

Set Up MFA Using the Microsoft Authenticator App

To access UTAS **single sign-on (SSO)** applications such as MYLO, UTAS webmail, Student Portal, Multi-Factor Authentication (MFA) is needed. It adds an extra layer of security, helping to keep the University and your student account safe from unauthorized access.



To Complete this task, you will need

- Your Utas email id @utas.edu.au and login password
- A **computer** with internet access
- A compatible **smart phone**
- Please allow up to 10 mins to complete this task

To get started with MFA, you'll only need to do it once using your computer and the Microsoft Authenticator app on your smartphone.

Remember, after setting it up, keep the app on your phone. It's essential for verifying your login when you use University SSO applications from time to time.

Should you ever remove the app from your phone, follow the recovery steps [here](#) or make sure to contact the IT **Service desk** at **03 62261818**. They'll need to reset your account before you can set up MFA again.

Setting up **MFA** involves **two** steps

1. Install the app on your **smartphone**.
2. complete the registration on your **computer**.

If you already have the **Microsoft Authenticator app**, proceed directly to **step 2**.

Part 1: Install the Microsoft Authenticator on your **Smart Phone**



1. On your **smartphone**, download the **Microsoft Authenticator app** for free from your app store (Google Play or App Store).

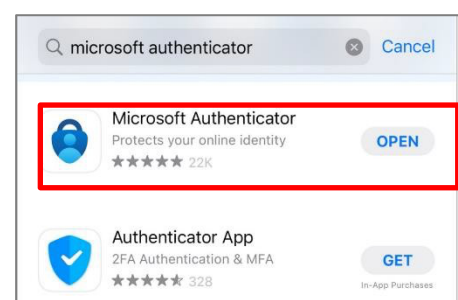
Note: The Microsoft Authenticator app is free and does not require a subscription.

Alternatively, by scanning a QR code from [Authenticator App](#)

Important: If the Google Play/Apple stores are not available in your country, use your phone's manufacturer store instead.

Ensure your smartphone's OS is compatible with Microsoft Authenticator, then install and open the app. Proceed to **Part 2**.

If you already have the app, move directly to **Part 2**.



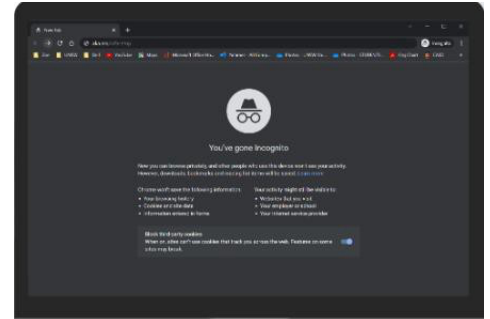
Part 2: Register Microsoft Authenticator on your computer

(make sure you have completed all 9 steps in part 2)

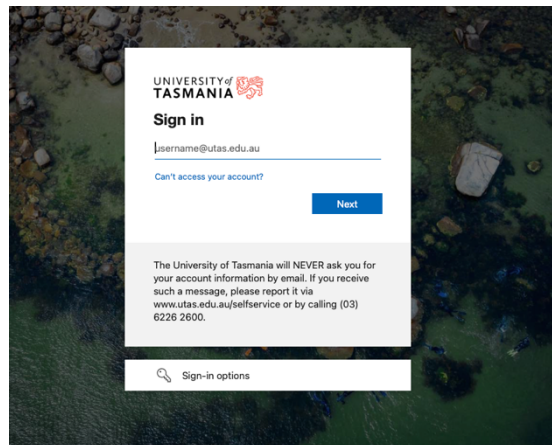
1. **On your computer**, open a web browser, (E.g., Chrome, Microsoft Edge, or Safari) and start an *Incognito*, *InPrivate* or *Private* window by pressing:

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

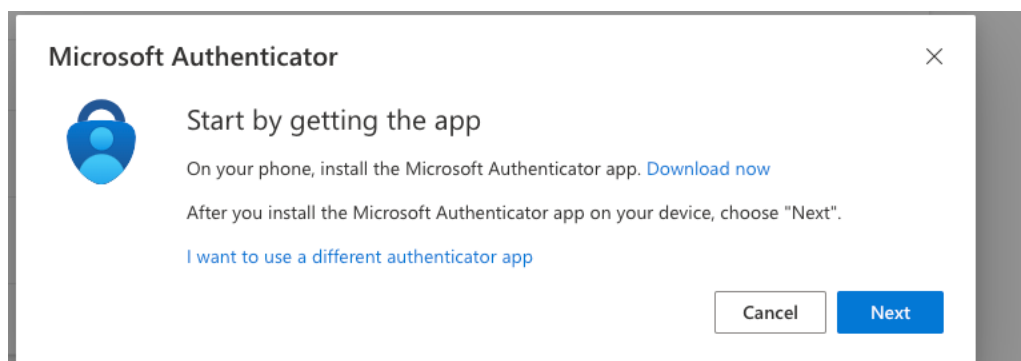
Copy and paste this url into that window: **https://aka.ms/mfasetup**
Press the **Enter** key on your keyboard.



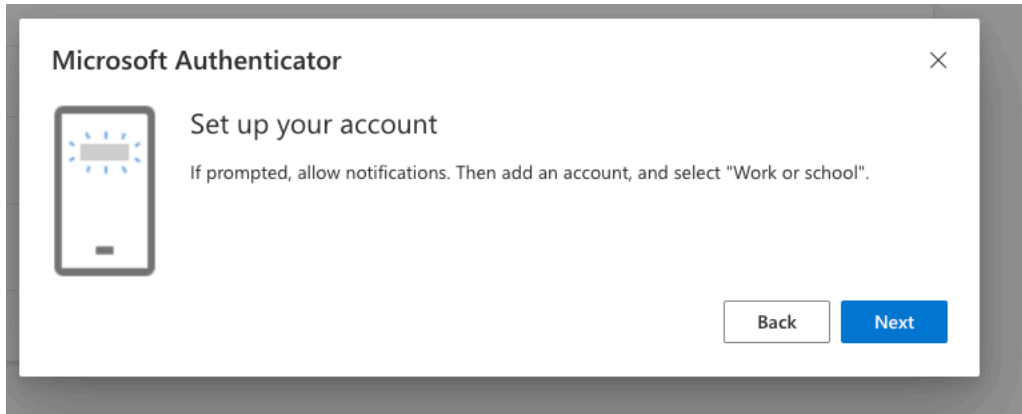
2. **On your computer**, at the *Sign in* window, sign in by entering your Utas email ID @utas.edu.au and password



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

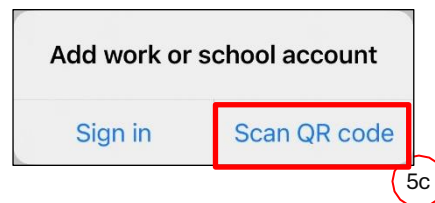
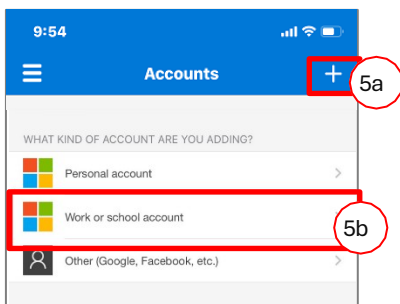


4. On your computer, at the *Set up your account* window click **Next**.



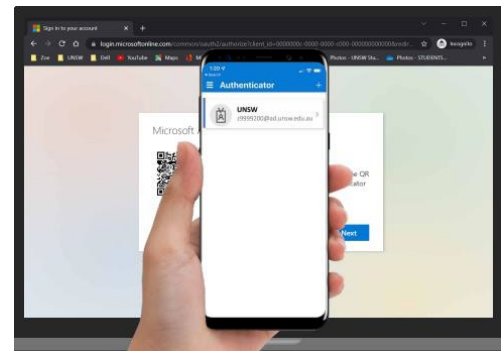
5. On your smartphone, Open the Microsoft Authenticator app, allow notifications/access to camera (if prompted), and

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

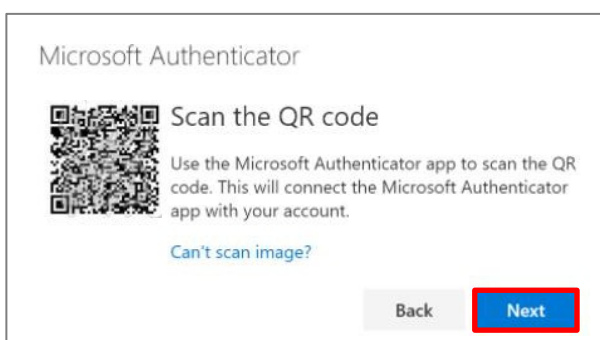


6. On your smartphone, use the Microsoft Authenticator app to scan the QR code shown on your computer screen.

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



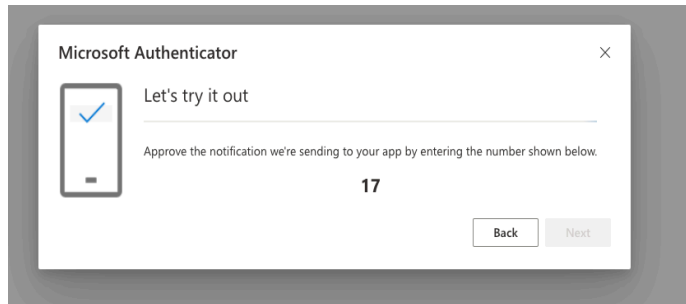
7. On your computer, after your phone has recognised the QR code scanned, click **Next**.



8.

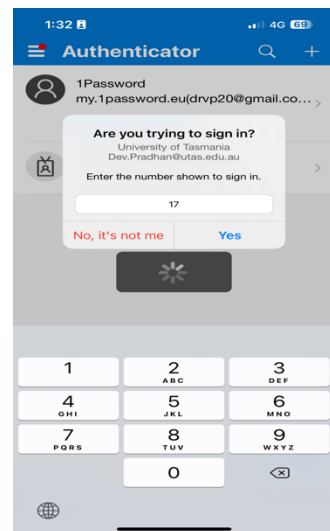
On your computer

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

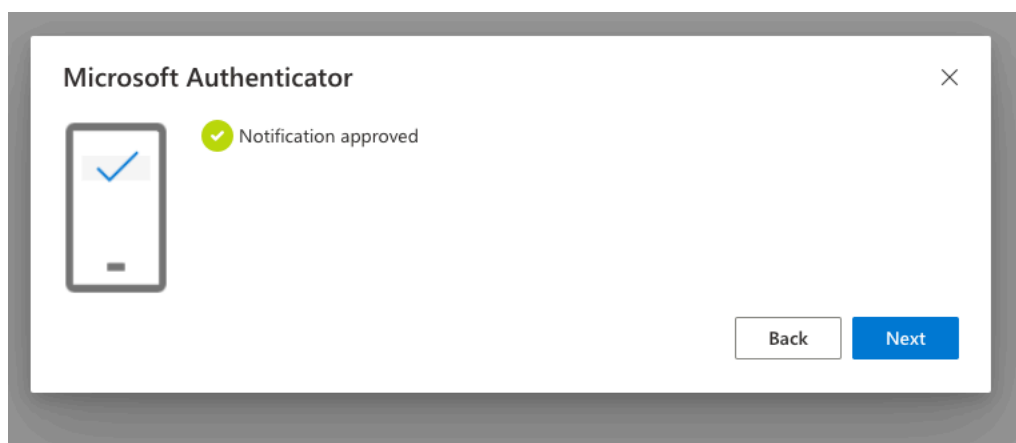


On your smartphone

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.



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



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