

Enable user account

1.

Generate temporary access code

1

2.

Multi-factor authentication

3

3.

Create Password

7

1. Generate temporary access code

We recommend doing all steps described below with your smart phone.

ONBOARDING PORTAL FIRST STEPS WITH YOUR USER ACCOUNT Sign in with your edu-ID to activate your user account. More information at uni.li/first-steps. Sign in with edu-ID	Open onboarding.uni.li, press “Sign in with edu-ID” and login with your private edu-ID you created before.
ONBOARDING PORTAL AFFILIATION CONFIRMED Activate account Your affiliation has been confirmed. Generate a one-time access code for your first login. Generate password	After successfully logging in, press Generate password.

ONBOARDING PORTAL LAST STEP Your access code %@6dv6^z Valid for 60 minutes · single use · won't be shown again 1. Open myaccount.microsoft.com. 2. Sign in with alexander.hasler@uni.li and the access code shown above.	The system will now generate a temporary access code. Make a screenshot or a photo of the displayed information. Open myaccount.microsoft.com.
Microsoft Sign in Email or phone Can't access your account? Next	Enter the email address are shown in the screenshot/photo you took and press Next.
UNIVERSITÄT LIECHTENSTEIN ← alexander.hasler@uni.li Enter Temporary Access Pass ☐ Show Temporary Access Pass Sign in another way Sign in	Enter the code is shown and press Sign in. After logging in, the MyAccount portal will open. Leave this window open and continue with the steps shown below.

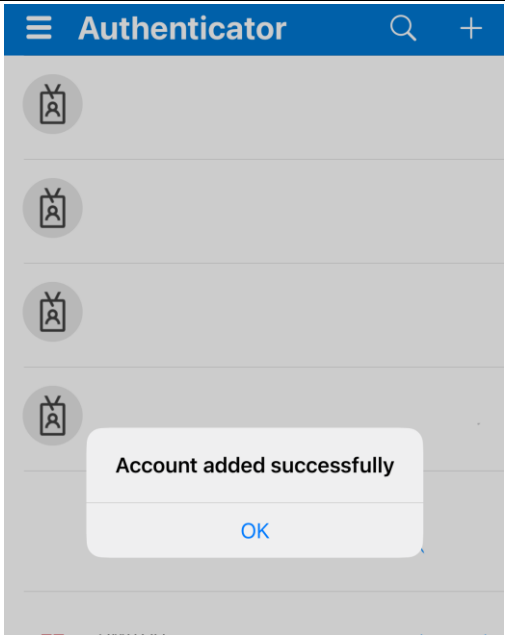
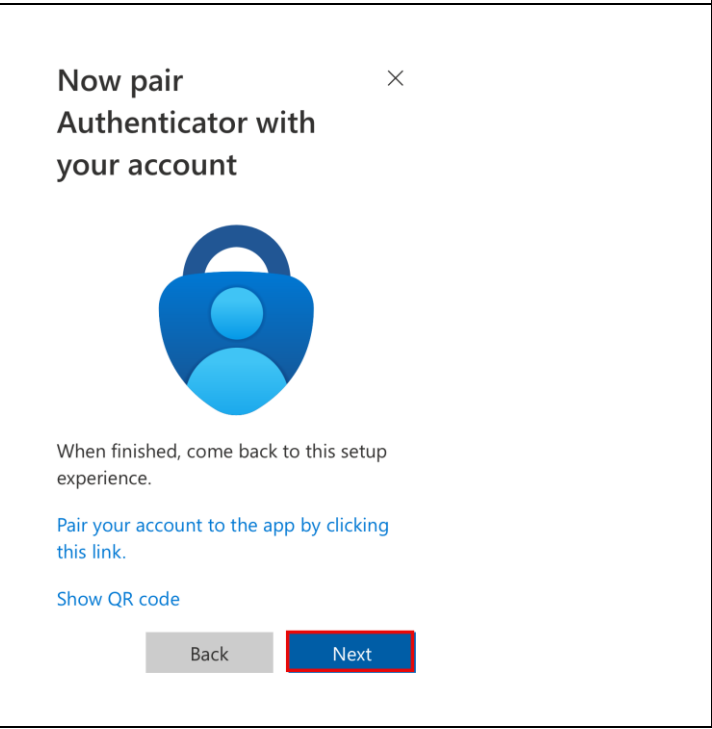
2. Multi-factor authentication

What is Multi-Faktor Authentication (MFA)?
Multi-factor authentication is a security process for accounts that requires two or more separate steps to verify the user’s identity. This step must be completed once and is mandatory for logging in to Moodle, Citrix and for resetting your password independently.

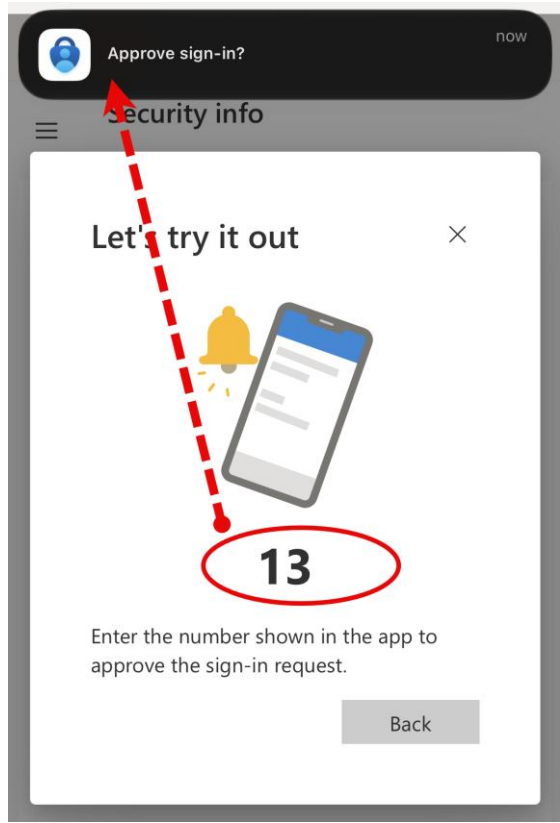
Manage access and security  View your devices Stay in control of your devices and get help if you lose access.  Change how you sign in Update your password, set up passwordless options, or manage two-step verification.	In My Account, scroll down and press Change how to sign in.
Security info These are 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. Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification Change + Add sign-in method *** Password Last updated: 10 months ago	Press Add sign-in method.
Add a sign-in method  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 Learn more about each method to help you choose.	Press Microsoft Authenticator.



Install Microsoft Authenticator × Install the app on your mobile device, then come back here to continue. Download on the App Store Set up a different authentication app Back Next	Go to the <u>App store</u> or <u>Playstore</u> and install the Microsoft Authenticator app. Back in your browser, press Next.
Now pair Authenticator with your account × When finished, come back to this setup experience. Pair your account to the app by clicking this link. Show QR code Back Next	Press Pair your account to the app by clicking this link.

	The Microsoft Authenticator will now open automatically, and you will see the message Account added successfully. <i>If the Authenticator does not open automatically, open it manually.</i>
	Go back to the browser and press Next.



	Enter the number are shown in the browser into the Microsoft Authenticator and approve with Yes.
✓ Authenticator Added  You can now use Microsoft Authenticator to approve sign-ins, get one-time codes, and more. This is now your default sign-in method. Done	You have successfully registered your smart phone for MFA. Press Done.

3. Create Password

Microsoft Get back into your account Who are you? To recover your account, begin by entering your email or username. Email or Username: * Example: user@contoso.onmicrosoft.com or user@contoso.com Next Cancel	Open moodle.uni.li and press “Lost password?”. Enter your email address (x.y@uni.li) and press Next.
UNIVERSITÄT LIECHTENSTEIN Get back into your account Why are you having trouble signing in? ☒ I forgot my password No worries, we'll help you to reset your password using the security info you registered with us. ☐ I know my password, but still can't sign in This might happen because you tried signing in with an incorrect password too many times. If you choose this option, you'll keep your existing password and we'll unlock your account so you can sign in again. Next Cancel	Select “I forgot my password” and press Next.
UNIVERSITÄT LIECHTENSTEIN Get back into your account verification step 1 > choose a new password Please choose the contact method we should use for verification: ☒ Approve a notification on my authenticator app Send a notification to your authenticator app on your mobile device. Send Notification ☐ Enter a code from my authenticator app Cancel	Select “Approve a notification on my authenticator app” and press Send Notification.

UNIVERSITÄT LIECHTENSTEIN Get back into your account verification step 1 > choose a new password Please choose the contact method we should use for verification: ☒ Approve a notification on my authenticator app ☐ Enter a code from my authenticator app Approve the notification we're sending to your app by entering the number shown below. 84	Enter the number shown into your Authenticator.
UNIVERSITÄT LIECHTENSTEIN Get back into your account verification step 1 ✓ > choose a new password * Enter new password: * Confirm new password: Finish Cancel	Enter a new password and press Finish. Please note our Password Policy below. The password must be at least 10 characters long and must meet at least three of the following four criteria: 1. Uppercase letters (A–Z) 2. Lowercase letters (a–z) 3. Numbers (0–9) 4. Special characters (e.g., !, \$, %, or &) Attention • The username may not be included in the password. • The password is valid for 180 days, after which it must be changed. • The password can only be changed once per day. • There is a password history of the last 24 passwords — these cannot be reused.