

uniLOGIN: Sign-in methods

[CC BY-NC 4.0](#) Uni Graz
Guide for students/staff
Status: Oktober 2026

1.) Access management

At <https://login.uni-graz.at/> you can manage your account's access settings. This platform is available after having successfully set up multifactor authentication for your account.

1.1. Adding an additional authentication method

To set up another device or an additional authentication method (app on the device), proceed as follows:

- Navigate to the heading **"Two-factor authentication"**
- Select **"Set up authenticator application"**

Two-factor authentication

Authenticator application

Enter a verification code from authenticator application.

[Set up Authenticator application](#)

Confirm the requested change by verifying your identity again (signing in):

uniLOGIN

Account Console

Please re-authenticate to continue

Login with uniACCOUNT

Email address (Uni Graz)

Password

[Password forgotten or expired?](#)

Login

Or sign in with

ID Austria

Sign-in is possible **either using your account credentials or via ID Austria.**

After successful sign-in you will be forwarded to the configuration window:

uniLOGIN



Mobile Authenticator Setup

1. For the one-time code to be calculated correctly, the time on your device must be correct. Check whether the time on your smartphone or any other device used is synchronised. If necessary, change the time setting to "obtain automatically".
2. Install one of the following applications on your mobile:
 - Google Authenticator
 - Microsoft Authenticator
 - privacyIDEA Authenticator
 - FreeOTP
 - TOTP compatible app

3. Open the application and scan the barcode:



[Unable to scan?](#)

4. Enter the one-time code provided by the application and click Submit to finish the setup.

You will need the one-time code from the app in the future to log in via uniLOGIN. The app must remain installed.

☐ Sign out from other devices

Cancel

Submit

Scan the QR code with the app you have selected.

Enter a device name or a reminder note for yourself in the field “**Device name**”. This entry serves to distinguish the apps/devices so that in future you can manage the activated devices yourself via the website <https://login.uni-graz.at>.

Confirm the setup of the additional device / the additional app by entering the one-time password that now appears there.

Afterwards, you can check at <https://login.uni-graz.at> whether the new setup appears under the name you specified.

During the setup process, recovery codes will also be displayed. Print these out, download them, or copy them into a password manager.

Recovery Authentication Codes

These recovery codes won't appear again after leaving this page

Make sure to print, download, or copy them to a password manager and keep them safe. Canceling this setup will remove these recovery codes from your account.

Confirm that you have stored/saved the recovery codes securely in order to complete the setup.

☒ I have saved these codes somewhere safe

☐ Sign out from other devices

Cancel setup

Complete setup

2. uniLOGIN – Configuration options via the sign-in window

2.1.) “Trusted device” (browser sign-in without a second factor)

This option allows you to sign in using the selected web browser **without an additional factor (one-time code) for a period of 30 days**. Use this option where required on devices that only you use, for example your work device.



uniLOGIN



Trust this device for 30 days?

Trusted devices do not need Multi-Factor Authentication (MFA) to sign in. Do NOT trust public or shared machines!

To activate this setting, proceed as follows:

1. Enter, in the **“Device name”** field, the browser being used or a keyword that makes it clear to you which browser/which device has been approved here.

Note: This designation will later appear for you at **login.uni-graz.at** for administration purposes.

Device name (e.g. smartphone)*
Edge on Windows

☐ Trust this device for 30 days?
This feature uses persistent cookies.

NoYes

2.) Tick the box **“Trust this device for 30 days?”**

☐ Trust this device for 30 days?
This feature uses persistent cookies.

NoYes

3.) Confirm your selection by clicking the **“Yes”** button.

☒ Trust this device for 30 days?
This feature uses persistent cookies.

NoYes



2.2.) Passkey Registration

Alternatively, select the button „Passkey Registration” to register a passkey.

Or sign in with

Passkey Registration

You will be redirected to the next step:

uniLOGIN



Passkey Registration

☐ Sign out from other devices

Cancel

Register

After selecting the “register” option, a window will be displayed where you can select the desired type of device. Follow the registration wizard to register the selected passkey.

2.3.) Sign-in using “ID Austria”

In case you are an Austrian national and have an ID Austria this option is already linked to your account. Access this sign-in option **by leaving the password field empty**.

uniLOGIN



Account Console

Login with uniACCOUNT

Email address (Uni Graz)
firstname.surname@uni-graz.at

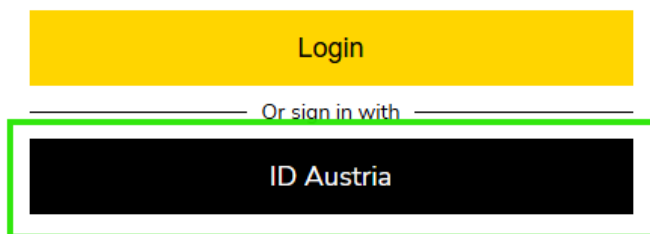
Password (leave blank for sign-in options)

[Password forgotten or expired?](#)

Login

After clicking the “Sign in” button, the “ID Austria” option will be displayed.

Select this button to sign in with your ID Austria.



Thank you for helping to improve IT security at our university by using MFA.