New accounts - first steps

Summary

To fully activate your WU account, new employees must complete the following steps:

1. **Register a second factor.**
   - Log in to the Controlpanel, you will be automatically redirected to the 2FA setup.
   - Follow the information and instructions on the page Zwei-Faktor-Authentifizierung (2FA) bei Conditional Access | EN .
   - *Recommendation:* Use the **Microsoft Authenticator** for a simple and straightforward setup.
   - Use the initial password (=first password received) from your **account data sheet** for your first login.
2. **Changing the initial password**
   - After successfully setting up 2FA, set a password of your own choice in the Controlpanel.
   - You can find tips for choosing a secure password on our website.
   - This step must be completed within 30 days after the account data sheet is issued.
     Please check the date stated on the data sheet, especially if you plan to use your account at a later time.
3. **Completing the Information Security Briefing**
   - Work through the linked content and confirm that you will follow the guidelines in your daily work.
   - Complete the briefing within 7 days after changing your initial password.
4. **Finalizing your account setup**
   - To make full use of your WU account, please also review the **Further Steps** section on this page.

If your WU account has been disabled, please contact IT Support: +43-1-313 36 - 3000

Please note

- Accounts for new employees can be activated no earlier than 7 days before the official start of employment.
- Accounts can be activated by the responsible supervisor via the Controlpanel.

(1) Setting up Two-Factor Authentication

Please refer to the page Zwei-Faktor-Authentifizierung (2FA) bei Conditional Access | EN for details on how 2FA works and which login methods are available.

We recommend using **authenticator apps.** The **Microsoft Authenticator app** in particular offers additional benefits when used with Windows 11, such as **biometric login** on your WU devices.

Attention

- Without a second factor, you cannot log in to IT services at WU Vienna.

- **New WU employees** need an *activated* second factor to participate in **IT onboarding** (i.e. receiving your WU notebook).
- If **new WU employees** wish to use a **hardware token** for 2FA, they must visit the IT Support Center (D2, entrance C – see campus map) for the initial registration of the second factor. Your WU notebook can therefore be issued no earlier than the afternoon of the day you activate the hardware token.

(2) Changing the initial password

1. Log in to the Controlpanel using the credentials from your account data sheet and your previously registered second factor.
2. You will be automatically prompted to change your password.
3. Choose a password or passphrase. The password must be known only to you to ensure that your digital identity at WU is well protected.

With your new password, you will gain access to Microsoft Teams and your WU email account. You can now also manage your WU account independently via the Controlpanel.

Attention

If you do not change the initial password, your account will be **disabled 30 days after the initial password is changed**.

(3) Completing the Information Security Briefing

After changing the initial password, the *Information Security Briefing* page is displayed in the Controlpanel. You can edit the content **immediately** or **within the following 7 days**. As long as the briefing is not completed, it is displayed in the Controlpanel every time you log in.

1. Work through the contents of the Information Security Briefing.
2. Confirm compliance with the measures using the checkboxes.

If you have not completed the briefing on the 6th day after changing the initial password, you will receive a reminder email. On the 7th day, your account will be disabled. If your account is disabled, please contact **IT support: +43-1-313 36 - 3000.**

Attention

If you do not confirm the stated issues in the *Information Security Briefing*, your account will be **disabled 7 days after the initial password is changed**.

Further steps

- **Register your mobile phone number in the Controlpanel**
  If you don't remember your account password, your registered cell phone can **easily help you to get a new password**.

- **Set your individual Wi-Fi password**

  To be able to use Wi-Fi at WU, you need a separate Wi-Fi password. You can set this password in the Controlpanel: *Controlpanel> My account > Password change* (similar to changing your account password).
- **Enable screen sharing for MS Teams**

  To share not only individual application windows but your entire screen in online meetings with Microsoft Teams, enable **Screen Sharing** and Screen Recording for Microsoft Teams - also in the Controlpanel.
- **Configure your VPN connection**

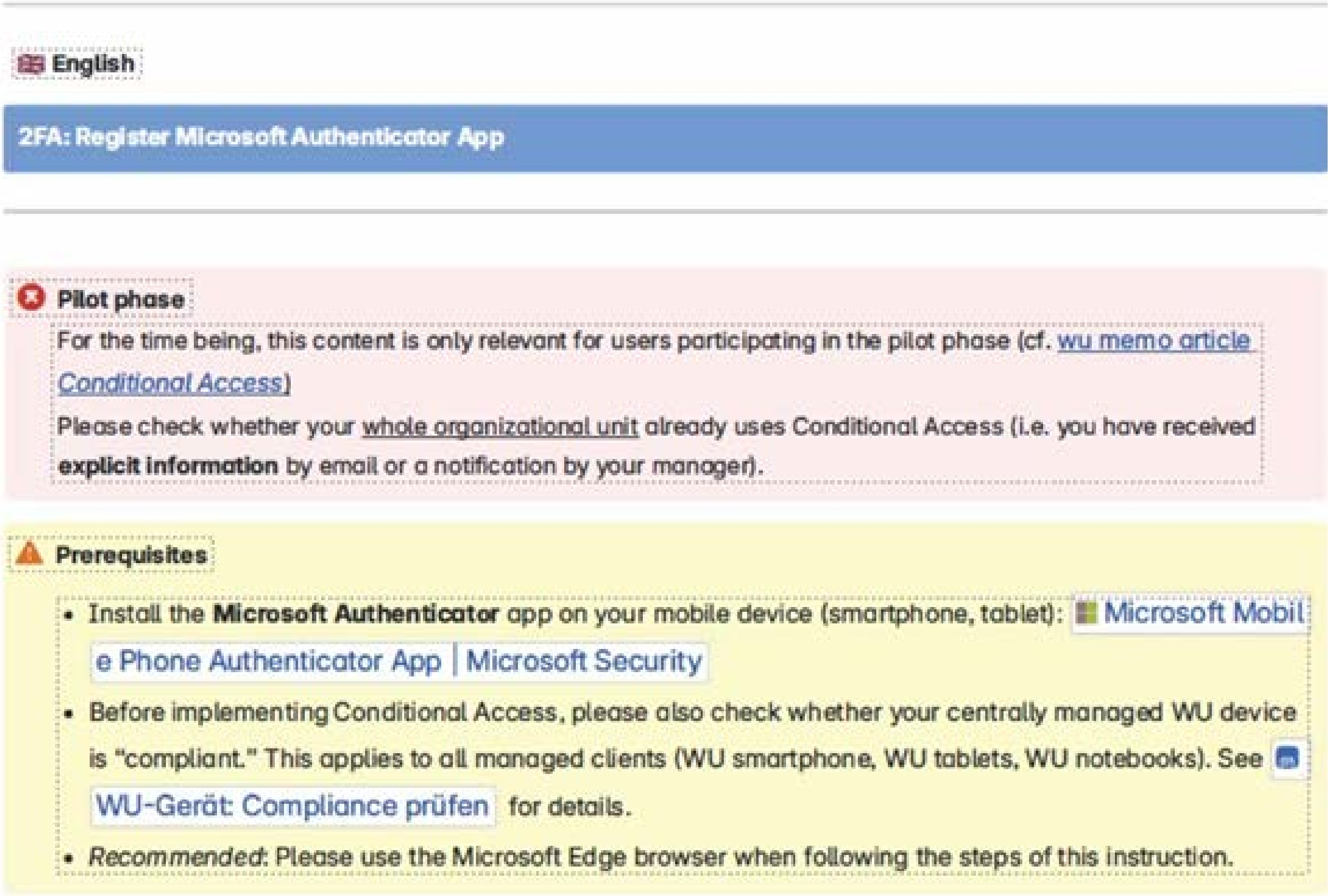
  A VPN connection provides access to IT services when you are:
  - **off campus**, or
  - using a **private device** or a **non-WU notebook**.

> ⚠
> - New employees can establish a VPN connection using the portal address: `evpn.wu.ac.at`.
> - WU-managed devices running **Windows 11** are automatically connected via VPN.

- **Install additional software**

  If you need additional software on your workplace computer, check the page Software and Workplace.

ⓘ For guidance on how to set up your WU account to match your daily work routine, see the page Account Management.



English

2FA: Register Microsoft Authenticator App

Pilot phase

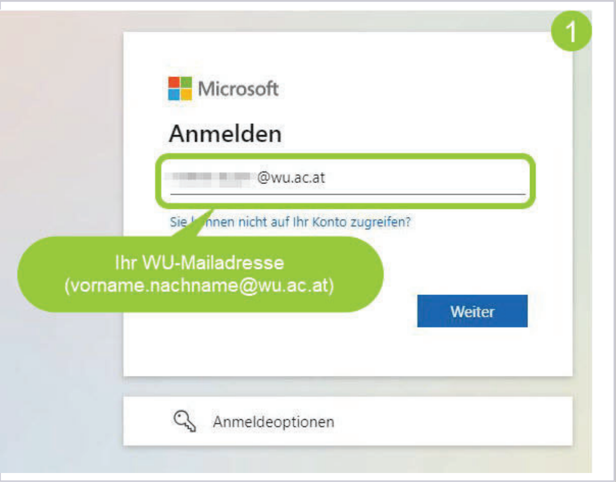
For the time being, this content is only relevant for users participating in the pilot phase (cf. wu memo article *Conditional Access*)

Please check whether your whole organizational unit already uses Conditional Access (i.e. you have received **explicit information** by email or a notification by your manager).

Prerequisites

- Install the **Microsoft Authenticator** app on your mobile device (smartphone, tablet): Microsoft Mobile Phone Authenticator App | Microsoft Security
- Before implementing Conditional Access, please also check whether your centrally managed WU device is "compliant." This applies to all managed clients (WU smartphone, WU tablets, WU notebooks). See WU-Gerät: Compliance prüfen for details.
- *Recommended*: Please use the Microsoft Edge browser when following the steps of this instruction.

1. Open the page [My Sign-Ins | Security Info | Microsoft.com] on your WU notebook.
   a. Log in with your **WU email address** (*vorname.nachname@wu.ac.at*).
   b. Then select *Continue*.



1

Microsoft

Anmelden

[redacted]@wu.ac.at

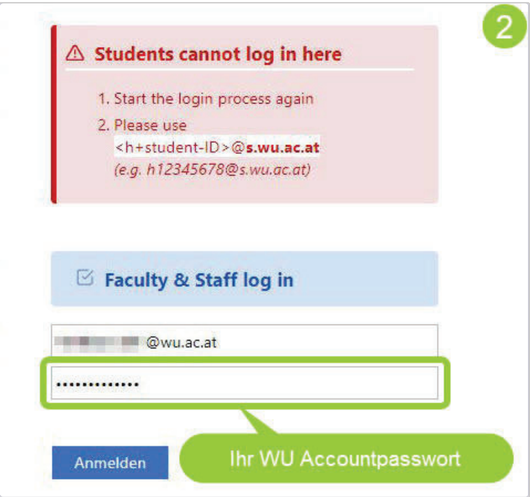
Sie können nicht auf Ihr Konto zugreifen?

Ihr WU-Mailadresse (vorname.nachname@wu.ac.at)

Weiter

Anmeldeoptionen

2. Enter your **WU account password** and select *Log in*.



2

⚠ **Students cannot log in here**

1. Start the login process again
2. Please use <h+student-ID>@**s.wu.ac.at** (*e.g. h12345678@s.wu.ac.at*)

☑ **Faculty & Staff log in**

[redacted]@wu.ac.at

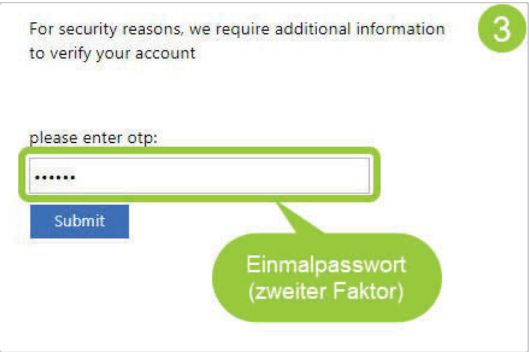
••••••••••••••

Anmelden

Ihr WU Accountpasswort

3. Please provide your **second factor** (*OTP token; one-time password*).

> **Note**
>
> ***Before switching to Conditional Access*** you still use the *previous second factor*, which you can manage in the Controlpanel application.



3

For security reasons, we require additional information to verify your account

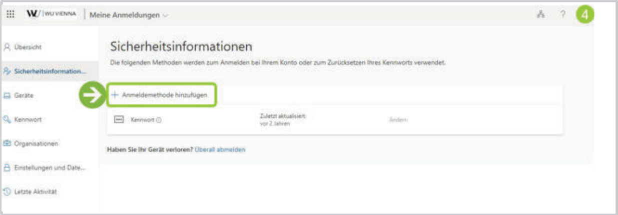
please enter otp:

••••••

Submit

Einmalpasswort (zweiter Faktor)

4. Open the *Security Information* section on the website. Select **Add Login Method**.



Sicherheitsinformationen

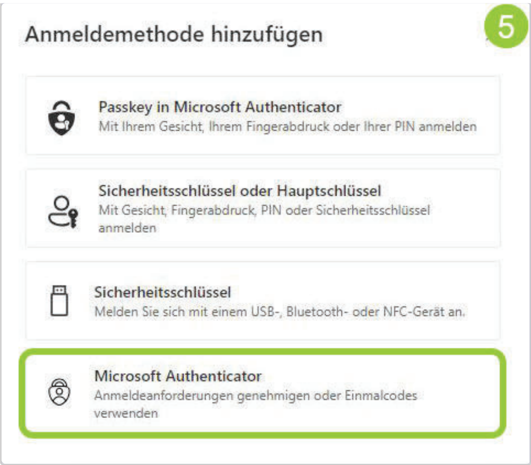
Die folgenden Methoden werden zum Anmelden bei Ihrem Konto oder zum Zurücksetzen Ihres Kennworts verwendet.

+ Anmeldemethode hinzufügen

Kennwort ⓘ	Zuletzt aktualisiert: vor 2 Jahren	Ändern

Haben Sie Ihr Gerät verloren? Überall abmelden

5. Select **Microsoft Authenticator** as your new sign-in method.



5

Anmeldemethode hinzufügen

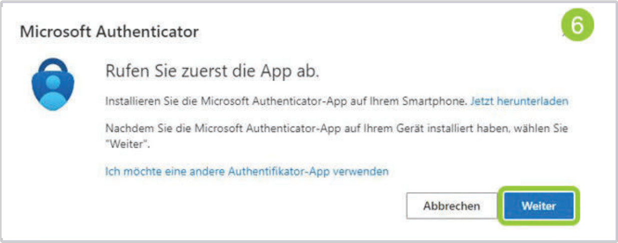
Passkey in Microsoft Authenticator
Mit Ihrem Gesicht, Ihrem Fingerabdruck oder Ihrer PIN anmelden

Sicherheitsschlüssel oder Hauptschlüssel
Mit Gesicht, Fingerabdruck, PIN oder Sicherheitsschlüssel anmelden

Sicherheitsschlüssel
Melden Sie sich mit einem USB-, Bluetooth- oder NFC-Gerät an.

Microsoft Authenticator
Anmeldeanforderungen genehmigen oder Einmalcodes verwenden

6. If you have already installed the app *Microsoft Authenticator* on your mobile device, select **Next**.
   a. If you do not have the app on your mobile device yet, install it now: Microsoft Mobile Phone Authenticator App | Microsoft Security . Then select **Next**.



6

Microsoft Authenticator

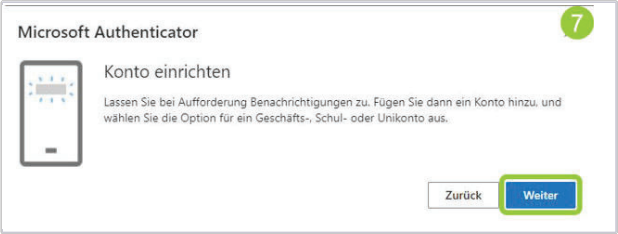
Rufen Sie zuerst die App ab.

Installieren Sie die Microsoft Authenticator-App auf Ihrem Smartphone. Jetzt herunterladen

Nachdem Sie die Microsoft Authenticator-App auf Ihrem Gerät installiert haben, wählen Sie "Weiter".

Ich möchte eine andere Authentifikator-App verwenden

7. Follow the instructions on your notebook and then click **Next**.



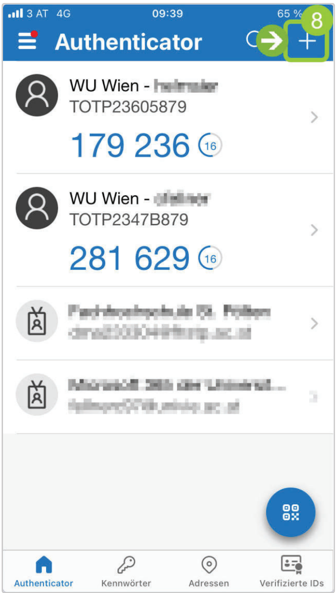
7

Microsoft Authenticator

Konto einrichten

Lassen Sie bei Aufforderung Benachrichtigungen zu. Fügen Sie dann ein Konto hinzu, und wählen Sie die Option für ein Geschäfts-, Schul- oder Unikonto aus.

8. On your mobile device: In the Microsoft Authenticator app, select the **"Plus" symbol ("+")** in the top right corner.



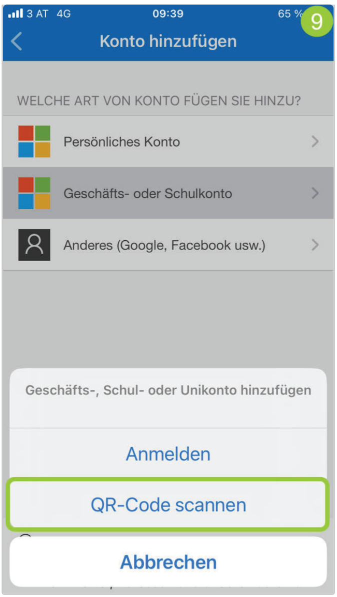
WU Wien - [redacted]
TOTP23605879
179 236 16

WU Wien - [redacted]
TOTP2347B879
281 629 16

[redacted]

[redacted]

9. Select **Business or School Account** and then **Scan QR Code**.



Konto hinzufügen

WELCHE ART VON KONTO FÜGEN SIE HINZU?

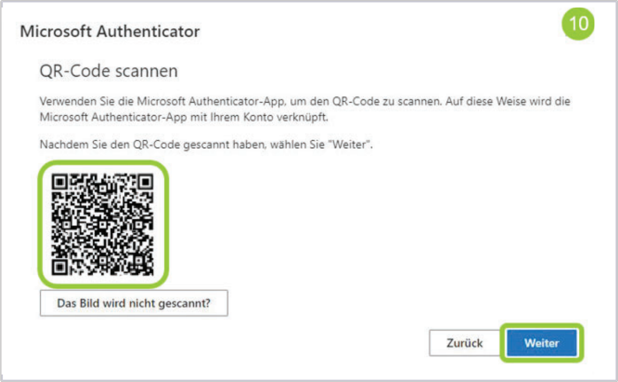
Persönliches Konto

Geschäfts- oder Schulkonto

Anderes (Google, Facebook usw.)

Geschäfts-, Schul- oder Unikonto hinzufügen

10. Now scan the **QR code** that is displayed on the notebook screen. Then select **Next**.



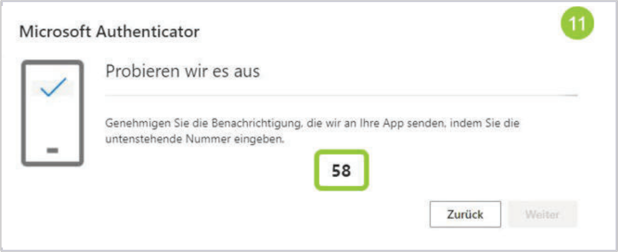
Microsoft Authenticator

QR-Code scannen

Verwenden Sie die Microsoft Authenticator-App, um den QR-Code zu scannen. Auf diese Weise wird die Microsoft Authenticator-App mit Ihrem Konto verknüpft.

Nachdem Sie den QR-Code gescannt haben, wählen Sie "Weiter".

11. A two-digit number is now displayed on your notebook screen. At the same time, you receive a prompt on your mobile device in the Microsoft Authenticator app.



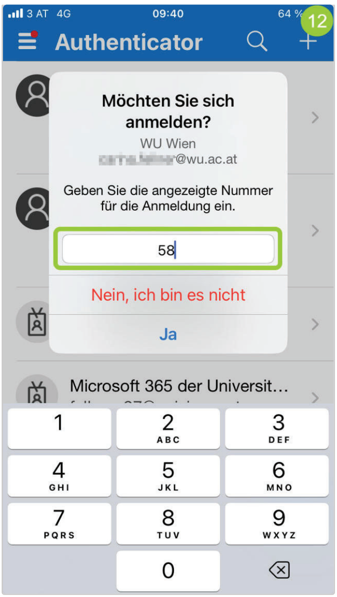
Microsoft Authenticator

Probieren wir es aus

Genehmigen Sie die Benachrichtigung, die wir an Ihre App senden, indem Sie die untenstehende Nummer eingeben.

58

12. Enter the **number** on your mobile device and select **Yes** to confirm the verification.



Möchten Sie sich anmelden?
WU Wien
[redacted]r@wu.ac.at

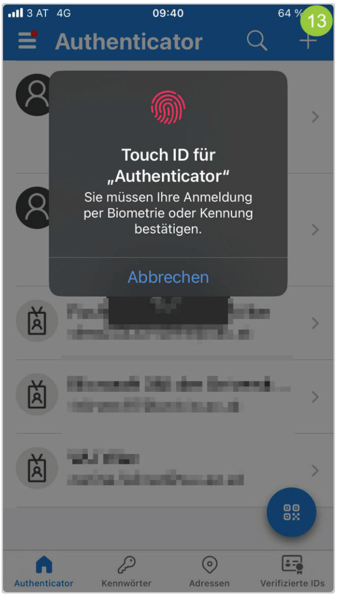
Geben Sie die angezeigte Nummer für die Anmeldung ein.

58

13. Confirm your input using **TouchID**, **face recognition**, or the **lock PIN** on the mobile device.

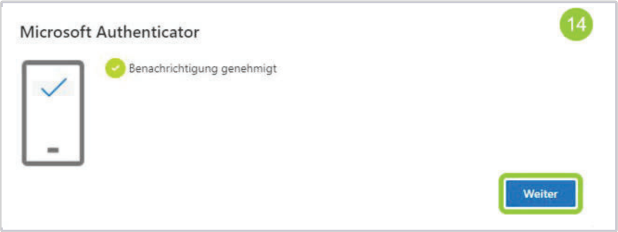
Good to know

- Biometric data provided by you (e.g. fingerprint, FaceID, etc.) is stored exclusively on your (mobile) device locally.
- WU Vienna has *no access* to biometric data on centrally managed devices.



Touch ID für „Authenticator“
Sie müssen Ihre Anmeldung per Biometrie oder Kennung bestätigen.

14. Select **Next** to complete the registration process. The Microsoft Authenticator app has been successfully registered.


Microsoft Authenticator

Benachrichtigung genehmigt