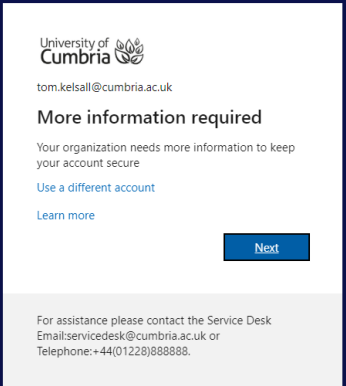
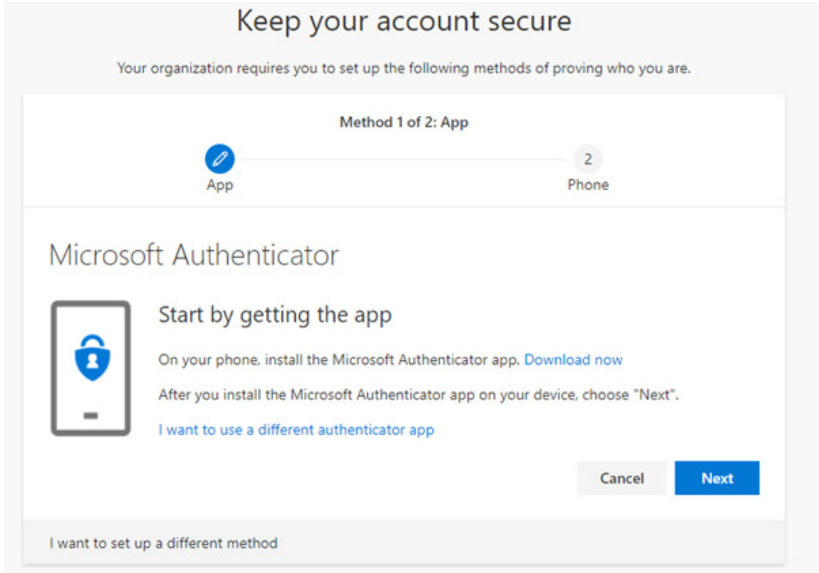


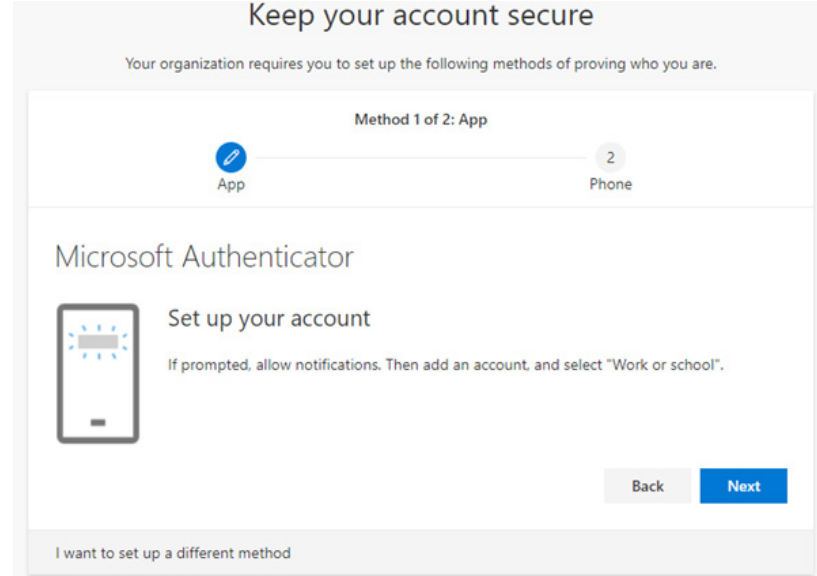


Multi Factor Authentication pairs your University password with an additional form of security, this could be an app on your corporate or personal smart phone, a phone call, or a text message. Before you can use MFA you will need to sign up to this service and choose your additional factors, the same sign up process will cover self service password reset. Every 180 days you will be asked to check all your information is still current.

1.	<p>When your account has been enabled for Multi-factor authentication the next time you sign in to your work or school account (off campus), you'll see a prompt that asks you to provide more information before it lets you access your account.</p>	
2.	<p>After you select Next from the prompt, a Keep your account secure wizard appears, showing the first method, the Microsoft Authenticator app. This app can be installed on any Android or iOS smart phone, personal or corporate – but this needs to be your phone and with you when you need to sign in off</p>	

3. Select **Download now** to download and install the Microsoft Authenticator app on your mobile device, and then select **Next**. Alternatively please search the AppStore on iOS or PlayStore on Android for "Microsoft Authenticator". For more information about how to download and install the app, see [Download and install the Microsoft Authenticator app](https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-download-install).

<https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-download-install>



4. Remain on the **Set up your account** page while you set up the Microsoft Authenticator app on your mobile device. Open the Microsoft Authenticator app, select to allow notifications (if prompted), select **Add account** from the **Customize and control** icon on the upper-right, and then select **Work or school account**.

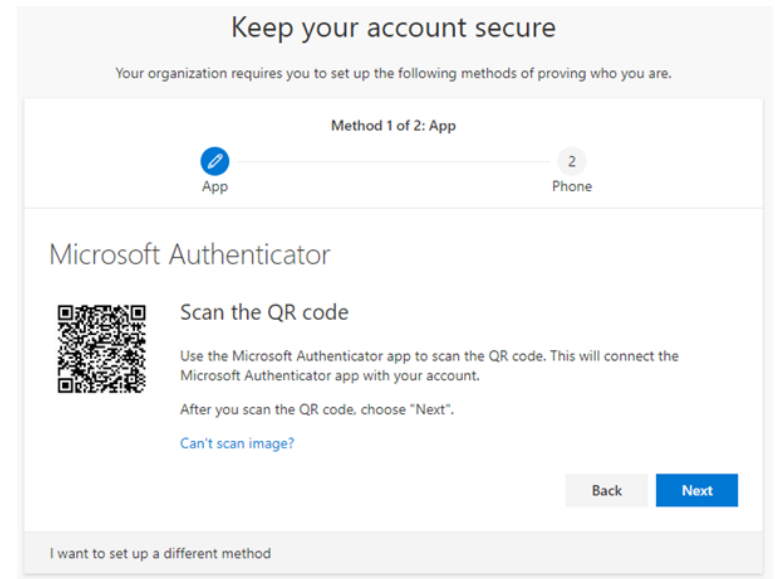
Note

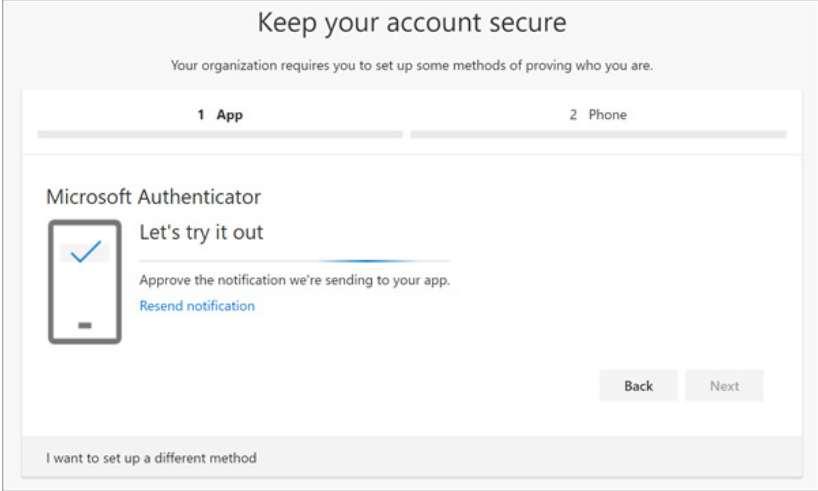
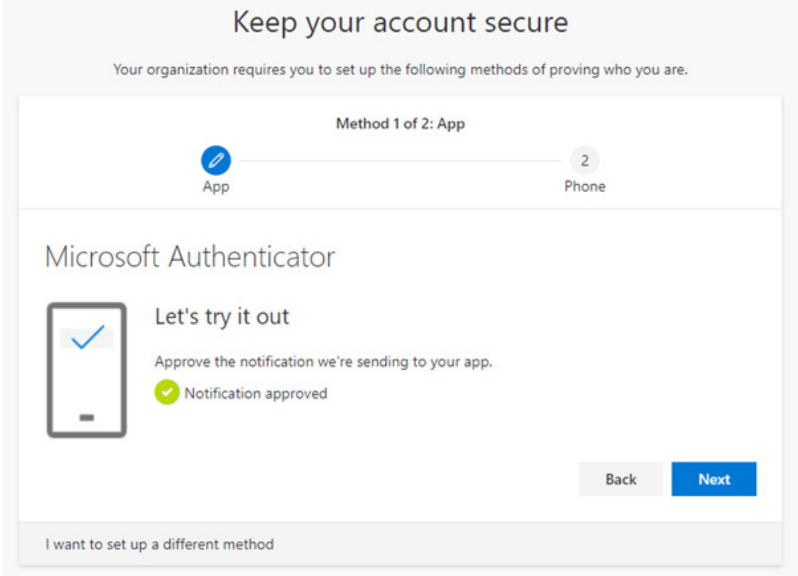
If this is the first time you're setting up the Microsoft Authenticator app, you might receive a prompt asking whether to allow the app to access your camera (iOS) or to allow the app to take pictures and record video (Android). You must select **Allow** so the authenticator app can access your camera to take a picture of the QR code in the next step. If you don't allow the camera, you can still set up the authenticator app, but you'll need to add the code information manually. For information about how to add the code manually, see [Manually add an account to the app](https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-add-account-manual).

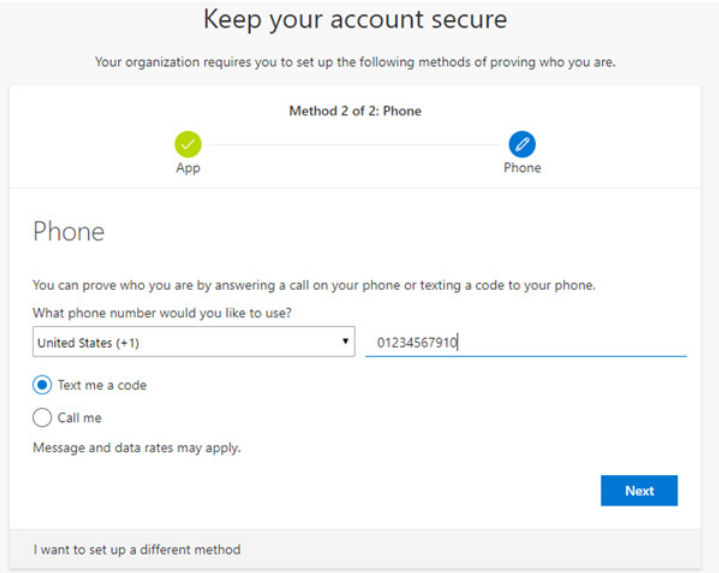
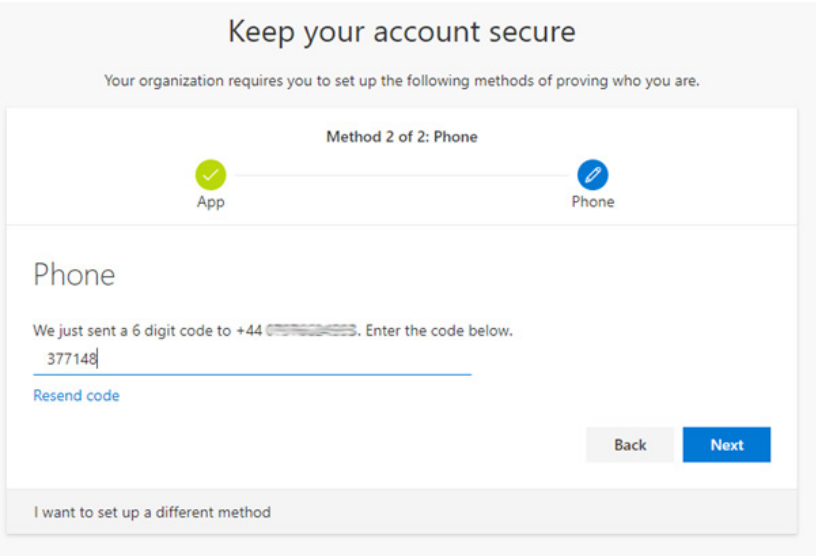
<https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-add-account-manual>

Return to the **Set up your account page** on your computer, and then select **Next**.

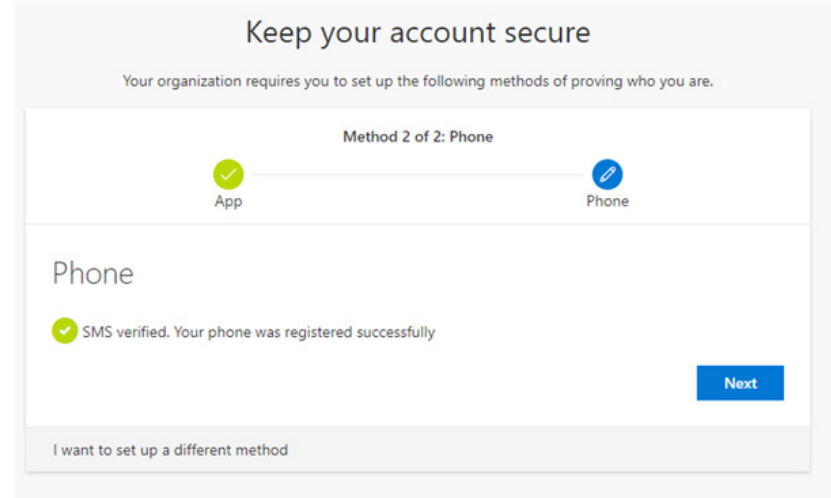
The Scan the QR code page appears.

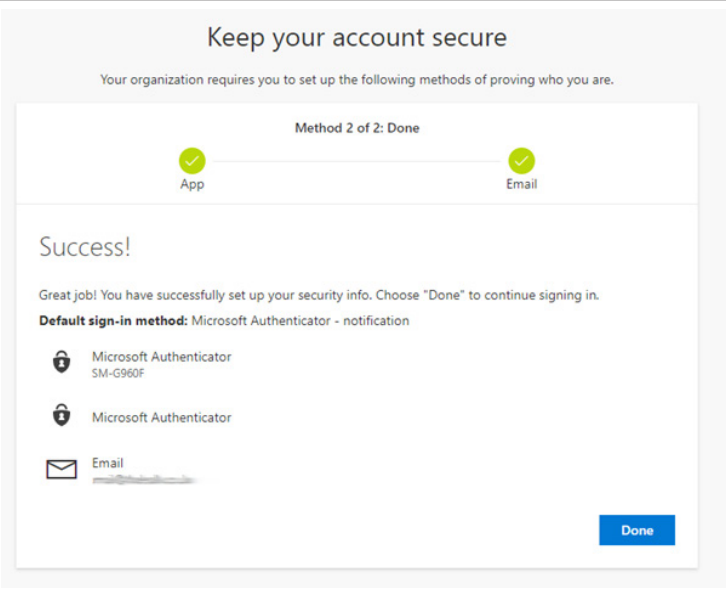
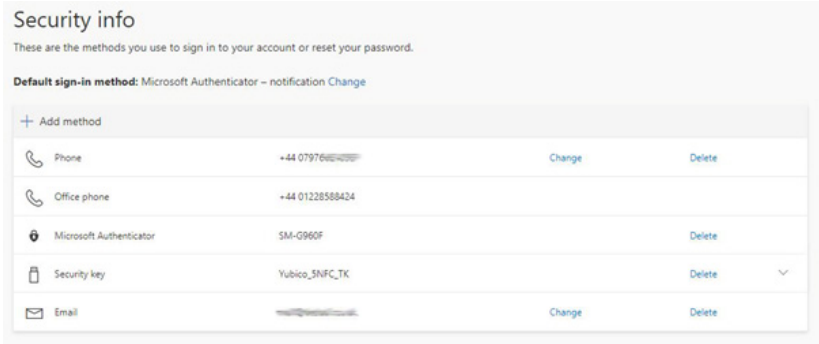


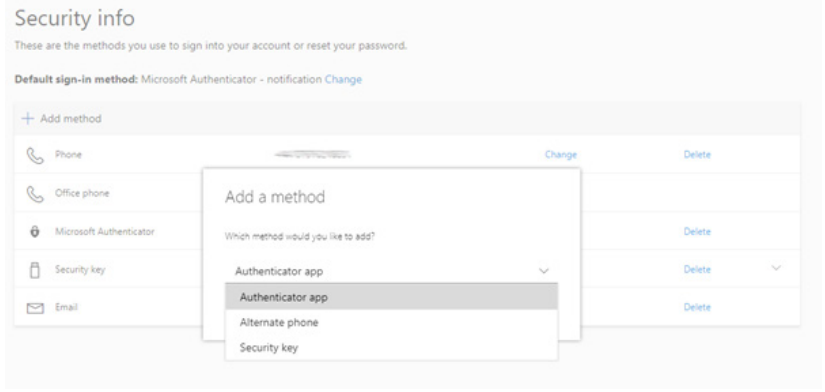
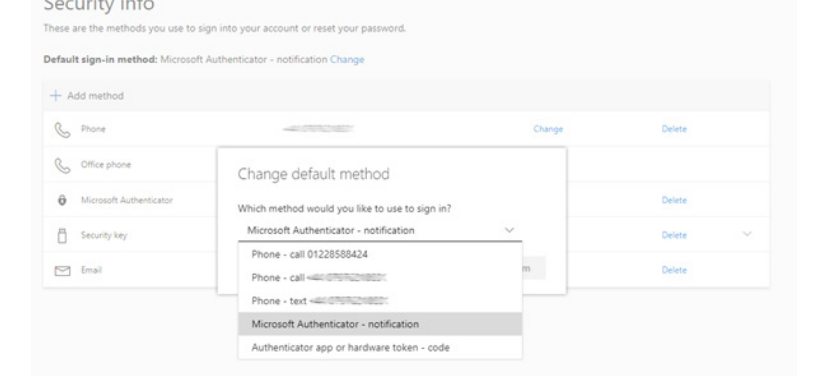
<p>5. Scan the provided code with the Microsoft Authenticator app QR code reader, which appeared on your mobile device after you created your work or school account in the previous step.</p> <p>The authenticator app should successfully add your work or school account without requiring any additional information from you. However, if the QR code reader can't read the code, you can select the Can't scan the QR image and manually enter the code and URL into the Microsoft Authenticator app. For more information about manually adding a code, see Manually add an account to the app.</p> <p>https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-add-account-manual</p> <p>Select Next on the Scan the QR code page on your computer.</p> <p>A notification is sent to the Microsoft Authenticator app on your mobile device, to test your account.</p>	
<p>6. Approve the notification in the Microsoft Authenticator app, and then select Next.</p> <p>Your security info is updated to use the Microsoft Authenticator app by default to verify your identity when using two-step verification or password reset.</p>	

<p>7. On the Phone set up page, choose whether you want to receive a text message or a phone call, and then select Next. For the purposes of this example, we're using text messages, so you must use a phone number for a device that can accept text messages. Personal phone numbers can be used here as the phone number will not be advertised to anyone else. The UK code of +44 needs to be selected.</p> <p>A text message is sent to your phone number. If you would prefer to get a phone call, the process is the same. However, you'll receive a phone call with instructions, instead of a text message.</p>	 <p>The screenshot shows a registration step titled 'Keep your account secure'. It indicates that the organization requires two methods of authentication. The 'App' method is already selected and marked with a green checkmark. The 'Phone' method is currently being configured. The user has chosen 'Text me a code' and entered the phone number '01234567910' with the country set to 'United States (+1)'. A 'Next' button is visible at the bottom right.</p>
<p>8. Enter the code provided by the text message sent to your mobile device, and then select Next.</p>	 <p>This screenshot shows the same registration step, but now the user is prompted to enter a 6-digit code. The text says: 'We just sent a 6 digit code to +44 [redacted]. Enter the code below.' The user has entered '377148'. There is a 'Resend code' link and 'Back' and 'Next' buttons at the bottom right.</p>

9. Review the success notification, and then select **Next**



<p>10.</p>	<p>Review the Success page to verify that you've successfully set up both the Microsoft Authenticator app and a mobile phone SMS and personal email method for your security info, and then select Done.</p>	
<p>11.</p>	<p>To Review your authentication methods.</p> <p>If you want to review these settings or would like to add or alter an authentication method please visit the following page. http://myprofile.microsoft.com. and select Security Info.</p> <p>You will always need to use MFA to gain access to this page. Below shows all possible methods added.</p>	

<p>12. You can change the default method by selecting Change. The recommendation is to use Microsoft Authenticator – notification – as this is the quickest approval method.</p>	 <p>The screenshot shows the 'Security info' page with a list of methods: Phone, Office phone, Microsoft Authenticator, Security key, and Email. A '+ Add method' button is at the top. A modal dialog titled 'Add a method' is open, asking 'Which method would you like to add?' and listing 'Authenticator app', 'Alternate phone', and 'Security key'.</p>
<p>13. Click + Add Method to add more phones, keys or Authenticator apps.</p>	 <p>The screenshot shows the 'Security info' page with the same list of methods. A modal dialog titled 'Change default method' is open, asking 'Which method would you like to use to sign in?' and listing 'Microsoft Authenticator - notification', 'Phone - call 01228588424', 'Phone - call', 'Phone - text', and 'Authenticator app or hardware token - code'.</p>