

# Set up MFA using Microsoft Authenticator app

## Multi-Factor Authentication (MFA)

Updated: 18 January 2023

Multi-Factor Authentication (MFA) is a requirement to access UNSW single sign-on (SSO) applications. MFA provides an additional layer of security to protect the University and your zID account from unauthorised access.

Use this guide to set up MFA by installing the Microsoft Authenticator app on your smartphone and completing the MFA registration on your computer. Watch this [short video](#) for an overview.

For Microsoft Authenticator support, or to discuss your [MFA alternatives](#) should Microsoft Authenticator not be suitable, call the **IT Service Centre on 02 9385 1333** and select MFA from the options presented. Alternatively drop into one of the many [IT Walk-In Service Centres on campus](#). Please have ID verification with you.

Refer to the [MFA website](#) for all MFA information and how-to guides:

- [Use Microsoft Authenticator](#)
- [Use Microsoft Authenticator without a data/internet connection.](#)
- [Transfer Microsoft Authenticator app to a new phone](#) from your old phone.
- [Set up and use a YubiKey](#)
- [Set up and use a YubiKey for non-Windows devices](#) such as Mac and Linux.
- [Set up MS Authenticator app on a second mobile device](#) as a backup after setting up MFA on your primary device.
- [FAQs for staff](#)
- [FAQs for students.](#)

**Attention: China-based students**

- If you are unable to download the Microsoft Authenticator app from your smartphone app store, please follow this [guide](#).

## To complete this task, you will need

- Your zID@ad.unsw.edu.au account and password.
- A computer with internet access.
- A compatible smartphone with data connection.
- Please allow approximately 5 minutes to complete the setup.
- Have all your equipment ready and complete the setup from beginning to end in one go.

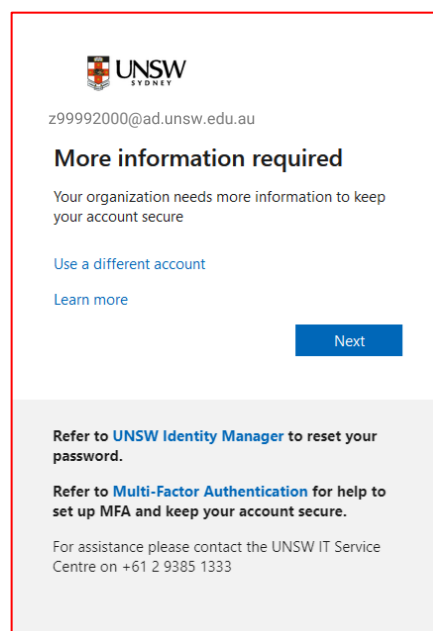
## Instructions to set up MFA

You only need to set up MFA once, using your computer and the Microsoft Authenticator app on your smartphone. After setup, do not delete/uninstall the app from your smartphone. You will need this app to verify your login when accessing University SSO applications periodically.

If you delete/uninstall the app from your smartphone, call the IT Service Centre first as they will need to reset your account before you can follow these instructions again.

**Note:** When accessing a single sign-on application such as Moodle, if you are presented with a **More information required** window (see image), it is an indicator that you have not set up MFA and MFA is enforced on your zID account.

At this point you must set up MFA before you can access the SSO application.



This instruction to set up MFA is in two parts: Part 1 is the installation of the app on your smartphone and Part 2 is to finish the registration using your computer.

If you already have Microsoft Authenticator app on your smartphone, please start from Part 2.

## Part 1: Install the Microsoft Authenticator app on your smartphone.

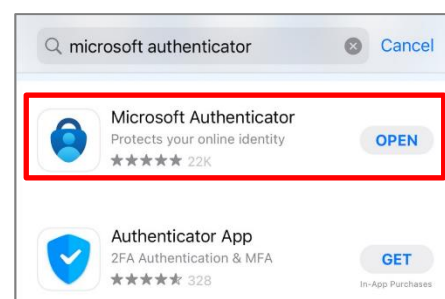


### 1. **On your smartphone**, Install the **Microsoft Authenticator app**.

- a. In your smartphone's app store (such as Google Play or App Store), search for the free **Microsoft Authenticator app** as shown.

*Be aware! Microsoft Authenticator app is free and will not require a subscription.*

Alternatively, you can [get the app on your phone](#) by scanning a QR code with your phone.



**Note:** If you are in a country that does not allow you to access the Google Play/Apple stores please use your phones' manufacturer provided store.

- b. Check that your smartphone operating system will support Microsoft Authenticator, and **install the app**. Leave the app open and go to Part 2.

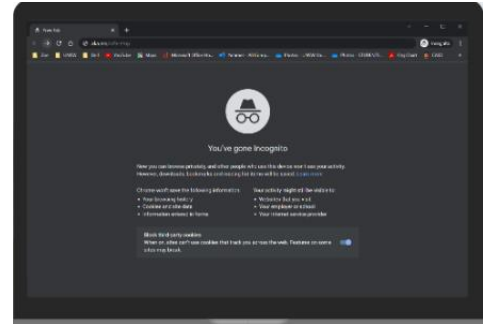
If you already have Microsoft Authenticator app installed on your smartphone, go to Part 2.

## Part 2: Register Microsoft Authenticator on your computer.

Part 2 has 13 steps. Please follow all steps to ensure that registration is complete.

1. **On your computer**, open a web browser, (E.g., Chrome, Microsoft Edge, or Safari) and start an *Incognito*, *InPrivate* or *Private* window by pressing:

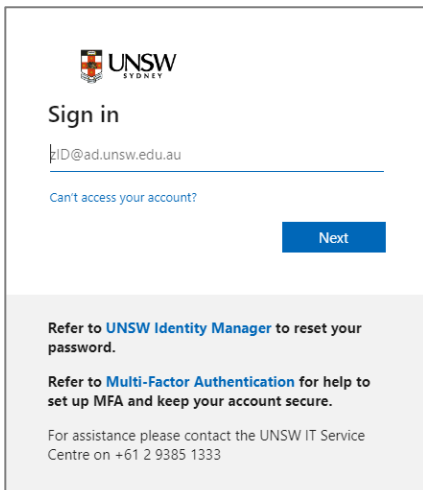
**Ctrl + Shift + n** (for Windows, Linux, or Chrome)  
OR  
**⌘ + Shift + n** (for Mac)



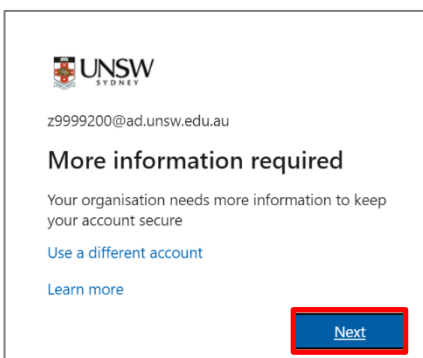
Please close any other active browser windows leaving only the current Incognito/ InPrivate /Private window open.

- a. Copy and paste this url into that window: **<https://aka.ms/mfasetup>**
- b. Press the **Enter** key on your keyboard.

2. **On your computer**, at the *Sign in* window, sign in by entering your `zID@ad.unsw.edu.au` and password.

A screenshot of the UNSW Sydney 'Sign in' page. The UNSW Sydney logo is at the top left. Below it, the text 'Sign in' is displayed. A text input field contains the email address 'zID@ad.unsw.edu.au'. Below the input field is a link that says 'Can't access your account?'. A blue 'Next' button is positioned to the right of the input field. At the bottom of the page, there is a grey box containing the following text: 'Refer to [UNSW Identity Manager](#) to reset your password.', 'Refer to [Multi-Factor Authentication](#) for help to set up MFA and keep your account secure.', and 'For assistance please contact the UNSW IT Service Centre on +61 2 9385 1333'.

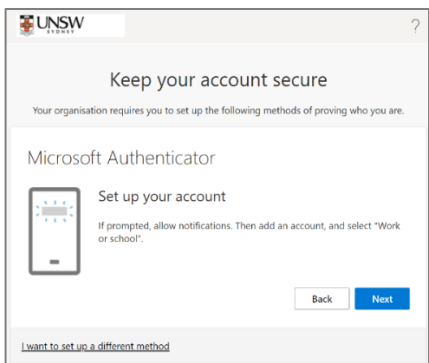
3. **On your computer**, at the *More information required* window, click **Next**.

A screenshot of the UNSW Sydney 'More information required' page. The UNSW Sydney logo is at the top left. Below it, the email address 'z9999200@ad.unsw.edu.au' is displayed. The main heading is 'More information required'. Below this, the text reads: 'Your organisation needs more information to keep your account secure'. There are two links: 'Use a different account' and 'Learn more'. A blue 'Next' button is located at the bottom right of the page, highlighted with a red border.

4. **On your computer**, at the *Start by getting the app* window click **Next**.



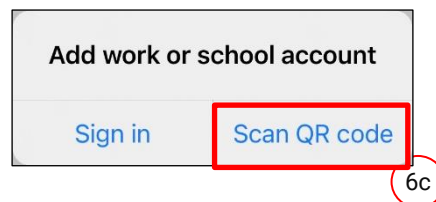
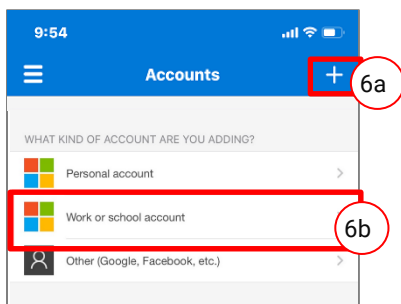
5. **On your computer**, at the *Set up your account* window click **Next**.



You will be shown a QR code on your computer screen.

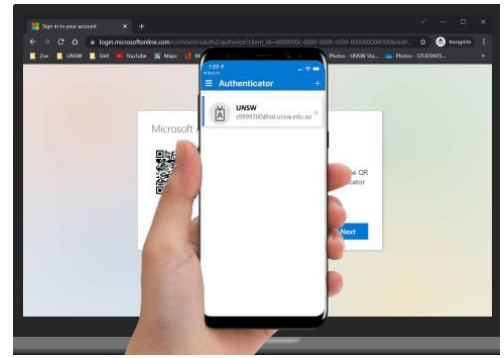
6. **On your smartphone**, Open the Microsoft Authenticator app, allow notifications/access to camera (if prompted), and

- a) Tap the **+** (Plus) sign
- b) Tap **Work or School Account**.
- c) Tap Scan QR code

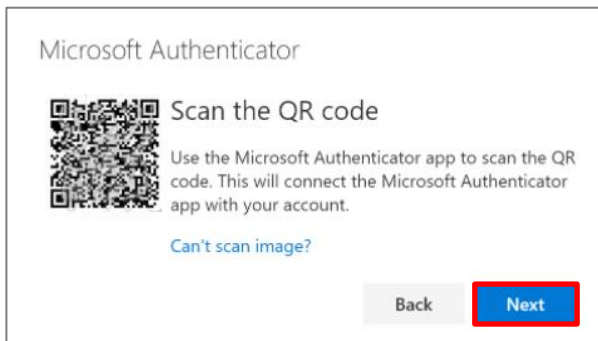


7. **On your smartphone**, use the **Microsoft Authenticator app** to scan the **QR code** shown on your computer screen.

The app should successfully add your work account on your smartphone.



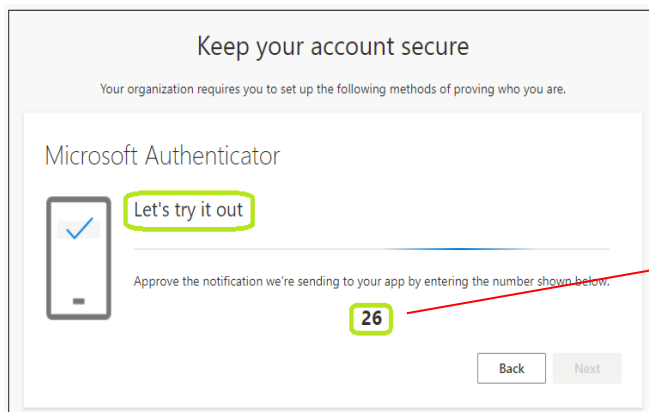
8. **On your computer**, after your phone has recognised the QR code scanned, click **Next**.



*Hint: If you are using a second monitor and having trouble scanning the QR code shown on your second monitor, try moving the QR code screen to your primary monitor, e.g., your laptop monitor.*

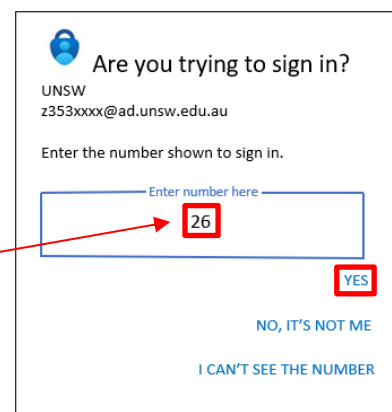
*If you are still unable to scan the QR code, click the **Can't scan image?** option and follow the prompts.*

9. **On your computer**
- You will be presented with the *Let's try it out window* which includes a 2-digit number. Now a push notification will be sent to your smartphone.

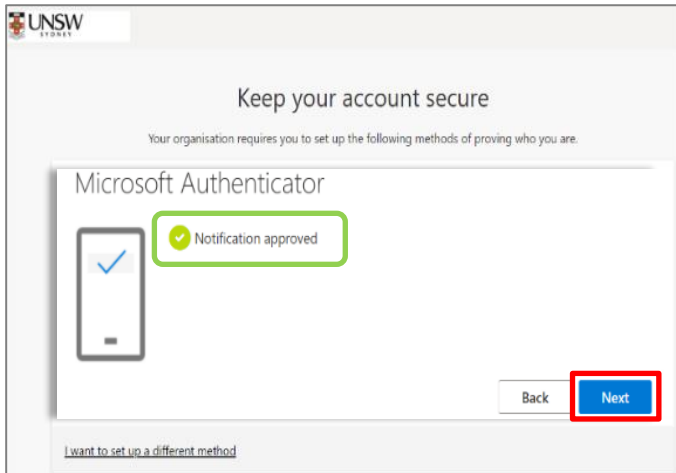


**On your smartphone**

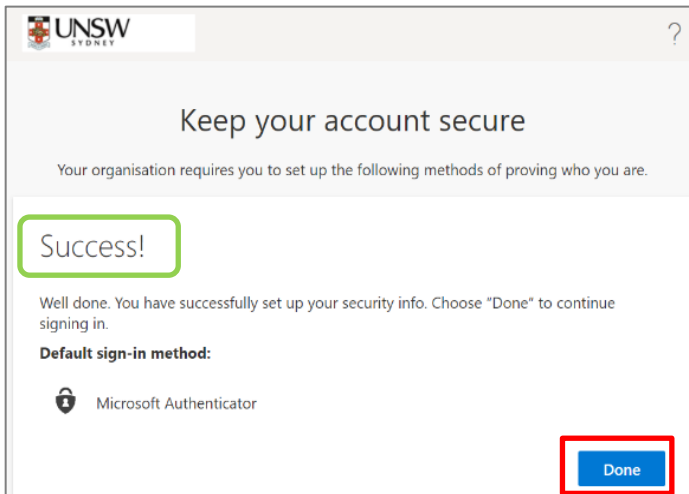
A push notification will ask you to verify your sign-in, enter the 2-digit number from the computer/sign-in screen into your smartphone & click YES.



10. **On your computer**, at the *Notification approved* screen, click **Next**.



11. **On your computer**, at the *Success* screen, click **Done** & close the browser.



**Congratulations**, you have registered your work account (zID) for MFA using the *Microsoft Authenticator* app on your smartphone.