Multi Factor Authentication (MFA) is an additional security method which ensures that only you can log into your account. It does this by requiring at least 2 methods of authentication – something you know (your password) and something you have (Microsoft Authenticator App, Authenticator Lite, text message code or a phone call). This guide will help you set up and register for MFA. Please make sure you have your laptop and mobile phone with you before you start.

Register for MFA

1. On your laptop, to register for MFA visit: https://aka.ms/setupsecurityinfo

2. On your laptop, login to your university account using your username@surrey.ac.uk.

3. Enter your password.

4. When you click Next you will be prompted to set up your mobile phone to approve authentication to your account.
Set up Microsoft Authenticator App

1. Using your mobile phone, download the Microsoft Authenticator app from your AppStore or follow this link https://aka.ms/getMicrosoftAuthenticator (Note: if you don’t have a smart phone please click ‘I want to use a different method’ (see page 6) Then on your laptop click Next.

2. On your mobile phone, open the Microsoft Authenticator app and click ‘Add account’.

   Click ‘Allow’ to send notifications and access contacts if requested.

   When prompted select ‘Work or School account’. When prompted ‘click allow access to the camera’.

3. Using your mobile phone scan the QR code on computer screen

   You will then see a 6 digit number appear in the app on you mobile phone.

   (Note: If you are unable to scan the image a code is also available on screen. To enter the manual code, you will need to click on Can’t scan image?).

   Click Next on your laptop.
4. The account is now added. A 2-digit number will appear on your login screen which you will need to type into the Authenticator app on your mobile device:

Enter the 2-digit number and Click ‘Yes’.

5. After you click ‘Yes’ on your mobile phone, you will see ‘Notification approved’.

Click **Next** on your laptop.

6. On your laptop add your mobile phone number to receive a text as a backup authentication method. Set the country code of your mobile. Enter a valid phone number. (Additional numbers can be setup later)

Click **Next** – a text with a code will be sent to this mobile phone number.

7. From the text received on your mobile phone enter the code onto your laptop.

On your laptop click **Next**.
8. The phone is now linked to your account.

   On your laptop click Next.

9. Setup of MFA is now complete.

   Click Done

10. On your laptop your security information will now be confirmed.

    The methods of authentication will be shown.
If you change your mobile phone please update your MFA

To update phone numbers or update your authentication methods carry on from above or go to https://aka.ms/setupsecurityinfo

1. To add/change a phone number or add another Authenticator phone/tablet:
   Click + Add method.
   Select Alternative phone.
   Note: email can NOT be used for authentication
   Click Add.

2. Click + Add method.
   Select new method from drop down list.
   Add the additional phone number.
   Click Add.

3. A text or phone call will be sent to your mobile phone.

4. You will receive a text or call.
   If text please enter the code on your Laptop.
   If call please answer then press #.

5. A confirmation will be received that the new number is registered successfully.

6. Set the default sign-in method to the most appropriate to you.
   ‘Microsoft Authenticator – notification’ is recommended.
I don’t have a smartphone, I want to use a different method

1. On your laptop click ‘I want to set up a different method’

2. On your laptop select ‘Phone’
   Click Confirm

3. On your laptop select the correct country code
   Enter your mobile phone number
   Click Next

4. You will receive a text message to your mobile phone.
   On your laptop enter the code from the text message
   Click Next

5. On your laptop you will now see ‘SMS verified’
   Click Next

6. Success! You are now setup for MFA
   On your laptop. Click Done
What is Authenticator Lite and who should use it?

Authenticator Lite is a new Microsoft Authenticator available to users who have not already installed the Microsoft Authenticator app.

It can be used to approve multifactor authentication requests for your University Microsoft account directly in your Outlook mobile app. Users receive a notification in Outlook mobile to approve or deny sign-in, or they can copy a Time-based One-Time Password (TOTP) to use during sign-in.

The Authenticator Lite aims to enhance security for users who have not already installed the Microsoft Authenticator app, which remains the most secure authentication method to use.

Authenticator Lite works on the Outlook mobile app on mobile devices (iOS and android) only and is more secure than sms text authentication.

To setup Authenticator Lite on your Outlook mobile app on your iOS or android mobile device, please follow the instructions on Microsoft’s website here: https://support.microsoft.com/en-us/topic/authenticate-with-outlook-mobile-a57026c0-26af-4d17-bf84-d9ec637efda1
When will I be asked for Authentication Approval?
University PCs and Laptops (windows only) will automatically sign in. In most circumstances you will only be prompted to approve login using number matching if a change or unusual activity is detected. You are likely to be prompted to authenticate more frequently if you are using a VPN or if you have recently travelled to another country.

Other devices will be prompted to authorise login every 14 days on each device. This can vary if there is a change to your account.

Approve sign in using the Microsoft Authenticator App
Once you have set up MFA on your device you will be able to use your smart device to authenticate your login if prompted. If you are asked to approve a sign in a screen similar to the one below will appear on your screen.

If this happens you will need to open the Microsoft Authenticator App from your device and enter the 2-digit number you see on your screen, onto your mobile device and tap ‘Yes’, to gain access or enter a code generated from the app to gain access to your account.

Remember to only approve notifications you know you have initiated. If you have not initiated it, ignore the request or click on deny.