Set up Microsoft Authenticator app on a second mobile device

Multi-Factor Authentication (MFA) Updated: 24 June 2022

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 a 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 app and if prompted allow notifications then tap Add Account.

   **For apple devices:**
   a) Tap the plus sign (Add Account)
   b) Tap **Work or School Account**.

   **For android devices:**
   c) Tap the 3 dots
   d) Tap **Add Account**
   e) Tap **Add work or school account**

3. **On your other mobile device**, tap **Sign in**

4. **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.

5. You will be presented with the **Approve sign-in** request window (shown).

6. **On your smartphone where you have set up MFA already**, a push verification request has been sent. Tap **Approve**.
   
   If the push notification is not immediately visible, open the Microsoft Authenticator app.

7. **On your other mobile device**, choose your preferred sign-in method and tap **Finish** to complete.
Important: Test that the Microsoft Authenticator app is now active on your other mobile device:

8. **On your computer**, in a web browser, (E.g., Safari, Chrome) open a *Private or Incognito* window. Copy and paste `https://aka.ms/mfasetup` into the url of that window.

9. **On your computer**, at the *Sign in* window, use your `zID@ad.unsw.edu.au` and password and then tap *Next*.

10. **On your other mobile device**, a push notification will ask you to verify your sign-in, tap Approve.

**Congratulations**, you have successfully set up the *Microsoft Authenticator* app on your other mobile device and tested that it works as a backup.