Multi Factor Authentication

Quick Start Guide

When you login to your University of Surrey email account for the first time you will need to set up security on your University of Surrey IT account.

This involves setting up:

1. Multifactor authentication and
2. Self-service password reset.

This guide will help you set up Multi Factor Authentication. Please make sure you have your laptop and mobile phone with you before you start.

What is Multi Factor Authentication (MFA)?

Multi-factor authentication (MFA) is an additional layer of security for your University IT account. Using MFA reduces the risk of someone gaining access to your account even if they find out your username and password, for example through a cyber attack or scam. Microsoft research suggests MFA can reduce such attacks by as much as 99.9%.

You can set up MFA before you arrive at Surrey (even if you are overseas), or you can set it up once you've arrived.

You will need to have a mobile phone which is usable in the UK.

Essential: For MFA to work correctly and for you to be able to re-set your MFA should you need to, please use the Microsoft Authenticator App on your mobile phone.

Don't use SMS text messages as a default authentication method as this is less secure.

For self-service password reset to work correctly, please set up the following authentication methods:

- security questions (for resetting your password)
- a personal email address (for resetting your password)

Please note:

- You cannot use an email address as an MFA authentication method.
- When setting up self-service password reset, you can use an email address as a method to reset your username and password.

Advisable: You can also put the MS Authenticator app onto another device such as a tablet or i-pad. This will give you another authentication option should you need it.

You can also use another phone number as a backup option (only if you have one).

Did you know?

When you have set up the MS Authenticator App on your phone you can add other accounts to it such as your personal Amazon, PayPal, and Facebook accounts, so providing additional security to those personal accounts.

To do this, open the MS Authenticator app and go to '+ new account' and follow the setup instructions in the App.

No smart phone? Please contact IT Services (01483 689898) explaining why you can't install the MS Authenticator App on a smart phone. We will provide an alternative solution.

If you lose your mobile phone, please call the IT Service Desk on 01483 689898, unless you've installed the MA Authenticator App on a second device such as a tablet or second mobile phone.

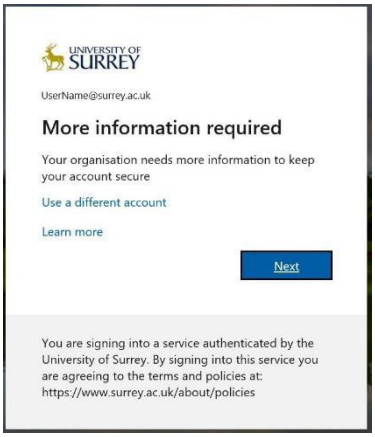
To set up MFA please use this quick start guide.

Register for MFA

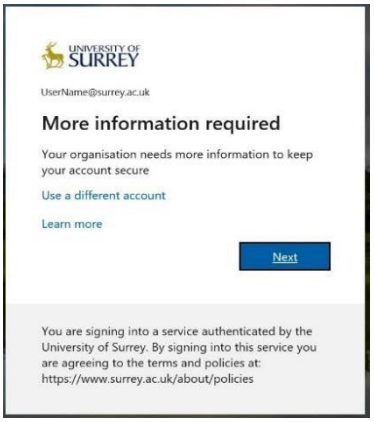
1. On your laptop, to register for MFA visit: https://aka.ms/setupsecurityinfo

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

3. Enter your password.



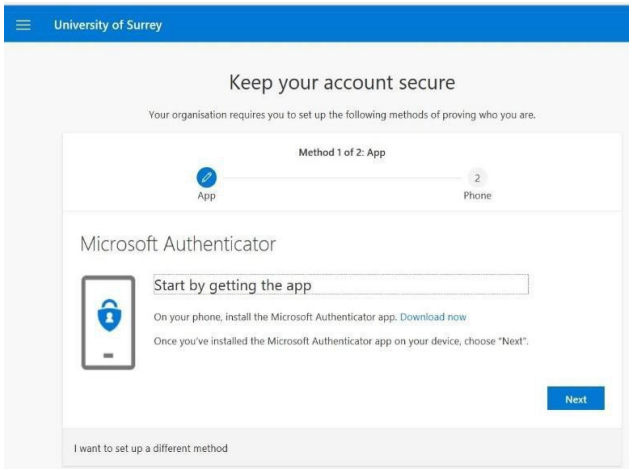
4. When you click ***Next*** you will be prompted to set up your mobile phone to approve authentication to your account.



Set up Microsoft Authenticator App

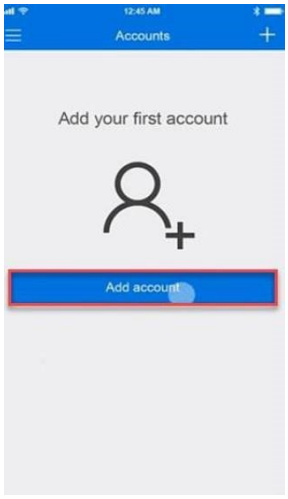
1. Using your mobile phone, download the Microsoft Authenticator app from your AppStore or click on this link https://aka.ms/getMicrosoftAuthenticator (Note: if you don't have a smart phone, please click 'I want to use a different method' (see page 6).

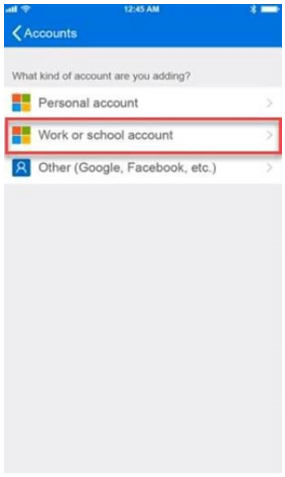
   Then on your laptop click ***Next.***



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'.

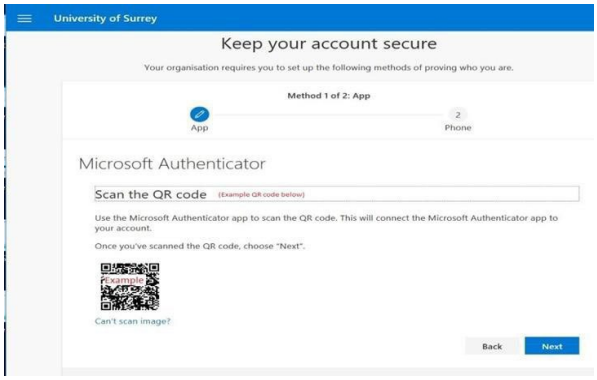


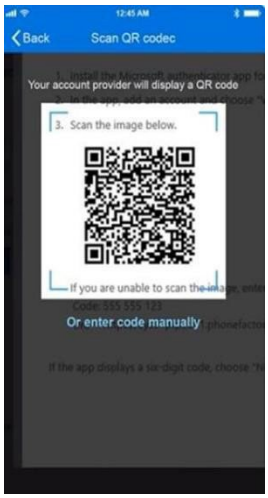


3. Using your mobile phone scan the QR code on computer screen you will then see a 6-digit number appear in the app on your mobile phone.

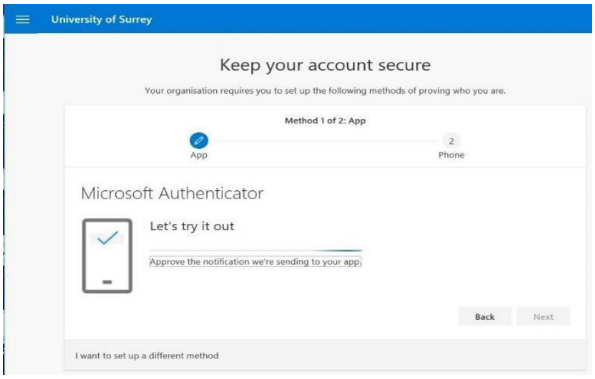
   (Note: If you are unable to scan the image a code is also available on screen. To enter the manual code, you will need to click on **Can't scan image?).**

   Click ***Next*** on your laptop.

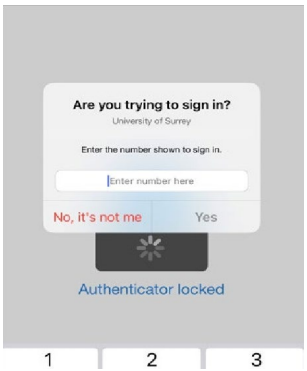




4. The account is now added. A 2-digit number will appear on your login screen which you will need to type into the Authenticator app on your mobile device:

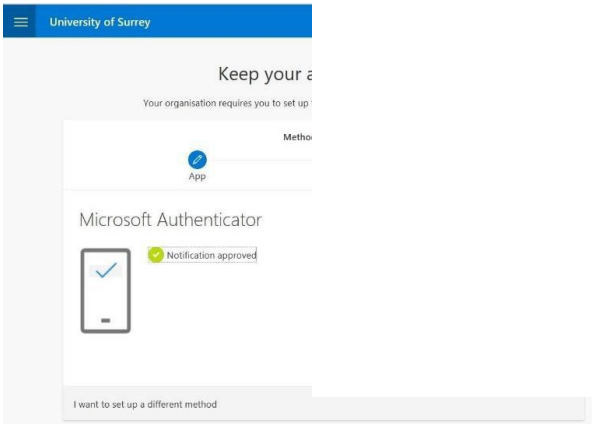


Enter the 2-digit number and
Click 'Yes'.



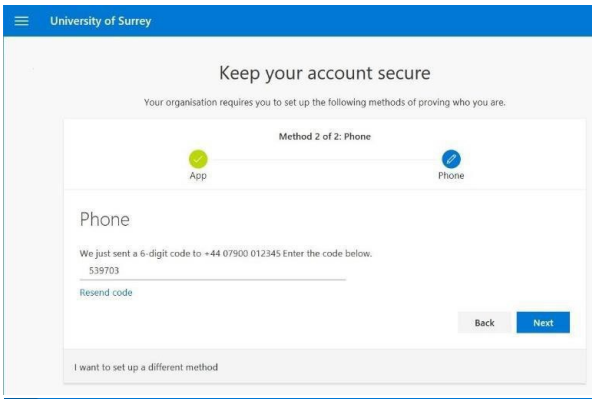
5. After you click 'Yes' on your mobile phone, you will see 'Notification approved'.

Click ***Next*** on your laptop.



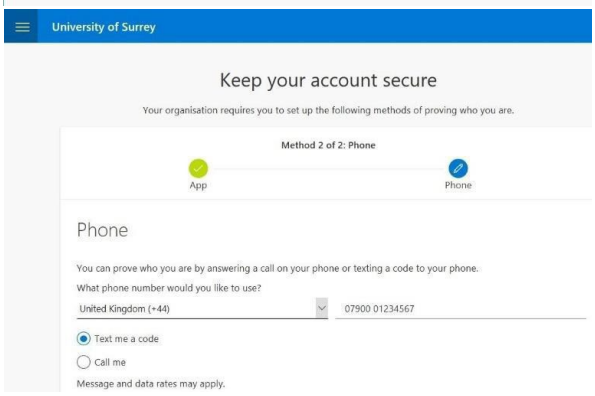
6. On your laptop add your mobile phone number to receive a text as a backup authentication method. Set the country code of your mobile.
Enter a valid phone number. (Additional numbers can be setup later)

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



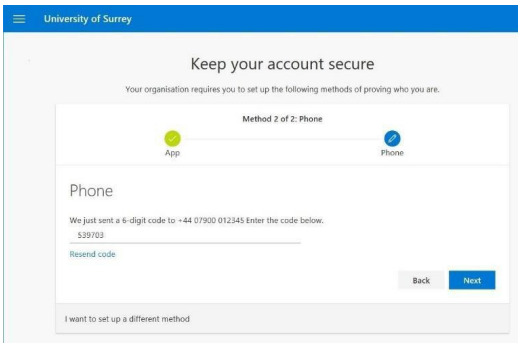
7. From the text received on your mobile phone enter the code onto your laptop.

On your laptop click ***Next.***



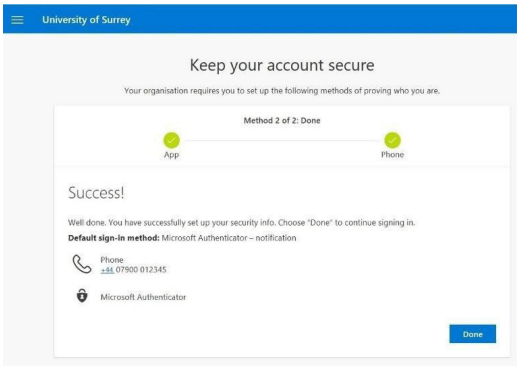
8. The phone is now linked to your account.

   On your laptop click ***Next.***



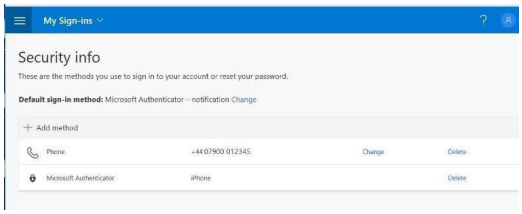
9. Setup of MFA is now complete.

   Click ***Done***



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

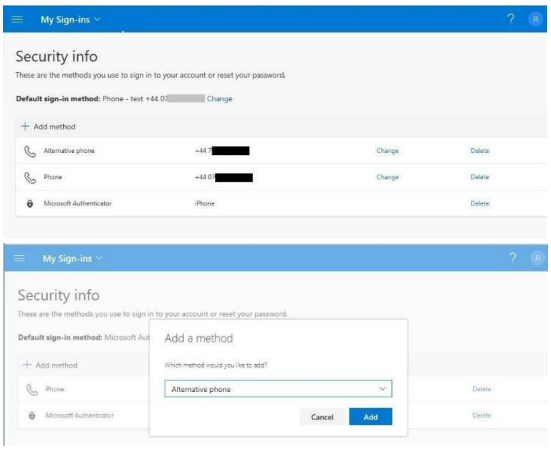
The methods of authentication will be shown.



If you change your mobile phone, please update your MFA

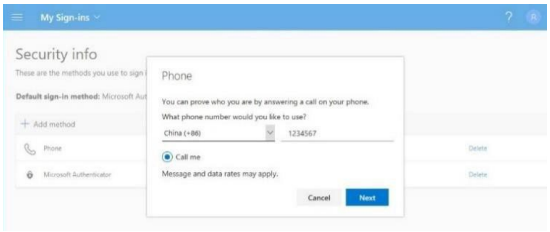
To update phone numbers or update your authentication methods go to https://aka.ms/setupsecurityinfo

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.***

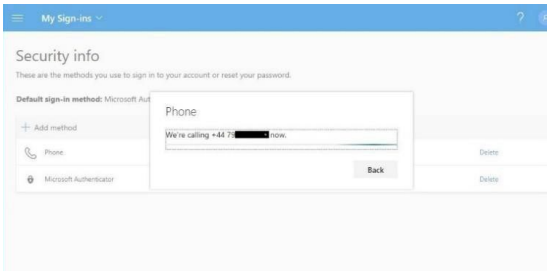


2. Click ***+ Add method***.
   Select new method from drop down list.
   Add the additional phone number.
   Click ***Add.***

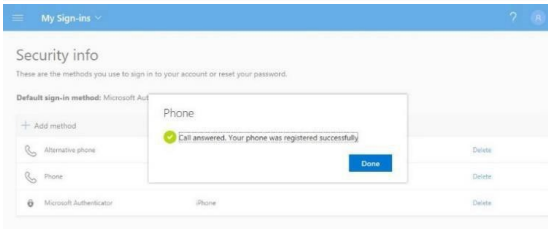
3. A text or phone call will be sent to your mobile phone.



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

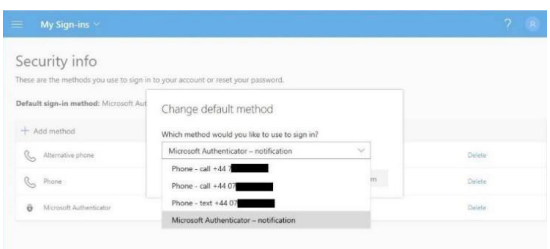


5. A confirmation will be received that the new number is registered successfully.



6. Set the default sign-in method to the most appropriate to you.

'Microsoft Authenticator – notification' is recommended.



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-bf84d9ec637efda1

When will I be asked for Authentication Approval?

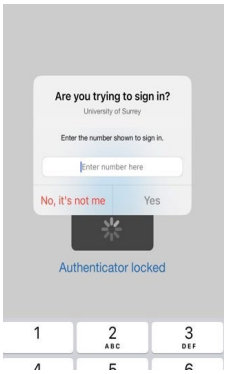
University PCs and Laptops (windows only) will automatically sign in. In most circumstances you will only be prompted to approve login using number matching if a change or unusual activity is detected. You are likely to be prompted to authenticate more frequently if you are using a VPN or if you have 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 like 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.



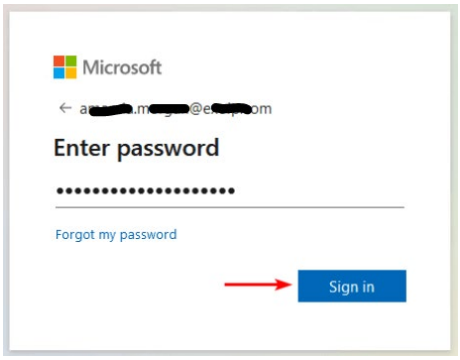
Remember to only approve notifications you know you have initiated. If you have not initiated it, ignore the request, or click on deny.

Microsoft Authenticator will now display geolocation on sign-ins.

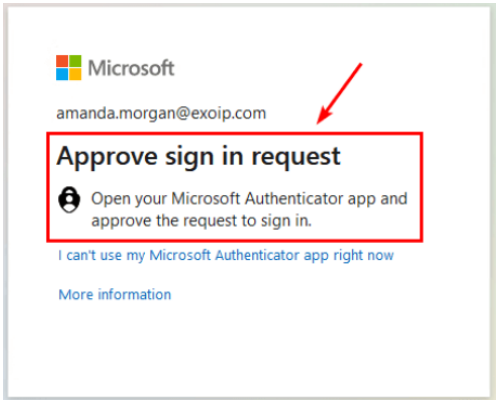
Microsoft Authenticator has added a new feature to show the geographic location of the device you are signing in with. This helps you verify that you are the one who is accessing your account and not someone else who might have stolen your credentials.

To use this feature, follow these steps:

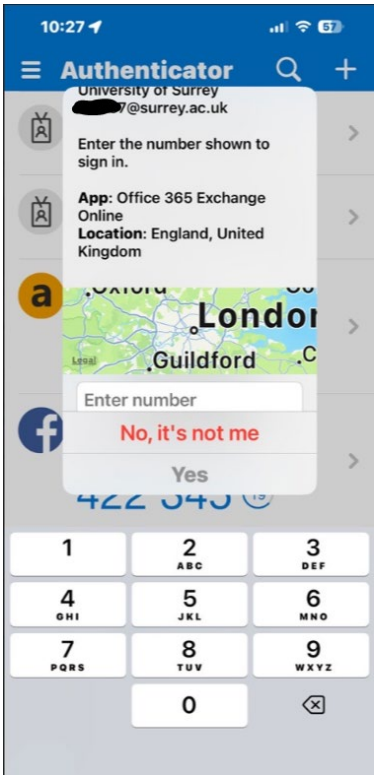
- Enter your username and password as usual to sign into your university account.



- You will receive a sign-in request message on your mobile phone.



- On your phone, you will see the location of the device and the application that is requesting access to your account. The location might not be very accurate, depending on your network settings. It should at least be from the country you are residing in and be within approximately one hundred miles of your actual location.



- If the location and the application match your expectations, on your phone, enter the number you see on your device screen and tap ‘Approve’ to complete the sign-in process.
- If you have not attempted to log in and you receive a request tap ‘Deny’ and change your password immediately.