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.

CRICOS Provider Code 00098G

FAQs – Setting up MFA

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 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.

Return to Contents

4. Which MFA verification methods does UNSW support?

Microsoft Authenticator app is the authenticator used and supported by the University.

Refer to the *Set up MFA* section on the MFA website for details.

The alternative supported authenticator is a physical security token known as a YubiKey. Staff can request a UNSW provided YubiKey when Microsoft Authenticator is not suitable.

Refer to *Your MFA Alternatives* section on the MFA website for full details (limitations, request process, etc).

Return to Contents

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

6. I cannot use the Microsoft Authenticator app because I do not own a smartphone.

UNSW Staff who do not own a compatible smartphone have an option to request an alternative authenticator: a UNSW provided YubiKey.

Refer to *Your MFA Alternatives* section on the MFA website for full details (limitations, request process, etc).

Return to Contents

7. 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 Microsoft Authenticator app. When in your phone's app store, check the operating system version required for Microsoft Authenticator app.

Return to Contents

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.

Please contact the dedicated MFA support team at the IT Service Centre on 02 9385 1333 and provide the conditions whereby you are not allowed to carry your smartphone with you while working at UNSW. Where there is a need, an alternative authenticator, a YubiKey, will be provided to staff.

Refer to the *Your MFA Alternatives* section on the MFA website for full details (limitations, request process, etc).

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-Factor Authentication (MFA) is the University's method for providing additional security to 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 information collected will only be accessible to University staff who require access to administer the Azure MFA service.

The University is using a third-party application, Microsoft Authenticator, to provide the MFA service to University zID account holders.

Both Microsoft and UNSW have no access to the app on your phone and cannot;

- view any of your data,
- other apps installed,
- monitor calls, or
- track your location.

The app requires the internet for push notifications but can also operate offline via the One-Time Password, a rolling 6-digit code, that updates every 30 seconds.

The Microsoft Authenticator app does not link to a phone number.

Refer to the *Tips and Privacy Information* section of the MFA website for more information on how the University is managing personal information collected via MFA.

Return to Contents

10. I do not want to download the Microsoft Authenticator app on my smartphone because I am concerned about using my personal smartphone.

Verification via a push notification on the Microsoft Authenticator app is easy and convenient if you already access UNSW single sign-on applications such as Outlook, SharePoint, and Teams on your smartphone.

Other benefits of using the Microsoft Authenticator app on your smartphone:

- Easy to use push notification.
- Free and available for Android and Apple devices.
- Takes up minimal space on your device.
- Uses minimal battery.
- Does not have access to your phone data/camera/apps
- Can be installed on other devices as a back-up.
- Can operate without internet connection by way of a one-time passcode.
- Used and trusted by over an estimated 50M users across the world and more than 10 universities across Australia.

UNSW staff may request an alternative verification method; a YubiKey, where they are unable to use Microsoft Authenticator app on their smartphone.

Refer to the *Your MFA Alternatives* section on the MFA website for full details (limitations, request process, etc).

Return to Contents

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 updates every 30 seconds. This option uses no internet data.

Return to Contents

12. How do I use Microsoft Authenticator as a backup factor?

Microsoft Authenticator can be used as a backup factor on another mobile device when your primary smartphone, is unavailable.

Refer to the *Guides & Videos* section on the MFA website to learn how to set up MFA and use Microsoft Authenticator.

Return to Contents

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

The Microsoft Authenticator app is a mobile application and not available for download on a computer.

Return to Contents

14. Can I use other authentication applications such as Authy and Google Authenticator?

Other authentication applications such as Authy or Google Authenticator are not supported by the IT Service Centre. Microsoft Authenticator and University provided YubiKeys are the only authenticators supported by UNSW.

Return to Contents

15. What operating system do I need on my smartphone to download Microsoft Authenticator?

Microsoft Authenticator is the supported authenticator used by UNSW. When installing Microsoft Authenticator app from your app store, check that your smartphone has the required operating system version.

To find your smartphone operating system:

iOS (Apple): Go to your devices' home screen, tap the *Settings* icon, then select *General* and *About*.
Android: Go to your devices' home screen, tap *Settings*, then select *About Phone* or *About Device*.

Return to Contents

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, it may not present the option to 'add work or school account' for your zID account.

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 in Microsoft Authenticator app but you will need to always use the One-time password code to verify your sign-in when prompted.

Refer to the *Guides & Videos* section on the MFA website to access the set-up MFA guide.

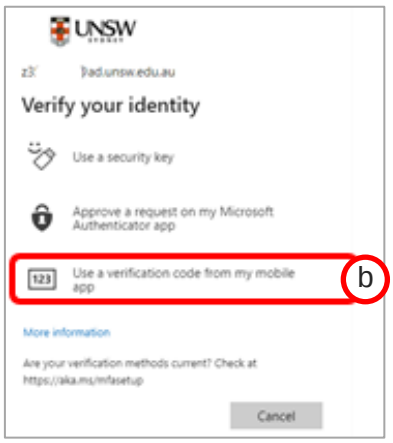
Return to Contents

18. How do I get my code if I don't have data connectivity?

The Microsoft Authenticator app provides a One-Time Password code when you do not have data connectivity, or you have elected to set *Airplane* mode on.

a) When presented on your computer with the Approve sign in request screen, 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 Passcode shown in your Microsoft Authenticator app.



For detailed instructions, refer to the *How to use Microsoft Authenticator without an internet connection* guide found in the *Guides & Videos* section on the *MFA website.*

Return to Contents

19. What is Microsoft Azure AD?

Microsoft Azure AD is UNSW's technology for authentication services including Multi-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-on applications and services. It is not possible to opt out of MFA or to set MFA to authenticate only on specified apps.

Return to Contents

21. Can Microsoft Authenticator be used for Linux server authentication?

No. Microsoft Authenticator is not currently available for such authentication, LDAP will be retained for now.

Return to Contents

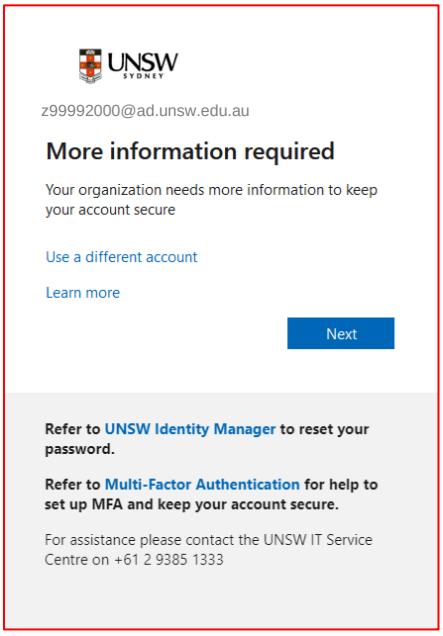
22. Why am I getting the More Information Required screen / counter when accessing SSO applications?

If you are presented with a **More information required** window when accessing single sign-on (SSO) applications such as Moodle, it is an indicator that you have not set up MFA and that MFA is enforced on your zID account.

At this point you must set up MFA before you can access the SSO application.

Refer to the SSO website to understand what applications are on SSO.

Return to Contents



FAQs – Using MFA

23. What are the security benefits of MFA?

MFA helps protect accounts by adding an additional verification step to confirm the identity of users. Even if a cyber-criminal knows an individual's password, the added verification step (by tapping ***No, It's Not Me*** when unknown MFA prompt occurs) will stop them accessing user accounts and key information such as:

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

If you select ***No, it's Not Me***, a Report Fraud message will appear. You can then select '**Report'** and the fraud attempt will be sent to UNSW IT Cyber Security Operations team for investigation.

Return to Contents

24. Can I turn off or opt out of MFA?

MFA is a mandatory requirement at UNSW, as per Cyber Security Policies and Standards, when accessing UNSW single sign-on (SSO) applications.

Return to Contents

25. When will I be prompted to verify my sign-in?

MFA will apply when you sign-in to UNSW single sign-on (SSO) applications. Verification will be required at least once every 30 days per device when accessing an SSO application and more often when accessing applications with a higher risk profile, such as the VPN will be more frequent (e.g. 12 hours)

You won't be asked to verify again unless;

- You use another computer, such as one on a lectern or a shared (library) computer,
- You use a new browser,
- You have cleared your internet browser cache/ cookies, or
- Any time you sign in from a location that is vastly different from the location you usually sign into or a country that is different to the country of your last login.

Note: Our MFA solution is adaptive, and you may be prompted to verify unexpectedly at other times if it considers that a risk-based event has occurred e.g., appear to have conducted impossible travel or connect to an unfamiliar internet connection.

Always carry your authenticator with you when accessing UNSW single sign-on applications.

Return to Contents

26. Can I use Microsoft Authenticator to verify my sign-in on multiple computers?

Yes. You can use Microsoft Authenticator to verify your sign-in on multiple computers. Microsoft Authenticator will treat a computer as *new* if it has not been used in the last ten authentications. Any new computer will trigger an MFA verification prompt.

Return to Contents

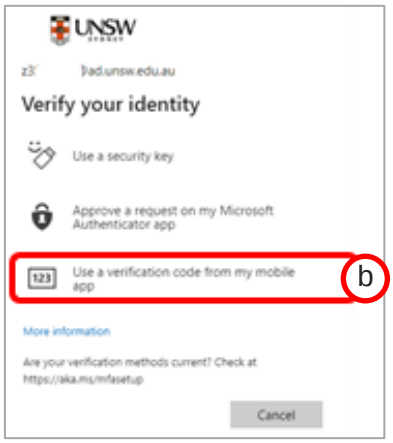
27. I'm not receiving push notifications from my phone when prompted to verify my sign-in, e.g., when I don't have data connectivity.

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 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 Microsoft Authenticator without an internet connection* guide found in the *Guides & Videos* section on the *MFA website.*

Return to Contents

28. How do I transfer the Microsoft Authenticator app from an old to a new smartphone?

For detailed instructions, refer to the *Transfer Microsoft Authenticator to a new phone* guide found in the *Guides & Videos* section on the *MFA website.* The guide will assist you through the process of transferring MS Authenticator app from your old to your new smartphone.

Note: you need both your new and old smartphone when following the guide. If your old phone is lost or unavailable, contact the IT Service Centre on 02 9385 1333.

Return to Contents

29. Will MFA be prompted on community/public computers used in the library (e.g., computers that can be used without a zID)?

No. MFA is only required when you log into a UNSW single sign-on (SSO) application where you need to enter your username (zID) and password.

Return to Contents

30. How will MFA work for staff/students who use lecterns, counters, and shared computers?

MFA will be prompted when accessing UNSW single sign-on applications when using lecterns and shared computers for the first time. Please ensure you have your smartphone with you for verification.

Note: UNSW staff using a YubiKey must remember to carry it everywhere. YubiKeys need to be inserted into the USB port of a computer, tapped, and the associated security pin entered.

Refer to the *Your MFA Alternatives* and *Guides & Videos* sections on the MFA website for details.

Return to Contents

31. How will MFA work for shared mailboxes/delegated access?

If you have access to a shared mailbox or have been given access to someone else's mailbox/calendar, you may be prompted to MFA when signing into your Outlook account using your zID and password.

Return to Contents

32. What do I do if my phone is lost, forgotten or unavailable?

Contact the IT Service Centre on 02 9385 1333 for assistance to MFA. Note: ID verification will be required. If you have installed Microsoft Authenticator on a backup device, you can use it to verify.

Return to Contents

33. How is the Microsoft Authenticator app accessible?

The Microsoft Authenticator app is compliant with the global W3C Web Content Accessibility Guidelines (WCAG 2.1), which also applies to mobile web apps. The WCAG document explains how all digital content is more accessible to people with disability. One of the key objectives of the guidelines is to ensure that the Microsoft Authenticator app content is directly accessible.

Quick Reference Guide of the WCAG 2.1 supported features - MFA accessibility is based on the principles of 'Perceivable', 'Operable' 'Understandable' and 'Robust', which include the following supported features:

Perceivable

- Provide *text alternatives* for non-text content.
- Provide *captions and other alternatives* for multimedia.
- Create content that can be *presented in different ways*, including by assistive technologies, without losing meaning.
- Make it easier for users to *see and hear content*.

Operable

- Make all functionality available from a *keyboard*.
- Give users *enough time* to read and use content.
- Do not use content that causes *seizures* or physical reactions.
- Help users *navigate and find content*.
- Make it easier to use *inputs other than keyboard*.

Understandable

- Make text *readable and understandable.*
- Make content appear and operate in *predictable* ways.
- Help users *avoid and correct mistakes.*

Robust

- Maximize *compatibility* with current and future user tools.

Return to Contents

34. What verification methods are available through the Microsoft Authenticator app?

Push Notification and One-Time Password (OTP) are available via the Microsoft Authenticator app.

The One-Time Password code within the Microsoft Authenticator app is available should your phone be in 'Airplane mode' or data (internet) connectivity is unavailable. The 6-digit code is refreshed every 30 seconds. Refer to the Use Microsoft Authenticator without a data connection .

Return to Contents

35. 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

36. 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.

Return to Contents

37. When should I use the *Lost device? Sign out everywhere* option on the *My Sign-ins* window?

Signing out of everywhere is a good security practice when you have lost your authentication device (mobile phone with authenticator app or YubiKey). This will sign you out of all your current application sessions.

Return to Contents

38. How will MFA work in labs and other restricted areas?

If the lab is designated a UNSW restricted area, the project is currently undertaking an assessment of technical options available in line with the UNSW restricted access areas policies and procedures. A strategic solution is currently being prioritised by the MFA technical team. Once approved, impacted stakeholders will be informed, and this FAQ updated.

Return to Contents

FAQs – Using a YubiKey

39. How can I request an alternative authenticator: a UNSW provided YubiKey?

The alternative supported authenticator for staff is a UNSW provided YubiKey. A YubiKey is a physical security token when Microsoft Authenticator is not suitable. UNSW provided YubiKeys must be returned when no longer required or the individual leaves UNSW.

Refer to the *Your MFA Alternatives* section on the MFA website for full details (limitations, request process, etc).

Return to Contents

40. Can I use a YubiKey to authenticate access to UNSW services on my mobile phone?

No. YubiKeys are available to UNSW staff only where Microsoft Authenticator is not suitable.

Refer to the *Your MFA Alternatives* section on the *MFA website* for full details and limitations.

Return to Contents