Authenticator app needs to be installed on your smartphone before completing the registration on your computer.

MFA website video

1. Set up MFA using Microsoft Authenticator on your smartphone
2. Set up MFA when Microsoft Authenticator is unavailable in your smartphone app store *(Note useful for some China-based students)*
3. Set up MS Authenticator app on a second mobile device as a backup, after setting up MFA on your primary mobile device.
4. Use Microsoft Authenticator
5. Use Microsoft Authenticator without a data/internet connection or when push notifications are not possible.
6. Transfer Microsoft Authenticator app to a new phone from your old phone
7. Set up and use a YubiKey
8. Set up and use a YubiKey for non-Windows devices such as Mac and Linux.

Contents - Click on the question to be taken to the answer.

Student FAQs – Setting up MFA

1. What is Multi-Factor Authentication (MFA)?
2. Who needs to set up MFA?
3. How do I set up MFA and use the Microsoft Authenticator app?
4. Which MFA verification methods does UNSW support?
5.

my privacy

9. How do I use Microsoft Authenticator as a backup factor?
10. Can I download the Microsoft Authenticator app on my computer?
11. Can I use other authentication applications such as Authy and Google Authenticator?
12. My phone O/S cannot be updated to support an authenticator app. What can I do?
13. What operating system do I need on my smartphone to download Microsoft Authenticator?
14. Can I use the Microsoft Authenticator app if I already have it set up on my phone?
15.

when setting up MFA. How do I add my zID account to the app?

16. How do I get verify if I don't have data connectivity?

Student FAQs – Using MFA

17. What are the security benefits of MFA?
18. Can I turn off or opt out of MFA?
19. When will I be prompted to verify my sign-in?
20. Can I use Microsoft Authenticator to verify my sign-in on multiple computers?
21. I'm not receiving push notifications from my phone when prompted to verify my sign-
have data connectivity.
22. How do I transfer the Microsoft Authenticator app from an old to a new smartphone?
23.

How d0 g0 GwntG3(t)11(i)-l(a)-3(t)1aA ad the Mrt?

1. What is Multi-Factor Authentication (MFA)?

   MFA is a security feature that helps protect your UNSW account through a second identity verification factor in addition to your zID and password.

   Using MFA helps to secure your account by adding an additional verification step that relies on possession of a trusted device, such as your smartphone, and this makes it much more difficult for a cyber-criminal to compromise an account.

   The goal of MFA is to keep your account secure by creating an additional line of defence to make it more difficult for unauthorised persons to access your and UNSW's resources.
   Refer to the *How MFA works* section of the

6. I cannot use the Microsoft Authenticator app because I have an older smartphone that does not support Microsoft Authenticator.

   Please attempt to upgrade your smartphone operating system to the latest version required for

10. Can I download the Microsoft Authenticator app on my computer?

    No. The Microsoft Authenticator app is a mobile application that can only be downloaded on a mobile smartphone or smart device such as an iPad

15. I do not have the option to ‘add work or school account’ when setting up MFA. How do I add my zID account to the app?

Microsoft Authenticator allows you to set up multiple accounts, however if you find that you already h

You then have two options:

a. You can uninstall the app and start again. Doing this will require you to set up the other organisation’s account also. OR

b. You can continue the setup by following this guide from Part 2. This will set up the zID account

17.

21. I'm not receiving push notifications from my phone when prompted to verify my sign-in, e.g., when I don't have data connectivity.

    If you are not receiving push notifications on your Microsoft Authenticator app or your phone does not have data connectivity:

    a) At the Approve sign-in request window, click on

'Airplane mode' or data (internet) connectivity is unavailable. The 6-digit code is refreshed every 30 seconds.

Note: SMS or email notifications are not used at UNSW.

Return to Contents

28. I'm concerned about the Microsoft Authenticator app draining my phone battery.

The Microsoft Authenticator app uses minimal battery on your smartphone. If the battery usage continues to be a concern, Microsoft recommends using the one-time passcodes which don't require you to be on the Internet or connected to data, so you don't need phone service to sign in. Additionally, because the app stops running as soon as you close it, it won't drain your battery.

Return to Contents

29. My one-time passcodes are not working. What should I do?

Make sure the date and time on your device are correct and are being automatically synced. If the date and time are wrong, or out of sync, the code won't work.

the guide to set up MFA where Microsoft Authenticator is not available in your smartphone app store.

Return to Contents

33. What can I do if my country blocks push notifications on my smartphone/device?

If your country blocks push notifications on your smartphone or you are not receiving push notifications on your Microsoft Authenticator app:

a) At the Approve sign-in request window, click on I can't use my Microsoft Authenticator app right now

b) Then select *Use a verification code from my mobile app* and enter the 6-digit One-Time Password code shown in your Microsoft Authenticator app and click *Verify*.

Note: The 6-digit code updates every 30 seconds.

For detailed instructions, refer to the *How to use Micro to the*