

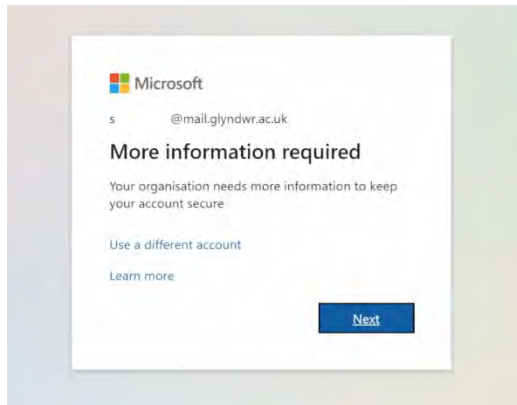
Setting up Microsoft Authenticator

Contents

Introduction.....	2
What is Two-factor Authentication?	2
How is Two-factor Authentication enabled?.....	2
Setting up the Microsoft Authenticator App.....	4
Returning to your computer	6
Sign-in options (With Authenticator)	7
Authenticating with other options.....	8
References	9

Introduction

You may have gone to log into Moodle and noticed a screen that looks like this:



This is asking for you to setup Two-factor Authentication (or abbreviated to 2FA) for your account, this is done to help keep the university secure from outside attacks and keep all of your files safe, and is an important security measure that is currently being implemented in lots of websites and apps.

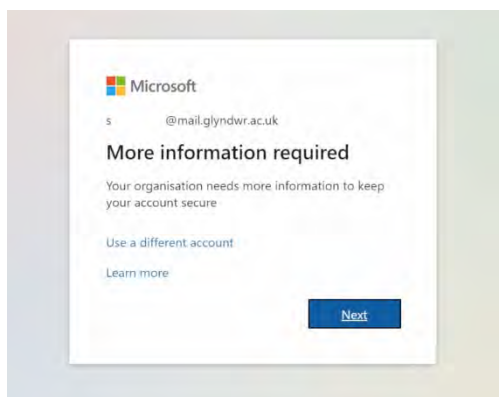
What is Two-factor Authentication?

You may be wondering what Two-factor Authentication (or 2FA) is, 2FA is a security measure that asks for two forms of identification to allow you to access the account you are logging into, in this example, Moodle, the reason why it is used is because it helps prevent any unwanted logins who may be trying to steal, destroy, or access important information, for example, student records. (Microsoft, 2022)

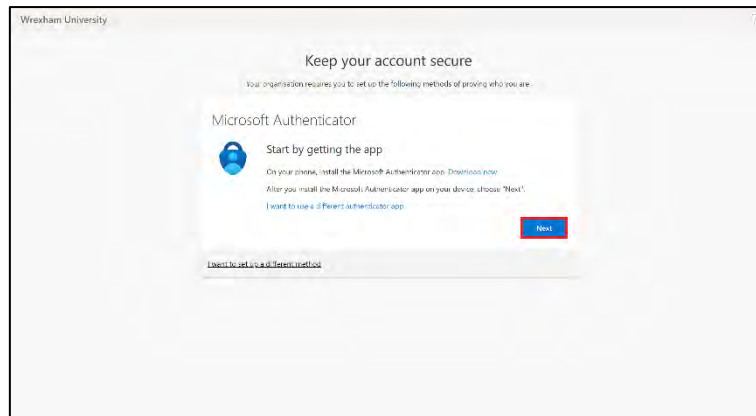
The university is always working to ensure strict IT security measures are in place and updated to keep the systems offered by the university safe and secure, and this is one of these important measures.

How is Two-factor Authentication enabled?

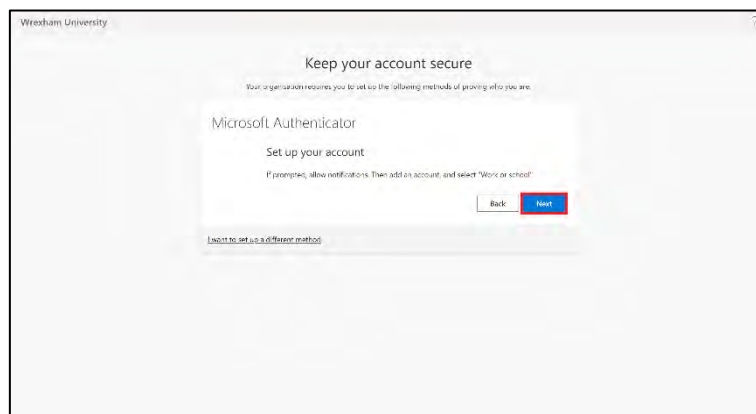
Now that you're up to date on what 2FA is, lets cover how to set it up, the process should be relatively quick, and this guide will walk you through it step by step.



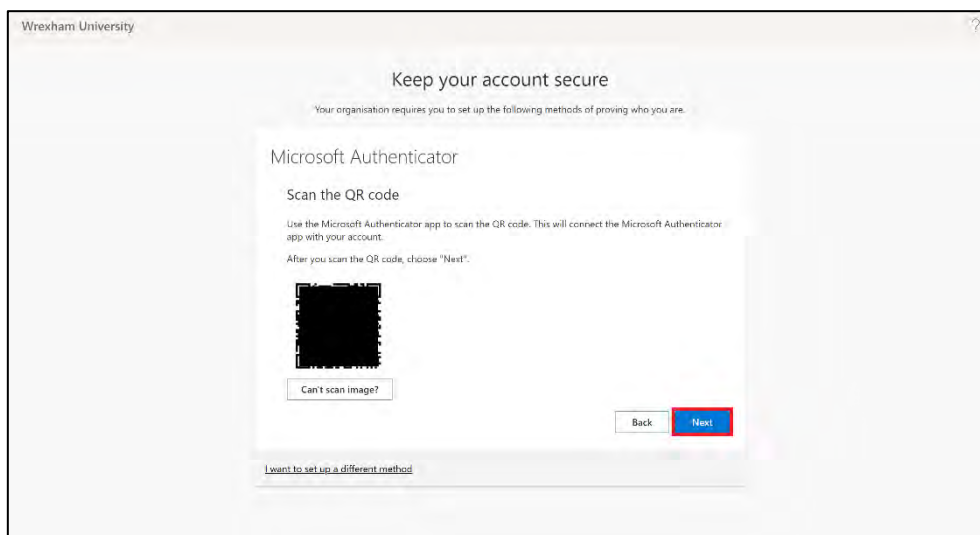
Returning to the screen above, the first step is to click 'Next', this will then take you to the Microsoft Verification setup screen. (Shown below)



Click 'Next' (on the screen shown above) then 'Next' again on the screen shown below.

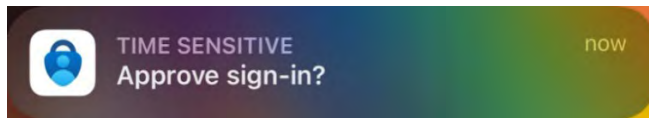


When you reach the third screen (shown below), you will need to scan a QR code, but before we can do that, we need to install the Microsoft Authenticator app.

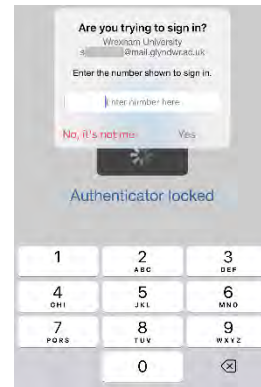


By using the app, you will receive a notification to verify your login, this means that you don't need to worry about having a phone signal, however, later on in the guide, you will be shown how to authenticate with other methods. (Some example images of the notification is shown below)

Receiving a notification for verification means that when you logon, your phone will ask you if you want to approve the sign-in, which will look something like this:



Approve sign-in notification

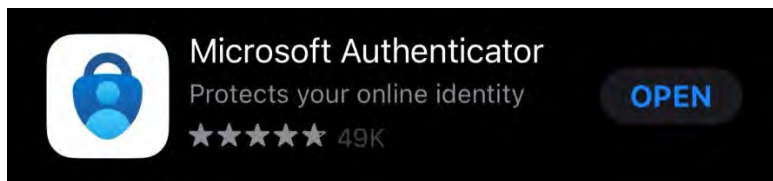


Approve sign-in dialog

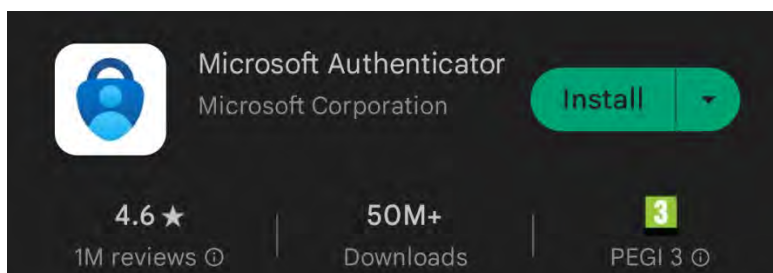
Setting up the Microsoft Authenticator App

The Microsoft Authenticator app can be downloaded on both an iPhone and an Android phone, and where the instructions used are using an iPhone, the instructions are the same for Android.

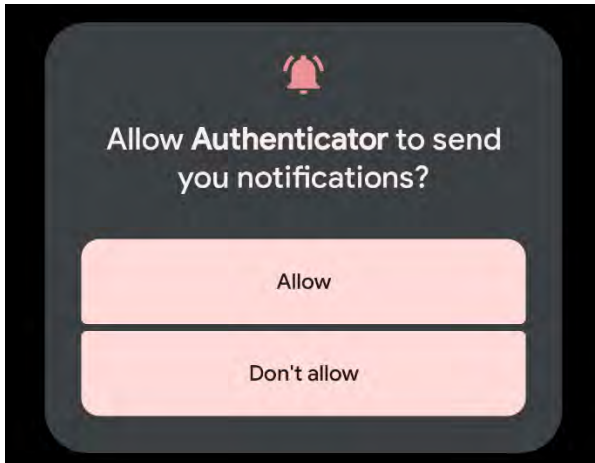
On iPhone: Head to the App Store and search for Microsoft Authenticator, the icon will look like this, when you have found it, click install.




On Android: Head to the Google Play Store, and search for Microsoft Authenticator, --

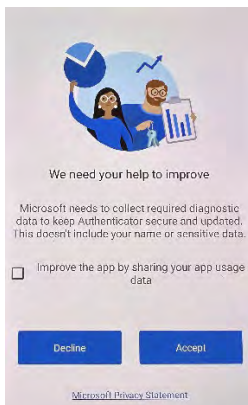


When the app has loaded you will be greeted with a screen asking you to allow notifications (both on Android and iPhone), you want to allow these notifications so when a request comes through you can quickly approve it.

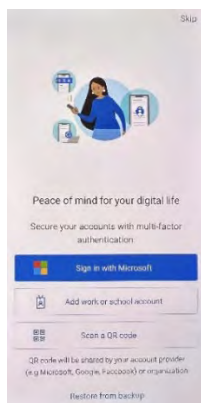


 **NOTE:** This dialog may look slightly different depending on the device you are using, but in general, you want to allow notifications.

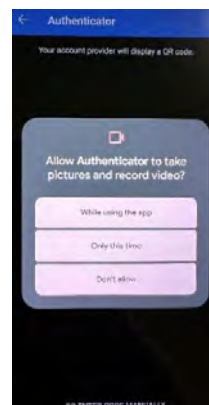
When you have entered the app, you will be presented with a screen asking you to accept or decline collection of required diagnostic data, unfortunately, this is not optional, and you need to accept this to continue with the app.



After clicking accept, you can now sign in, however, we want to tap on 'Scan a QR code', when you've tapped that, you will then be asked to allow access to your camera (you want to allow this so you can capture the QR code with your camera)



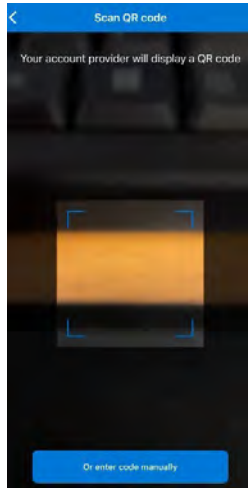
App sign-in screen



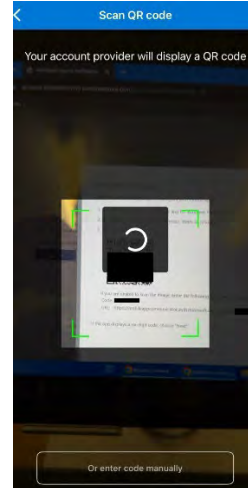
Screen asking for permission to use the camera

If your camera screen looks like the one shown above (on the right), then tap 'While using the app', meaning the camera will only be accessed when the app is open.

You will see a screen like the ones below, where you need to position your camera to have the QR code line up with the box, and it will scan automatically. When it has, return to your computer.



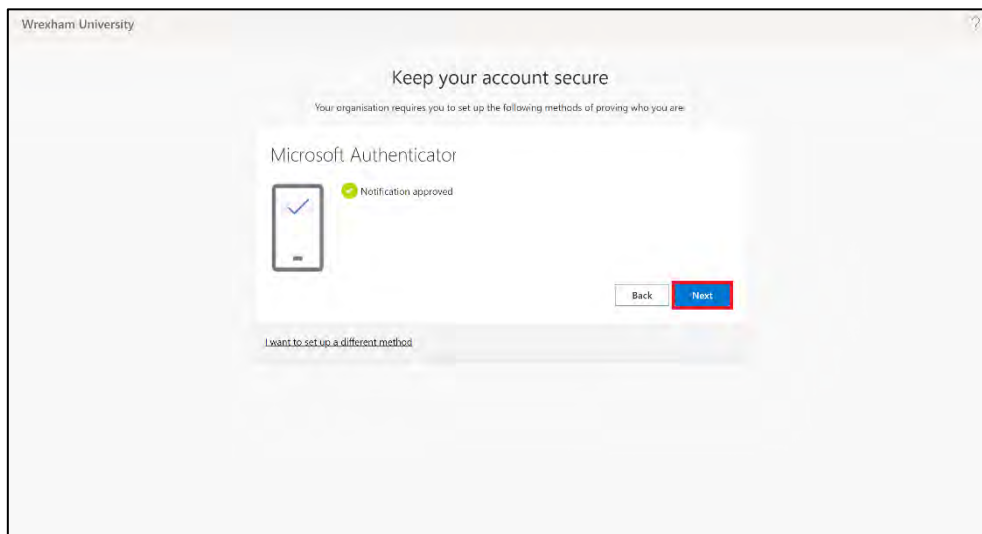
An example of the QR code scanner screen



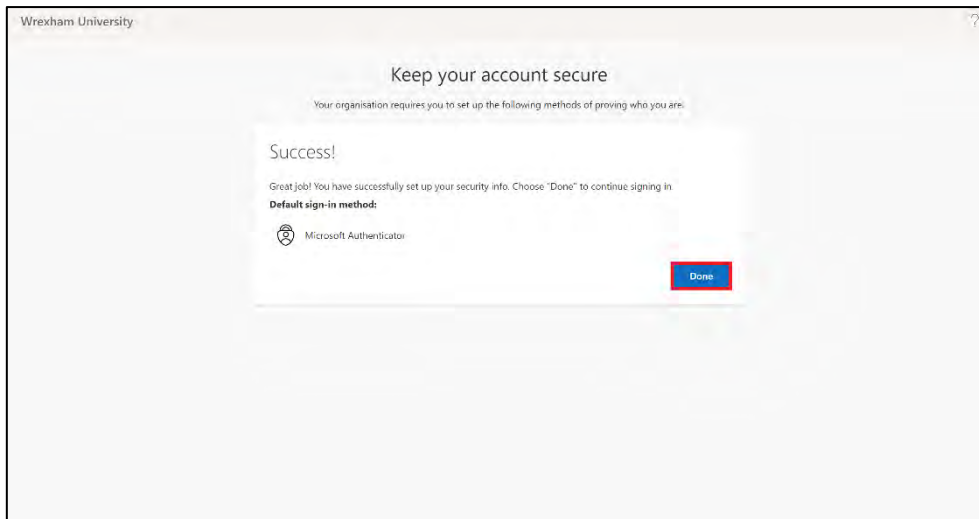
An example of a scanned QR code

Returning to your computer

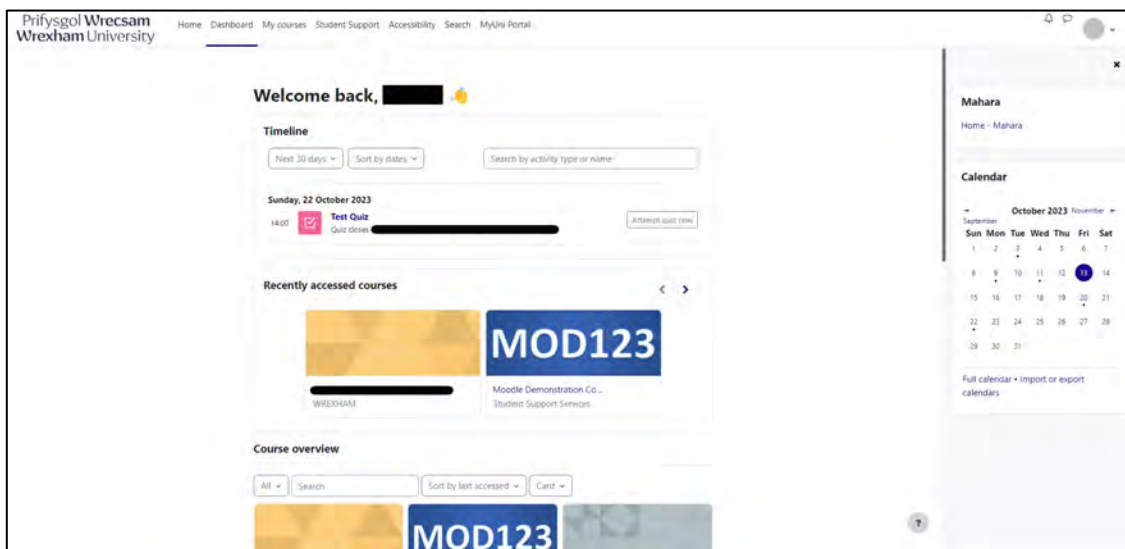
Once you've set up the Microsoft Authenticator app, and approved the notification (with a two-digit code), your screen on your computer should inform you that the notification was approved, where you can now click 'Next'.



As shown on the next page, when the setup is complete, click 'Done'.

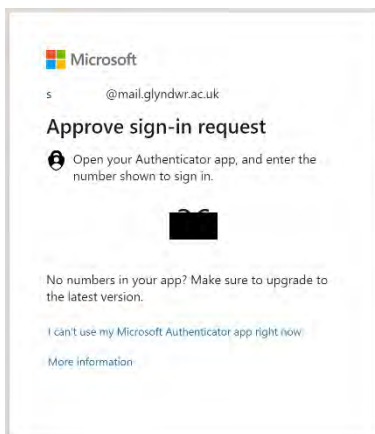


You should now be taken directly to Moodle.

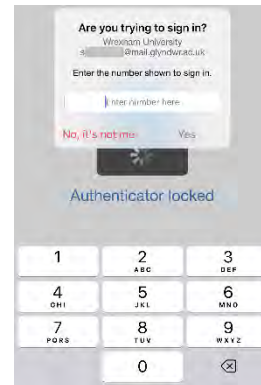
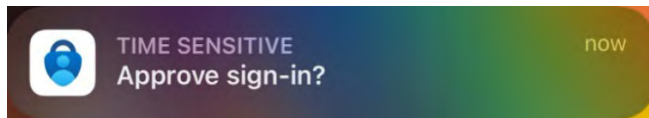


Sign-in options (With Authenticator)


The next time you come to log onto Moodle (or Office), you will be greeted with a screen that looks like this:



As shown on the images below, you will receive a notification on your phone, where you will need to type in the two-digit number on the Authenticator app.



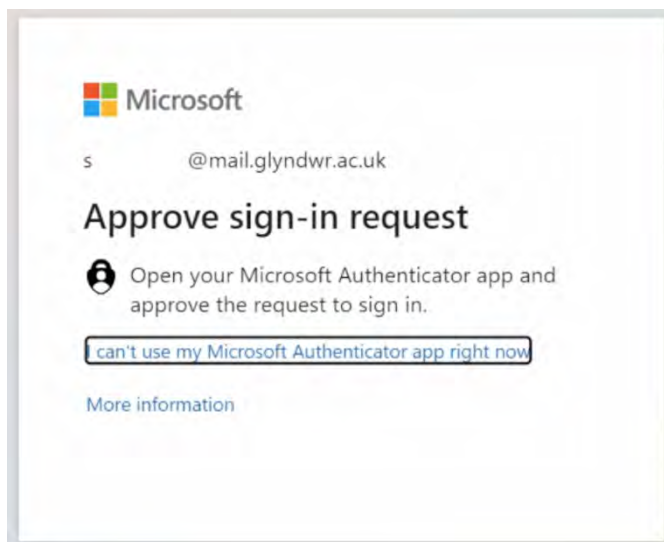
When you tap on the notification (or open the Microsoft Authenticator app), you will see a screen like the ones above, when you reach the second screen (pictured on the right), you will need to enter the number that will be displayed on your screen. And your login will be approved, and you can continue to Moodle or Office.

 **NOTE:** If you did not try to sign in and you receive this notification, click 'Deny' to block that attempted access, and speak to IT if you think there was a suspicious attempt to login to your account. (Please make sure you didn't attempt to sign in before you ask IT to avoid any false positives, but also being vigilant will help keep you and the university safe)

Authenticating with other options

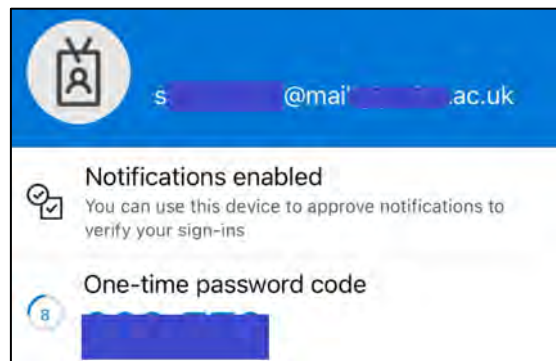
If you did not receive the notification, or you open the app and there is no approval request (for example, if you don't have an internet connection), don't worry, you can still login.

On the same screen as above, click the option that says, 'I can't use my Microsoft Authenticator app right now', and you'll then be brought to a different screen. (As shown on the next page)





From the image above, you will be presented with these options, this is where you can get access to your account through different methods, the easiest one is 'Use a verification code', when you pick this option, you can open the Microsoft Authenticator app and get a one-time password code (shown below on the left), even if you don't have an internet connection.



Once you have the code, you can enter it into the screen shown above, and click 'Verify'.

References

Microsoft, 2022. *What is two-factor authentication?*. [Online]
Available at: <https://www.microsoft.com/en-gb/security/business/security-101/what-is-two-factor-authentication-2fa>
[Accessed 25 November 2022].