Multi-Factor Authentication: Guide for Authenticator App

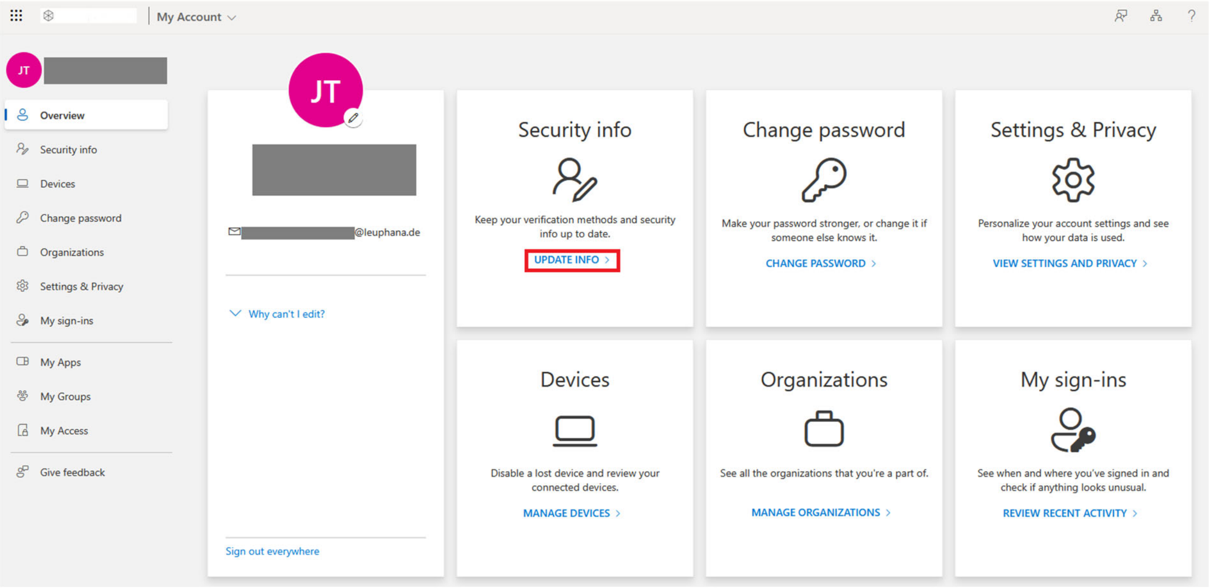
To secure your Leuphana account, a multi-factor authentication will be introduced. This means that you will need an additional, independent factor in addition to a password to log in to many Leuphana systems, such as myCampus, myStudy, email, Office, etc. This factor can be an authenticator app or a physical token.

In this guide, we will explain how to use an authenticator app, such as the Microsoft Authenticator, as a second factor. You can download this app for free from the respective app stores.

To follow this guide, you will need:

- Your email address (e.g. first name.last name@stud.leuphana.de or first name.last name@leuphana.de)
- The password for this email address (cloud password)
- Your smartphone

Log in to https://myaccount.microsoft.com with your account.



[redacted]

[redacted]@leuphana.de

Security info

Keep your verification methods and security info up to date.

Change password

Make your password stronger, or change it if someone else knows it.

Settings & Privacy

Personalize your account settings and see how your data is used.

Devices

Disable a lost device and review your connected devices.

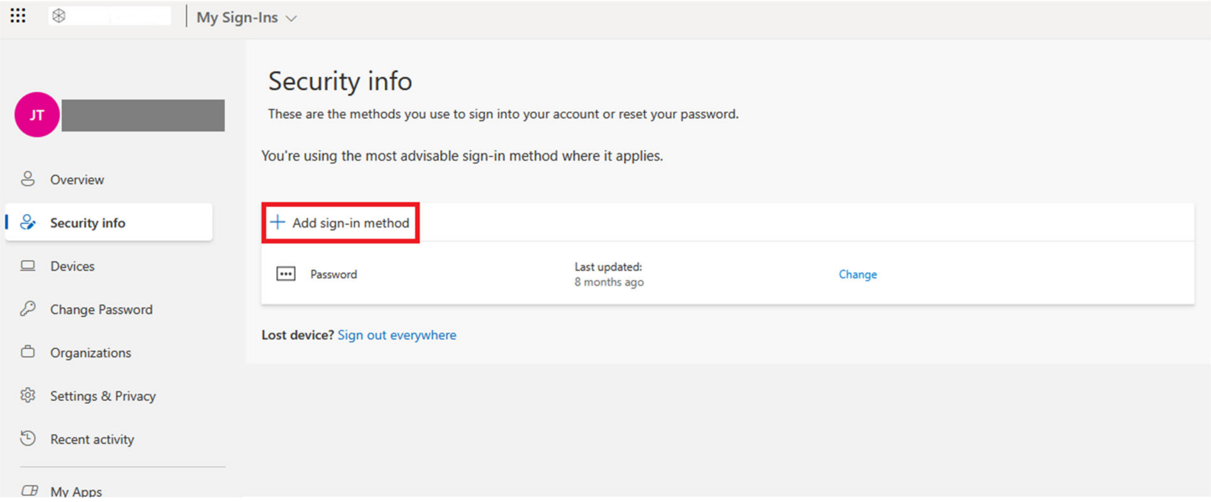
Organizations

See all the organizations that you're a part of.

My sign-ins

See when and where you've signed in and check if anything looks unusual.

On the **Security Info tile**, click **Update Info**.



My Sign-Ins

JT [redacted]

- Overview
- Security info
- Devices
- Change Password
- Organizations
- Settings & Privacy
- Recent activity
- My Apps

Security info

These are the methods you use to sign into your account or reset your password.

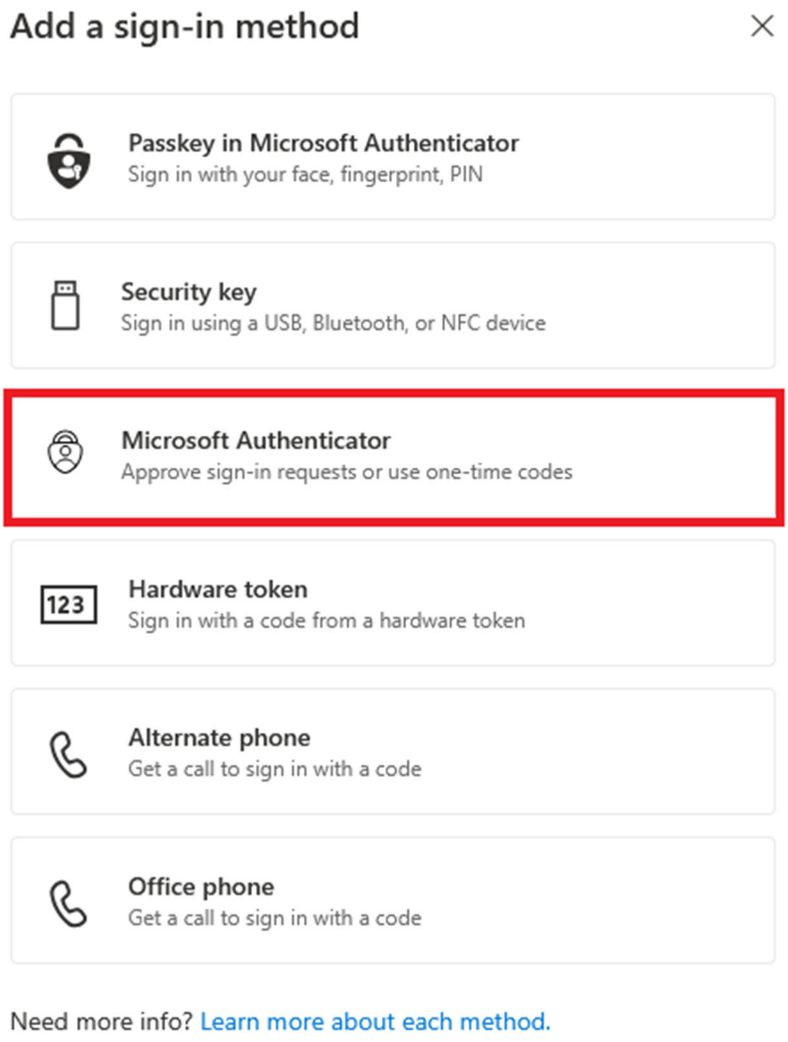
You're using the most advisable sign-in method where it applies.

+ Add sign-in method

Password	Last updated: 8 months ago	Change

Lost device? Sign out everywhere

Under **Security Info**, click **Add sign-in method**.



Add a sign-in method

Passkey in Microsoft Authenticator
Sign in with your face, fingerprint, PIN

Security key
Sign in using a USB, Bluetooth, or NFC device

Microsoft Authenticator
Approve sign-in requests or use one-time codes

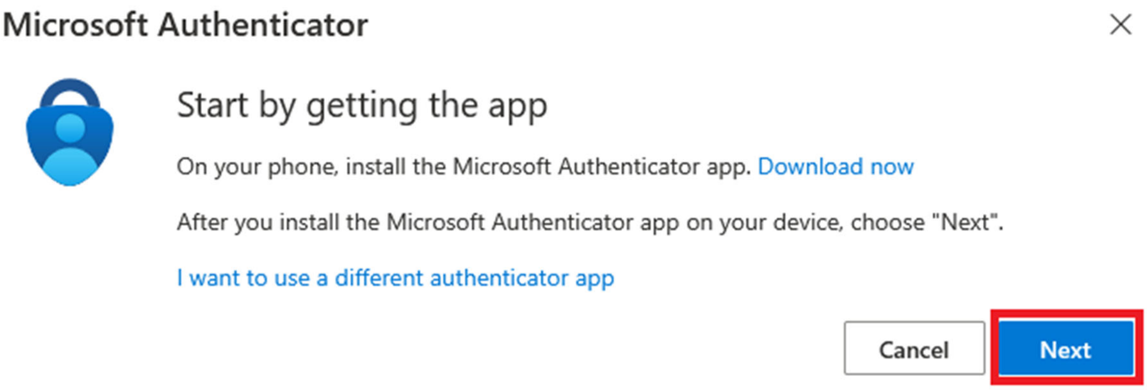
Hardware token
Sign in with a code from a hardware token

Alternate phone
Get a call to sign in with a code

Office phone
Get a call to sign in with a code

Need more info? Learn more about each method.

and then on **Microsoft Authenticator**



Microsoft Authenticator

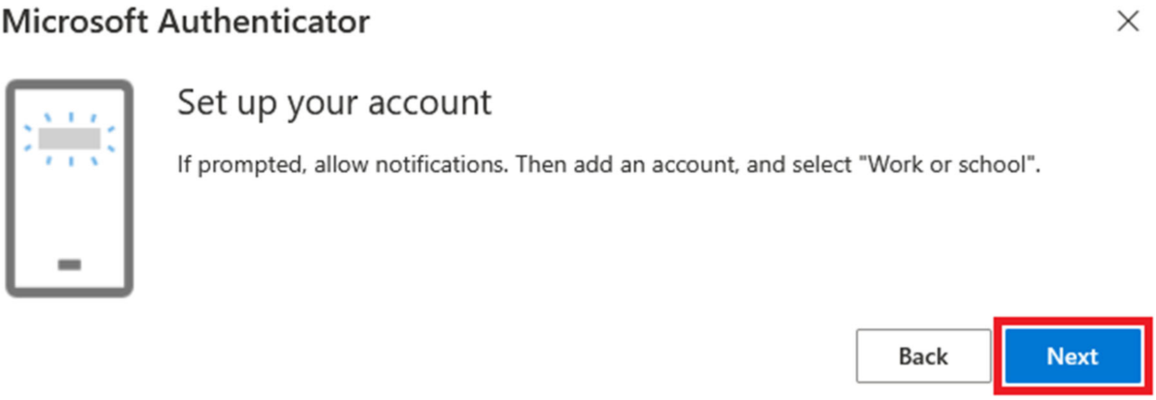
Start by getting the app

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

The window that appears will prompt you to download the Microsoft Authenticator app. Download the app if you have not already done so and click **Next**.



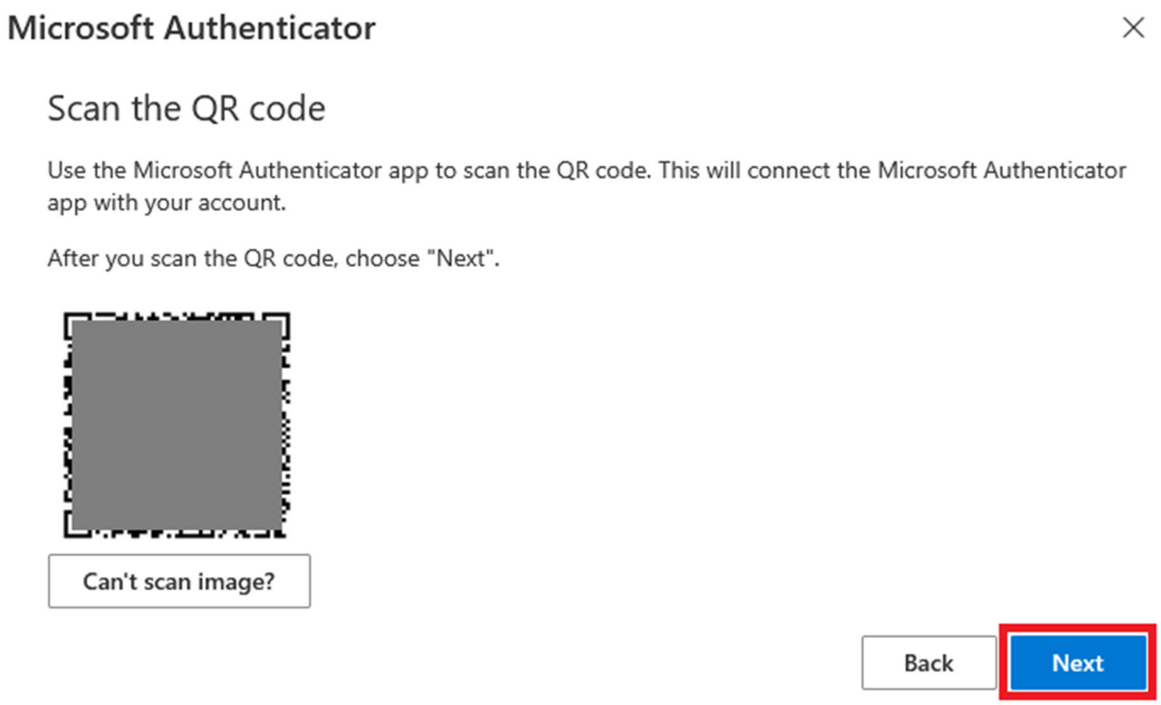
Microsoft Authenticator

Set up your account

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

When you launch the app on your smartphone for the first time, you will be asked to allow notifications. Allow this and select **Business or school account (Uni account)**. Then log in with your access data, i.e. your email address and password.

After successfully logging into the app, return to the Microsoft page and confirm by clicking **Next**.



Microsoft Authenticator

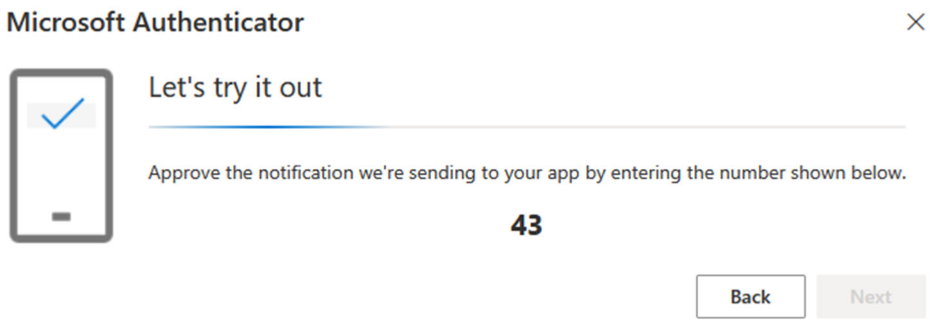
Scan the QR code

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".

[redacted]

Scan the QR code with your Authenticator app on your smartphone.
After scanning, click Next and a two-digit number will be displayed in the next window.
Enter this number in your app. A pop-up window will appear in the app for you to enter the number.



Microsoft Authenticator

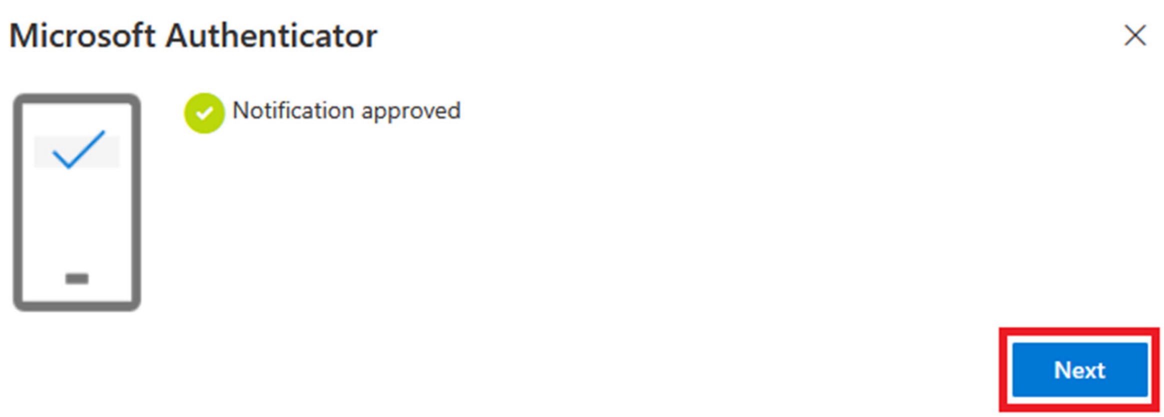
Let's try it out

Approve the notification we're sending to your app by entering the number shown below.

43

If you are setting up the device exclusively via your smartphone, or if you are unable to scan the QR code for any other reason, you can activate the device manually.

1. Click on **Can't scan image**.
2. Go to the QR code scanner in the app.
3. Choose “Enter code manually”
4. Select “Business or school account.”
5. Enter the code and URL displayed. Alternatively, you can simply copy the code and URL.
6. Tap “Finish.”



Microsoft Authenticator

You will then receive confirmation that the setup was successful.

You have now set up a second factor to protect your account.