

Multifactor Authentication Overview

Office 365 Multi Factor authentication (MFA) provides additional security for your user account. MFA is a method of verifying who you are that requires more than just a username and password. Sign in can only be completed once you have acknowledged a sign in verification process either by text message, voice call or via a smartphone authenticator app.

Instructions to configure MFA

At this stage no action is required, we recommend you wait to be prompted before configuring MFA

Once IT have enabled your account for MFA, you will be prompted to follow the instructions below and you will be guided through the configuration process.

Following the steps below will configure MFA notifications on the mobile app which is the most convenient way to verify your identity.

If your preference is to configure the application in advance, please go to this link

<https://aka.ms/MFASetup>

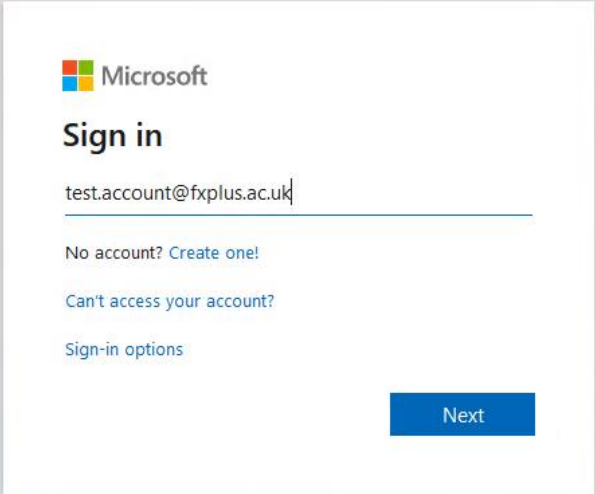
This will take you directly to your security info page;

Complete the steps below

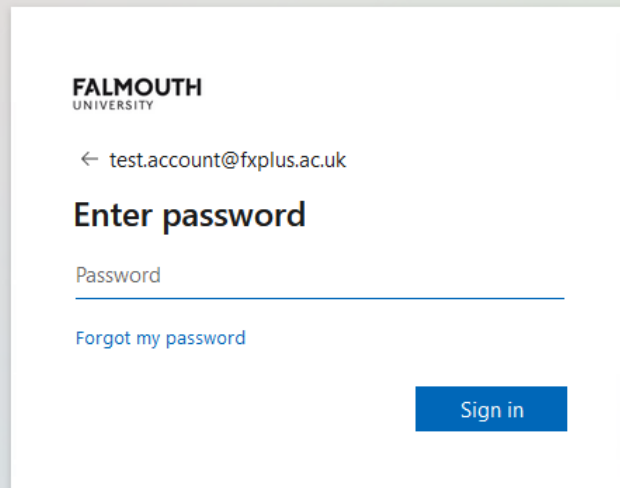
- Click the “Add Method”,
- Choose Authenticator app and follow the instructions below from step 4

##NOTE##

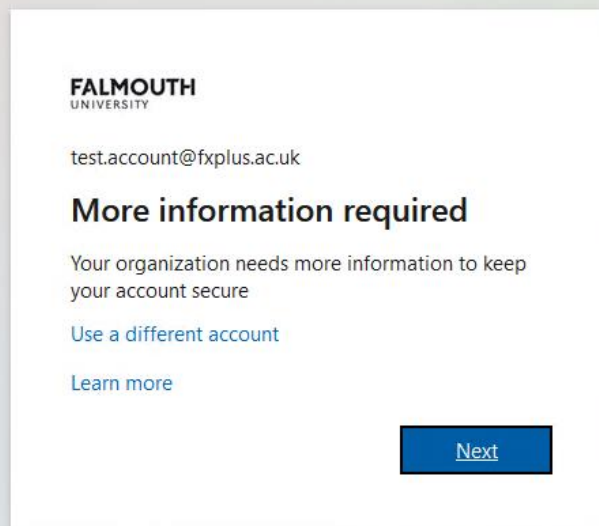
If pre-configuration is completed, you will still **not be prompted** for MFA validation until your account is enabled by IT

<p>1. On your computer</p> <p>Go to portal.office.com and enter your @fxplus.ac.uk or @falmouth.ac.uk email address if prompted.</p> <p>##NOTE##</p> <p>If already logged into office 365 App go straight to Step 3</p>	
---	--

2. Enter your account password as requested.



3. After authentication you will be prompted to provide additional information to enable MFA. Click **Next**.



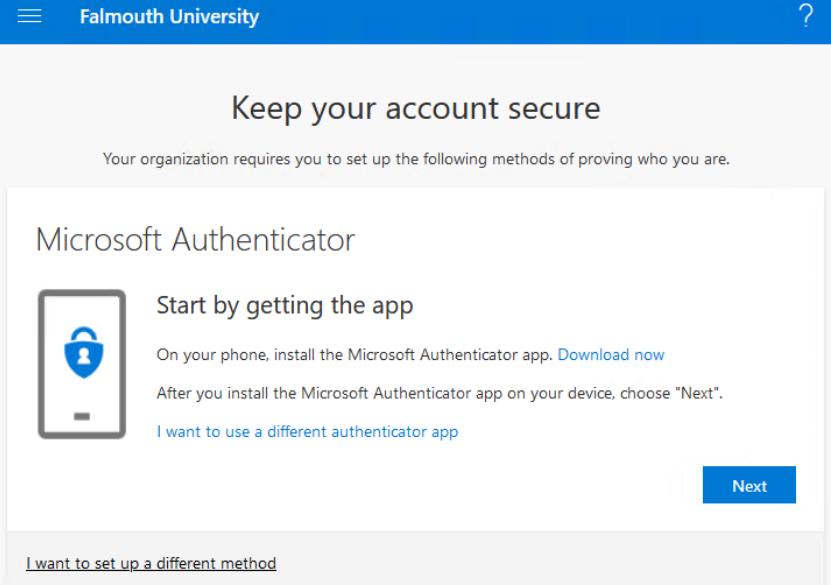
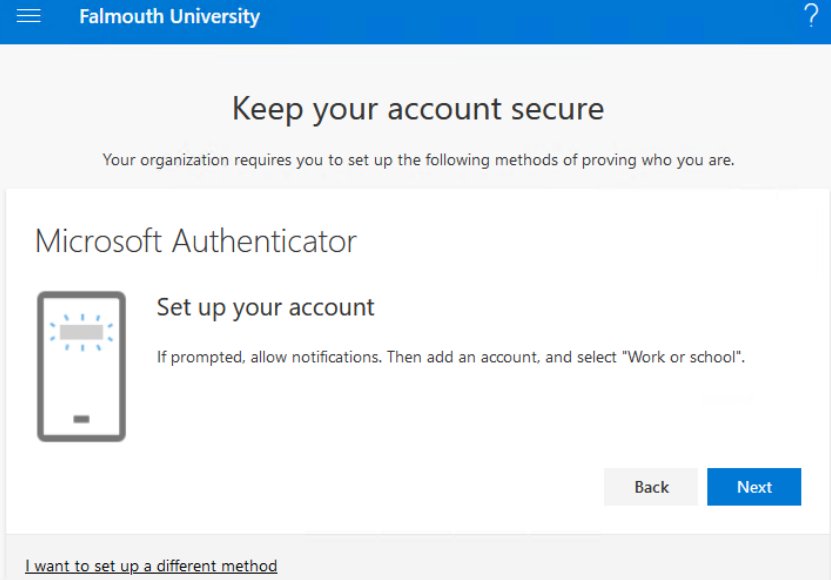
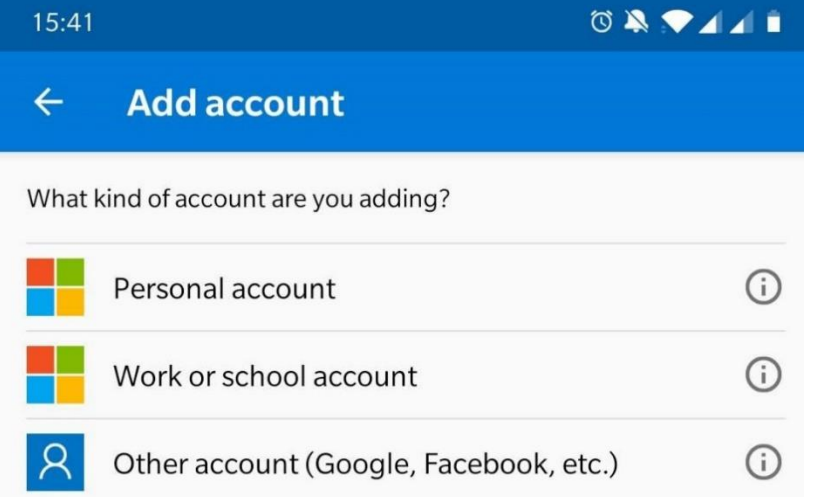
4. Download the **Microsoft Authenticator app** from the Google Play Store or the Apple App Store

##NOTE##

Don't Disable Push Notifications the MFA App requires this functionality

##NOTE##

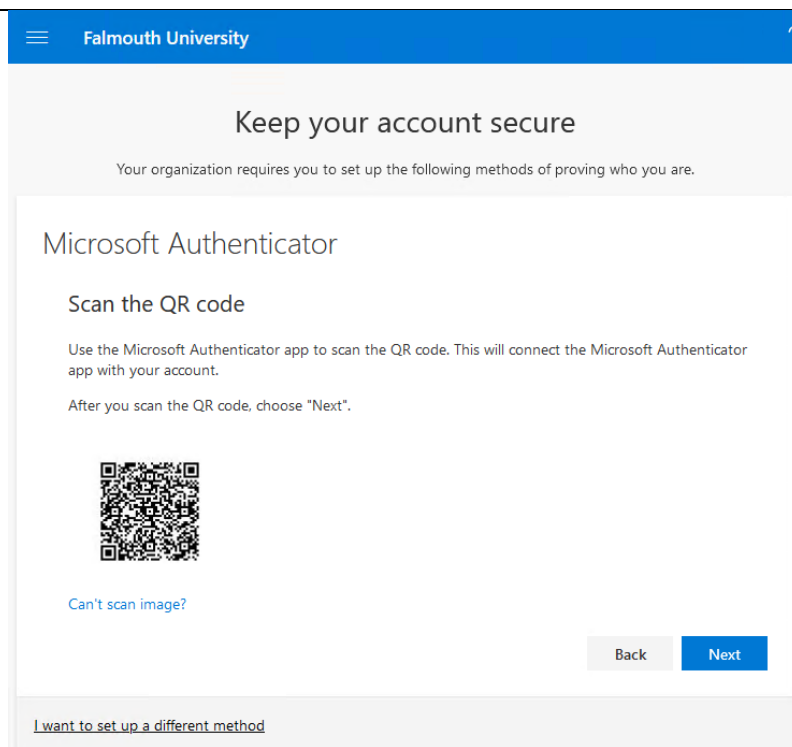


<p>If you already have the Authenticator App installed go to Step 5</p>	
<p>5. We strongly recommend you configure the Microsoft Authenticator app by clicking Next. This is the most convenient way MFA method. Other applications are supported by choosing “I want to set up a different method”.</p>	
<p>6. Press Next</p>	
<p>7. Launch the mobile app and choose Add an account. Then select work or school account. Present the QR code on your screen to the app.</p>	

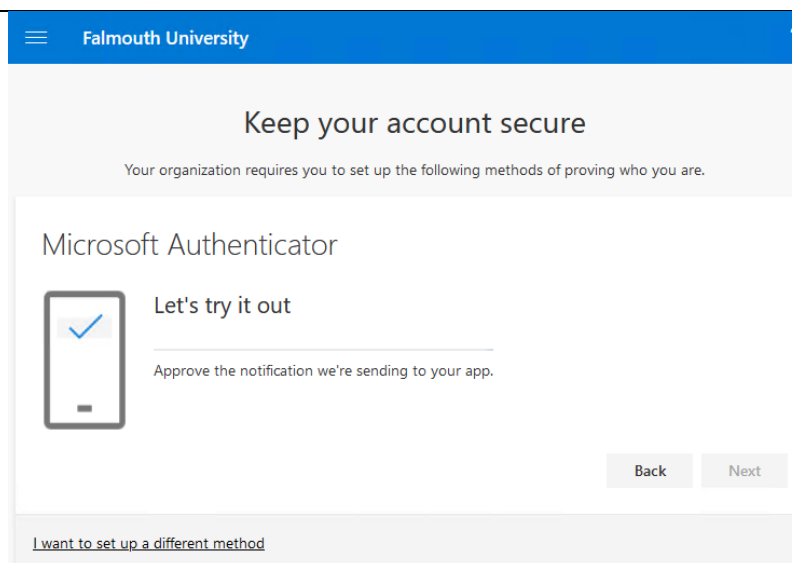
8. Scan the QR code presented on the **screen** using the **Microsoft Authenticator app**. Once successfully added press **Next**

##NOTE##

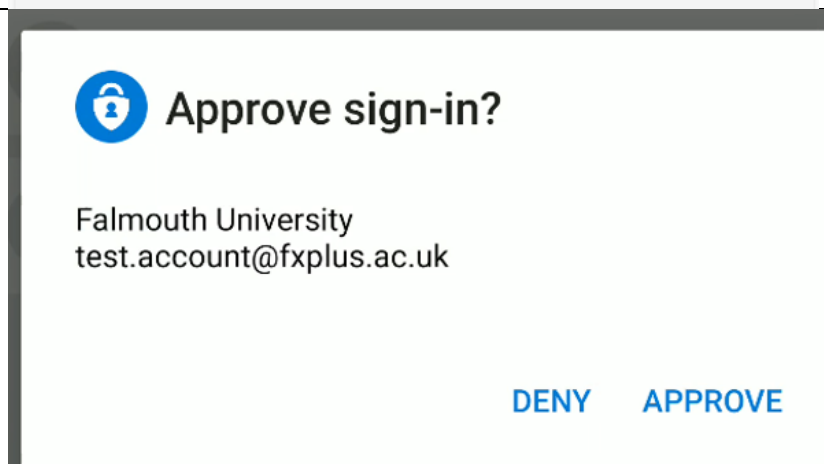
The QR Code Generated is unique to your set up and time sensitive so if a significant delay occurs between scanning from your phone it is recommended that you press back, then next and the code will be refreshed.

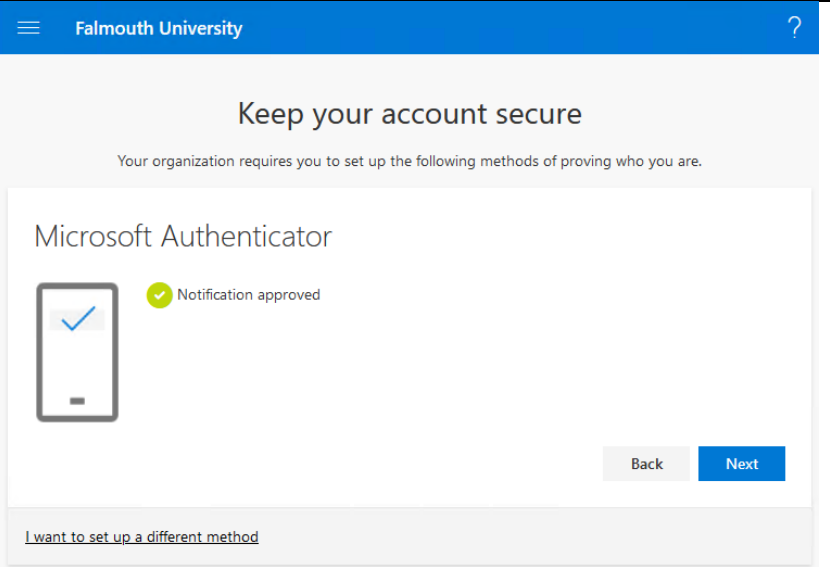
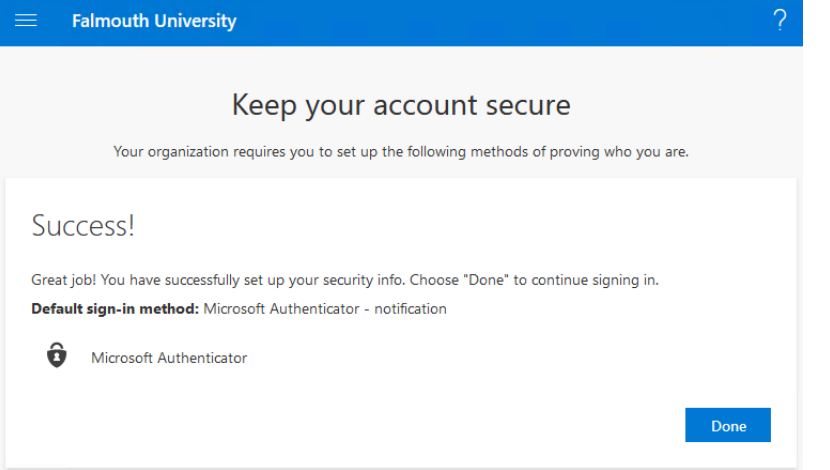


9. A test notification will be sent to your phone to approve



10. **Approve** the sign in prompt on your smartphone.



<p>11. Click Next.</p>	
<p>12. Success! Click Done to complete your MFA configuration.</p>	
<p>13 . Restart Any Microsoft Apps prompting for password</p> <p>##NOTE##</p> <p>Restart recommended as some tasks requesting credentials may be hidden</p>	<p>If you have any Microsoft 365 App that were open during this process (such as Outlook) you may see they are prompting for password authentication.</p> <p>Simply restart the application and they will continue to function as expected.</p> <p>To ensure all background tasks are refreshed the easiest solution is to simply restart your PC / Mac</p>

Frequently asked questions

How many often will I have to provide MFA verification?

Once you have performed an MFA authentication you should not be prompted again unless you change your password. If you clear your browser cookies, use a different browser or use a private browsing window you will have to perform MFA again to verify your identity. If you keep being asked to provide MFA verification, please speak with the IT ServiceDesk.

Why does it show a “one-time passcode” when there is no-where to enter it?

The “one-time passcode” generated by the Microsoft app just in case there is no active data signal at the point you are presented with an MFA challenge, in most instance the App will just request “Approve” so this will not be used, however it is there as a back-up for potential future requirements and should you have no active data connection on your device as the time of the request.

Does the App retain, track or hold any of my personal data?

The Microsoft Authenticator app does not any retain information outside of the information provided when setting up your work credentials.

It is purely a number generator for security keys.

I've lost access to my phone and cannot access my account, what should I do?

If you have lost access to the app and the backup phone number, please contact the ServiceDesk. IT will have to reset your MFA settings.

Can I use a third party MFA application (e.g. Google authenticator, Authy)

Most authenticator applications can be used. However, push notifications (a message that pops up on your mobile device) are only supported with the Microsoft Authenticator app.

To add a third-party app complete the following steps:

- Go to your MFA dashboard [here](#)
- Click Add method
- Select Authenticator app
- Click Add
- Click "I want to use a different authenticator app" and then follow the onscreen instructions.

I'm having issues configuring the Authenticator App.

Try using text message verification as a workaround. If you continue to have issues, please speak to the IT ServiceDesk.

How can I change my MFA settings?

Go to <https://aka.ms/MFASetup> and sign in to change your verification options at any time.

What do I do if I'm offline?

The Authenticator app enables you to generate MFA codes completely offline without access to the internet. This is ideal if you are abroad and concerned about data roaming costs.

For more information about the Microsoft Authenticator app, please see [here](#)