Set up Microsoft Authenticator app on a second mobile device

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 Microsoft Authenticator app (with your zID account) on a second mobile device, such as an iPad, and use it as a backup. Note: Microsoft Authenticator app cannot be installed on a computer or laptop.

If you need technical assistance call the **IT Service Centre on 02 9385 1333**. Alternatively visit the MFA website to access all available guides and FAQs.

To follow these instructions, you will need

- Your zID and password.
- Your current smartphone with a data/internet connection.
- Your new device, eg iPad with a data/internet connection.

Instructions

Microsoft Authenticator app can be installed on a second mobile device such as an iPad or other smartphone and used when your primary smartphone is unavailable.

1. **On your other mobile device,** open the app store (such as Google Play or App Store), search for Microsoft Authenticator app. Check that your smartphone operating system will support it, and **install the app**.

   Be aware! Microsoft Authenticator app is free and does not require a 'subscription'.

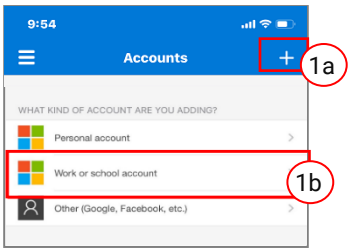
   Alternatively, you can get the app on your device by scanning a QR code with your phone.

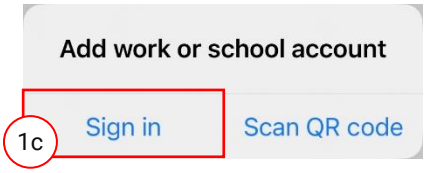
   

   Note: If you are in a country that does not allow you to access the Google Play/Apple stores please use your phones' manufacturer provided store.

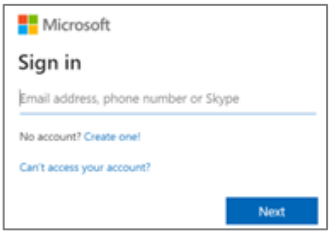
2. **On your other mobile device**, Open the Microsoft Authenticator app, allow notifications/access to camera (if prompted), and

a) Tap the **+** (Plus) sign
b) Tap **Work or School Account**.
c) Tap Sign in





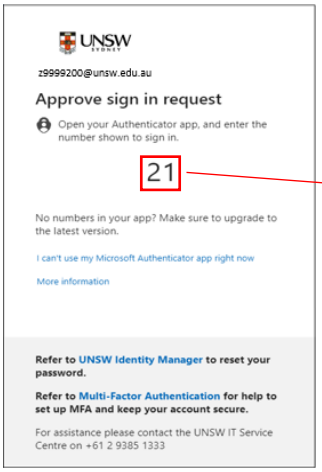
3. **On your other mobile device**, at the *Sign in* window, sign-in using your zID@ad.unsw.edu.au and enter your password when prompted.



4.

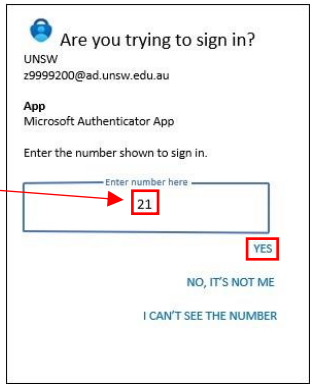
On your other mobile device

When **MFA** is triggered, you will be presented with the *Approve sign-in request* window which includes a 2-digit number. Now a push notification will be sent to **original** smartphone.



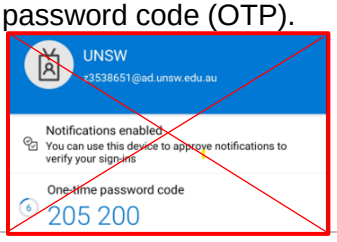
On your original smartphone where you have set up MFA.

A push notification will ask you to verify your sign-in, enter the 2-digit number from the **other mobile device** sign-in screen into your original smartphone & click YES.



If the push notification is not immediately visible open the Microsoft Authenticator App.

Note, the 2-digit number is not your 6-digit one-time password code (OTP).



Congratulations, you have successfully set up the *Microsoft Authenticator* app on your other mobile device.