WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

TWO-FACTOR AUTHENTICATION

for online services at WU

Content

1 General Information 2

2 Using Authenticator Apps 2

2.1 Create a TOTP Token 3

2.2 Set up Microsoft Authenticator 4

2.3 Set up PrivacyIDEA Authenticator 5

3 Using SMS delivery 6

4 Feedback and Support 7

TIP Read the **FAQs on two-factor authentication** to find out how it fits in practice at work: **short.wu.ac.at/community-faqs-2fa-en**

1 General Information

Two-factor authentication (2FA) improves the protection of online services and systems at WU. When logging in, authorized users must enter a second, unique piece of information in addition to their password (e.g. a numeric code). This so-called second factor is generated or delivered independently from the first one (e.g. via an app on a mobile device or via SMS).

What is the "second factor"?

At WU, the second factor consists of a 6-digit numerical code that is valid only for a short period of time and can be used only once. This is called a "***T**ime-based **O**ne-**T**ime **P**assword*" (abbreviated: **TOTP**).

PLEASE NOTE

- You can activate and set up the two-factor authentication via the *Two-factor authentication* menu in the **Controlpanel application**
- There are two options available to get the second factor:
  1. use an **authenticator app** (recommended)
  2. receive an **SMS** message to a cell phone number registered for this service
- When logging in to an online service with 2FA, you are required to enter:
  - your **WU account password** (*first factor*)
  - a **6-digit sequence of numbers** (TOTP) that is valid for a short period of time (*second factor*)

2 Using Authenticator Apps

IMPORTANT

A **TOTP token** is required when using an authenticator app. You can create this token anytime in the Controlpanel application and get a QR code in the process. Scan the QR code with your authenticator app.

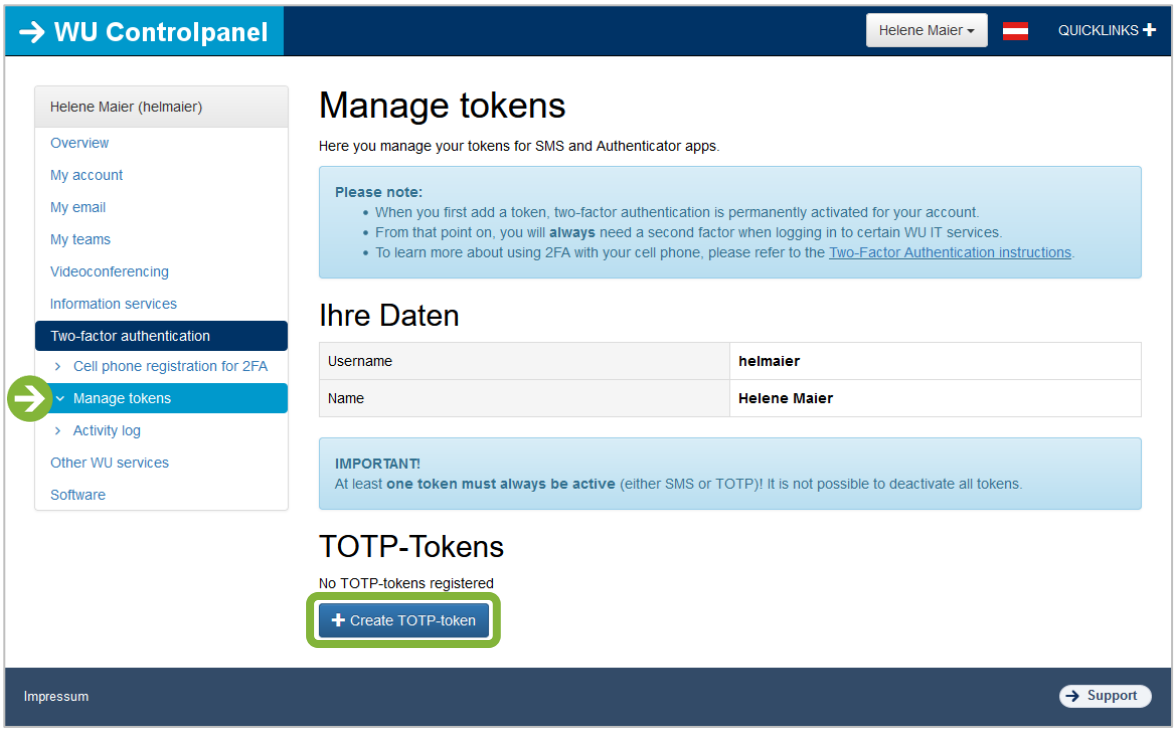
Please follow these steps to use **2FA** with an **authenticator app**:

1	Create a TOTP token in the **Controlpanel application**.	see details **on page 3**
2	Please choose and install <u>one</u> of the two authenticator apps on your mobile phone.	• Microsoft Authenticator **on page 4** *or* • privacyIDEA **on page 5**
3	Scan the QR code displayed in the Controlpanel application with your authenticator app.	• Microsoft Authenticator **on page 4** *or* • privacyIDEA **on page 5**

2.1 Create a TOTP Token

To generate a **TOTP token**, please log in to the **Controlpanel application**.

Select ***Two-Factor Authentication > Manage Tokens*** from the menu on the left.
Then click on ***Create TOTP-token***.



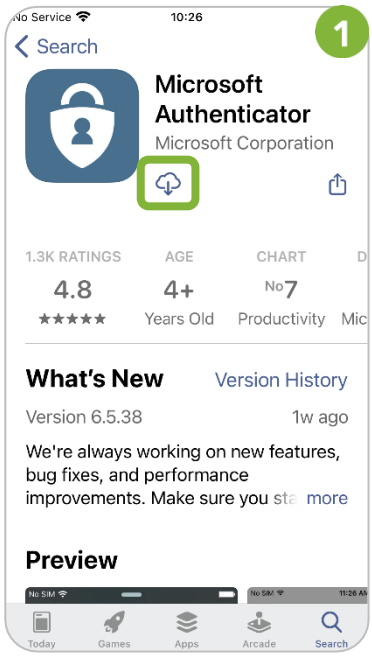
Your TOTP token is displayed in the form of a **QR code**.
Please use your authenticator app to scan this QR code.

- Use this QR code **only once** and **exclusively** with your authenticator app!
- The QR code contains the secret key for your token and is subject to the same **secrecy requirements** as your account password.
- If you suspect unauthorized use or misuse of your token, **deactivate** the TOTP token currently in use and generate a new one.

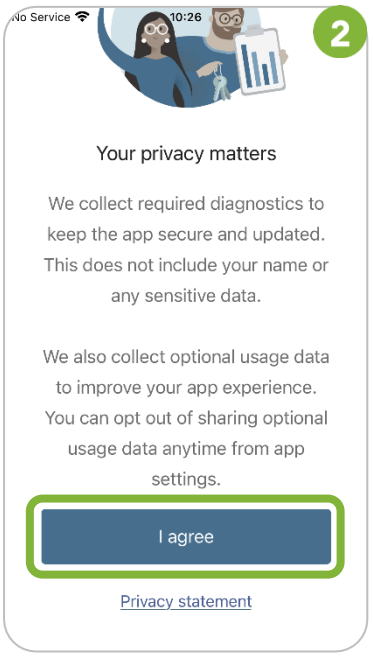
2.2 Set up Microsoft Authenticator

• **Apple** App Store:	**Microsoft Authenticator**
• **Google** Play Store:	**Microsoft Authenticator**

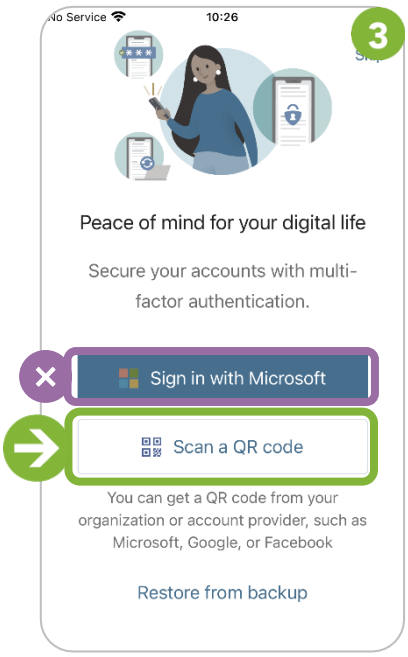
Download the app from the store



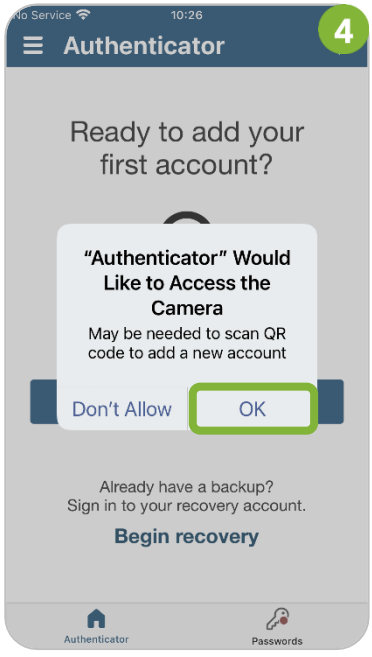
Agree to the privacy policy



Select ***Scan a QR code***

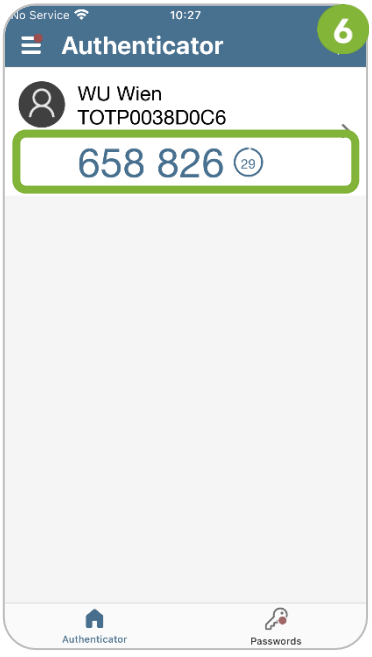


Allow access to camera: please select ***OK***



Scan the **QR code** displayed in the Controlpanel application

Your one-time password (**TOTP**) is now available

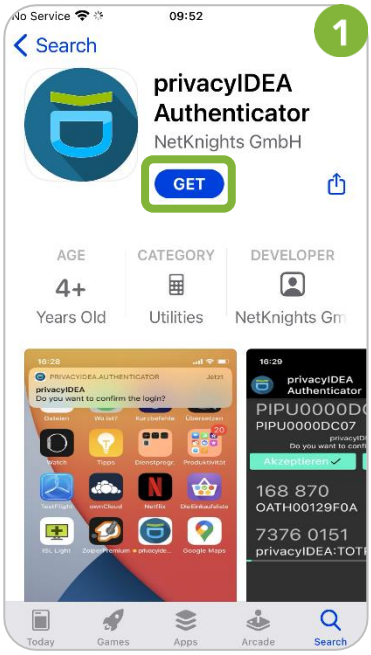


SUPPORT We are ready to help if you experience difficulties or have questions about 2FA. Please send us your support request via the **Service Desk**.

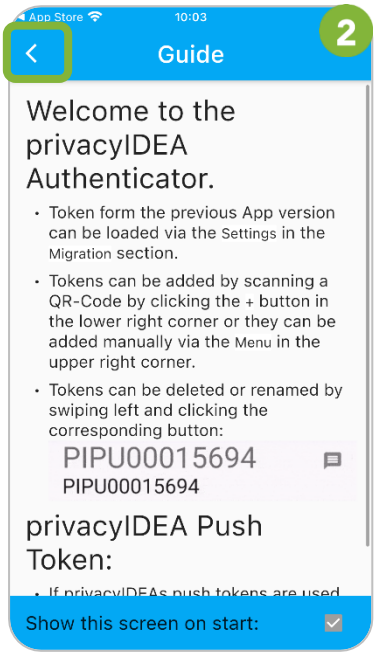
2.3 Set up PrivacyIDEA Authenticator

• **Apple** App Store:	**privacyIDEA Authenticator**
• **Google** Play Store:	**privacyIDEA Authenticator**

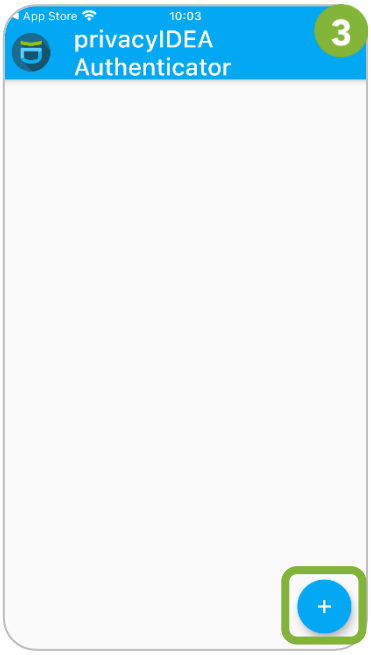
Download the app from the store



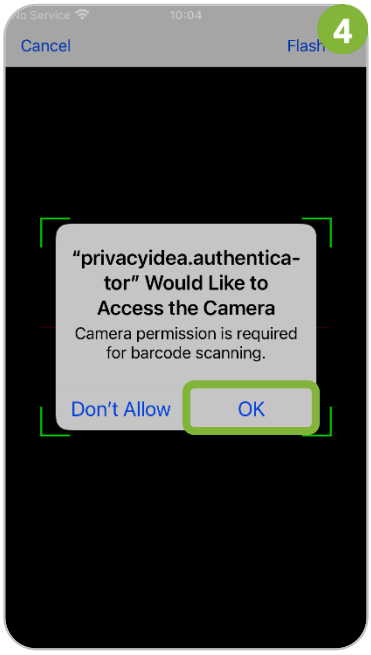
Exit the app guide: select the ***'back' arrow***



Select the ***plus symbol*** on the bottom right

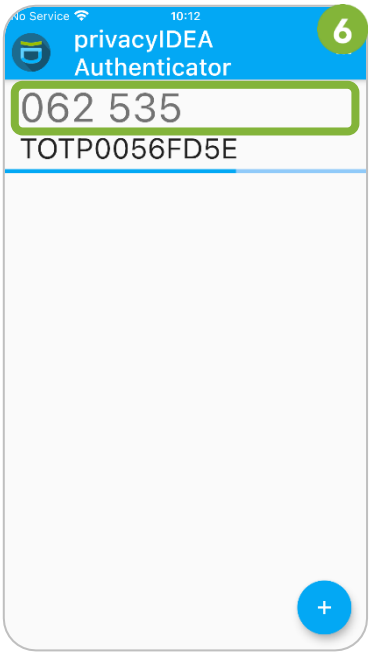


Allow access to camera: please select ***OK***



Scan the **QR code** displayed in the Controlpanel application

Your one-time password (**TOTP**) is now available

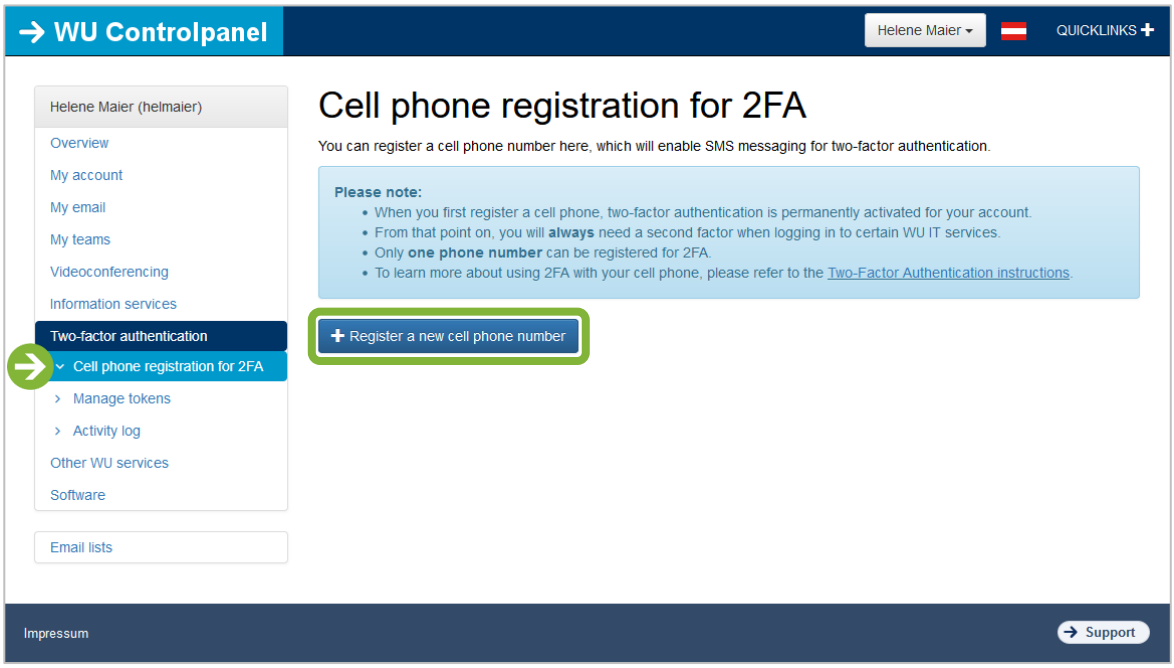


SUPPORT We are ready to help if you experience difficulties or have questions about 2FA. Please send us your support request via the **Service Desk**.

3 Using SMS delivery

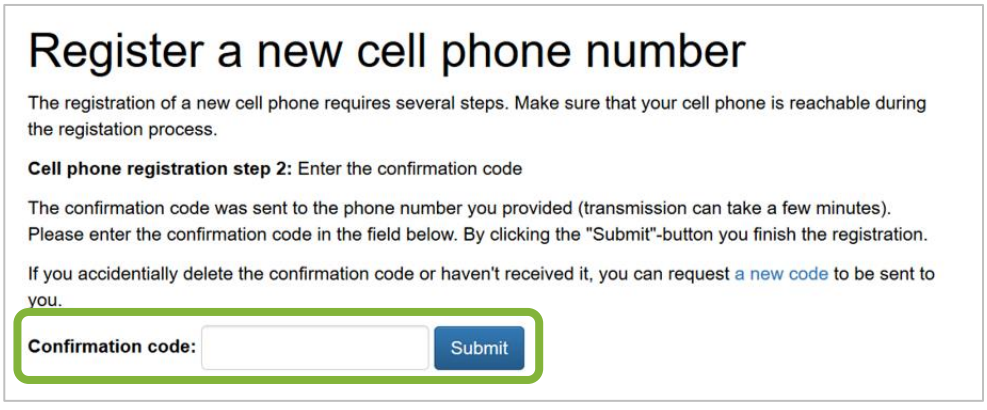
You can also receive your one-time password (TOTP) via SMS on your cell phone. To do this, please register your **Austrian cell phone number** in the **Controlpanel application**.

Select ***Two-factor authentication*** > ***Cell phone registration*** in the menu on the left.
Please select ***Register a new cell phone number***.

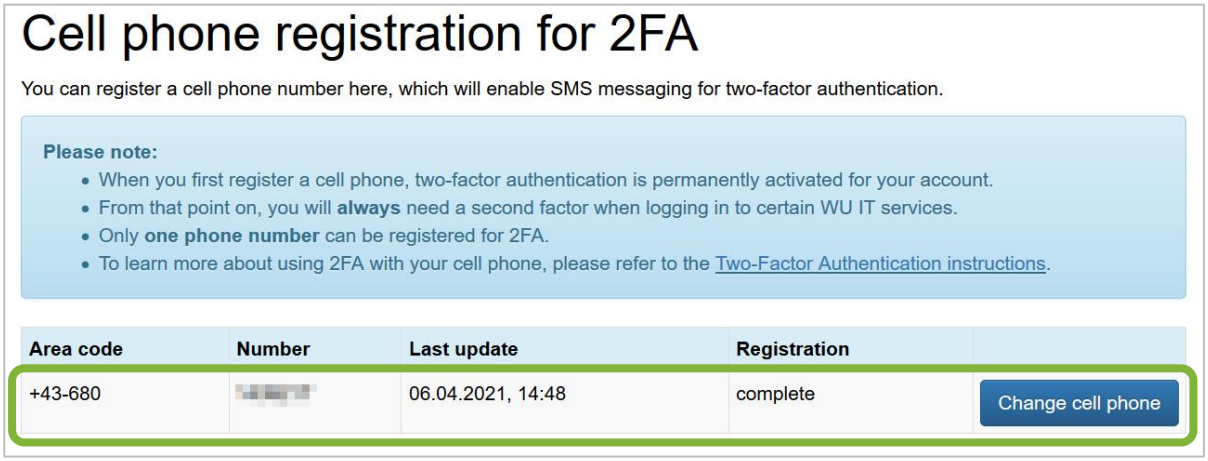


Enter your (Austrian) cell phone number. Then click **Next**.

You will receive a confirmation code via SMS.
Please enter the code in the field ***Confirmation code*** and click **Submit**.



Your cell phone has been registered and will be displayed in the table.



PLEASE NOTE

- You can register only **one** cell phone number for two-factor authentication.
- Click the ***Change cell phone*** button if you want to receive the SMS on a different phone number.

4 Feedback and Support

The **IT Support Center** at the Vienna University of Economics and Business is the first point of contact for WU faculty, staff, and students in all IT-related matters. We are available to provide additional help and are also interested in your feedback on these instructions.

Hotline	+43 1 313 36 – 3000
Email	hotline@wu.ac.at
Availability	short.wu.ac.at/it-support-hours
Website	www.wu.ac.at/en/it/support