

Using Multi-Factor Authentication in China to access Durham IT resources

Multi-Factor Authentication (MFA) – also known as Two Factor Authentication (2FA) – is an added layer of security during the Microsoft sign-in process, helping protect the University systems from unauthorised access.

It involves using an app on your mobile device to authenticate (approve) your login to certain systems or software. It's a way to make sure it's really you logging in, not a scammer.

Features

With MFA, you can:

- Approve sign-ins quickly and easily
- Use a one-time code if you don't have internet access.
- Add more than one device to avoid getting locked out.

Who needs to set up MFA

- Everyone with a Durham University account must use MFA.

Microsoft Authenticator:

Most Durham University students and staff approve sign-ins using the Microsoft Authenticator app on their phone ([Microsoft Mobile Phone Authenticator](#) | [Microsoft Security](#)).

Downloading the app:

iOS: Microsoft Authenticator is available in the Apple app store

Android: You can find the Microsoft Authenticator app on the Lenovo, Oppo and Samsung Galaxy app stores

App notification issue:

The Microsoft Authenticator app is unable to send push notifications to Android phones in China. This means you cannot select the 'Approve a request on my Microsoft Authenticator app' option.

You can use the other ways including:

- Opening the Microsoft Authenticator app and using the 'one-time password code' method

- Using an alternative TOTP authentication app

We are aware however there are some limitations for users in China in being able to access the Microsoft Authenticator app.

Alternative options to Microsoft Authenticator:

if you are unable to use the Microsoft Authenticator app, other options are available, and the following should help solve any issues:

You can use a different authenticator app that supports TOTP (Time-Based One-Time Passwords) instead of the Microsoft app. Options include 2FAS, Cisco DUO, Google Authenticator.

How to Set Up

On a mobile device (recommended)

- Go to the Microsoft MFA registration page: aka.ms/mfasetup.
- Sign in with your Durham University IT account details.
- Choose to add an **Authenticator app**.
- When Microsoft asks you to install Microsoft Authenticator, look for the option:
 - **"I want to use a different authenticator app"** (wording may vary slightly).
- Microsoft will display a QR code.
- Open your chosen authenticator app (for example, Google Authenticator or 2FAS).
- Add a new account and scan the QR code, or manually enter the secret key if provided.
- Enter the six-digit code generated by the app to verify the setup.
 - Or use the Code and URL to configure an alternative authenticator app.

Set up backup access (recommended)

- Add a second device (e.g. tablet or spare phone) on the [MFA setup page](#). On the **Security Info** page, choose **"Add Method"** at the top and follow the steps.

You can add up to five devices. Always add a new device before removing your old one to avoid losing access.

If you run into problems:

- Contact the IT Service Desk - [Help and Support - Durham University](#)