Multi-Factor Authentication (MFA)

Frequently Asked Questions

Table of Contents

Why is Torrens enabling Multi-factor Authentication?

A: Torrens is enabling Multi-factor Authentication to provide an additional layer of password protection before allowing user access to University systems. This industry security standard better reduces the risk that sensitive data (research, personal identifiable information, financial) could be compromised should someone learn a user's NetID password.

What Outlook version is supported with MFA?

A: User must be running Outlook 2016 application. Anything below office 2016 is not recommended and will not work with MFA.

What should I do if I receive a "403 Forbidden" error when I begin the registration?

A: If you receive this error, you should clear your browser cookies, and cache. After clearing cache, close and restart your browser, you should be able to access the "Begin Registration" page.

Why is Torrens recommending users register a smartphone and use the Azure authenticator Mobile app to confirm their identity?

A: It is recommended that smartphone users who are comfortable installing apps use the Azure Authenticator Mobile app for:

- Security - because the app is specific to your device, there is less risk that a phone call could be forwarded to an unregistered device or that an approval on a keypad could be duplicated.
- Flexibility - You can just hit the approve button on your smartphone with the "Notify me through app" functionality and you can avoid reading and entering the code.
- Redundancy - the app can generate a one-time passcode to enable logins even in locations with no mobile or Wi-Fi access.

What should I do if I lost/misplaced my registered phone or my phone is not working properly?

A: If you have lost/misplaced your registered phone or your phone is not functioning, contact the Student Support team

Can I log into a system with MFA if I don't have access to my registered primary phone?

A: No. You must have access to your phone to successfully log into a system with MFA. Please contact Student Support team.

Can I use the default mail app in my iOS or Android device?

A. **We recommend every user to use Microsoft Outlook application as Torrens does not support legacy applications**. iOS version 11 or greater supports modern authentication and you will be able to use the default mail application. The default mail application on Android device does not support modern authentication, you must download the free Microsoft Outlook application from the play store to have seamless experience.

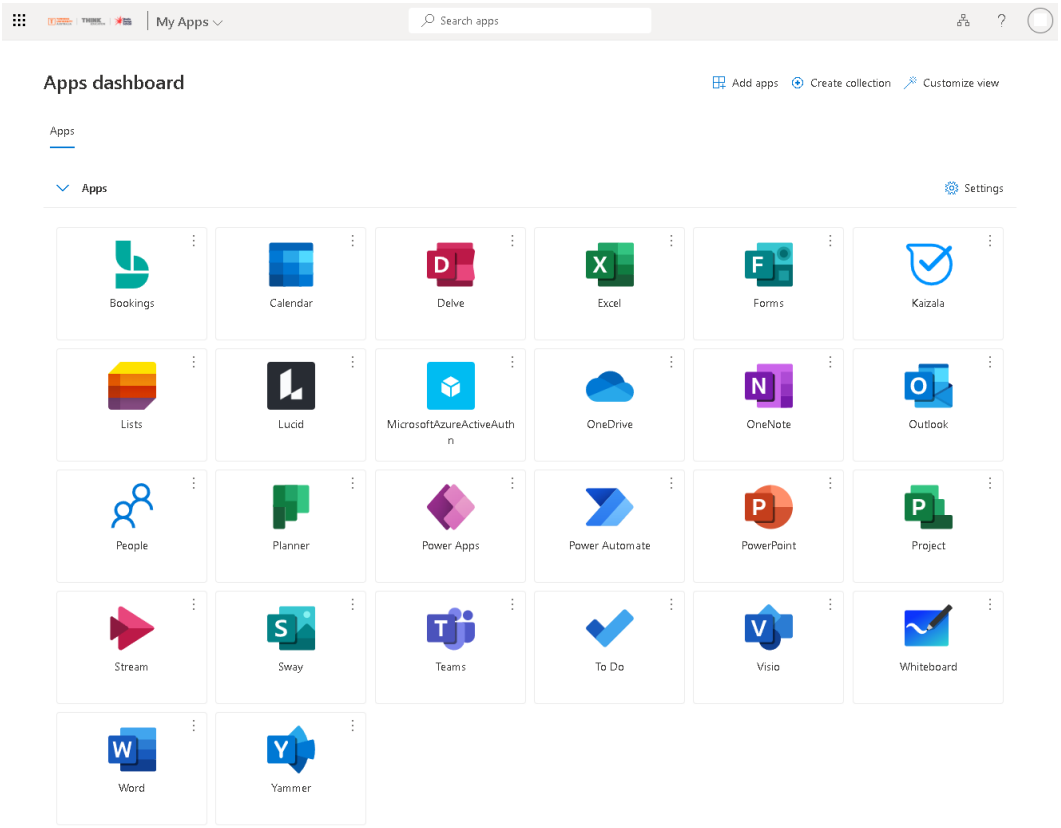
Where to manage my Multi Factor Authentication preferences?

A: Follow the steps below to change your MFA preferences:

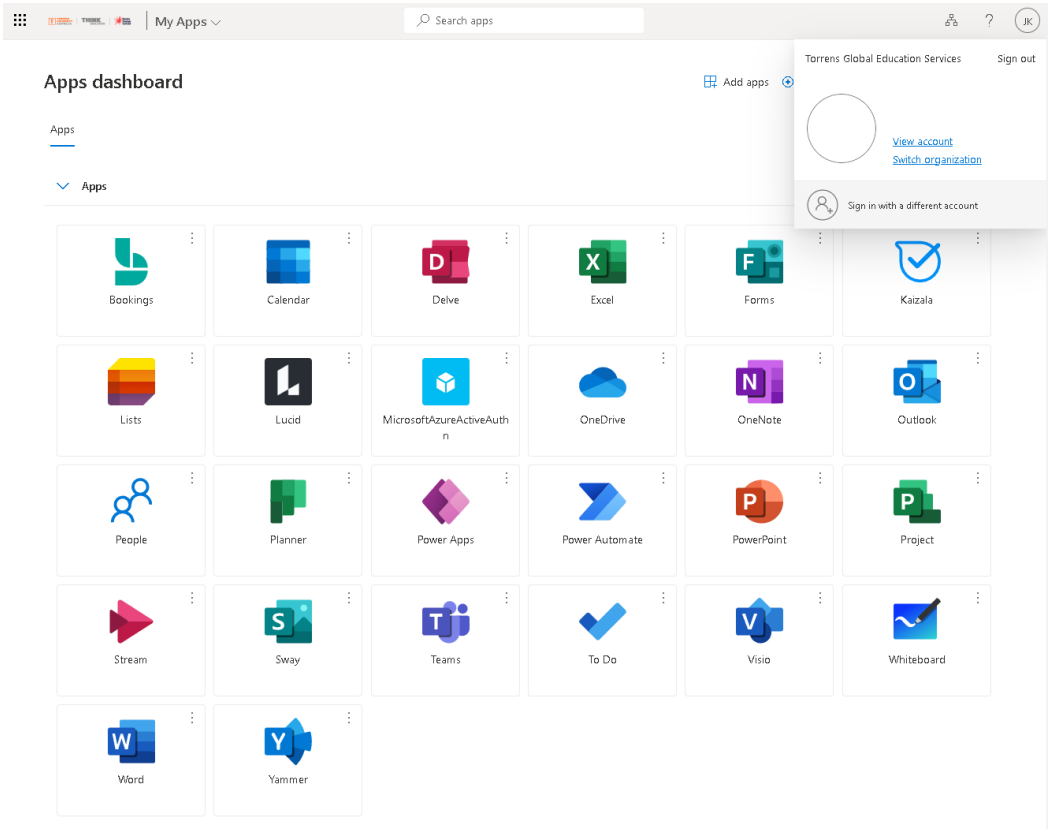
1. Go to "Security info."
2. Sign in with your credentials if you are not signed-in
3. Provide/change authentication phone

Or

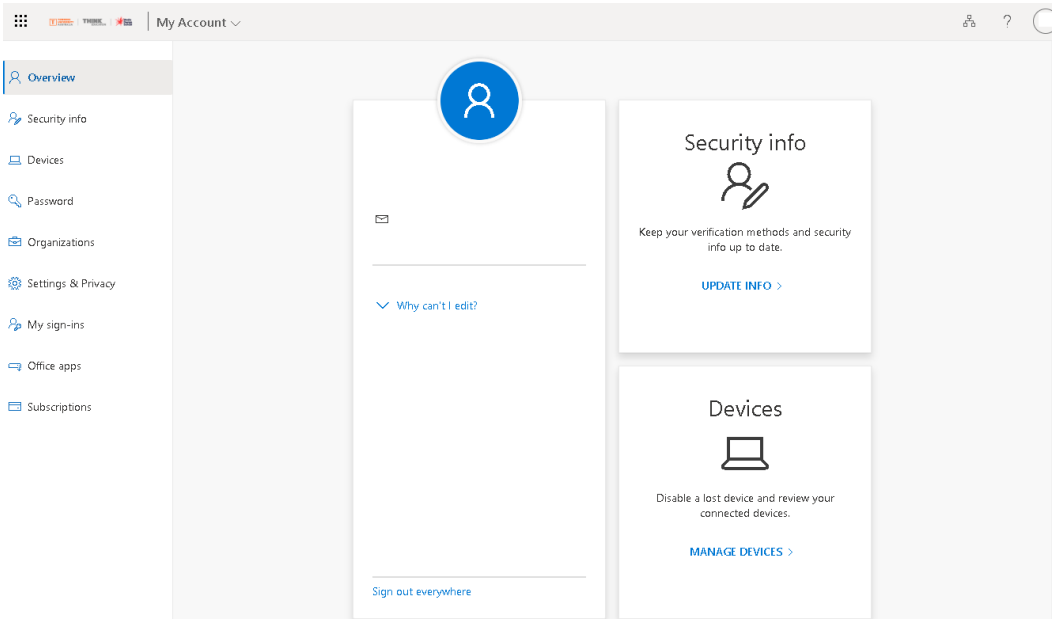
1. Go to https://myapps.microsoft.com
2. Sign in with your credentials if you are not signed-in



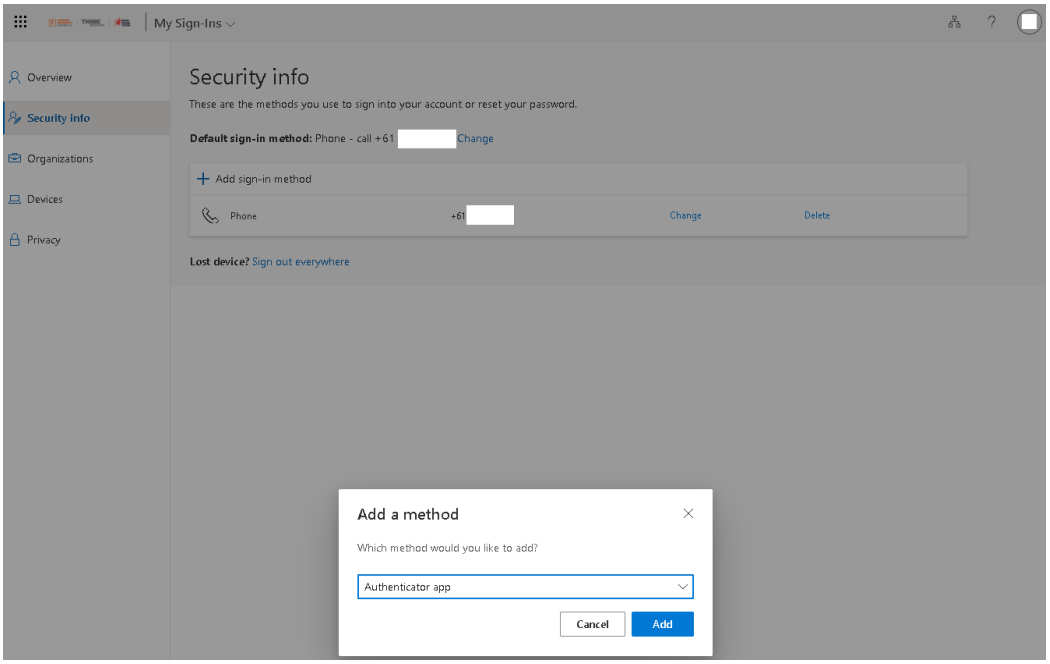
3. Navigate to “View account” by clicking on your name on the top right corner as shown in the screenshot below.



4. Click on “Security info” as shown in the screenshot below.



5. Watch our instructional video how to configure our recommended way using Microsoft Authenticator. Alternatively, change your authentication phone and save the changes.



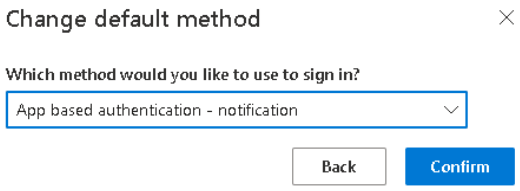
How do I configure azure authenticator application on my phone?

A: Please watch our instructional video how to install and configure Microsoft Authenticator (mfastu.torrens.edu.au).

How do I set up default option of authentication as notification on authenticator application?

A: Go to "Default sign-in method"

Go to "Default sign-in method?" and select "App based authentication - notification" to receive notification on your azure authenticator application or any other choice you use the most.



What are my options if I have limited or no cell phone coverage?

A: If you have a smartphone, we recommend registering it to receive notifications via the authenticator application. Once you have the app installed on our smartphone, you can generate a one-time code to be used in place of "Approving" or "Denying" the notification. If you don't have a smartphone and have limited cell coverage, consider registering a land line.

What should I do if I get a new/replacement phone?

A: If you have replaced your phone with a new phone of the same type (e.g., replaced an Android with another Android, or replaced your old iPhone with a newer model), and use Azure authenticator for authentication, follow these instructions:

1. On your new phone, download the Azure authenticator Mobile app from the Google Play, iPhone App Store, or Windows Market Place. Make sure you have the app installed before proceeding.
2. On your computer go to https://mysignins.microsoft.com/security-info and log in with your ID and Password.
3. Follow the process to **Add sign-in method** and configure Microsoft Authenticator application (Authenticator app).

The do not send me for X days, option is grayed-out and cannot be selected.

A: Please first try clearing the cookies from the browser of your mobile or desktop device. Then confirm your browser is configured to allow third party cookies. This option is typically found in the "Advanced or Advanced Options" section within your browser settings.