Multi Factor Authentication (MFA)
Setup Guide for Students
Multi-Factor Authentication (MFA) – Setup Guide for Students

**About Multi-Factor Authentication (MFA)**

Multi-Factor Authentication (MFA) adds an additional "Second Factor" layer of security by requiring an extra step to validate your login. This extra step makes it more difficult for an attacker to access your account, even if they discover your username and password.

It is recommended that this "Second Factor" be the Microsoft Authenticator app, which can be installed on a smartphone or tablet. The app is the most convenient and secure MFA method, and can even work offline.

**Why is UWS using Multi-Factor Authentication?**

The University is adding an extra layer of security when accessing Office 365 (O365) off campus by implementing Multi-Factor Authentication (MFA). This is being done in response to an increase in the number of successful attacks against University accounts.

You need to take action if you access your University email and calendar outside of the University e.g. from a mobile device, or home computer.

**What is the Microsoft Authenticator App?**

The Microsoft Authenticator app allows enterprises and educational institutions around the world to perform Multi-Factor Authentication (MFA). You can even secure personal accounts with it, including Facebook.

UWS uses the Microsoft Authenticator app for MFA purposes only. By installing the app and syncing your UWS account, you are not providing the institution with any personal data or means through which to control your device.

Further information can be found on the [Microsoft website](https://microsoft.com).

=========

This document explains how to set up Multi-Factor Authentication (MFA) for the first time, allowing access to Office 365 services (including email, calendar and OneDrive) from outside the University Network.
Frequently Asked Setup Questions

What do I need to set up MFA?

You will need:

1. A smartphone or tablet connected to the internet. This is the device on which you will install the Microsoft Authenticator app so that it can be your "Second Factor"
2. A PC/MAC or Laptop which you will use to setup your MFA account

What if I don't have a smartphone or tablet?

- MFA can be bound to a mobile number, even if you don’t have a smartphone
- Follow the instructions to set up MFA and choose "I want to set up a different method" – you will then be sent a 6 digit code
- If you do have a smartphone then we recommend using the App wherever possible as it is more reliable, secure and convenient

Does my device support Multi-Factor Authentication?

Information Services recommends the use of the Microsoft Authenticator app for Multi-Factor Authentication (MFA) - it offers the most convenient and secure MFA experience.

This can be installed on:
- iPhones
- iPads
- Android devices

On iPhones and iPads you will find the Microsoft Authenticator app on the App Store on your iPhone or iPad. It supports devices with an iOS version of 13.0 or newer.

Android device support varies by manufacturer. You will find the Microsoft Authenticator on the Play Store of your device to see if your device is compatible. Generally if your device is 8 years old or newer it will be.

If your device does not support the Microsoft Authenticator App, then as long as your device can receive an SMS message it can be used for Multi-factor Authentication.

Do I need to authenticate when I'm on campus?

No – MFA is only used when you are accessing Office 365 from an external network; on campus eduroam and wired networks are exempt
How often do I need to authenticate?

You need to authenticate when you are accessing emails or files off campus. You should only be asked for authentication:

- once every 30 days if you have set up your work emails on Outlook on your own device
- when you change your password
- every time* you log in to the UWS Webmail service at https://outlook.office.com
- every time* you log in to your UWS OneDrive online (if you are not already logged in to Webmail) – OneDrive online can be accessed at https://onedrive.live.com

* Unless you tick the ‘Don’t ask again for 30 days’ option

What do I do if I lose or replace my phone?

If you no longer have access to your MFA Authentication device, contact IT Helpdesk - they will clear your settings then you will be prompted to register for Multi Factor Authentication with another device the next time you log in.

If you get a new device, you will need to:

- use the app on the old device to log in at https://aka.ms/mfasetup
- deactivate the Authenticator app on the old device
- change the verification option to 'text a code' until you have set up the app on your new device
- enter your new phone number if it has changed.

Where do I get Microsoft Outlook?

UWS staff and students can get Office 365 free of charge – download the full package from https://office.com (you will need to log in with your full UWS email address and network password)

What do I do if I can’t install the Outlook app on my mobile device?

To access emails on older devices, open a browser and go to https://outlook.office.com

Where can I get help?

Visit the Common problems with two-step verification for a work or school account page on the Microsoft Support site

Contact IT Helpdesk:

Helpdesk@uws.ac.uk +44 (0)141 848 3999 0141 848 3998
First time setup guide

Step 1 – Download the Microsoft Authenticator App

On your smartphone or tablet, download and install the Microsoft Authenticator app, available on the App or Play store

Note: Don't add an account just yet!

Step 2 – Set up your MFA preferences

- On the PC/MAC or laptop, open a web browser and navigate to https://aka.ms/mfasetup - this is the official Microsoft MFA website
- Log in with your full UWS email address and network password
- You will be prompted to provide additional information - select Next to continue
- Select Mobile app (1) from the 'How should we contact you?' drop down list
- Select Receive notifications for verification (2) from the 'How do you want to use the mobile app?' options
- Click on Set up (3)
Multi-Factor Authentication (MFA) – Setup Guide for Students

**Step 3 – Pair your account to the App**

To pair your account to the App:

- Open the **Authenticator App** on your device
- Click the 3 dots in the top right and select **+ Add Account**
- Select **Work or School account**
- You will be asked to scan the QR code that is shown on the computer screen – once scanned, click **Next**

**Note:** if you are unable to scan the QR code, enter the **Code** provided into the App

**Step 4 – Verify the connection**

- The Authenticator app is now linked to your account and you will see this message while the connection to your App is tested
- You will receive a Notification through the Authenticator App on your mobile device - **approve it**

**Step 5 – Stay safe in the future!**

⚠️ You will only ever receive a notification when you have manually triggered its generation and are expecting one

If you receive a notification out of the blue, it is an indication that your account has been compromised!

If this happens, contact IT Helpdesk immediately and request a password reset
For additional security

On first set up, you will be prompted to add your mobile number to allow you to receive a text message code if the Authenticator App has no internet access

- Enter your mobile number and click Finished

You will also be able to add additional options for using your office phone or a second mobile device if you require.

- Select a verification option from the drop down list
- Enter the relevant mobile or phone number
- Click Save

You will be taken to your Security info page where you can manage your MFA settings and devices

You can go to https://aka.ms/mfasetup at any time to set up or edit these preferences