Multi Factor Authentication

Quick Start Guide

Multi Factor Authentication (MFA) is an additional security method that ensures that only you can log into your account. It does this by requiring at least 2 methods of authentication – your password and another piece of information (Microsoft Authenticator App, 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

5. 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*

6. 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'
When prompted 'click allow access to the camera'

7. 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
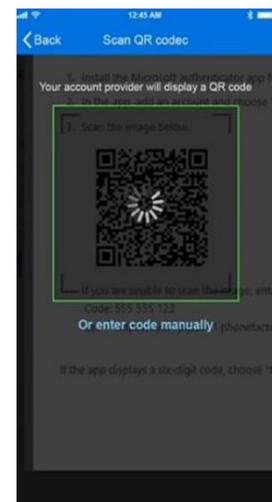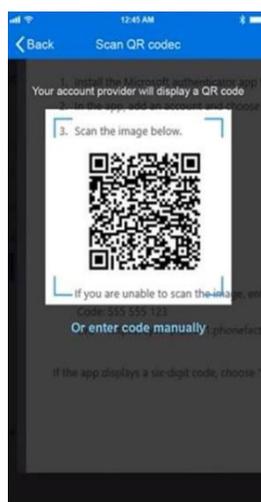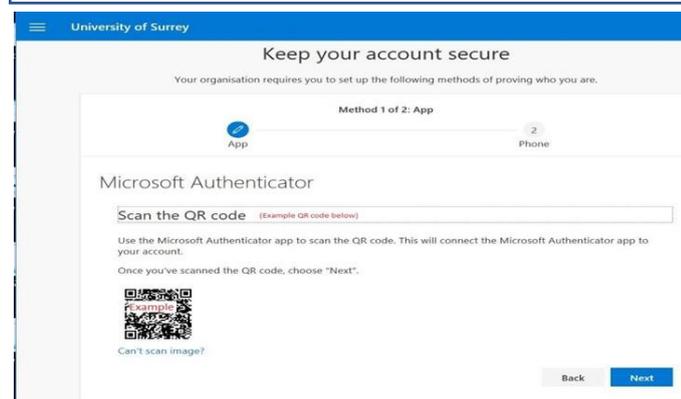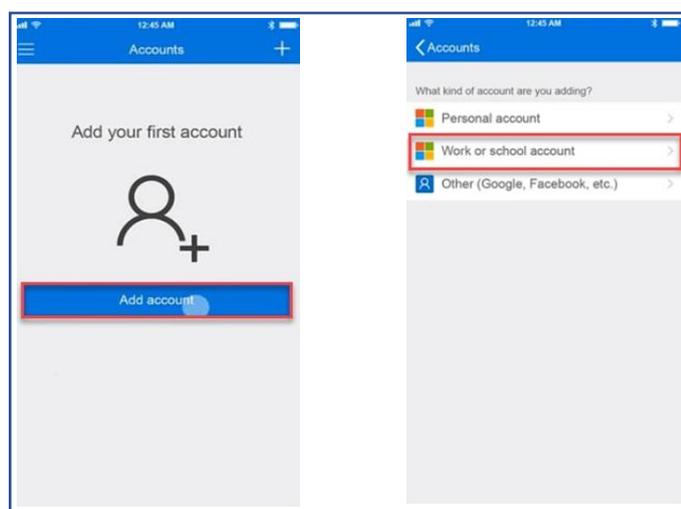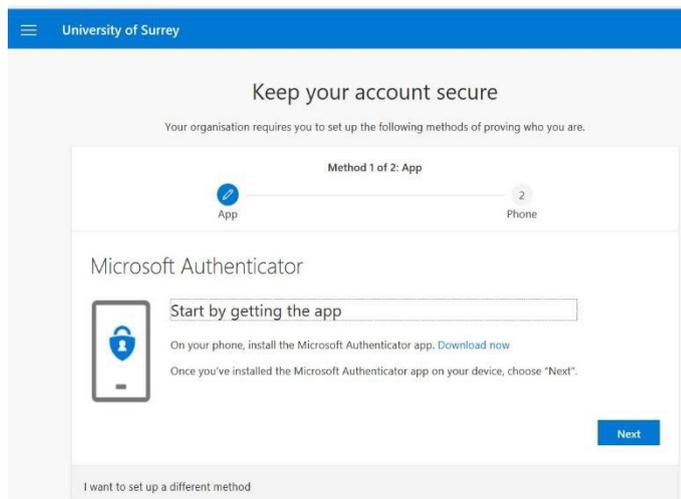
1. The account is now added. An approval request is now sent to your mobile phone.

   Click 'Approve'
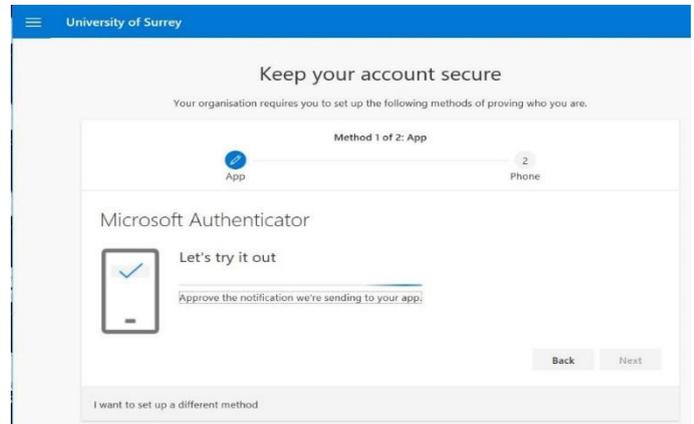
2. After you click 'Approve' on your mobile phone, you will see 'Notification approved'

   Click *Next* on your laptop

3. On your laptop add your mobile phone number to receive a text as a backup authentication method
   Set 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
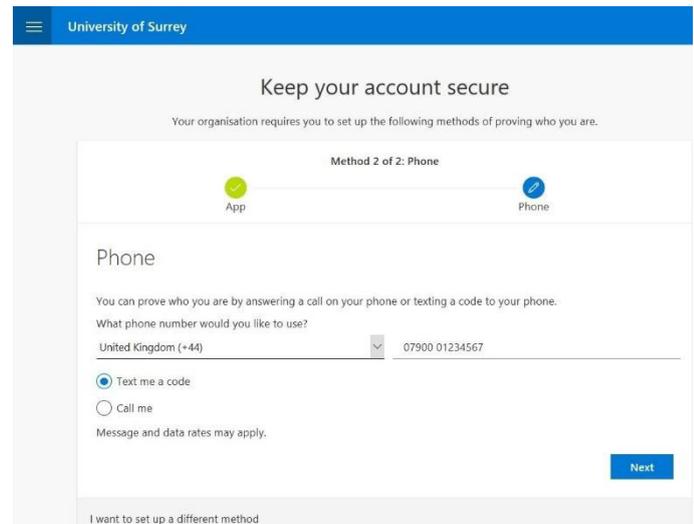
4. From the text received on your mobile phone enter the code onto your laptop

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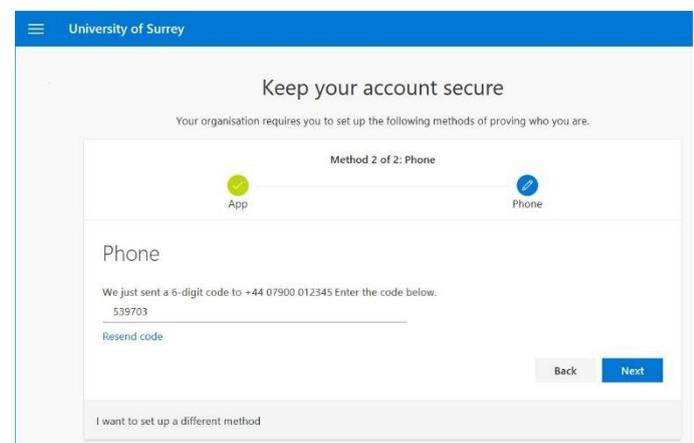
5. The phone is now linked to your account

On your laptop click *Next*
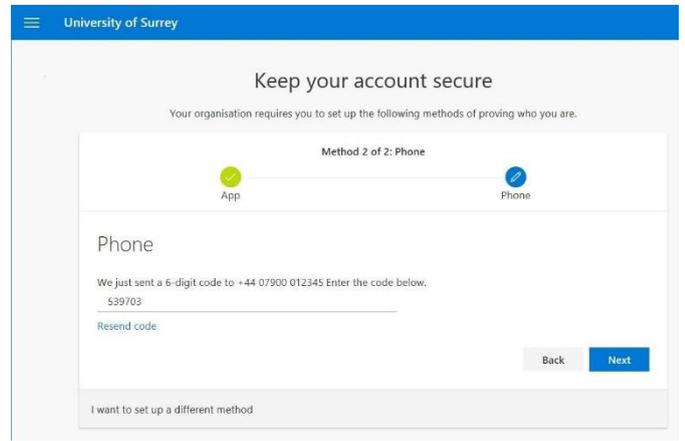
6. Setup of MFA is now complete

Click *Done*
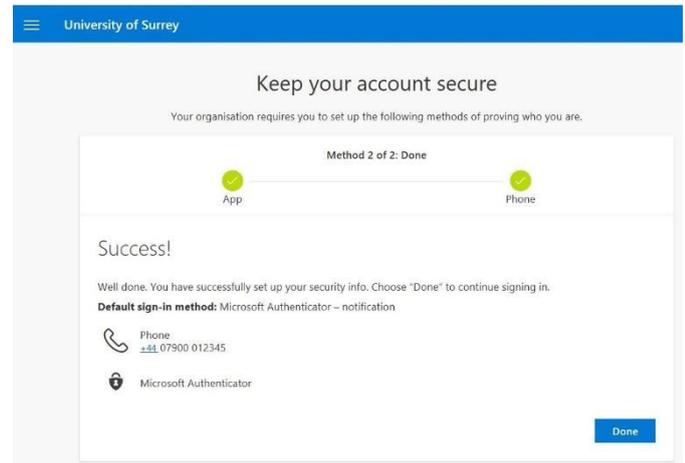
7. On your laptop your security information will now be confirmed

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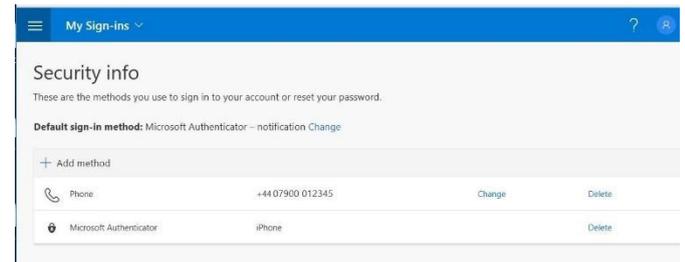
If you change your mobile phone please update your MFA

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
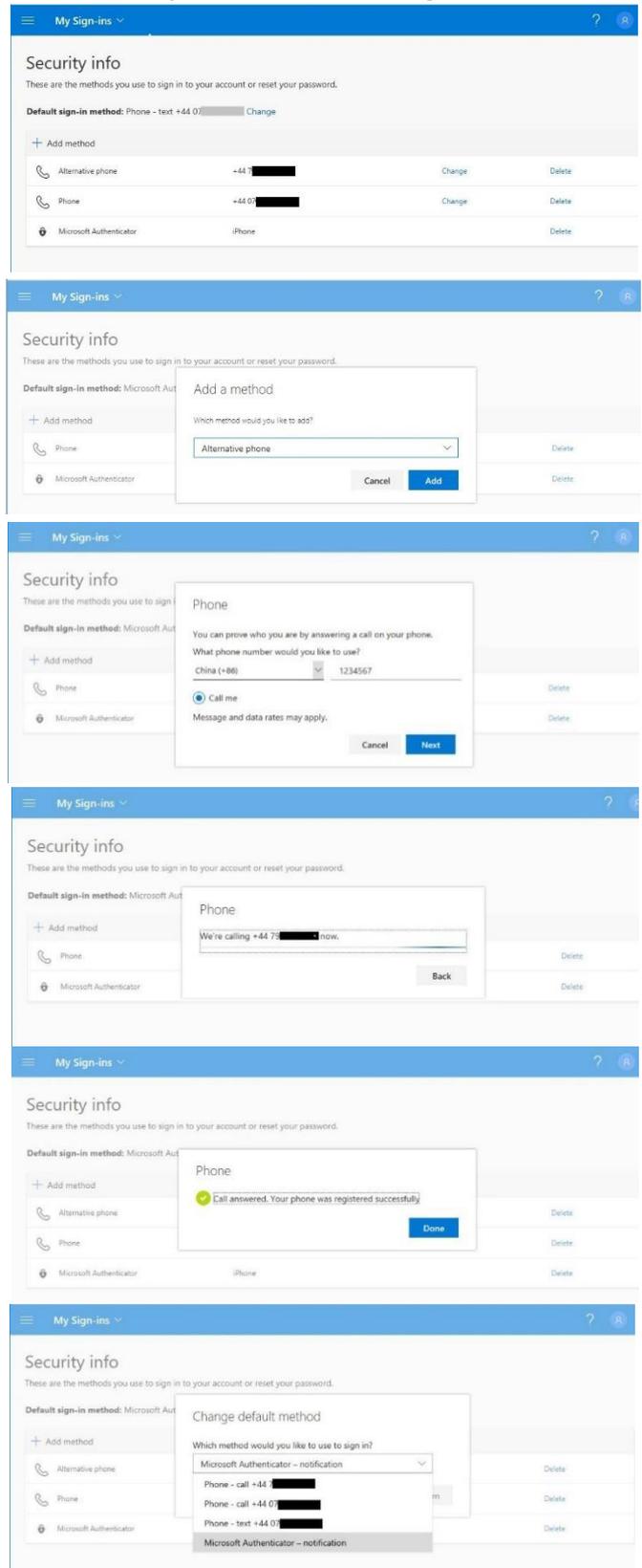
I don't have a smartphone, I want to use a different method

1. On your laptop click 'I want to set up a different method'
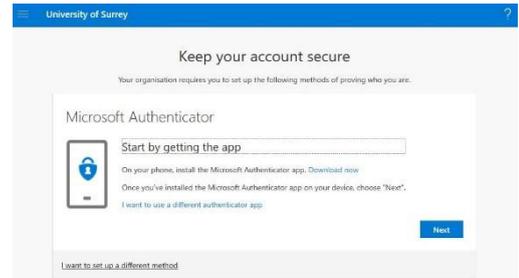
2. On your laptop select 'Phone'
    Click *Confirm*
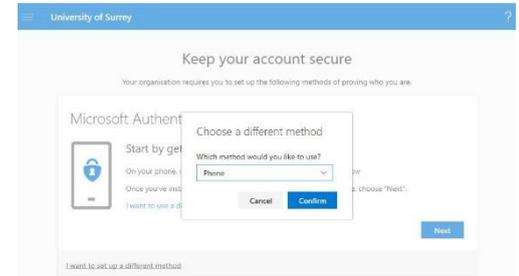
3. On your laptop select the correct country code
    Enter your mobile phone number
    Click *Next*

4. You will receive a text message to your mobile phone.
    On your laptop enter the code from the text message
    Click *Next*
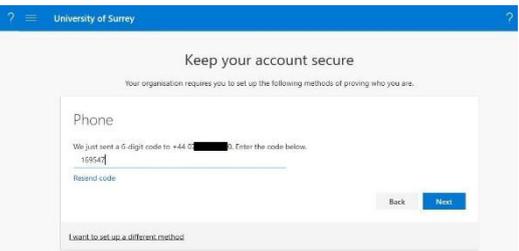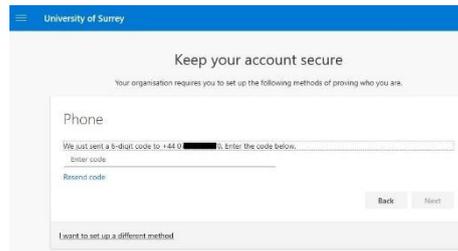
5. On your laptop you will now see 'SMS verified'
    Click *Next*
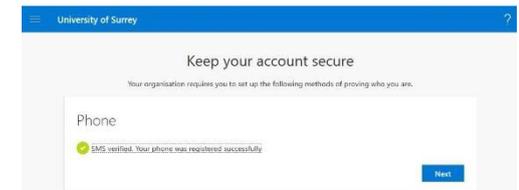
6. Success! You are now setup for MFA
    On your laptop Click *Done*

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 if a change or unusual activity is detected.

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.
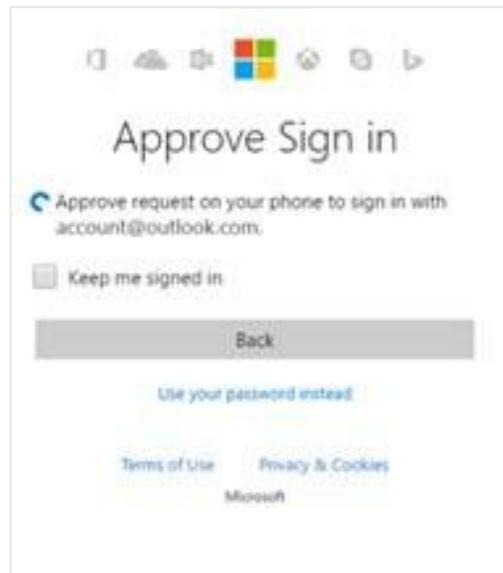
If this happens you will need to open the Microsoft Authenticator App from your device and click on **Approve** to gain access or enter a code generated from the app to gain access to your account.

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