USER GUIDE

MULTIFACTOR AUTHENTICATION (MFA) FREQUENTLY ASKED QUESTIONS

What is Multi-Factor Authentication (MFA)

MFA is a multi-step login process which uses two factors to verify your identity: something you know (your login details) and something you have (your smart phone). This extra layer of security helps protect accounts from cyber crime by ensuring that only the legitimate user can log in.

What is MFA registration?

MFA registration is required in order to synchronise your device with your UniSC account and set up MFA. It takes around 5 minutes.

Which Authenticator app should I be using?

Microsoft Authenticator is the preferred app for use at UniSC. It is the most secure, reliable, and easy-to-use option. Microsoft are always working on new features, bug fixes, and performance improvements. Ensure you stay updated with the latest Android and iOS version for the best (and safest) authentication experience.

I have an existing authentication app. Can I continue to use this?

Yes, you can. However if you choose to use an authentication app other than the Microsoft Authenticator, it will not be supported by the IT Student Help Desk.

The app I downloaded is asking me to pay for it. Is this the right app?

The Microsoft Authenticator app is FREE. If the app you have downloaded is asking you to pay for it, please uninstall it and install the Microsoft Authenticator app instead. If you have already paid for the app, contact the app store for a refund.

Is registering a device agreeing to give UniSC access to my device?

Registering a device gives you access to UniSC's services but does **not** allow UniSC to access to your device.

Do I need to restart my computer after I have activated MFA on my device?

Yes. It is recommended that you restart your computer once you have had MFA activated to provide your browsers with the ability to reset any saved cookies.

How is my location information used and stored?

UniSC has not enabled any location tracking for the Authenticator app. We have configured restricted destinations from which new app registrations can be completed based upon the "Do Not Travel" listing from smarttraveller.gov.au. This location is estimated based on the internet address of the device you are logging in from (not necessarily your phone).

I do not want to or cannot use my personal phone. What options do I have?

MFA is mandatory for all users across the University. If it is impossible for you to use your phone, you can apply for an exception by completing the Exception Request Form and we will work with you to find a solution.

How do I apply for an MFA exception?
To apply for an exception, you can complete the MFA Exception Request Form.

Will the app drain my phone battery?
No. The app stops running as soon as you close it so it won't drain your battery.

What are the codes in the app for?
When you open Authenticator, your accounts will have six- or eight-digit numbers visible in the full screen view of the account (accessed by tapping the account tile). These codes can be used when notifications prompts are unavailable (eg. your device is not connected to the Internet).
After you sign in with your username and password, you'll be able to choose 'Use a verification code' or 'I can't access my app right now', then type in the verification code that's associated with that account.

Do I need to be connected to the Internet or my network to get and use the verification codes?
The codes don't require you to be on the Internet or connected to data, so you don't need phone service to sign in.

Why does the number next to the code keep counting down?
The active verification code changes every 30 seconds so that if somebody were to learn what code you used to verify your sign in yesterday, or even a minute ago, they wouldn't be able to use that code to get into your account. This timer is the countdown to the verification code changing to the next code. Unlike a password, we don't want you to remember this number. Only someone with access to your phone should be able to get your temporary verification code. Do not share these codes with anyone.

Caution: A common trick of attackers is to contact you via text or phone pretending to be your bank, IT support, or other service provider and saying they need you to read them the code from your authenticator app to verify your identity on the call. Do not give them the code - they're trying to break into your account and they are stuck at the verification prompt. No real company should ever ask you to read your verification code to them over the telephone - especially if they called you.

What do I do if I have lost my phone/left my phone at home and cannot MFA?
If you need to MFA but don't currently have access to your phone, you can contact the IT Student Help Desk for a temporary passcode.

I got a new device or restored my device from a backup. How do I set up my accounts in Authenticator again?
If you turned on Cloud Backup on your old device (recommended), you can use your old backup to recover your account credentials without re-registering for MFA. For more info, see the Backup and recover account credentials with Authenticator article.

I lost my device and can't get MFA notification anymore. How do I restore MFA on a new device?
If you've lost your device or no longer have access to your previous device, you will need to contact the IT Student Help Desk to receive a temporary passcode in order to change your MFA methods to the new device.

What data does the Authenticator collect and store on my behalf and how can I delete this data?
The Authenticator app collects three types of information:

- Account info you provide when you add your account. This info is limited to your **UniSC information only**. **Your personal info is not provided.**

- Non-personally identifiable usage data, such as aggregate details about success or failure of important operations that are used to detect decreased reliability and bugs. This minimal data is needed to keep the app updated and secure.

- Diagnostic log data that stays **only in the app** until you select **Send feedback** in the app's top menu to send logs to Microsoft. These logs can contain personal data such as email addresses, server addresses, or IP addresses. They also can contain device data such as device name and operating system version. **You can choose not to send this information.**

For more information, review the Microsoft Privacy Statement.

Why does the app request so many permissions?
Here's the full list of permissions that might be asked for, and how they're used by the app.

What is App Lock, and how can I use it to keep me more secure?
When App Lock is enabled, you'll be asked to authenticate using your device PIN or biometric every time you open Authenticator. App Lock also helps ensure that you're the only one who can approve notifications by prompting for your PIN or biometric (eg. Face ID) any time you approve a sign-in notification. You can turn App Lock on or off on the Authenticator Settings page. By default, App Lock is turned on when you set up a PIN or biometric on your device.

Are Apple Watch or Android wearable devices supported for Authenticator?
You can receive notifications on your wearable device but you won't be able to respond to the notification from that device.

What is a Verified ID?
Verified ID is not currently used by UniSC.