



Frequently Asked Questions – for staff

Multi-Factor Authentication (MFA)

Updated: 18 January 2023

Multi-Factor Authentication (MFA) is a requirement to access UNSW single sign-on applications. MFA provides an additional layer of security to protect the University and your zID account from unauthorised access. Our University is using Microsoft Authenticator app, which needs to be installed on your smartphone before completing the MFA registration on your computer.

For more help, call the dedicated MFA support team at the IT Service Centre on 02 9385 1333. Alternatively visit the [MFA website](#) to access all information including support [guides and videos](#).

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

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. Can I download the Microsoft Authenticator app on more than one device?
6. I cannot use the Microsoft Authenticator app because I do not own a smartphone.
7. I cannot use the Microsoft Authenticator app because I have an older smartphone that does not support Microsoft Authenticator.
8. I cannot use the Microsoft Authenticator app because I am not allowed to carry my smartphone with me, as part of my UNSW conditions of employment.
9. I do not want to download the Microsoft Authenticator app on my smartphone because I am concerned about my privacy
10. I do not want to download the Microsoft Authenticator app on my smartphone because I am concerned about using my personal smartphone.

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

Refer to the [How MFA works](#) section of the [MFA website](#) for details.

[Return to Contents](#)

2. Who needs to set up MFA?

Everyone with a zID account, including staff, students, and affiliates who access [UNSW single sign-on \(SSO\)](#) applications.

[Return to Contents](#)

3. How do I set up MFA and use the Microsoft Authenticator app?

Install the Microsoft Authenticator app and finish the registration on your computer.

Refer to the [Guides & Videos](#) section on the [MFA website](#) to access the [Set up MFA using Microsoft Authenticator](#) guide or watch this [introduction video](#), at the bottom of the MFA Website.

5. Can I download the Microsoft Authenticator app on more than one device?

Yes. It is recommended that you install it on another device (e.g., iPad) so that it can be your backup should you forget/lose your smartphone.

Refer to the [Guides](#) section on the [MFA website](#) to learn how to [set up Microsoft Authenticator on second mobile device](#).

[Return to Contents](#)

9. I do not want to download the Microsoft Authenticator app on my smartphone because I am concerned about my privacy

Multi-

protect your University account (zID) from unauthorised access. Information that is provided to the University via MFA is collected for the sole purpose of facilitating this additional security. The

11. I don't want to download the Microsoft Authenticator app on my smartphone because I am concerned about the performance impact on my smartphone.

The Microsoft Authenticator app;

- uses minimal resources on your phone,
- prompts you only when it needs you to verify your current login through the app,
- takes up minimal space on your device,
- uses minimal battery, and
- can operate offline, without internet via the One-Time Password (rolling 6-digit code) that

16. Can I use the Microsoft Authenticator app if I already have it set up on my phone for MFA use at another organisation?

Yes, Microsoft allows you to set up multiple accounts. When setting up MFA for UNSW, within the Microsoft Authenticator select *Add account* then *Work/School account* and follow the guide: [Set up MFA using Microsoft Authenticator](#), from Part 2.

Refer to the [Guides & Videos](#) section on the [MFA website](#) to access the set-up MFA guide.

[Return to Contents](#)

17. 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 have an account set up from another organisation,

You then have to

19. What is Microsoft Azure AD?

-Factor

Authentication (MFA) and Single Sign-On (SSO). Microsoft provides the Microsoft Authenticator app for end users to download and use MFA.

[Return to Contents](#)

20. Can MFA be set up to be optional to specific applications?

No. MFA will be applied to all UNSW single sign-

- Your name
- Your address
- Bank details
- Your work and files
- Any other information you have provided

27. 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

- 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

Robust

FAQs Using a YubiKey

39. How can I register an alternative authenticator on my UNSW-provided YubiKey?

The alternative supported authenticator for my UNSW-provided YubiKey is:

Key: A YubiKey is