Set up MFA when Microsoft Authenticator app is unavailable in your smartphone's app store

Multi-Factor Authentication (MFA)

Updated: 14 July 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.

Only use this guide when the Microsoft Authenticator app is not available in your smartphone's app store. This process requires you to scan the QR code and install the *Lenovo app store* first so that you can then download Microsoft Authenticator app on your smartphone (Part 1 instructions). Part 2 then follows on as the instructions to complete the MFA registration on your computer.

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:

- Set up MFA using Microsoft Authenticator (if you can download the app from the phone app store)
- Use Microsoft Authenticator
- Use Microsoft Authenticator without a data/internet connection
- Transfer Microsoft Authenticator app to a new 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
- FAQs for staff
- FAQs for students.

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

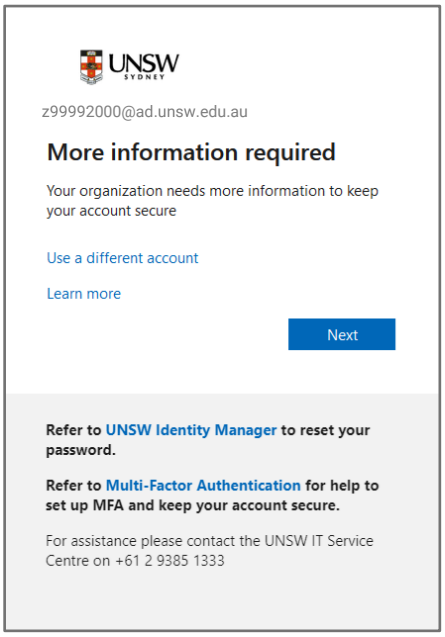
You only need to set up MFA once, using your computer and the Microsoft Authenticator app on your smartphone. After setup, do not delete/uninstall the app from your smartphone. You will need this app to verify your login when accessing University SSO applications periodically.

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.

*If the screen contains a counter, then you have a limited amount of time to defer the set up. Once the counter expires you will not be able to ac**cess any SSO applications until you set up MFA**.*



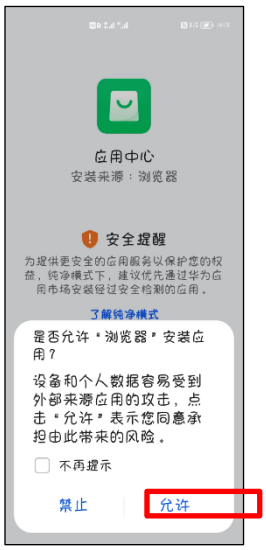
This instruction to set up MFA is in two parts: Part 1 is the installation of the app on your smartphone and Part 2 is to finish the registration using your computer.

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 (when you do not have access to the app in your smartphone app store).

1. Go to Authenticator (lenovomm.com) and scan the QR code shown to install the Lenovo app store on your smartphone.

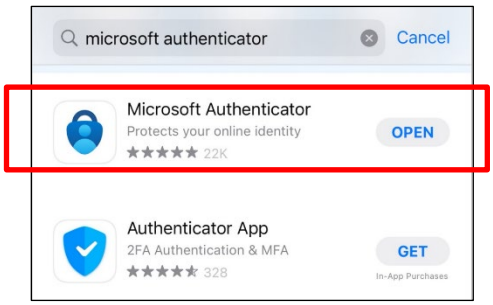
2. Tap *Allow* to give permission for the app to install and continue



3. Tap *Continue installation* to proceed.

4. Once the Lenovo app store is installed, search for the free Microsoft Authenticator app as shown.

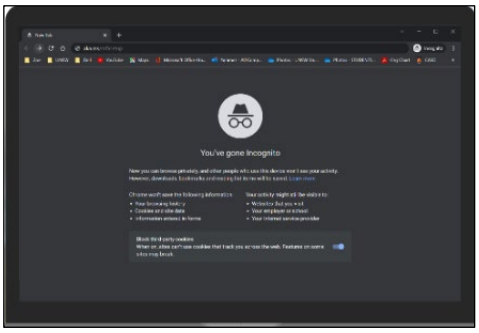
Be aware! Microsoft Authenticator app is free and will not require a subscription.



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

Part 2: Register Microsoft Authenticator on your computer.

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:

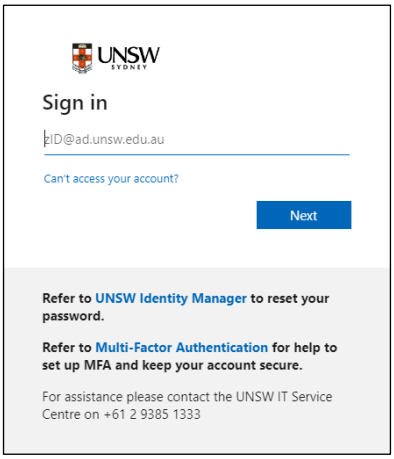


   Ctrl + **Shift** + **n** (for Windows, Linux, or Chrome)
   OR
   ⌘ + **Shift** + n (for Mac)

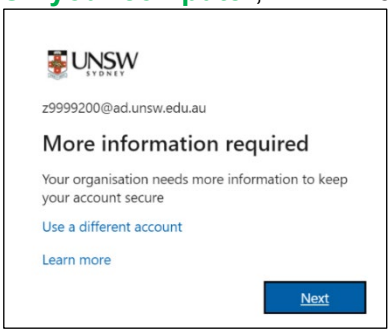
   Please close any other active browser windows leaving only the current Incognito/ InPrivate /Private window open.

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

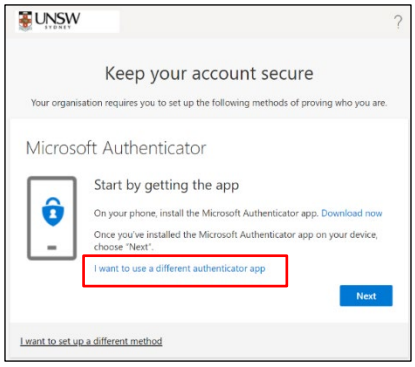
2. **On your computer**, at the *Sign in* window, enter your zID@ad.unsw.edu.au and password.



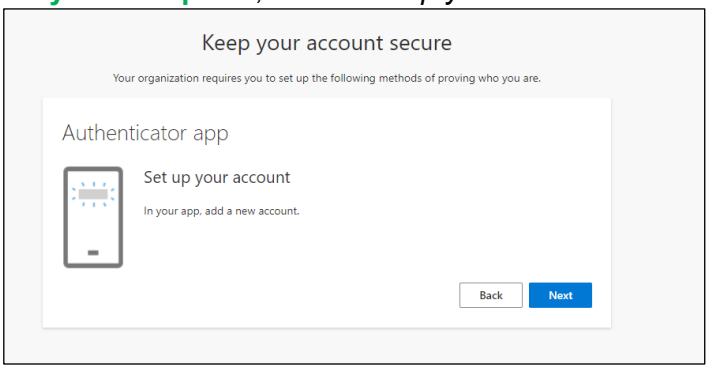
3. **On your computer**, at the *More information required* window, click **Next**.



4. **On your computer**, at the *Start by getting the app* window click **I want to use a different authenticator app**.

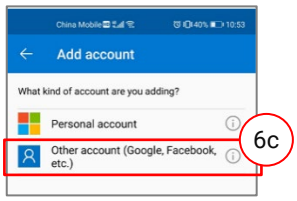


5. **On your computer**, at the *Set up your account* window click **Next**.



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

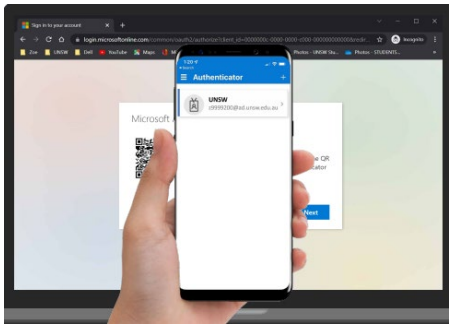
6. **On your smartphone,** within the Authenticator app:



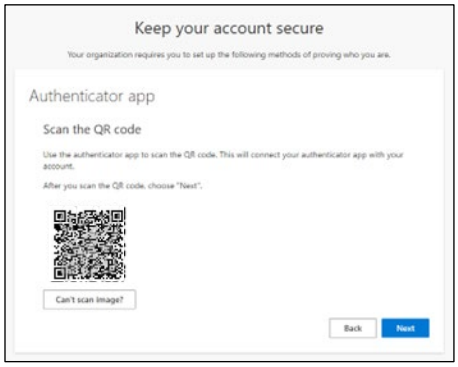
a) Tap the 3 dots
b) Tap **Add Account**
c) Tap **Other account (Google Other Facebook, etc)**

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

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

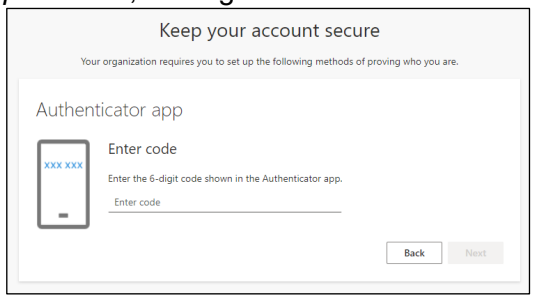


8. **On your computer**, after your phone has recognised the QR code scanned, click **Next.** If you are unable to scan the QR code, click the **Can't scan image**? option and follow the prompts.

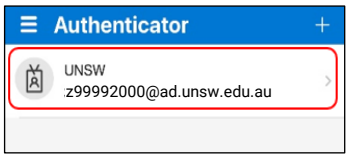


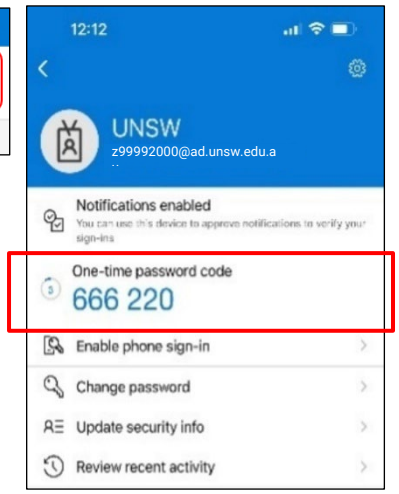
<u>Hint:</u> If you are using a second monitor and having trouble scanning the QR code shown on your second monitor, try moving the QR code screen to your primary monitor, e.g., your laptop monitor.

9. **On your computer**, the *Keep your account secure* window requires you to enter a *One-time password*, a 6-digit code from within the Authenticator app.



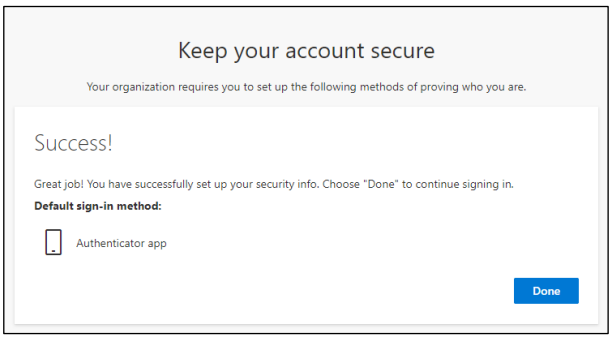
10. **On your smartphone**, open the Authenticator app and tap on your zID account to see the One-time password code.



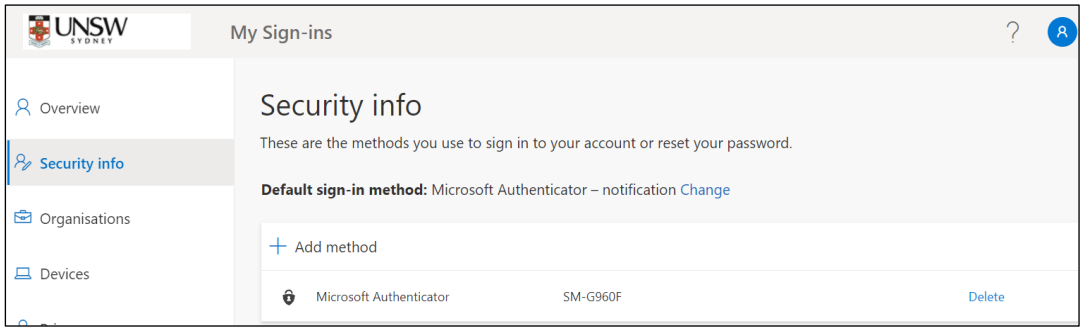


Note: *The one time 6-digit code changes after 30 seconds. If this happens when you are entering it, use the next code.*

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



12. **On your computer**, the *My Sign-ins* window displays the Microsoft Authenticator that you just set up. **Close the browser window**.



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