Account and Security

Log into your account for the first time

Just received your first login details and don't know what to do now?

Forgotten your password?

Locked out of your account?

There are four **STEPS** to this guide. You will:

1. log in using our Microsoft **Single Sign-on** system and create a strong **new password**
2. set up **Multi-factor Authentication** using the **Microsoft Authenticator** app
3. learn how to change your password while logged **in**
4. learn how to change your password while logged **out**.

For your convenience, use two devices:

- **Your computer** (which could be a **personal device** or University-issued one such as a **Surface Pro** or **Dell laptop**) – prepare by opening a web browser to **myltu.leedstrinity.ac.uk**
- **Your smartphone** (Android or Apple) – prepare by going to the Play Store or App Store to find the Microsoft Authenticator app.

It is *less intrusive* and *more secure* to use the Microsoft Authenticator app on your smartphone than to provide your mobile number and receive plain SMS texts.

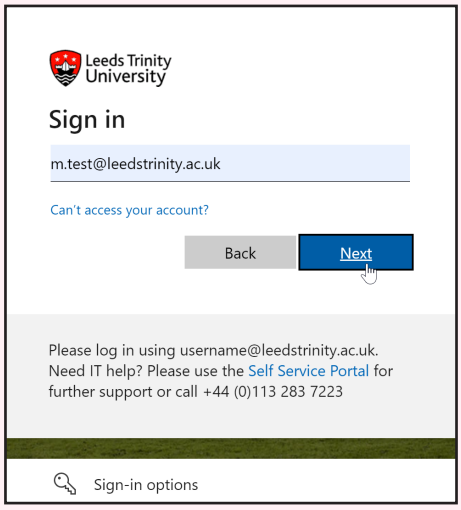
Changing your password here will change it for ALL your Leeds Trinity University IT Services logins.

STEP 1 is on the next page.

If you have already set up Multi-factor Authentication using the Microsoft Authenticator app and are logged **out**, jump straight to **STEP 4** on page 6.

STEP 1: Log in for the first time

It's best to set this up as soon as you get your login details from the University. You will need to change your password as soon as possible anyway to use some services, so now is a good time to do it.

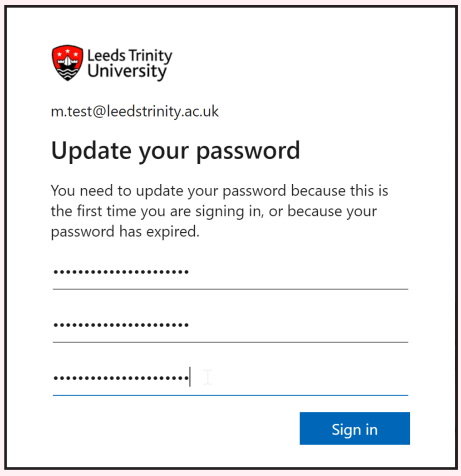


On your computer, open a web browser to myltu.leedstrinity.ac.uk and enter your University email address and the randomly-generated temporary password you received.

Your University email address is username-or-student-number@leedstrinity.ac.uk

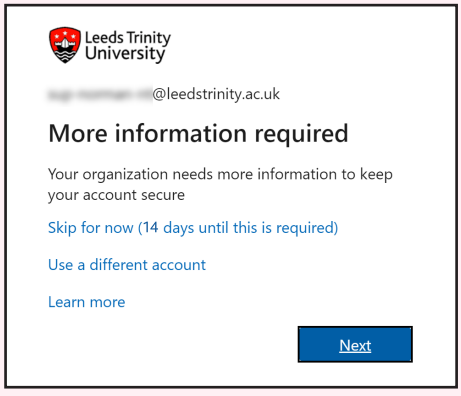
e.g., 2412345@leedstrinity.ac.uk

Click **Next** each time.



When you log in for the first time, you will need to change your password to one only you know.

Your temporary password is not secure enough for normal use, so it can only be used once.



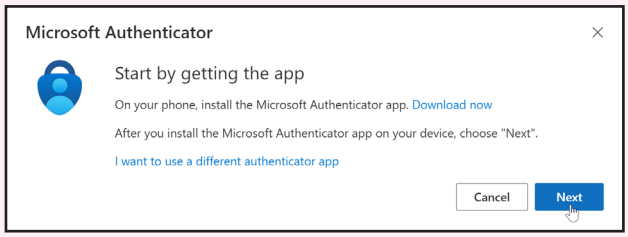
You will be prompted for more information. This is where we set up Multi-factor Authentication.

Click **Next** and proceed to **STEP 2**.

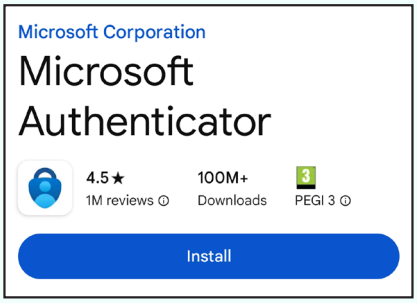
STEP 2: Download and install the Microsoft Authenticator app

You will need your computer and your smartphone during this step.

1: On your computer, you will see this screen:

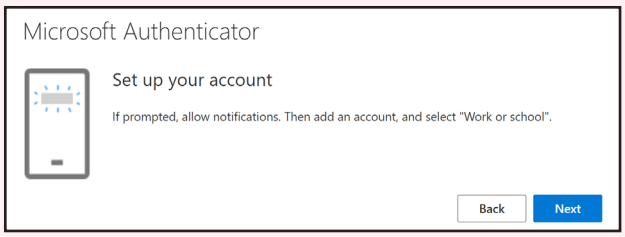


2: On your smartphone, find the **Microsoft Authenticator** app on the **Play Store** or the **App Store** and **install** it on your device.

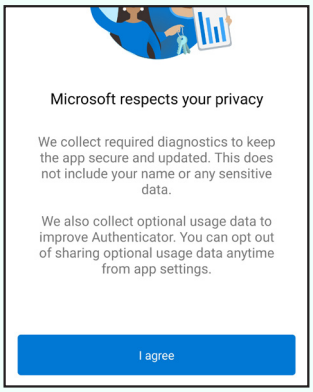


3: On your computer, click **Next** on the screen above.

You will see this screen:

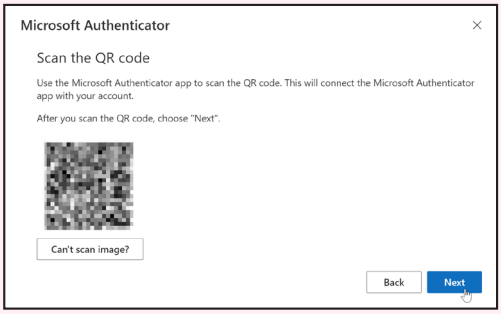


4: On your smartphone, tap **I agree** to dismiss the notifications like the one below. You may also get a notification that prompts you to allow the app to take pictures and record video. Agree to this too.

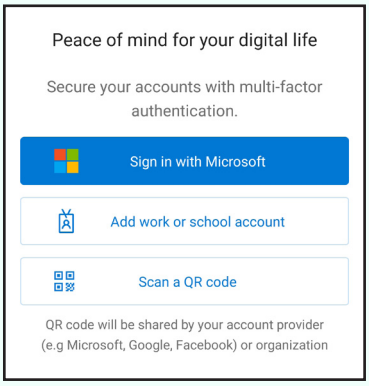


5: On your computer, once you have agreed to all the notifications on your phone, click **Next**.

You will see this screen:



6: On your smartphone, tap **Scan a QR code**.



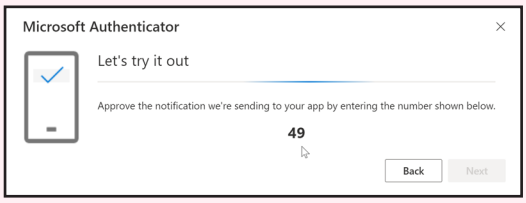
This STEP continues on the next page.

7: On your smartphone, the camera will activate and a square will appear in the middle of the image. Hold your phone up to your computer screen to capture the QR code displayed there.

The code will be captured automatically once the code is visible and in focus.

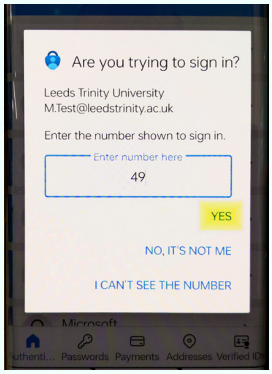
8: On your computer, click **Next**.

You will see this screen:



9: On your smartphone, enter the number shown and tap **YES**.

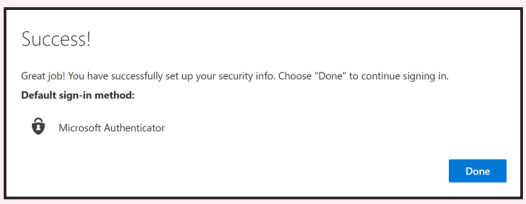
(You are not logging in yet. The server is simply verifying that your phone is getting the messages.)



10: On your computer, the screen below confirms that your Leeds Trinity University account is now paired with the Microsoft Authenticator app.

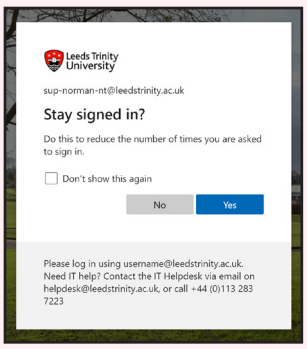
Click **Next**.

This final screen shows that you have the app assigned to your account as your normal sign-in method.



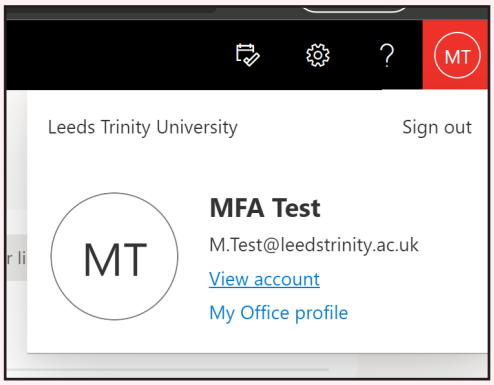
Click **Done** to finish the process.

11: Choose whether to stay signed in between sessions. After this you will see the Microsoft 365 portal homepage.



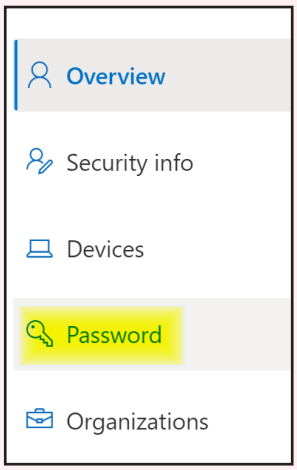
STEP 3: Reset your password while logged in

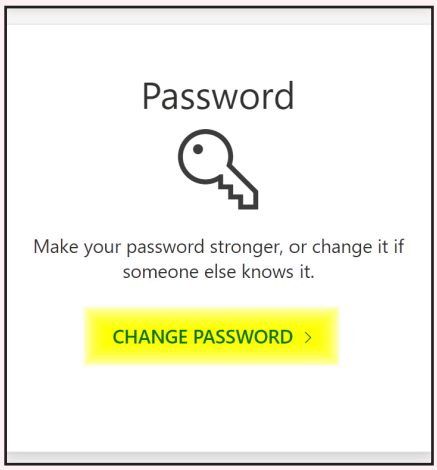
You will need **your computer** during this step.



On your computer, from the Office365 homepage, click on **your profile pic** on the top right (it might be a circle with initials in it).

Then choose **View account**.

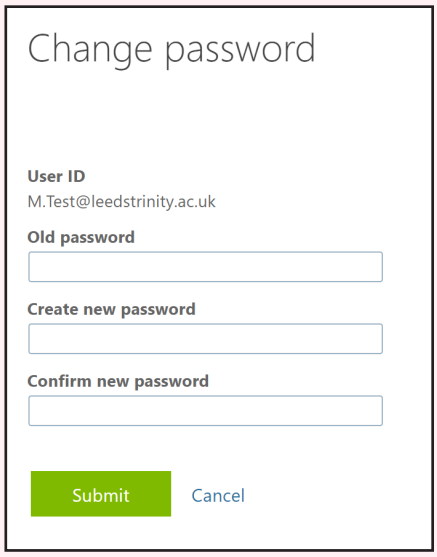




From the next screen you can either find the Password menu option on the left, or scroll to find the larger Password section on the main page.

They are both the same: you might see one before the other depending on your device.

Click the **Password menu item** or **Change password** in the larger box.



Enter your old password and type a new one.

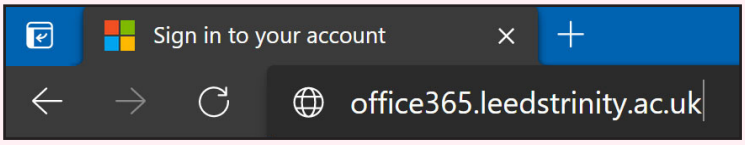
Advice on how to choose a good password or passphrase is on the last page of this guide.

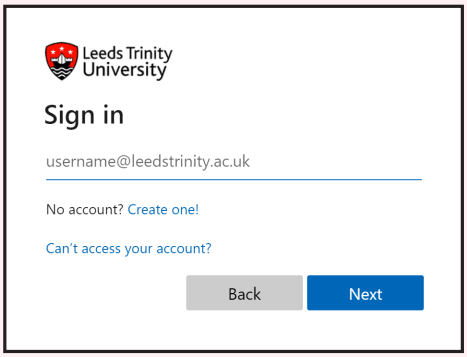
Click **Submit** to finish.

STEP 4: Reset your password while logged out

You will need **your computer** and **your smartphone** during this step.

1: On **your computer**, open a web browser and navigate to **office365.leedstrinity.ac.uk**



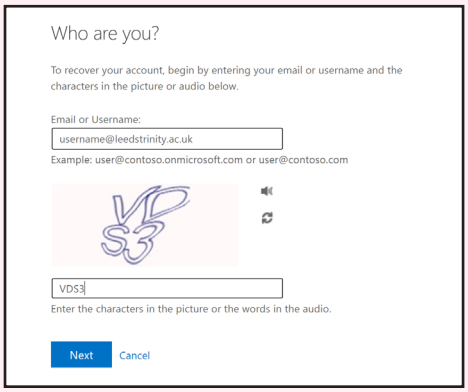


Enter your University email address in the box.

Your University email address is

username-or-student-number@leedstrinity.ac.uk

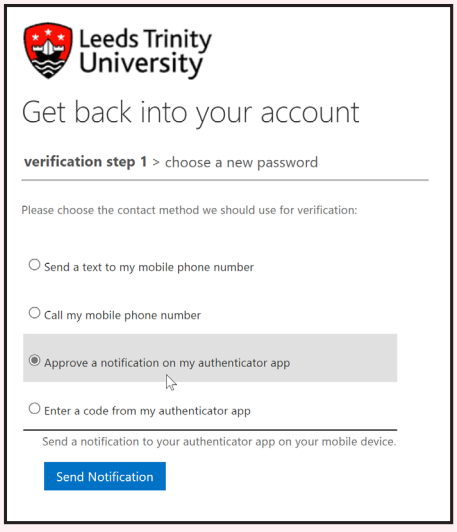
Click **Next**, then click **Forgotten my passsord**.



Type in the letters and numbers shown in the shaded area (the CAPTCHA). The letters are **case sensitive** and there are no spaces. If you are having trouble reading the characters on-screen, listen to the audio version instead.

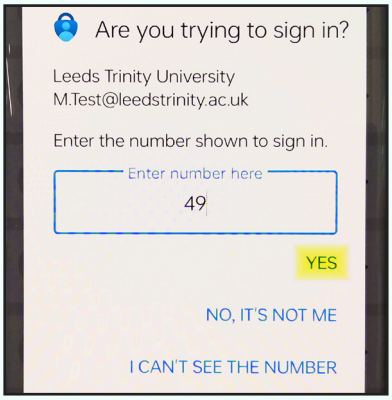
Click **Next**.

2: On **your computer**, you see the following screen. Choose "**Approve a notification**".

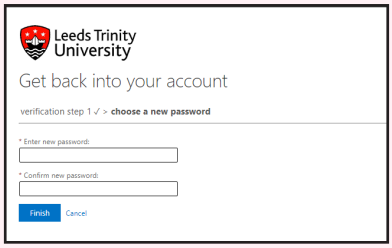


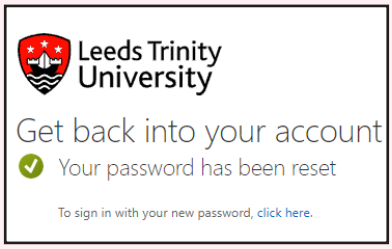
3: On **your smartphone**, look for a notification from the **Microsoft Authenticator** app.

Type the number shown and tap **YES**.



This STEP continues on the next page.





5: On **your computer**, enter a new password or passphrase and confirm it in the two boxes provided. Make sure it meets the **Password Guidelines**:

Strong Password Guidelines

- A memorable pass**phrase** is stronger than a pass**word**.
  Examples of good passphrases: *Everyoneloveseatingpizza!*
  Didwelandonthemoon69
- Your new passphrase must be **at least 12 characters** and include:
  - at least one capital letter
  - at least one symbol or number.
- Don't:
  - use any first names, surnames or variations on the word "Trinity"
  - use three consecutive numbers or the same number three times: 123, 654, 989, 111, etc.
  - reuse an old password.

Security Guidelines

- Always lock your device when you're not using it.
- Use a **separate** passphrase from any other online accounts, such as banking or shopping. If one gets compromised, you don't want any hacker to have access to both.
- If you must write your passphrase down, use a secure password storage app such as **LastPass**.
- **Don't use a passphrase that you have used before.**
- **Never reveal your passphrase to anyone.** The IT Helpdesk will never ask you for your passphrase.

If your chosen password or passphrase is **unsuitable**, you will see this error message:

"This password does not meet the length, complexity, age or history requirements of your corporate password policy."

Finally, click Finish.

Remember:
Make sure you update all your devices (phones, tablets and PCs) with your new password for logins and Wi-Fi access.

For your security, multiple wrong password attempts will lock your account automatically, so if you don't update all your devices, you will keep getting locked out.

The new password may not work straight away as it needs to sync to (where applicable):

- My LTU App
- Remote Access
- Office 365
- Campus Wi-Fi (eduroam)
- e-Vision
- Moodle
- Library
- Student Union

You have now completed this guide.