

## Multi-factor authentication is coming – act now

As part of UCEM's commitment to digital security you will soon be required to use **multi-factor authentication (MFA)** to access your UCEM Office 365 account.

This is a more secure way for you to access your account, using a unique code generated by an app on your smartphone, alongside your password. You might be familiar with this approach to digital security from your online banking, for instance.

**It will be rolled out to all students between Tuesday 10 October and Thursday 26 October 2023.**

Multi-factor authentication will be attached to your UCEM Office 365 account ONLY. This means you will need to use it to access your Microsoft applications (Outlook, Word, Excel, PowerPoint, for example).

Even if you do not regularly use the version of Office 365 provided by UCEM, **it is an expectation that all students activate multi-factor authentication in order to continue to receive and access important information** sent to their UCEM email accounts.

## Activating multi-factor authentication for your UCEM account

It's important you take part in the following process in order to avoid being locked out of your UCEM Office 365 account, and to ensure you can continue to access all your Microsoft apps without delay or interruption.

To get your MFA up and running, you will need a smartphone or a similar device which runs Android or Apple iOS, and which can download and run third-party applications.

The process to move over to multi-factor authentication is straightforward, but we have provided some guidance below to help you through it step-by-step.

It is a three-stage process:

- 1** On your smartphone, download and install the Microsoft Authenticator App (or Google Authenticator) from the place you get your apps
- 2** Check for an email from UCEM, telling you that you've be switched over to MFA. Once you have received this email, you will need to act to ensure you don't get locked out of your UCEM MS Office account at next log-in
- 3** Enable multi-factor authentication as soon as possible after you receive the above email (see below)

## 1 Installing the Authenticator application You can do this now

We recommend doing this as soon as possible so you're ready for the next stage.

Visit the App Store (iOS) or Play Store (Android) on your smartphone and download and install the **Microsoft Authenticator** application.

More details about Microsoft Authenticator can be found at <https://www.microsoft.com/en-gb/security/mobile-authenticator-app>

**Google Authenticator** can also be used for MFA; the setup process will be very similar.

## 2 Check your email account for information We will contact you after 10 October 2023

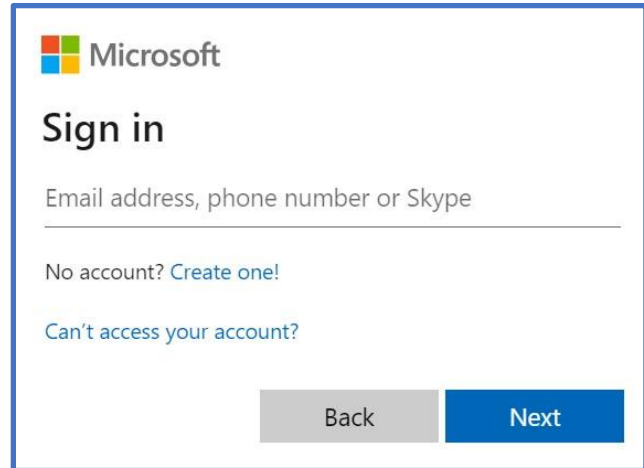
We will contact you by email to confirm multi-factor authentication is ready on your **UCEM Office 365 account**. Once we do so, please follow the steps below as soon as you can.

## 3 Enable multi-factor authentication You can do this when we confirm MFA is ready for you

1. Navigate to <https://www.office.com> on your computer and select **Sign in**

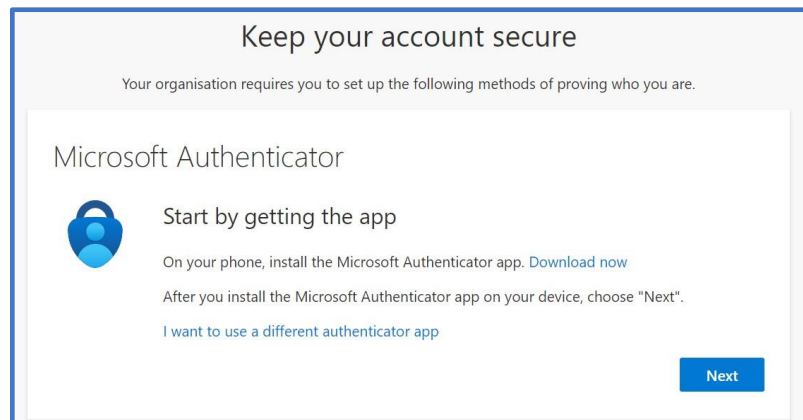


2. Enter your UCEM account email address (\*\*\*\*\*@student.ucem.ac.uk) and click 'Next'.



The screenshot shows the Microsoft 'Sign in' page. At the top left is the Microsoft logo. Below it is the heading 'Sign in'. There is a text input field labeled 'Email address, phone number or Skype'. Below the input field are two links: 'No account? Create one!' and 'Can't access your account?'. At the bottom right, there are two buttons: a grey 'Back' button and a blue 'Next' button.

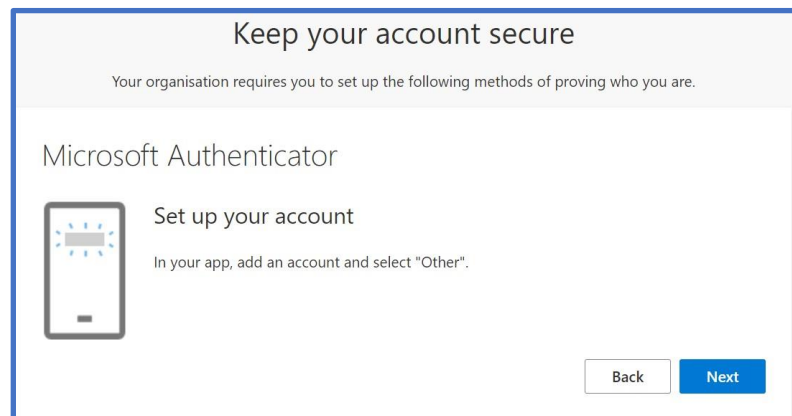
3. Ensuring you have the Authenticator app installed on your smartphone (see stage 1 above), select **Next** to continue.



The screenshot shows the 'Keep your account secure' page for Microsoft Authenticator. The heading is 'Keep your account secure' with a sub-heading 'Your organisation requires you to set up the following methods of proving who you are.' Below this is the 'Microsoft Authenticator' section, which includes an icon of a smartphone with a blue lock. The text says 'Start by getting the app' and provides instructions: 'On your phone, install the Microsoft Authenticator app. Download now' and 'After you install the Microsoft Authenticator app on your device, choose "Next".' There is a link 'I want to use a different authenticator app' and a blue 'Next' button at the bottom right.

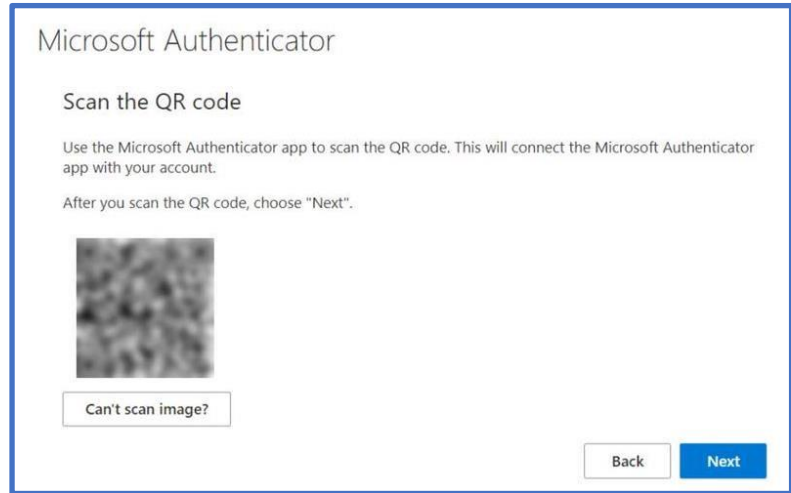
4. Open the Microsoft Authenticator application on your mobile device.

Select 'Add' a new account, and select 'Other' for type of account.

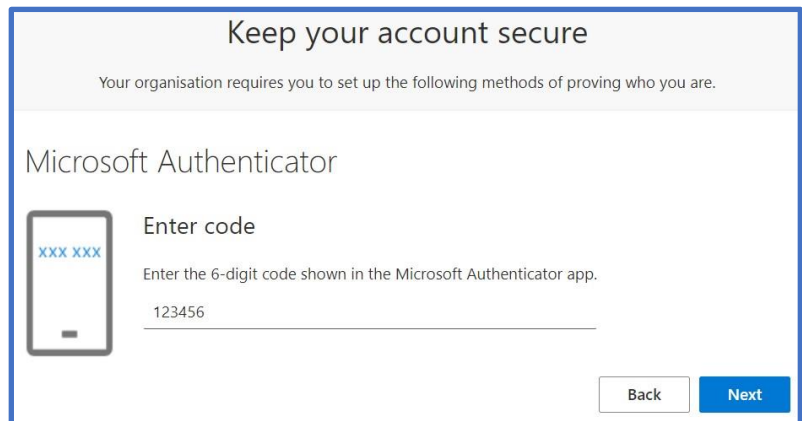


The screenshot shows the 'Keep your account secure' page for Microsoft Authenticator. The heading is 'Keep your account secure' with a sub-heading 'Your organisation requires you to set up the following methods of proving who you are.' Below this is the 'Microsoft Authenticator' section, which includes an icon of a smartphone. The text says 'Set up your account' and provides instructions: 'In your app, add an account and select "Other".' At the bottom right, there are two buttons: a grey 'Back' button and a blue 'Next' button.

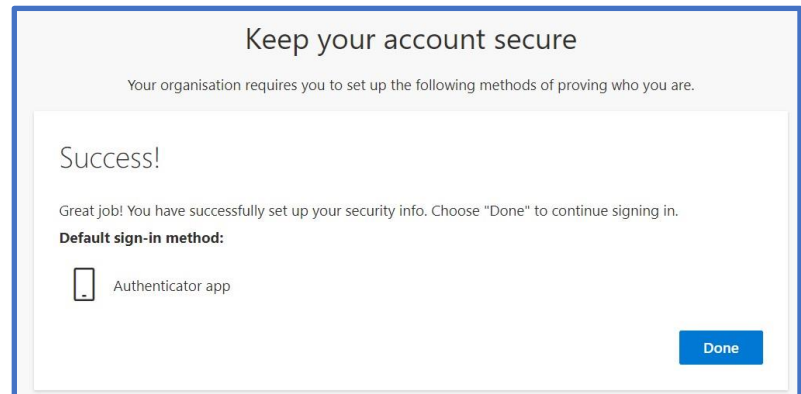
5. Use your mobile device to **scan the QR code** that is shown on your screen.



6. Once the QR code has been successfully scanned, the Microsoft Authenticator application will provide a code that you will need to enter on the screen, once entered, select **Next**.



7. At this stage you will see confirmation that the Multifactor Authentication has been successfully set up and you can select '**Done**'



8. You will see the option to remain signed in, if you are on a **secure private computer** this can be a useful option to avoid re-entering your details.

Select **Yes** or **No**, depending on your preference.



The screenshot shows the UCEM login interface. At the top is the UCEM logo and the email address [redacted]@student.ucem.ac.uk. Below this is the heading 'Stay signed in?' followed by the text 'Do this to reduce the number of times you are asked to sign in.' There is a checkbox labeled 'Don't show this again' which is currently unchecked. At the bottom right, there are two buttons: 'No' (grey) and 'Yes' (blue).

9. On the next window, you will prompted to enter a code from the Microsoft Authenticator Application on your mobile device.

If you are using a secure private computer, you can select '**Don't ask again for 14 days**' to reduce the number of times a code is requested for login.

Select '**Verify**' to continue.



The screenshot shows the UCEM login interface. At the top is the UCEM logo and the email address [redacted]@student.ucem.ac.uk. Below this is the heading 'Enter code' followed by the text 'Enter the code displayed in the authenticator app on your mobile device'. There is a text input field labeled 'Code'. Below the input field is a checkbox labeled 'Don't ask again for 14 days' which is checked. There is a link for 'More information'. At the bottom right, there are two buttons: 'Cancel' (grey) and 'Verify' (blue).

The setup of multi-factor authentication for your UCEM Office 365 account is now complete.

You will be prompted to enter an access code from the Authenticator app next time you log in – or in 14 days if you selected that option in step 9.

If you require any further assistance, please contact us via [Student Central](#) or via telephone:

UK: 0800 019 9697 (press option 2)

International: +44 (0)118 921 4696