Multifactor Authentication With edu-ID

Certain services may require **multifactor authentication** (or **MFA**, **strong authentication**, or **two-factor authentication**) to increase the security level of our applications (more info on our blog, in French). In addition to your password, you will be asked for either:

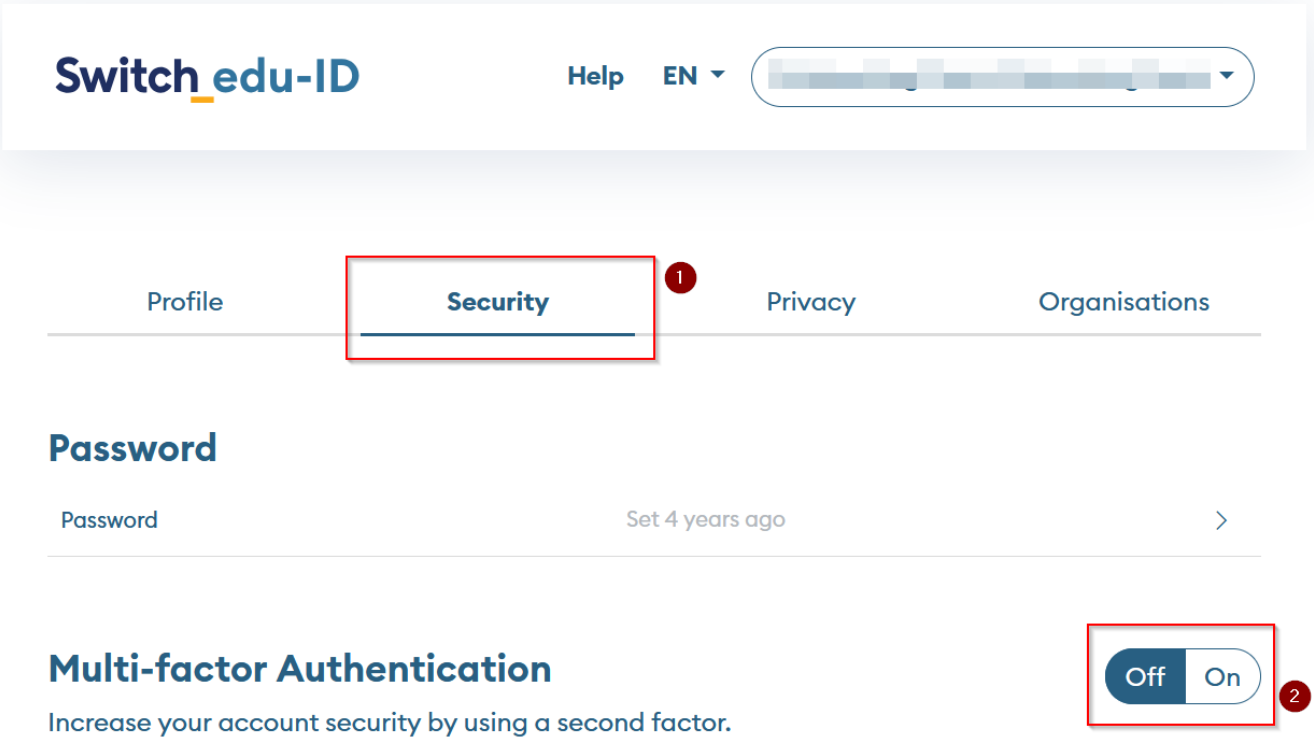
- A **one-time code** generated in an application designed for this purpose, called TOTP (such as Google Authenticator),
- To validate an authentication request **without a password** using **Passkey** technology
- ~~(or received via SMS, but this is not recommended for reliability reasons)~~. *(SMS will no longer be accepted as a 2nd factor token in 2026)*

The edu-ID identity includes the use of multifactor authentication, and its activation is easy. To read the official SWITCH documentation on MFA and edu-ID, visit the following page: https://help.switch.ch/fr/eduid/docs/services/login/two-step-login/

Activation

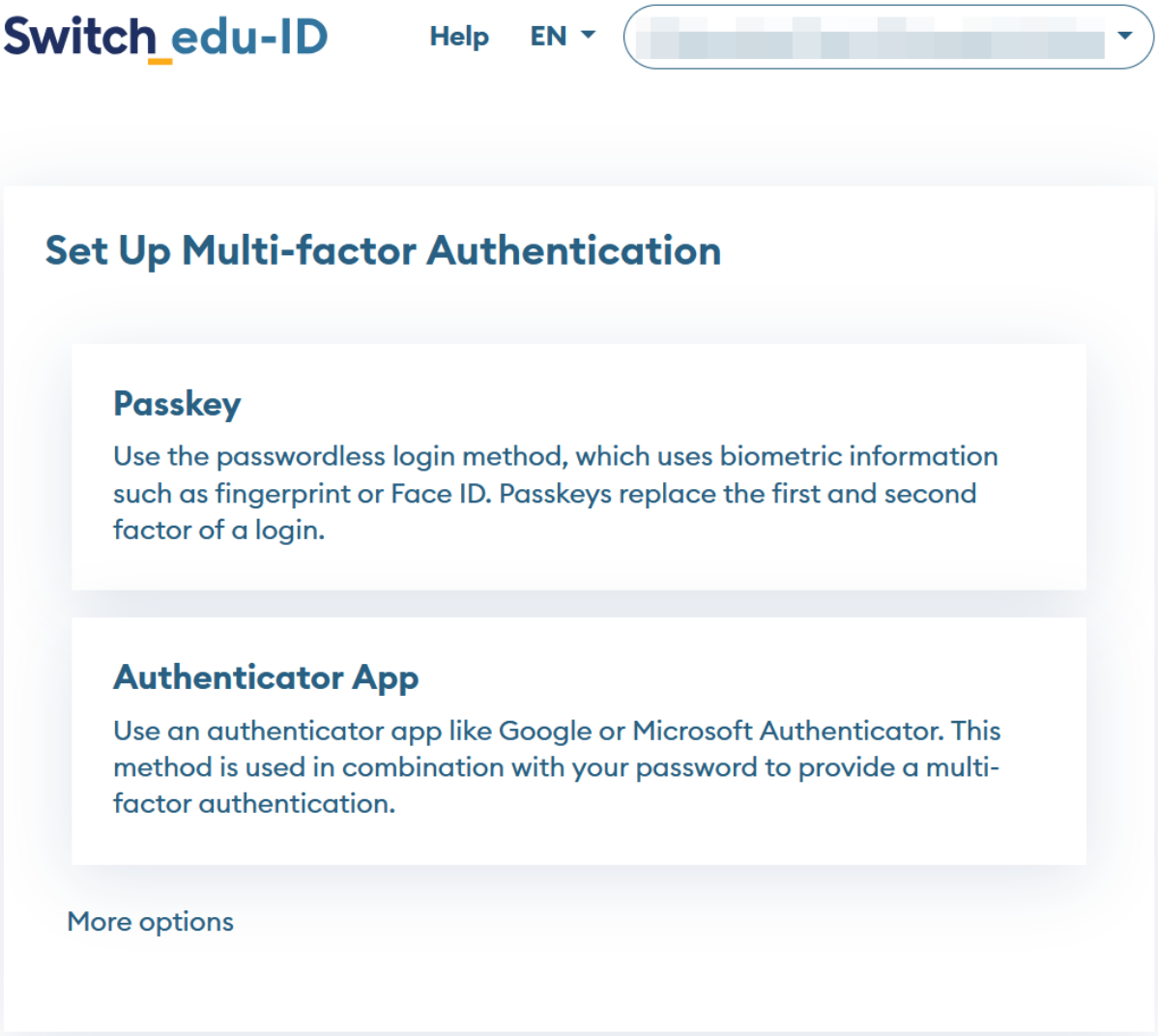
(adapted from the official SWITCH documentation)

To **enable** two-step login, go to your SWITCH edu-ID account at https://eduid.ch and click on the **Security** tab, and then click the On button next to **Multifactor Authentication**,



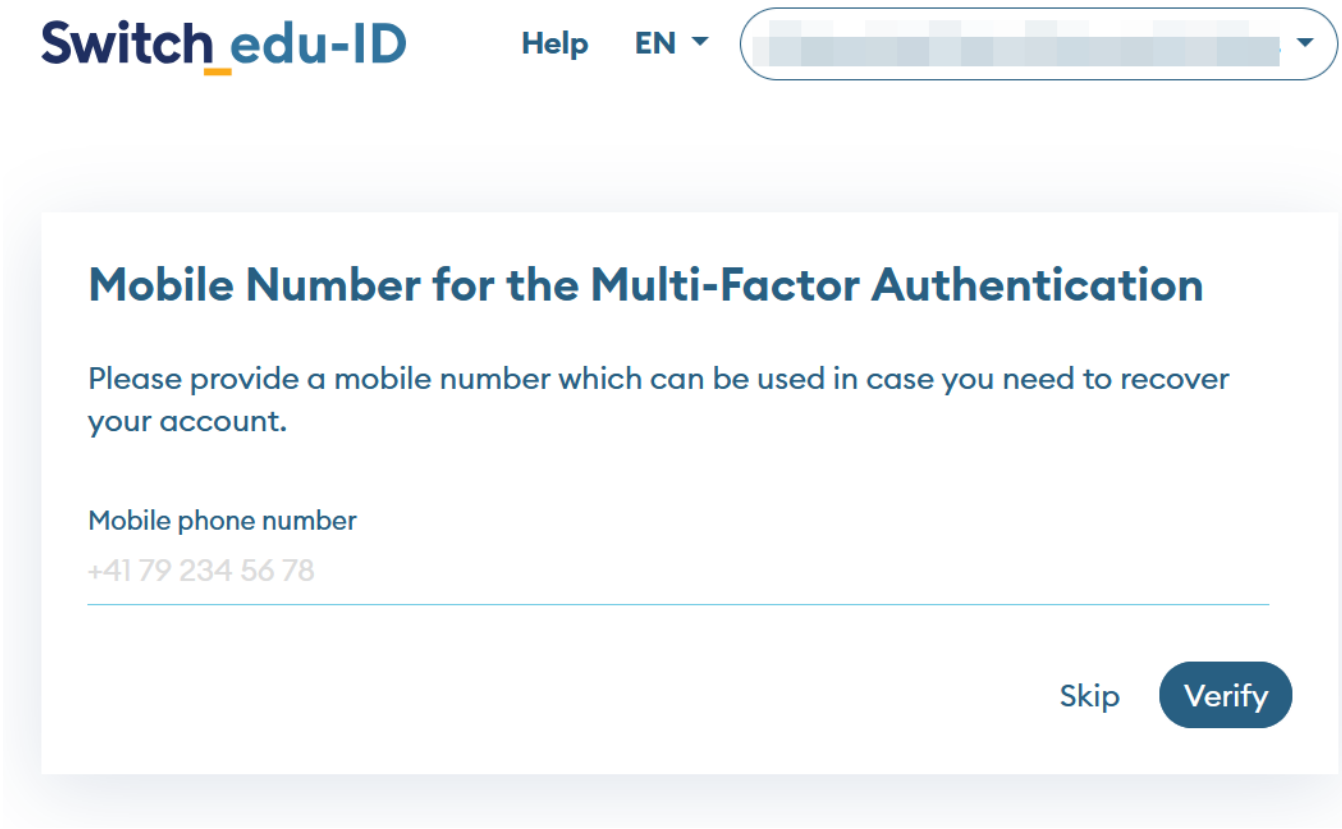
or go *directly to the two-step login settings* (https://eduid.ch/mfa/initial).

Next, activate one of the two-step authentication methods. We recommend using a **mobile authenticator app** to obtain your codes.

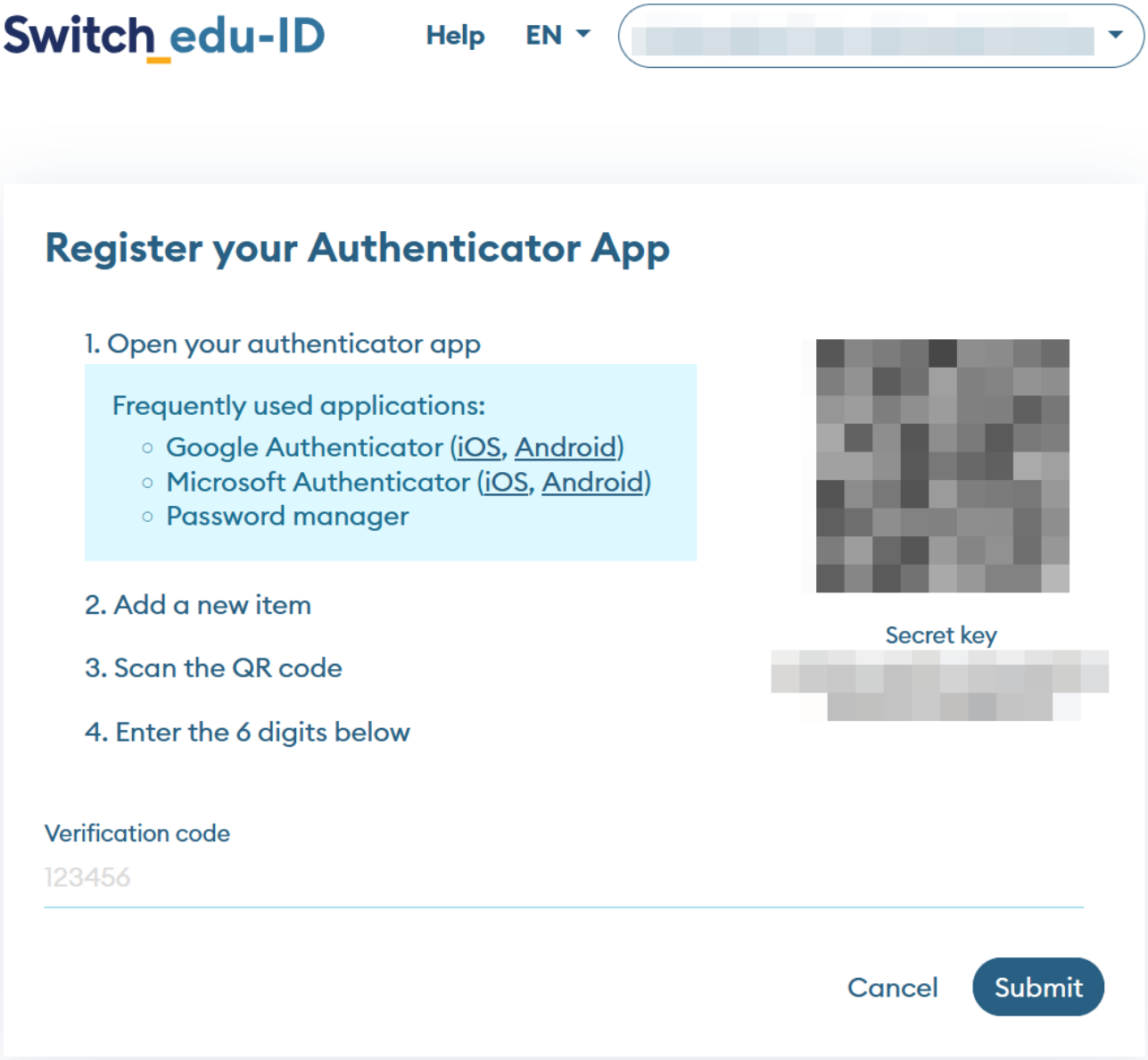


Authenticator app

You will first be asked for a mobile phone number in case you need to recover your account:



Next, you need to register your secret key, which will be used to generate the codes:

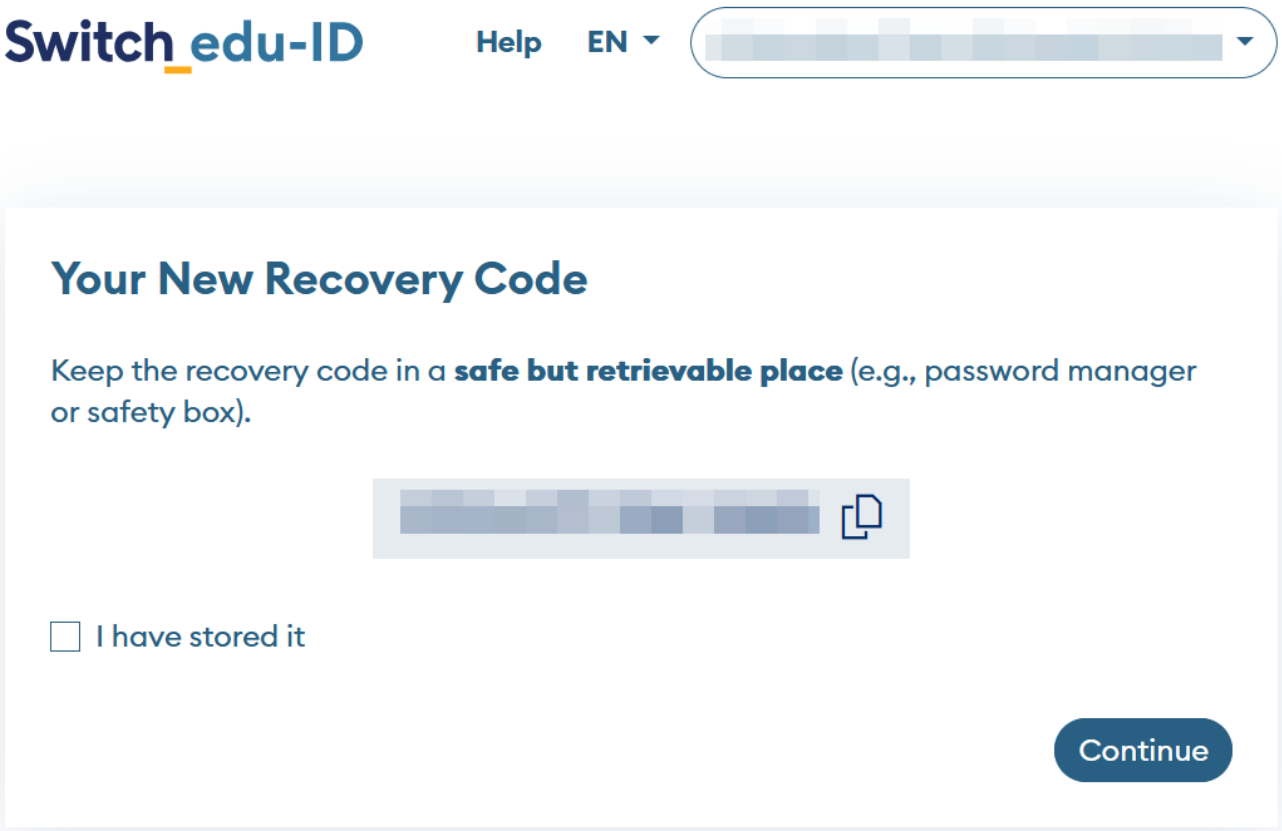


The following mobile apps, among others, work: **Ente Auth**, Twilio Authy, FreeOTP, Google Authenticator, Microsoft Authenticator, BitWarden Authenticator, and OTP Auth. (Other applications that support the TOTP standard can also be used.) More information on iBarry.ch. The Ente Auth application and the 2FAS browser extension can be used without a mobile phone.

Most of the authenticator apps mentioned above work with multiple account providers too, such as Google, Facebook, etc.

> More and more password managers offer the ability to manage both your passwords as well as the 2nd factor within a single app, such as macOS Keychain (latest version) or BitWarden (premium version).). This also has the advantage of being synchronised across different devices.

Don't forget to take note of your recovery code and save it.



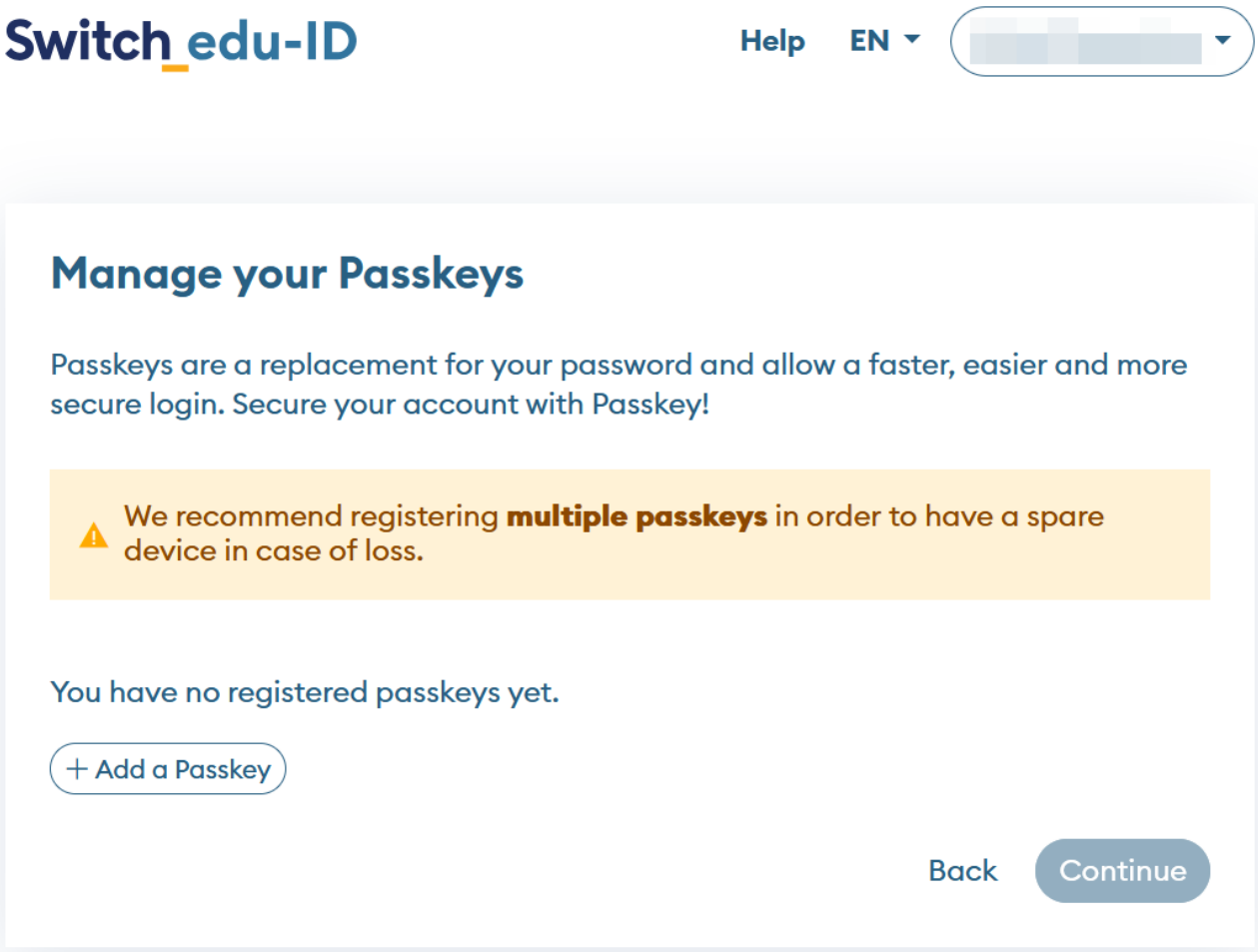
Passkey

Passkeys are a new and highly secure authentication technology, now supported by major internet platforms and by **SWITCH edu-ID**. Once configured, they allow truly *passwordless* login—no need to enter your password. You can find more information here:

https://help.switch.ch/eduid/docs/services/login/auth/passkey/ and an additional overview article here: https://www.ibarry.ch/en/safe-devices/passkeys/.

> Although Passkeys are considered the future standard for secure authentication, the technology is still emerging. Compatibility varies: not all operating systems, apps, or devices support Passkeys yet, and there are several configuration methods. Importantly, Passkeys are configured **per device**, meaning you will typically need to set one up on every laptop, phone, or browser you use—unless you rely on a synchronised password manager like BitWarden, which allows Passkeys to work across multiple devices.You can fin more information in the Switch FAQ.

> If you encounter problems or compatibility issues while configuring or using Passkeys, please report them to the helpdesk.



SMS

> **Starting in 2026, SMS will no longer be useable as a 2nd factor at UNIL. You need to configure an Authenticator app or use Passkeys.**

The other option, **which we do not recommend for reasons of reliability** and will be gradually retired, is to use SMS. A code will be sent to you for each connection requiring a 2nd factor.

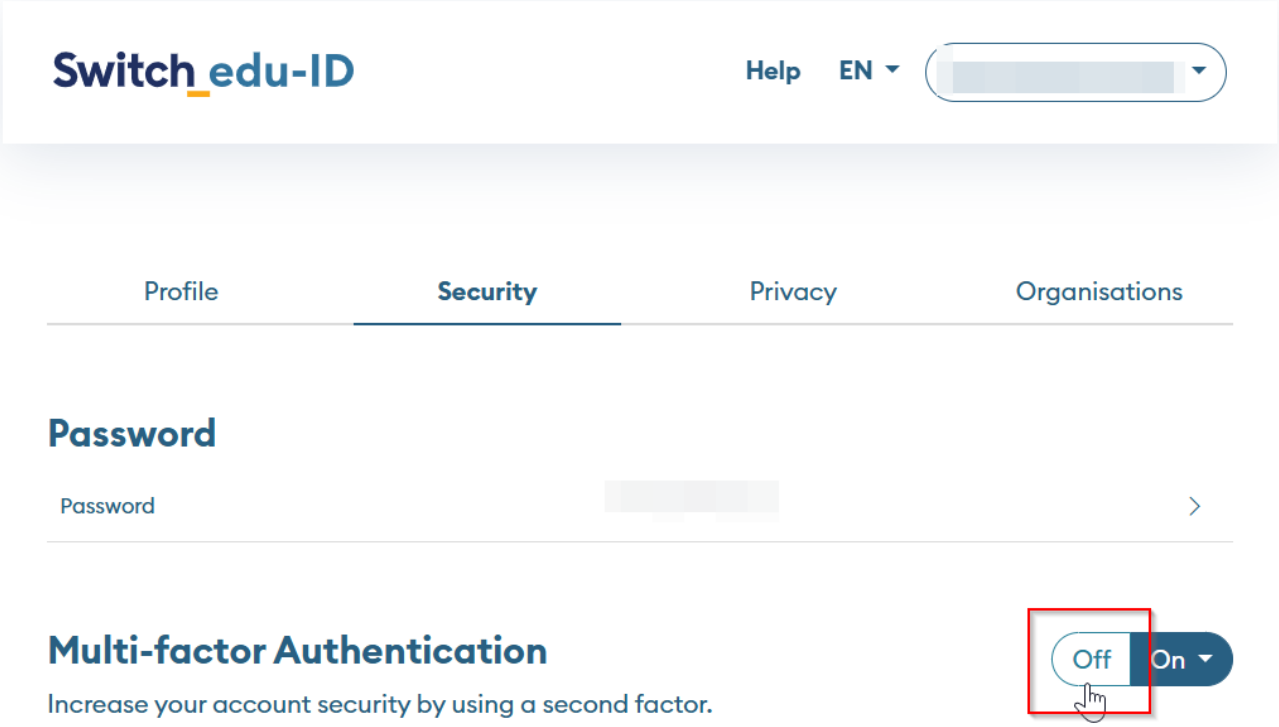
> If you use a non-Swiss phone number, please be aware that certain countries and operators may limit the delivery of SMS messages, or charge for them. In this case, we recommend you use an authenticator app rather than the SMS option.

It is possible to enable more than one login method and multiple Passkeys.

Disabling MFA

> If you deactivate MFA, you risk losing access to certain resources or services which require MFA. You will have to restart the processus if you reactivate it later.

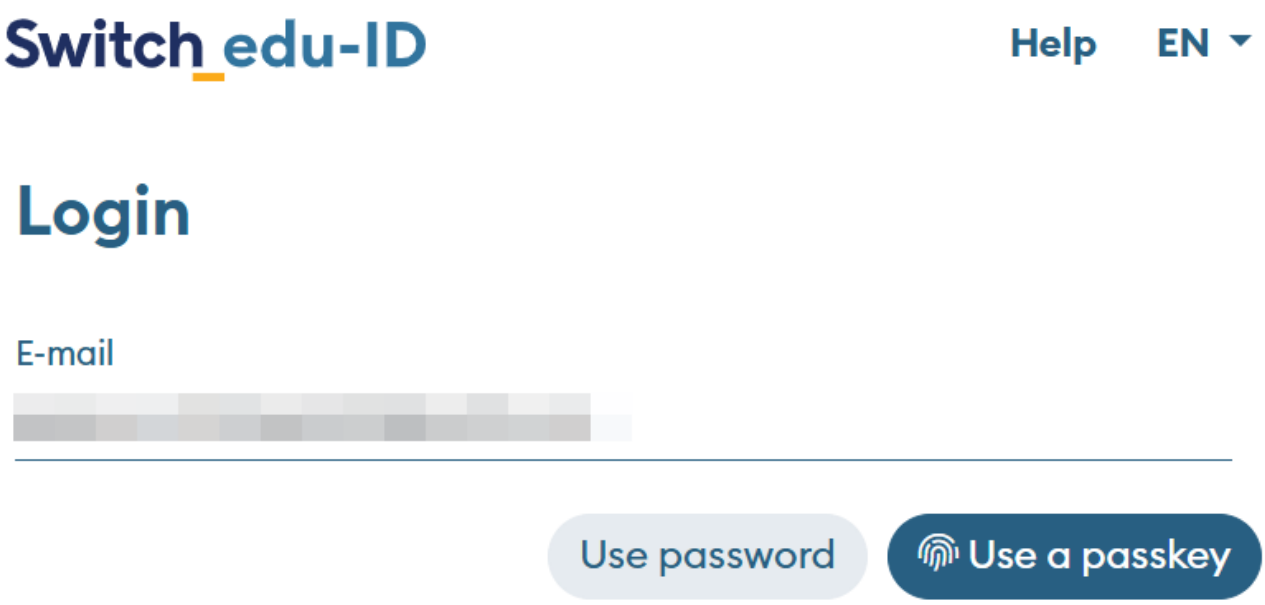
To **disable** two-step authentication, go back to the *Security* tab and click the Off button next to the *Multifactor Authentication* option (https://eduid.ch/account/security).



Please note that this may mean that you need to reinitialise or reverify the verification code if you reactivate a certain method later on.

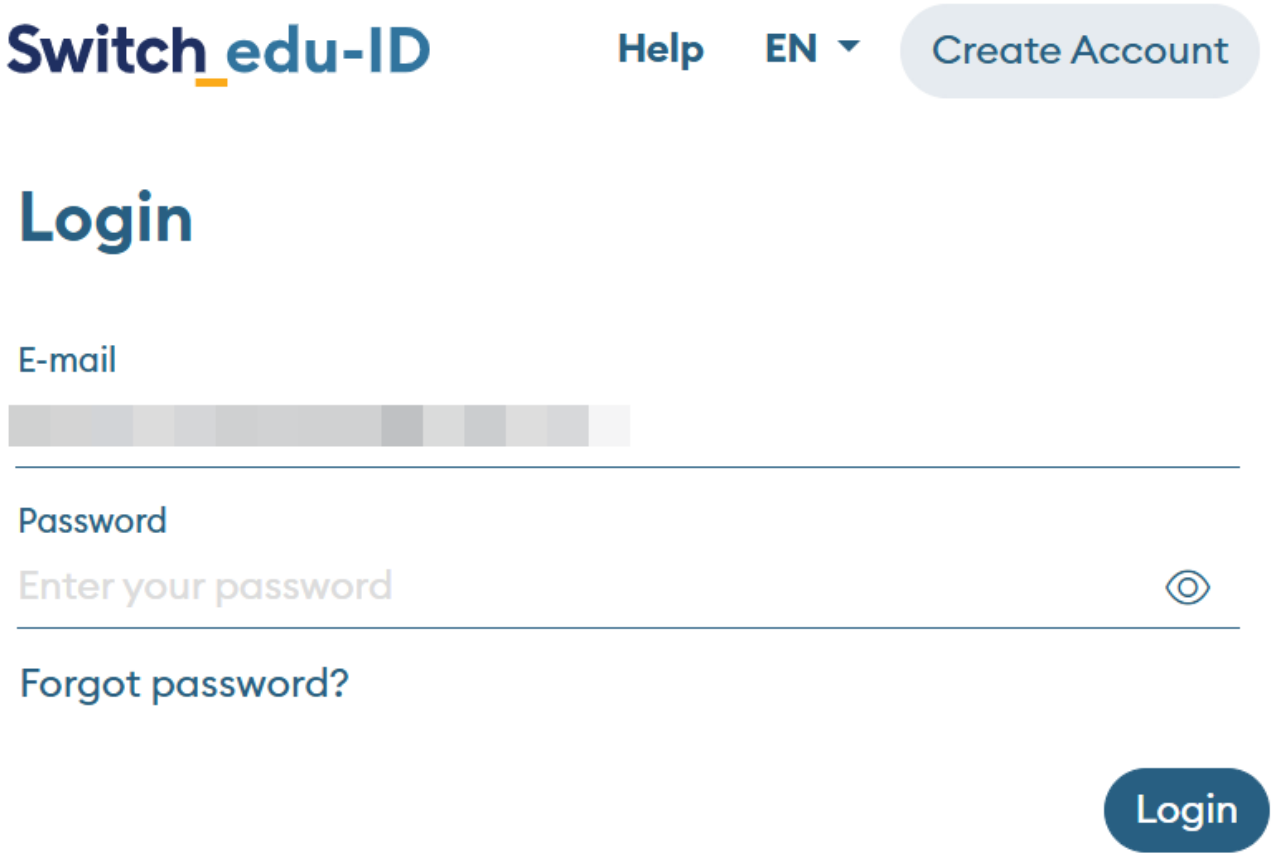
Login

When you log in to a page requiring a second factor, after entering your email address, depending on your MFA configuration, you will need to either enter a password or proceed via a Passkey:

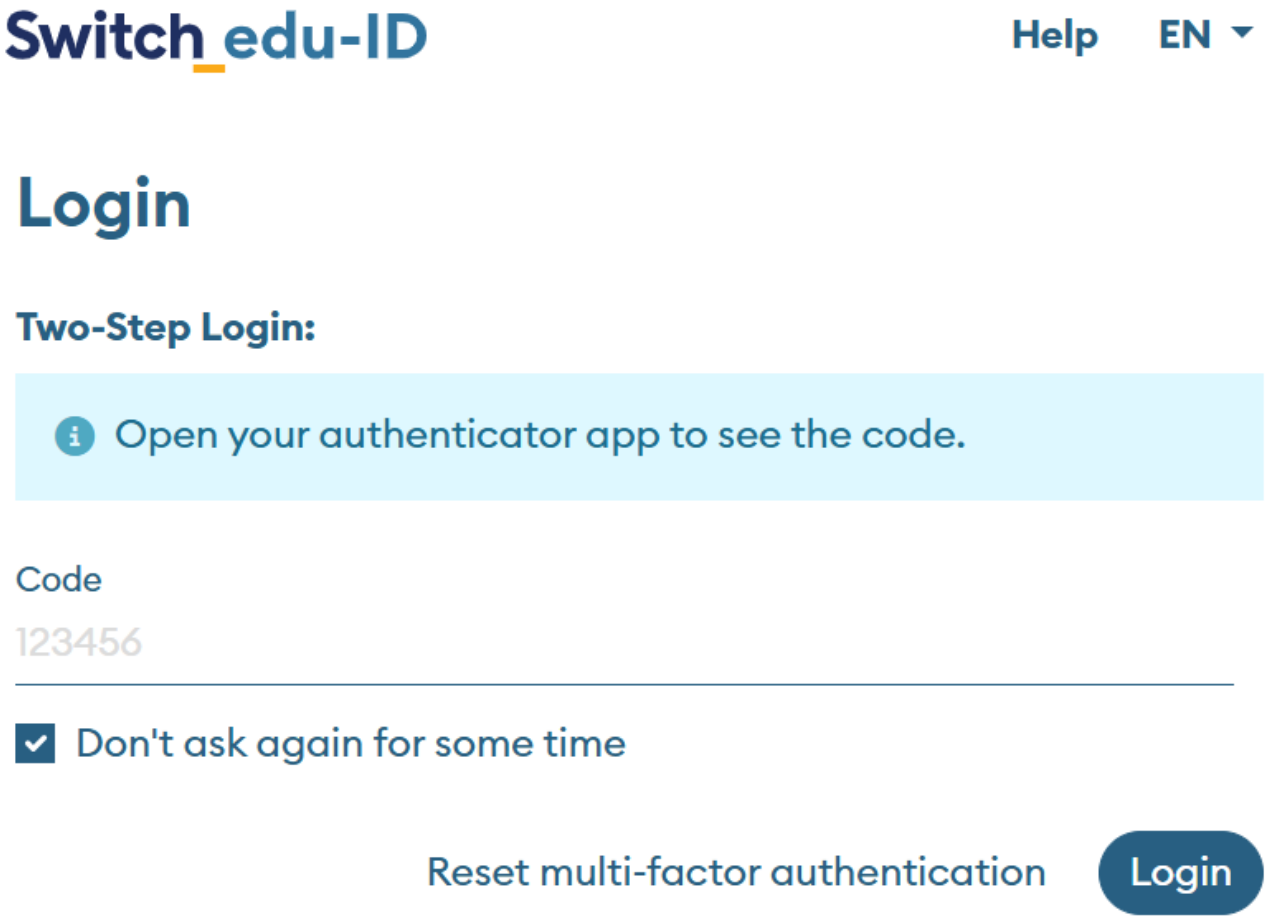


TOTP

If you choose the password, enter it



then enter the TOTP code generated in the app you previously configured



Questions / Problems

You will find the answers to multiple questions concerning multi-factor authentication on the official SWITCH edu-ID website: https://eduid.ch/help?lang=en#two-step-login-accordion

I lost my second factor, what should I do?

Please go to https://eduid.ch/mfa-recovery and follow the instructions.

Révision #25
Créé 8 avril 2021 06:42:22 par Chr Gr
Mis à jour 12 février 2026 15:22:23 par Chr Gr