

MFA registration campaign for students and alumni.

What is Multi-Factor Authentication (MFA)?

Multi-Factor Authentication (MFA) is an additional security measure that seeks to protect your accounts and personal data. Instead of traditional authentication that is based on a single method (password), MFA requires two or more methods to verify our identity.

What are its advantages?

- Increased security: There is less risk of unauthorized access when asking for multiple verifications.
- Password theft prevention: Without the second factor, the password is not enough to enter.
- Flexibility: You can choose from a variety of methods as you like, such as app codes, text messages, or authenticator apps.

In which services or applications will you ask us to use this type of authentication?

At IE University, one of our goals is to ensure the protection of our community's personal and educational information.

To achieve this, we work to ensure that all the services we offer have the appropriate authentication and security measures.

Currently, the main services we offer at IE University, including *Blackboard, Zoom, Google Workspace, Microsoft Office 365, Library, IE Connects, Service portal, etc.*, already have the security offered by MFA Multi-Factor Authentication.

*If we have any questions during the configuration of the MFA, we can contact our **IT Support** team at **00 34 915 689 623** or through the service portal <https://ie.service-now.com/>*

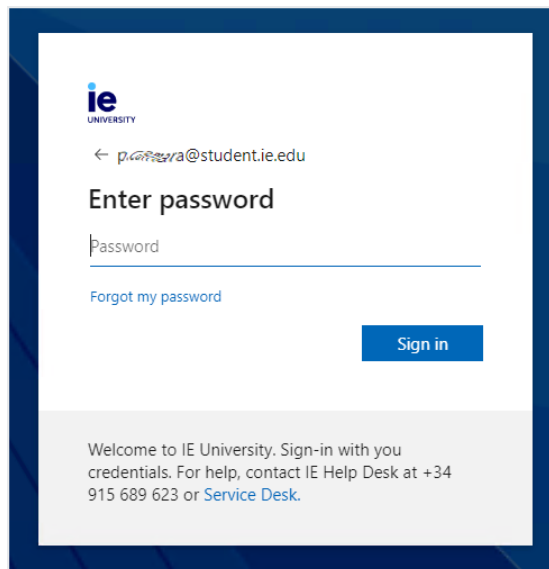
How do we configure MFA?

The following instructions are for the Microsoft Authenticator app.

These are the steps to configure MFA for our user. The images may be different, depending on the operating system and browser we use.

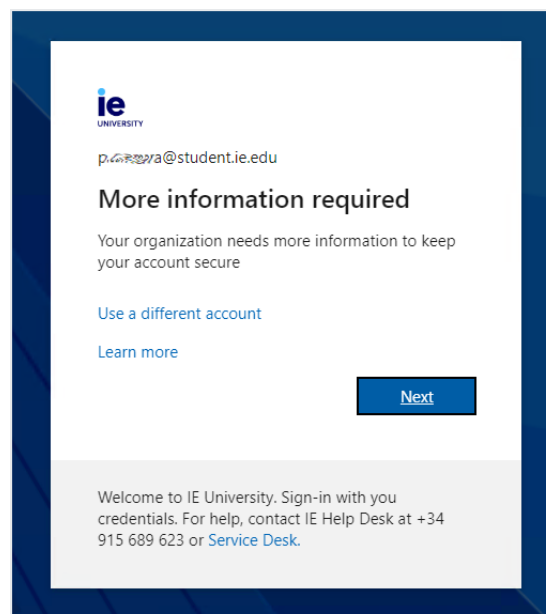
1. Log into your IE University account using your username and password.

Your username should include [@student.ie.edu](mailto:student@ie.edu) or [@alumni.ie.edu](mailto:alumni@ie.edu).



The screenshot shows the IE University login interface. At the top left is the 'ie UNIVERSITY' logo. Below it, the email address 'p.gonzalez@student.ie.edu' is displayed with a back arrow. The main heading is 'Enter password'. There is a password input field with the placeholder text 'password'. Below the input field is a link for 'Forgot my password'. A blue 'Sign in' button is positioned to the right. At the bottom, a grey footer contains the text: 'Welcome to IE University. Sign-in with you credentials. For help, contact IE Help Desk at +34 915 689 623 or [Service Desk](#).'

The first time you use your IE University username and password to try to access a university service, you will reach a screen saying '*More information required. Your organization needs more information to keep your account secure*'. We recommend you do this on your PC or tablet using a browser.



The screenshot shows the 'More information required' screen. It features the 'ie UNIVERSITY' logo at the top left and the email address 'p.gonzalez@student.ie.edu' below it. The heading is 'More information required'. The text below reads: 'Your organization needs more information to keep your account secure'. There are two links: 'Use a different account' and 'Learn more'. A blue 'Next' button is located at the bottom right. The same grey footer with contact information is present at the bottom.

Keep your account secure

Your organization requires you to set up one or more of the following methods to prove your identity.

Microsoft Authenticator



Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

Next

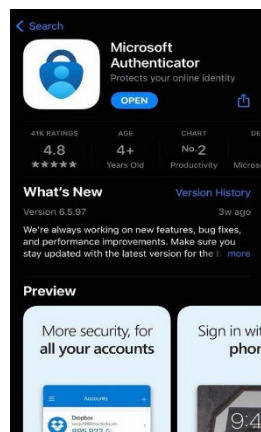
[I want to set up a different method](#)

Once signed in, you will see a message *'Start by getting the app'*.

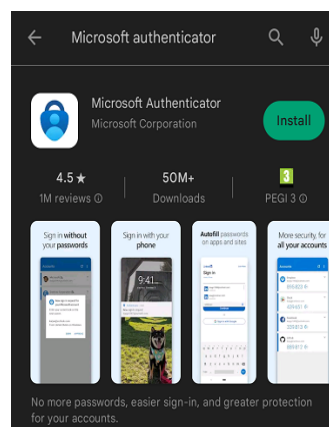
2. Leave this window open while you download the app to your smartphone.

- On your smartphone, download and install the *'Microsoft Authenticator'* app from the App Store or Google Play.
- If prompted allow notifications in the app.
- Once you have downloaded the app on your phone, click *'Next'* on your computer.

App Store



Google Play



Keep your account secure

Your organization requires you to set up one or more of the following methods to prove your identity.

Microsoft Authenticator



Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

Back

Next

[I want to set up a different method](#)

3. In your **browser**, a QR code will be generated which you need to **scan using the camera on your phone**.

Keep your account secure

Your organization requires you to set up one or more of the following methods to prove your identity.

Microsoft Authenticator

Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".



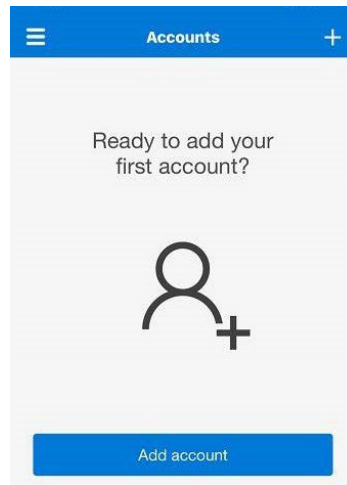
Can't scan image?

Back

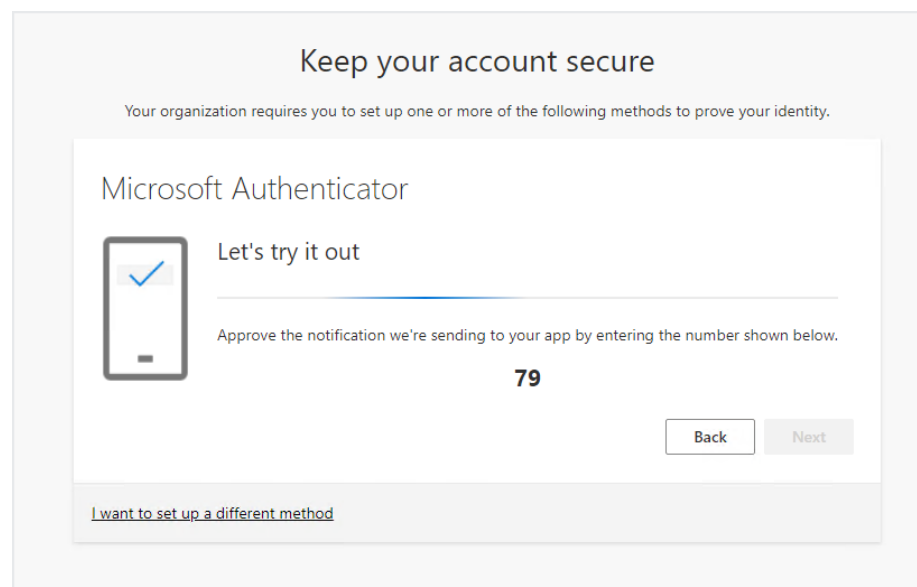
Next

[I want to set up a different method](#)

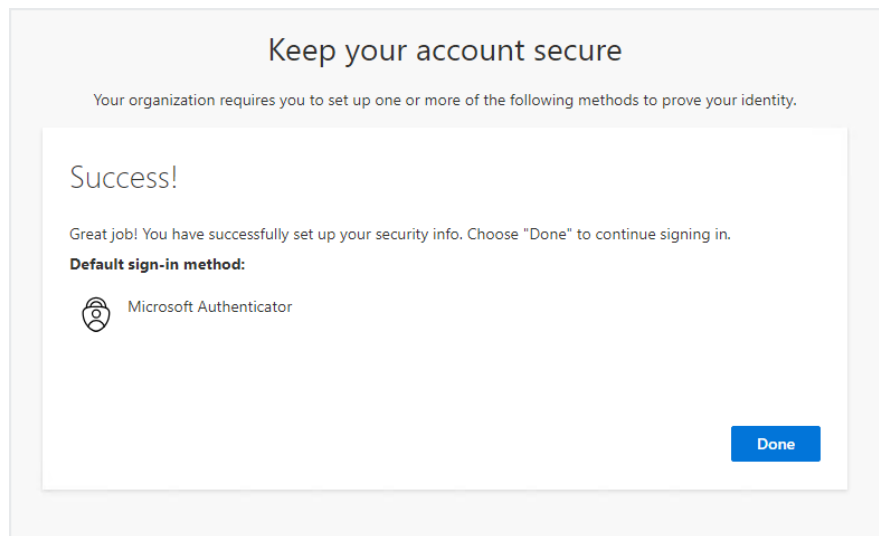
4. In the app, select *'Add an account'* choose the option *'Work or school account'*, and scan QR code.



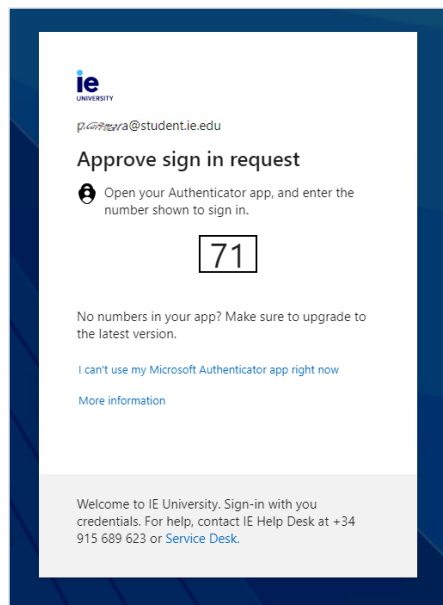
5. Next, you need to try out the app. **In the app on your phone**, type the number shown on your computer screen or other device and click 'yes' to confirm sign in.



If it is correct and the digits match, the test will be correct.



From now on, when the system asks us for MFA, we will have to go to the app and indicate the number it shows us.



We recommend that you add a second authentication method, preferably one you can access using a different device.

So, we can prevent problems if we forget, lose or change the device we use for MFA.

To set up a second method, log into the Microsoft Security Information page <https://mysignins.microsoft.com/security-info> Add sign-in method and follow the steps on-screen.

In this video you can learn more about Multi-Factor Authentication (MFA) [How to apply the Microsoft Multi-Factor Authentication at IE University? on Vimeo](#)