Office 365 account.

You should set up two or more of these authentication methods:

- Use the Microsoft Authenticator app on a smartphone or tablet (recommended)
- Receive a code by text
- 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

> Set aside 10 minutes of uninterrupted time to work through this process.
>
> You will be required to work on both your smartphone *and* PC, Mac, or Tablet during the setup.
>
> 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.**

Available on the **App Store**

Get it on **Google play**

On your PC, Mac, or Tablet	4. Open a browser and go to: https://aka.ms/setupsecurityinfo
	5. If prompted, **sign in** with *your* @aberdeen **email address**, e.g. j.bloggs2.18@aberdeen.ac.uk
	6. Enter your **password** at the prompt

Microsoft

← j.bloggs2.18@aberdeen.ac.uk

Enter password

••••••••

Forgot my password

Sign in

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

j.bloggs2.18@aberdeen.ac.uk

More information required

Your organisation needs more information to keep your account secure

Use a different account

Learn more

Next

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

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

Click **+ Add method**

My Sign-Ins

- ○ Overview
- ○ Security info
- ○ Organizations
- ○ Devices
- ○ Privacy

Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Phone - text   +44 9999999999   Change

+ Add method

📞 Phone   +44 9999999999   Change   Delete

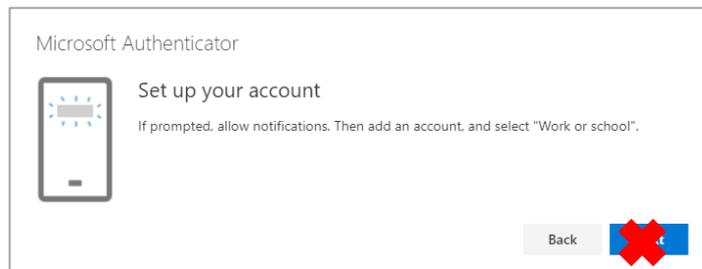Choose **Authenticator app** as your method, and click **Add**
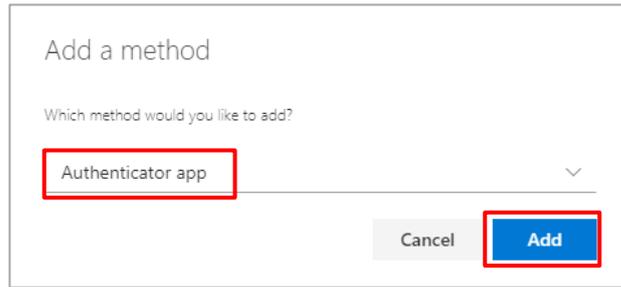
9. The following instruction window opens.

   As you have already downloaded the app, click **Next**
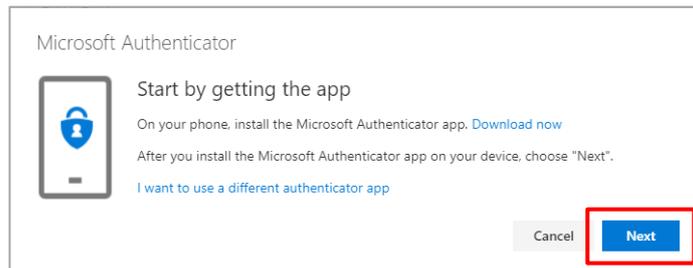
10. You will see the following message:

   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

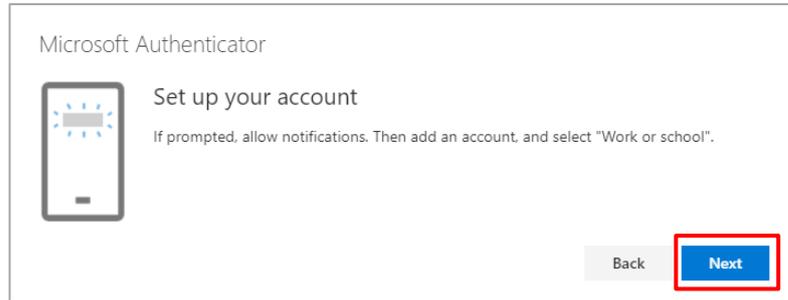12. When prompted **Tap Scan a QR code**
    Your camera will open, ready to scan a QR code.

13. **LEAVING THE QR SCAN CODE WINDOW OPEN, return to the browser on your PC, Mac, or Tablet.**
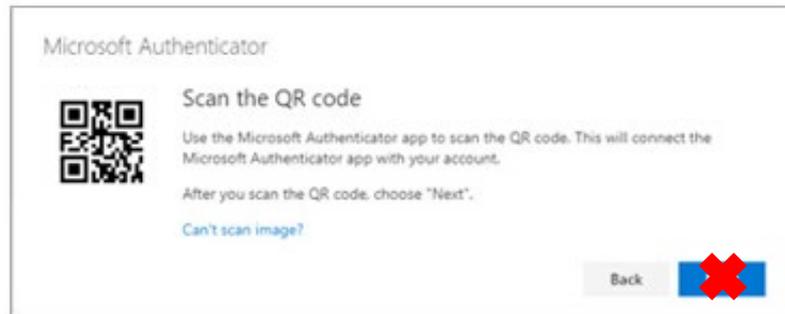
|	
On you PC, Mac, or Tablet	14. Click **Next** in the Microsoft Authenticator window.
	15. A QR code will appear on screen. **DO NOT CLICK ANYTHING! Instead, leave this message open and return to your smartphone, ready to scan the QR code.** (**Note**: If for some reason it is not possible to use your 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.
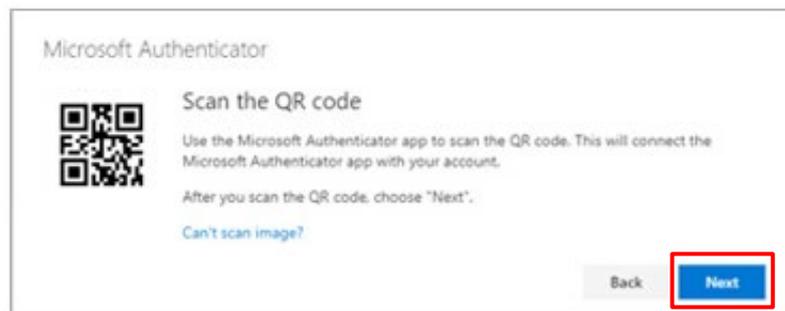
20. You will see a **Let's try it out** message and a **notification** will be sent to your smartphone.
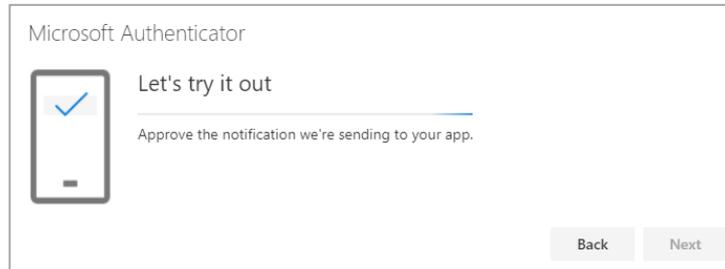
21. **Return to your smartphone.**

On your smartphone	22. Click **Approve** 23. **Return to the browser on your PC, Mac, or Tablet.**

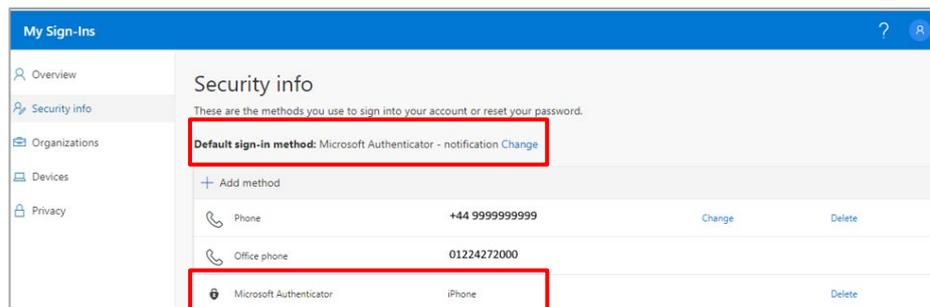|	
On your PC, Mac, or Tablet	24. You will see confirmation that the notification is **approved**. Click **Next**. 25. Click **Done** 26. Microsoft Authenticator is now listed as a method of notification alongside details of your device. We recommend you set Microsoft Authenticator app to be the **Default sign-in method**.
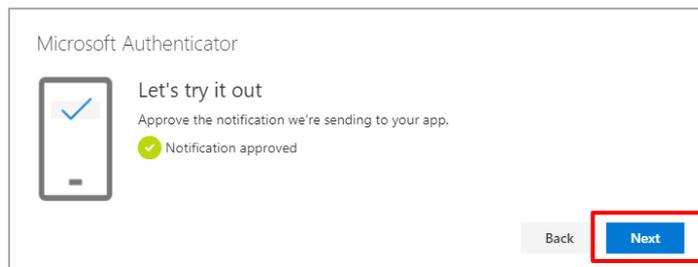
> ⚠️ At this point, we *strongly* recommend you *set up a second method* of authentication. You can do this in the **My Sign-Ins** window:
>
> 1. Click on **+ Add method**
> 2. Choose **Phone** – work through instructions in our separate phone guide

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* @aberdeen **email address**, e.g. j.bloggs2.18@aberdeen.ac.uk

4. Enter your **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 a dialog box asking you to approve your sign in request:

   j.bloggs2.18@aberdeen.ac.uk

   ### Approve sign in request

   🔓 We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.

   Having trouble? Sign in another way

   More information

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. If your response is slow you will be offered options dependent on the authentication methods you have set up.

11. When you have completed the set up and tested the authentication methods, go to the profile icon at top right and choose **Sign Out**.

    > ⚠️ **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.

What to expect after MFA is enabled on your account…

Help! I see a message saying my account is blocked! My email no longer works!

If you receive an email to say your account is blocked, or if your email/calendar no longer work on a smartphone, *don't panic*!

Your email account is not permanently blocked. It will be trying to connect using an old authentication method and we need it to use Modern Authentication as part of MFA.

To do this you can either:

– delete the account and set it up again, or

– install and use the Outlook app from the app store.

You will find guides to help you with this under the Help section below.

Already signed into Outlook?

If you were already signed into the Outlook app on a smartphone or tablet, or the Outlook desktop client on a personal computer, you will be required to *sign in again* with the extra step of authenticating, approving the notification.

From now on

Whether you use an email client or app, or Outlook Web Access (OWA) on any device, you will be asked to authenticate when you sign in to your @aberdeen email account, i.e. you will be prompted to:

• Enter *your* @aberdeen **email address**, e.g. j.bloggs2.18@aberdeen.ac.uk

• Enter your **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 @aberdeen office 365 account? If not, then **Deny**!

Further information and help

Use MyIT to report an issue with the IT Service Desk: https://myit.abdn.ac.uk

Configuration guides for email apps and clients

– Office 365 email on iOS using Mail app

– Office 365 email on iOS using Outlook app

– Office 365 email on Android using Outlook app

– Office365 email on Mac using Apple Mail