Authentification edu-ID

L'authentification edu-ID (anciennement AAI (Authentication and Authorization Infrastructure)) est un service d'authentification et d'autorisation, fourni en partenariat avec SWITCH, qui permet de simplifier l'accès aux ressources informatiques entre universités et hautes écoles membres des fédérations SWITCHaai et eduGAIN.

- Doc publique
  - Authentification multifacteur avec edu-ID
  - Multifactor Authentication With edu-ID
  - Comment intégrer le SSO dans mon service?

Doc publique

Documentation publique du service

Doc publique

Authentification multifacteur avec edu-ID

L'**authentification multifacteur** (ou **MFA**, **authentification forte** ou encore **authentification à deux facteurs**) est parfois requis pour divers services afin d'augmenter le degré de sécurité de nos applications (plus d'infos sur notre blog). En plus de votre mot de passe, il vous sera demandé soit

- un **code à usage unique**, généré dans une application prévue à cet usage, appelée **TOTP** (comme **Google Authenticator**),
- de valider une demande **authentification sans mot de passe** utilisant la technologie **Passkey**

L'identité edu-ID inclut l'utilisation de l'authentification multifacteur, et son activation est facile. Pour lire la documentation officielle de SWITCH sur la MFA et l'edu-ID, rendez-vous ici: https://eduid.ch/help?lang=fr#two-step-login.

Activation

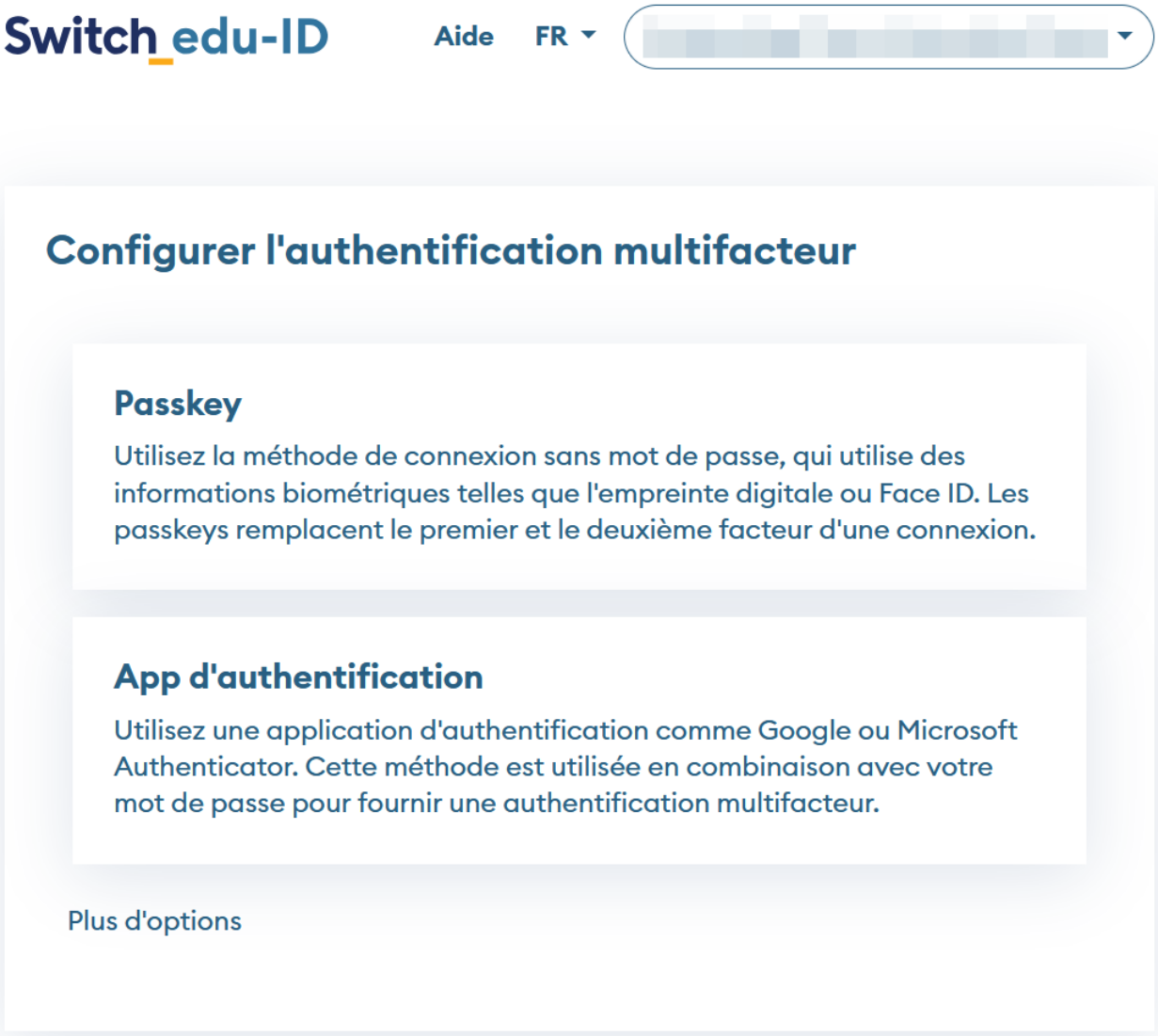
(adapté de la documentation de SWITCH)

Pour **activer** l'authentification en deux étapes, rendez-vous sur votre compte SWITCH edu-ID à l'adresse https://eduid.ch et cliquez sur l'onglet **Sécurité** et cliquez sur le bouton On à côté de **Authentification multifacteur**,



ou allez *directement aux paramètres de l'authentification en deux étapes* (https://eduid.ch/mfa/initial).

Activez ensuite l'une des méthodes d'authentification en deux étapes. Nous vous recommandons d'utiliser une **application mobile d'authentification** pour obtenir vos codes.



App d'authentification

Il vous saura d'abord demandé un numéro de téléphone portable au cas où vous auriez besoin de récupérer votre compte :



Ensuite, il vous faut enregistrer votre clé secrète qui servira à générer les codes :



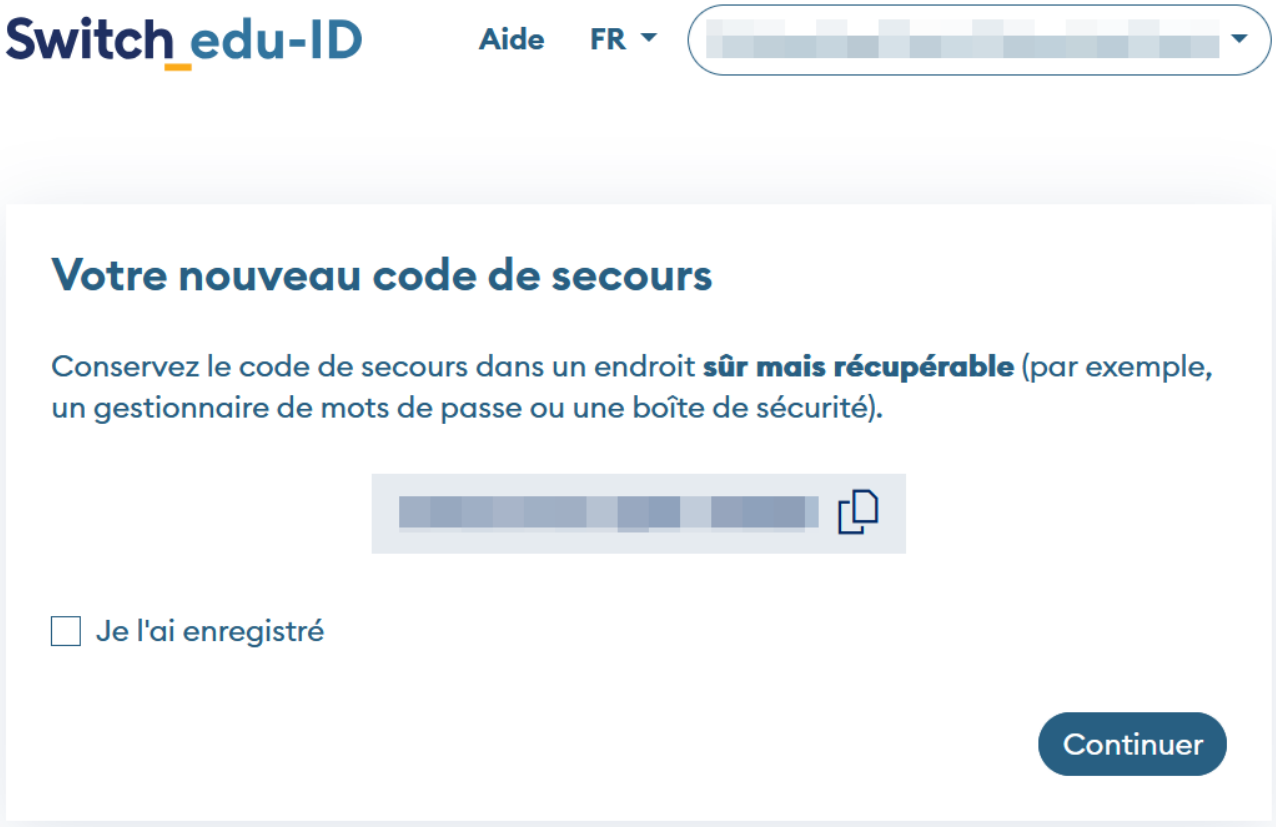
Les applications mobiles suivantes fonctionnent entre autres : **Ente Auth**, Twilio Authy, FreeOTP, Google Authenticator, Microsoft Authenticator, BitWarden Authenticator, ou encore OTP Auth. (D'autres applications qui supportent le standard *TOTP* peuvent également être utilisées.) Plus d'informations sur iBarry.ch. L'application Ente Auth ou l'extension de navigateur 2FAS peuvent être utilisés sans téléphone mobile.

La plupart des applications d'authentification mentionnées ci-dessus fonctionnent également pour d'autres fournisseurs de services, comme Google, Facebook, etc.

> De plus en plus de gestionnaires de mot de passe offrent la possibilité de gérer à la fois vos mots de passe ainsi que le 2e facteur au sein d'une seule et unique app, comme le trousseau macOS (dernière version) ou

BitWarden (version premium). Cela a aussi l'avantage d'être synchronisé sur différents devices.

N'oubliez pas de bien prendre note de votre code de secours et de le sauvegarder.



Passkey

Les *Passkeys* sont une nouvelle technologie d'authentification hautement sécurisée, désormais prise en charge par les principales plateformes internet ainsi que par **SWITCH edu-ID**. Une fois configurées, elles permettent une connexion réellement *sans mot de passe* — plus besoin de saisir votre mot de passe. Vous trouverez plus d'informations ici :

https://eduid.ch/help?lang=fr#two-step-login
ainsi qu'un article de présentation ici :

https://www.ibarry.ch/en/safe-devices/passkeys/

Bien que les Passkeys soient considérées comme le futur standard de l'authentification sécurisée, la technologie est encore émergente. Leur compatibilité varie : tous les systèmes d'exploitation, applications ou appareils ne les prennent pas encore en charge, et plusieurs méthodes de configuration coexistent. Il est important de noter que les Passkeys sont configurées **par appareil**, ce qui signifie que vous devrez généralement en créer une sur chaque ordinateur, téléphone ou navigateur que vous utilisez — sauf si vous utilisez un

gestionnaire de mots de passe synchronisé comme BitWarden, qui permet d'utiliser la même Passkey sur plusieurs appareils.

Vous trouverez plus d'informations dans la FAQ de SWITCH.

Si vous rencontrez des problèmes ou des incompatibilités lors de la configuration ou de l'utilisation des Passkeys, veuillez les signaler au helpdesk.



Il est possible d'activer plus d'une méthode de connexion, et de multiples Passkey.

Désactivation de la MFA

Si vous désactivez la MFA, vous risquez de ne plus avoir accès à certaines ressources ou services qui requiert un 2e facteur. Il vous faudra recommencer le processus de 0 si vous souhaitez la réactiver par la suite.

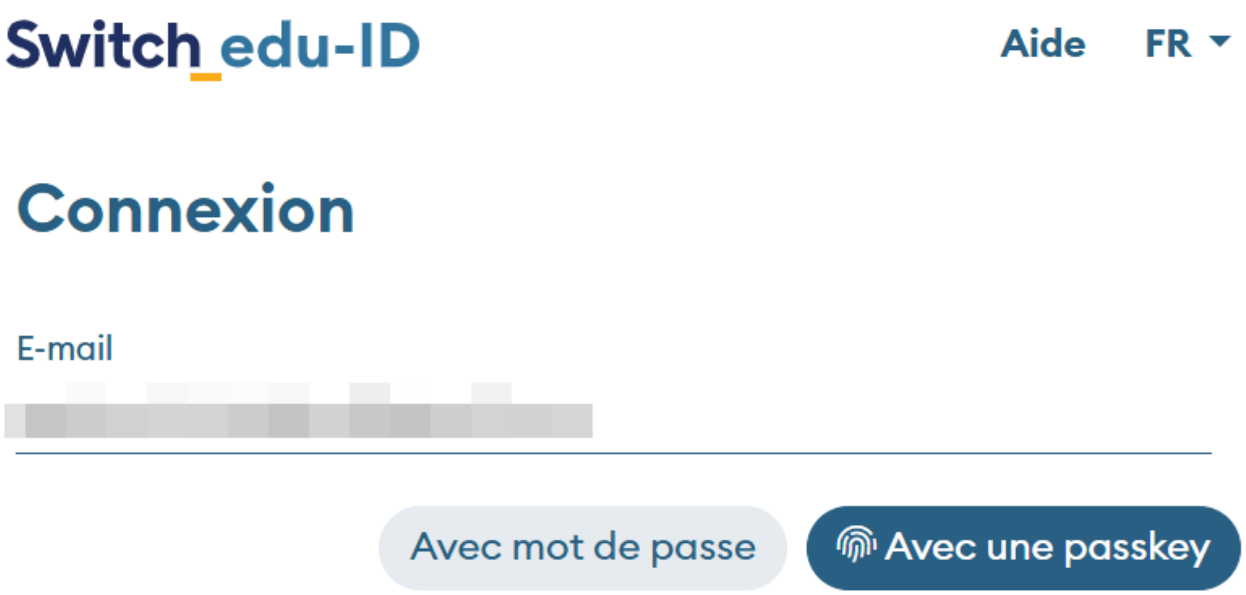
Pour **désactiver** l'authentification en deux étapes, retournez vers l'onglet *Sécurité* et cliquez sur le bouton Off à côté de l'option *Authentification multifacteur* (https://eduid.ch/account/security).



Vous devrez peut-être réinitialiser ou revérifier le code de vérification si vous réactivez ultérieurement une méthode particulière.

Connexion

Lorsque vous vous connecterez à une page nécessitant un deuxième facteur, après avoir entré votre adresse email, selon votre configuration MFA, vous devrez sélectionner soit d'entrer un mot de passe, soit de procéder via une Passkey :



TOTP

Si vous utilisez un mot de passe, renseignez-le



entrez ensuite le code TOTP généré dans l'app que vous aurez configurée au préalable



Questions / Problèmes

Vous trouverez réponse à plusieurs questions concernant l'authentification multifacteur sur le site officiel de SWITCH edu-ID: https://eduid.ch/help?lang=fr#two-step-login

J'ai perdu accès à mon 2e facteur, que faire?

Rendez-vous sur la page https://eduid.ch/mfa-recovery et suivez les instructions.

Doc publique

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:

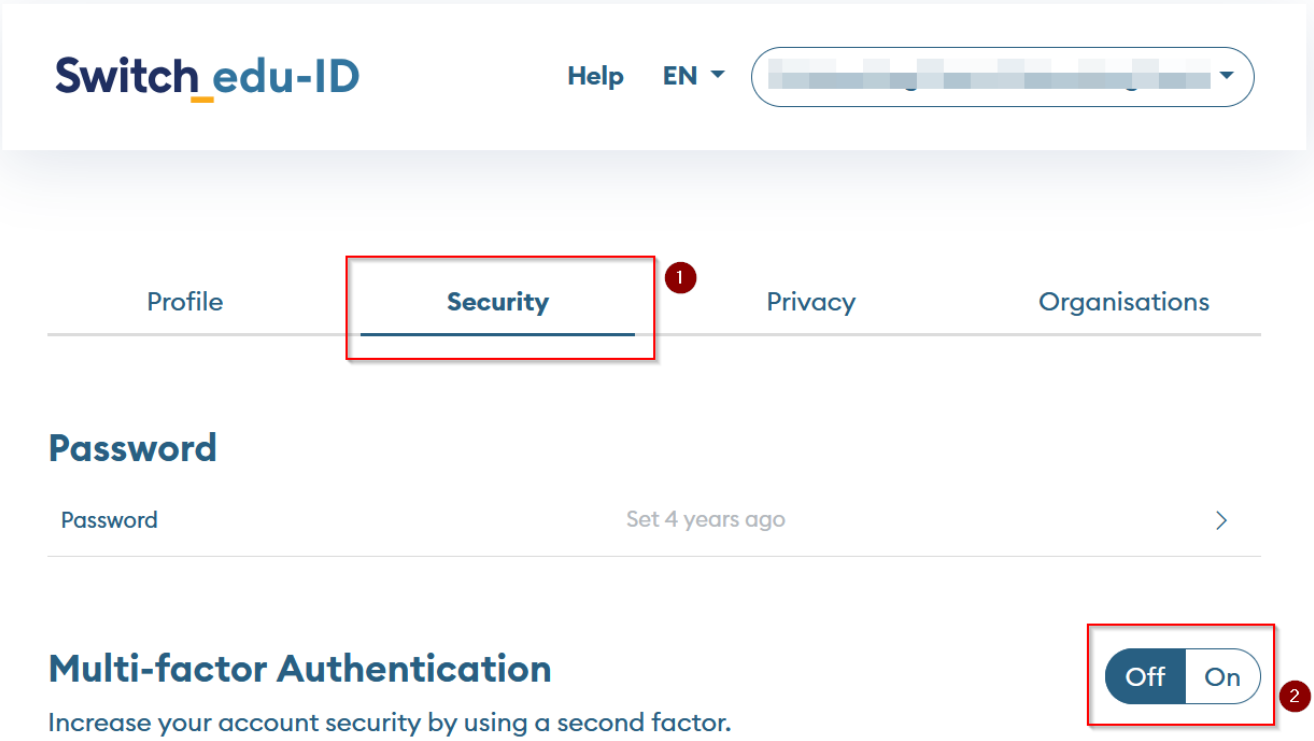
- A **one-time code** generated in an application designed for this purpose, called TOTP (such as Google Authenticator),
- To validate an authentication request **without a password** using **Passkey** technology

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://eduid.ch/help#two-step-login

Activation

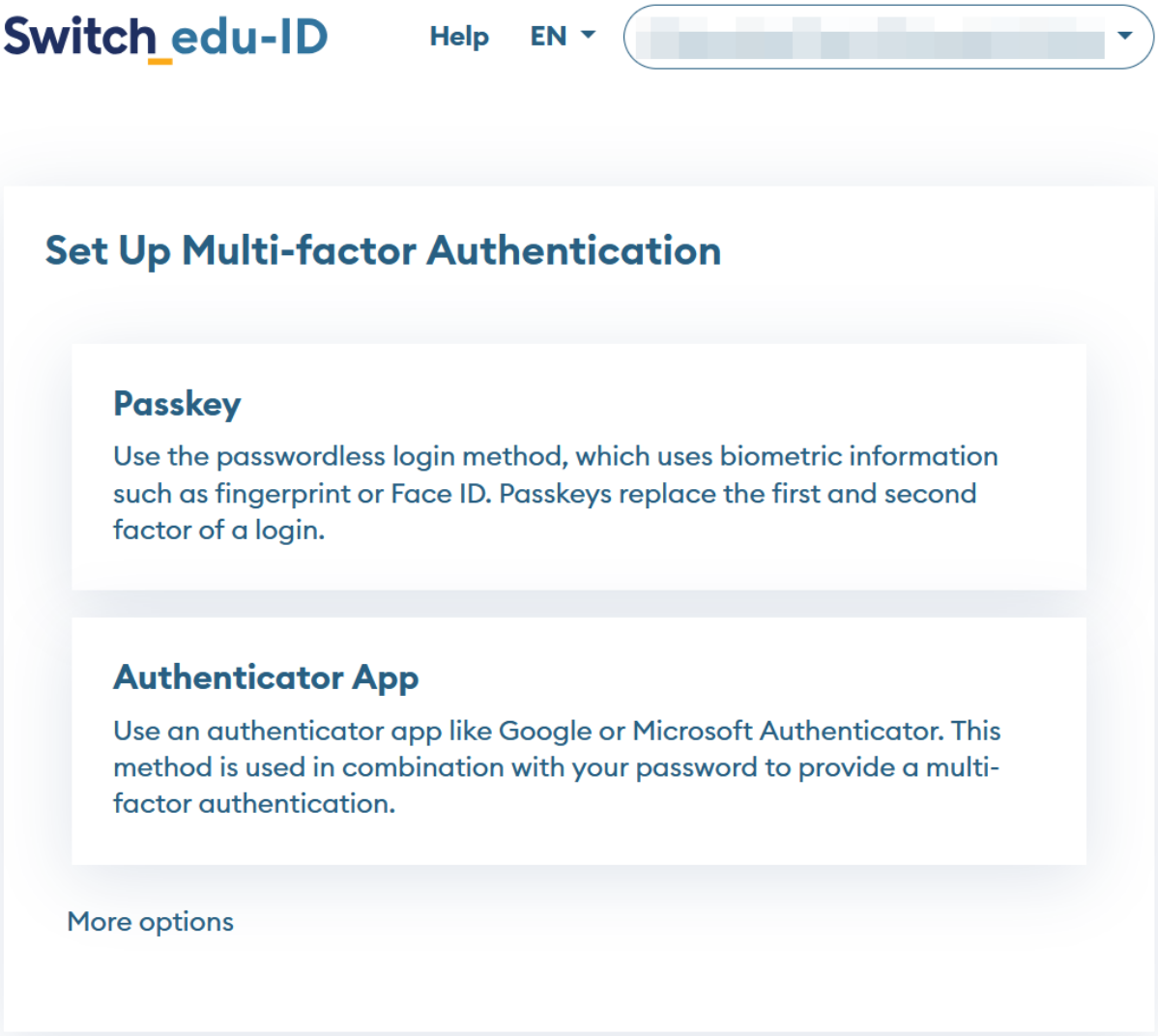
(adapted from the official SWITCH documentation)

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**,



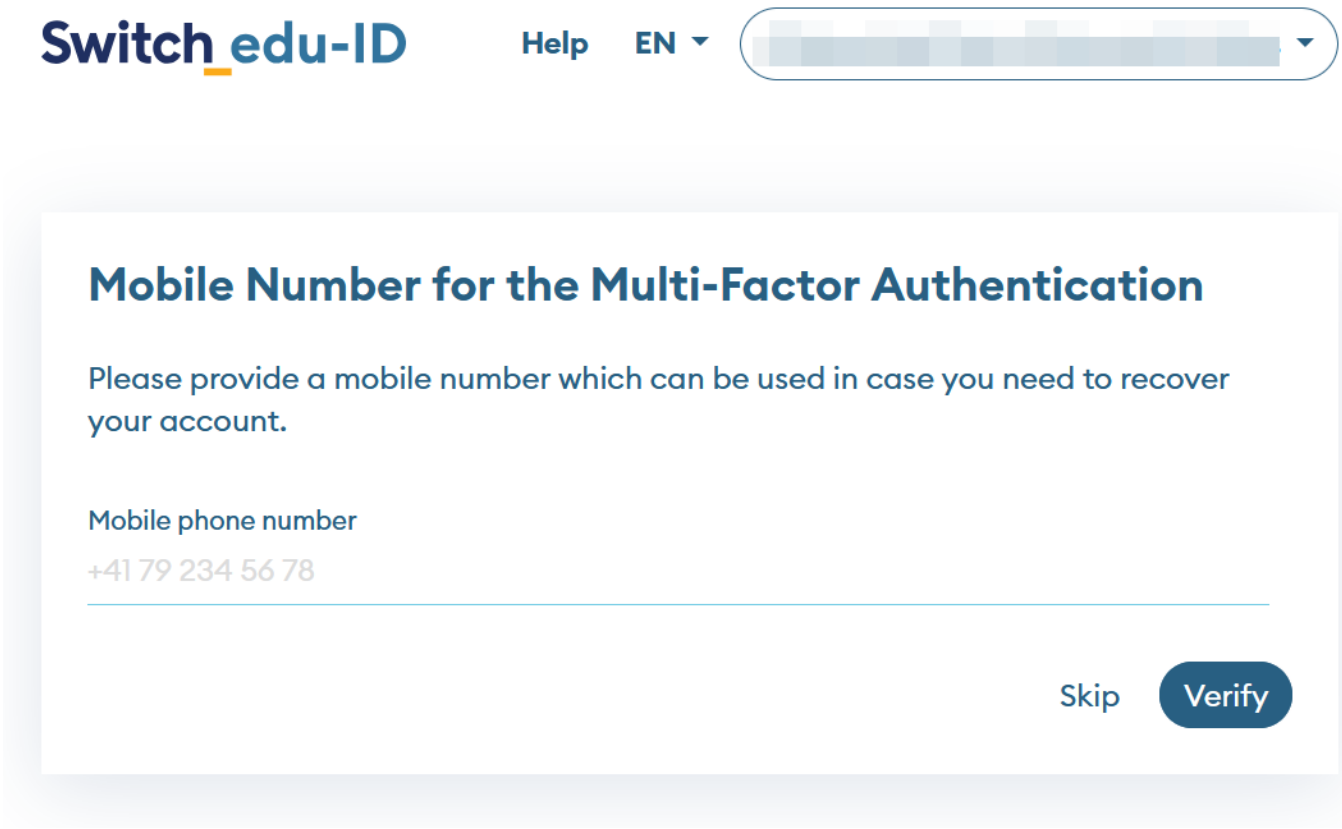
or go *directly to the two-step login settings* (https://eduid.ch/mfa/initial).

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

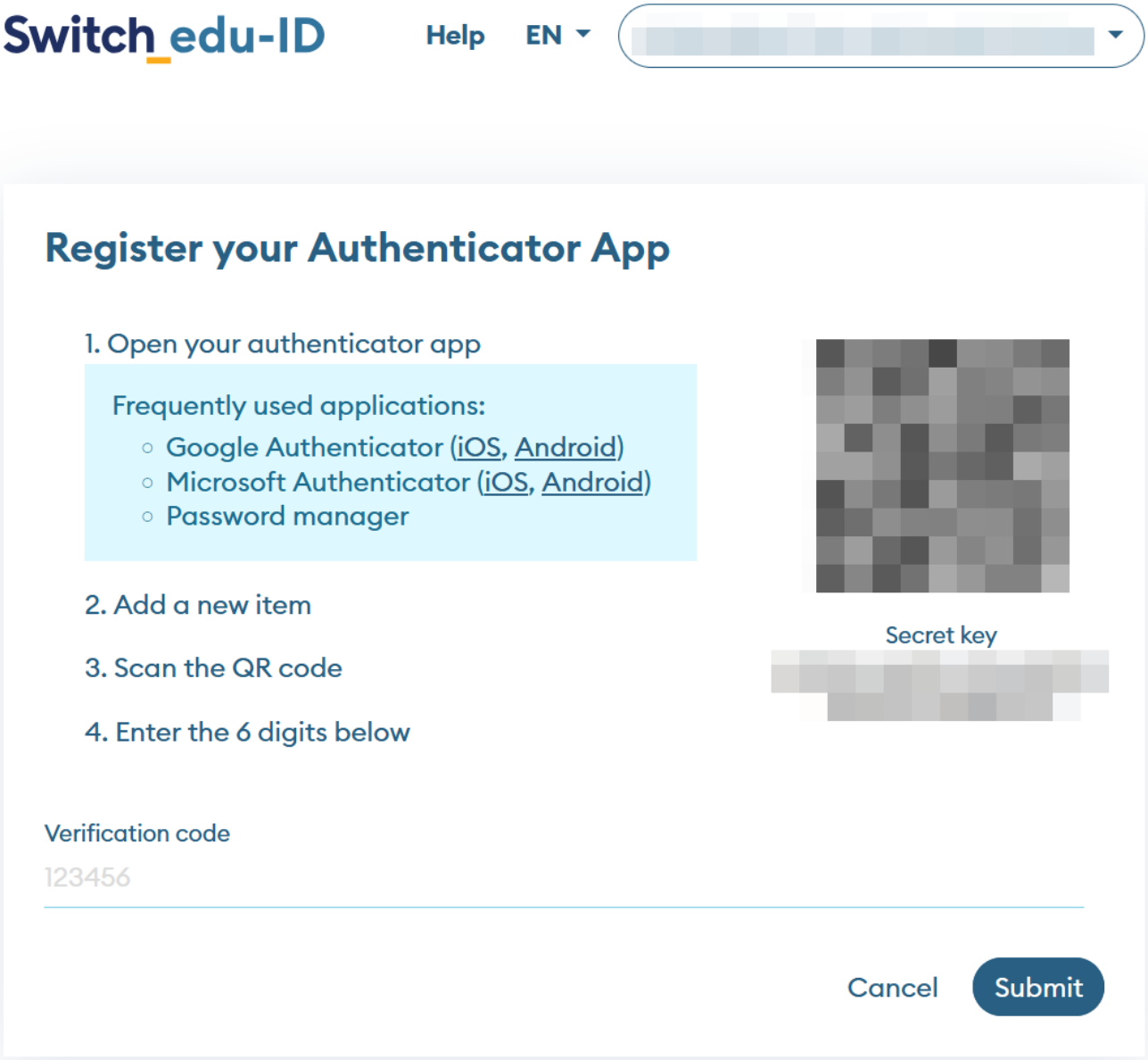


Authenticator app

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:

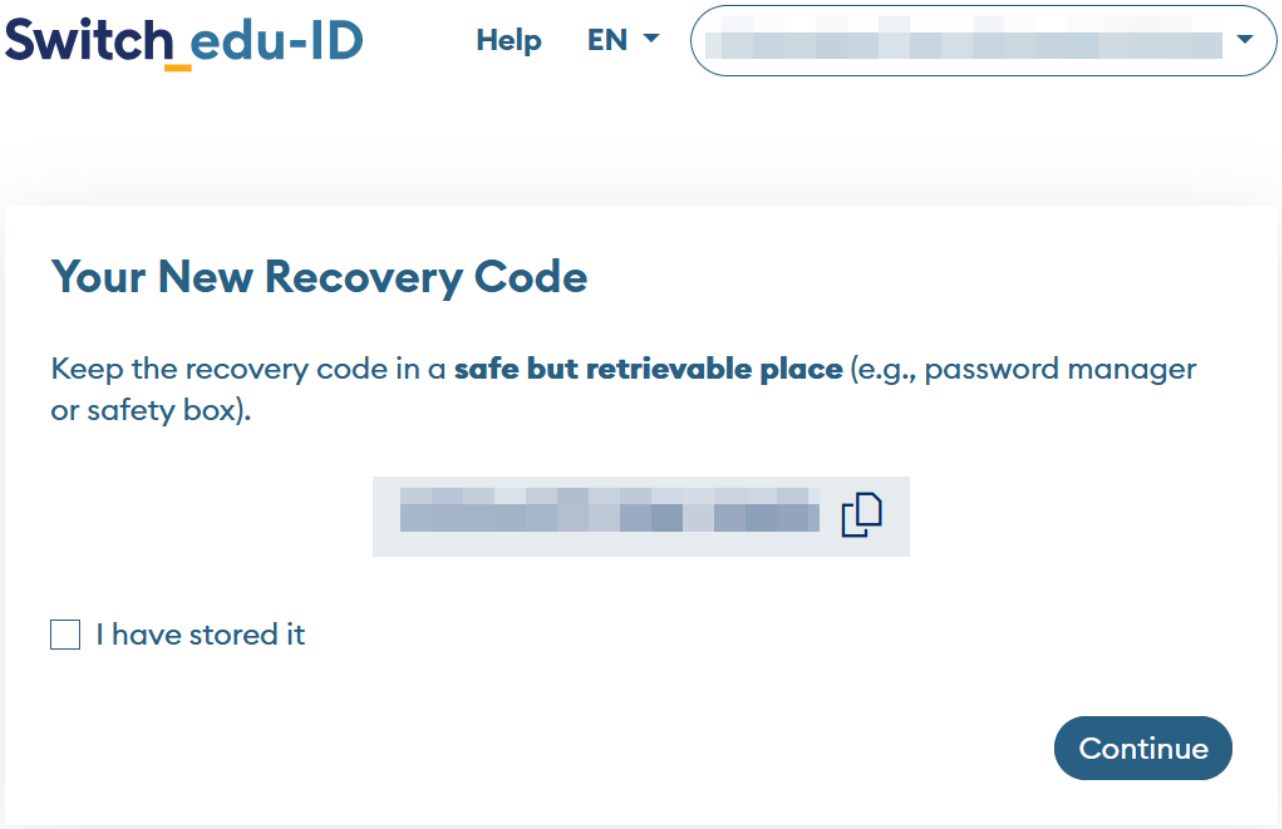


The following mobile apps, among others, work: **Ente Auth**, Twilio Authy, FreeOTP, Google Authenticator, Microsoft Authenticator, BitWarden Authenticator, and OTP Auth. (Other applications that support the TOTP standard can also be used.) More information on iBarry.ch. The Ente Auth application and 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

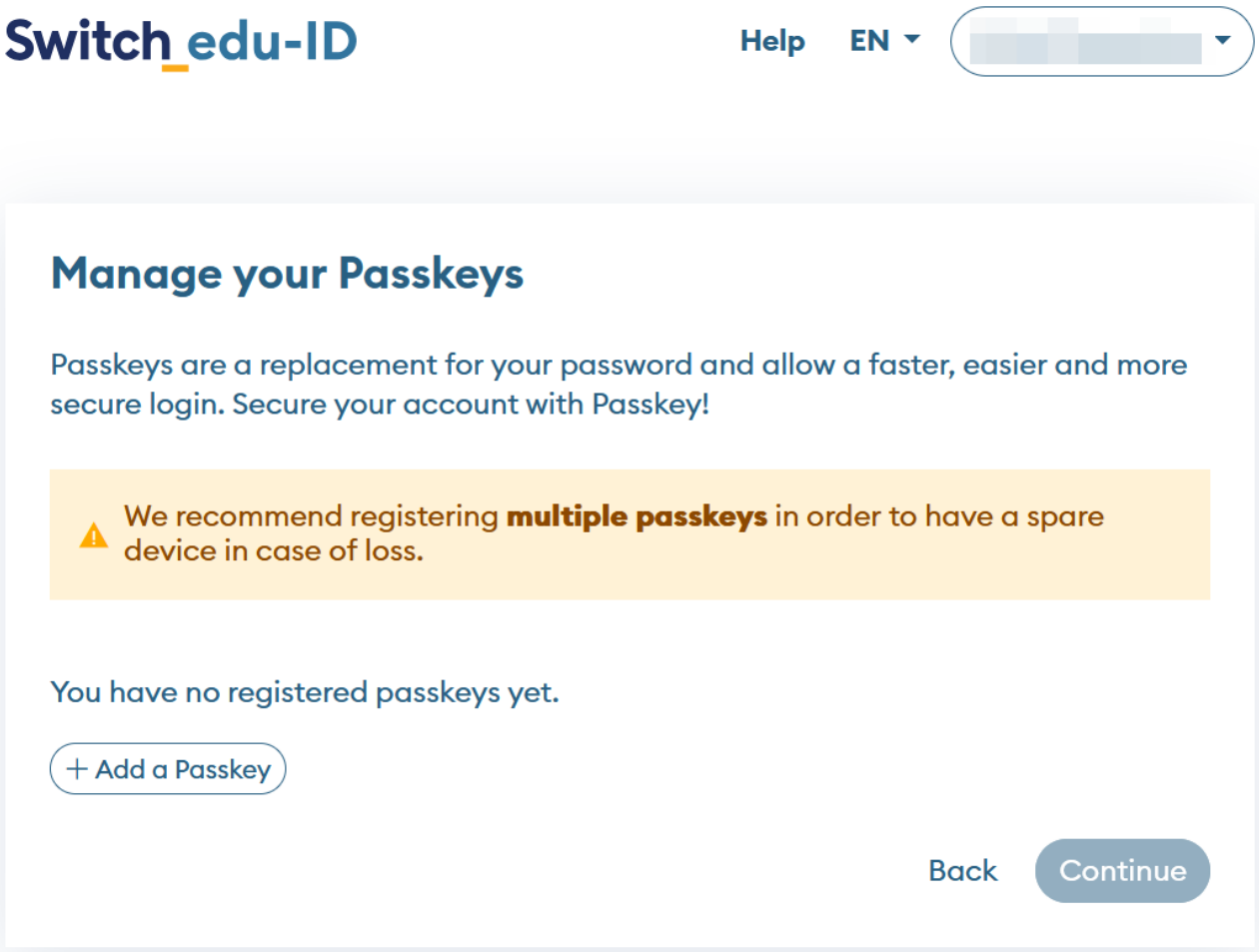
Passkeys are a new and highly secure authentication technology, now supported by major internet platforms and by **SWITCH edu-ID**. Once configured, they allow truly *passwordless* login—no need to enter your password. You can find more information here:

https://eduid.ch/help#passkeys 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.

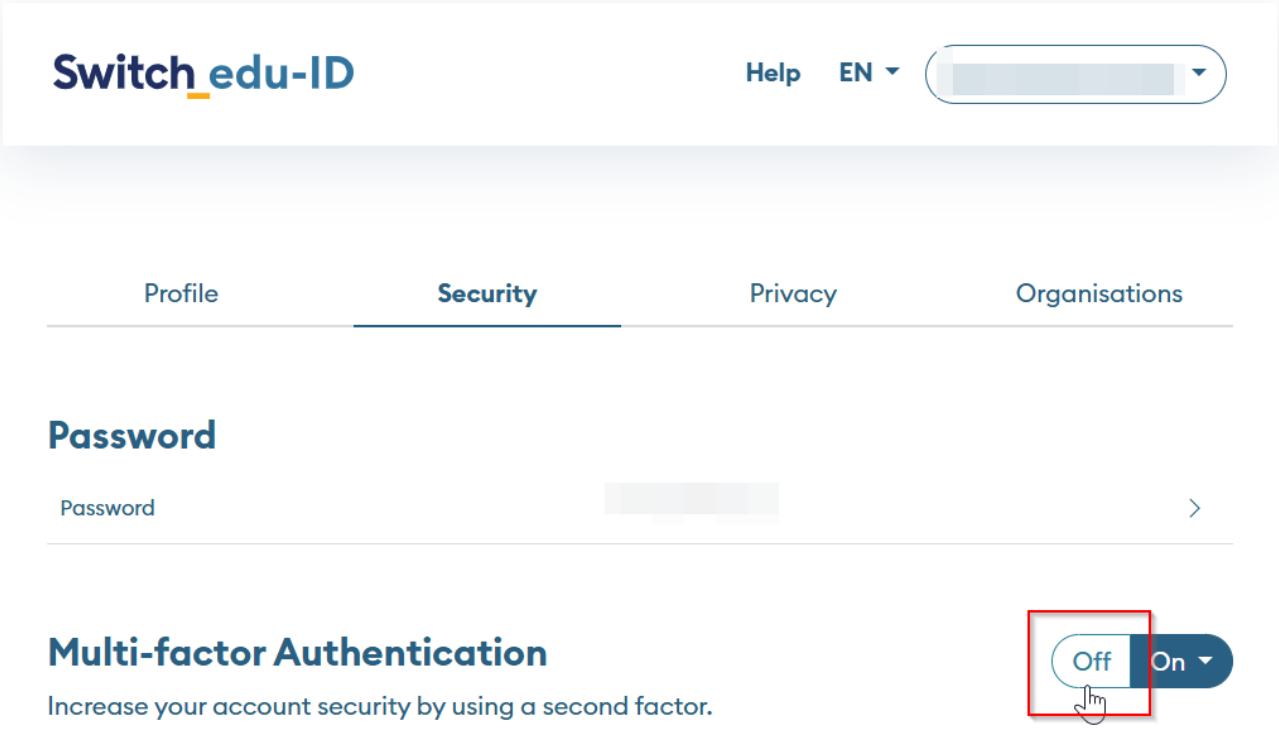


It is possible to enable more than one login method and multiple Passkeys.

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.

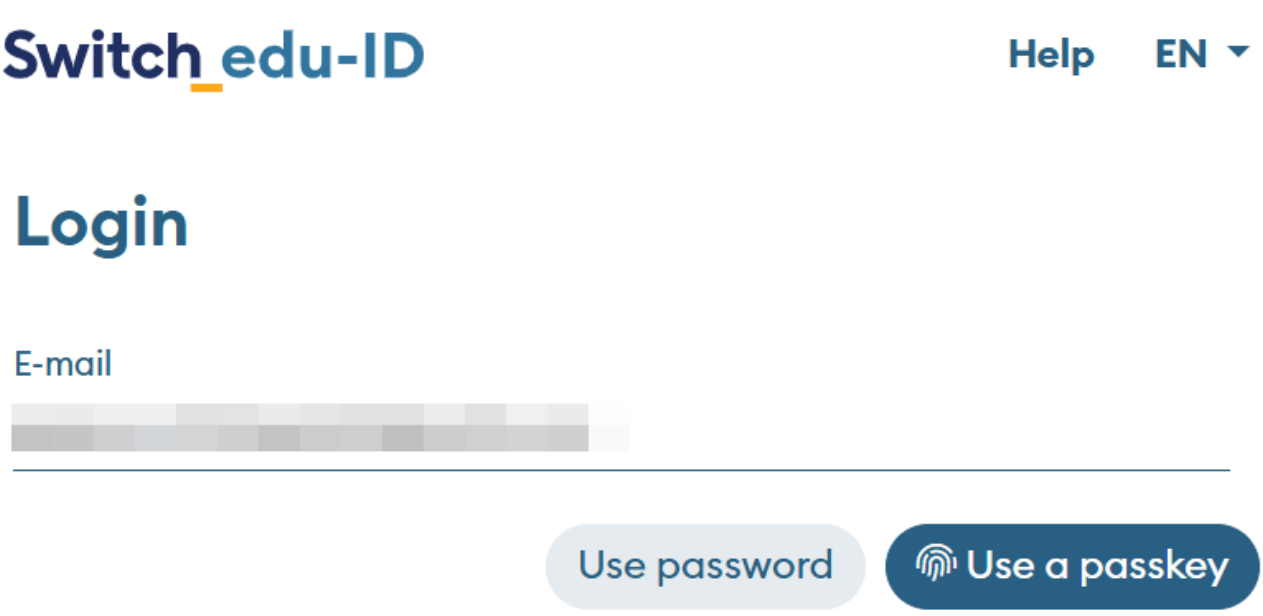
To **disable** two-step authentication, go back to the *Security* tab and click the Off button next to the *Multifactor Authentication* option (https://eduid.ch/account/security).



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

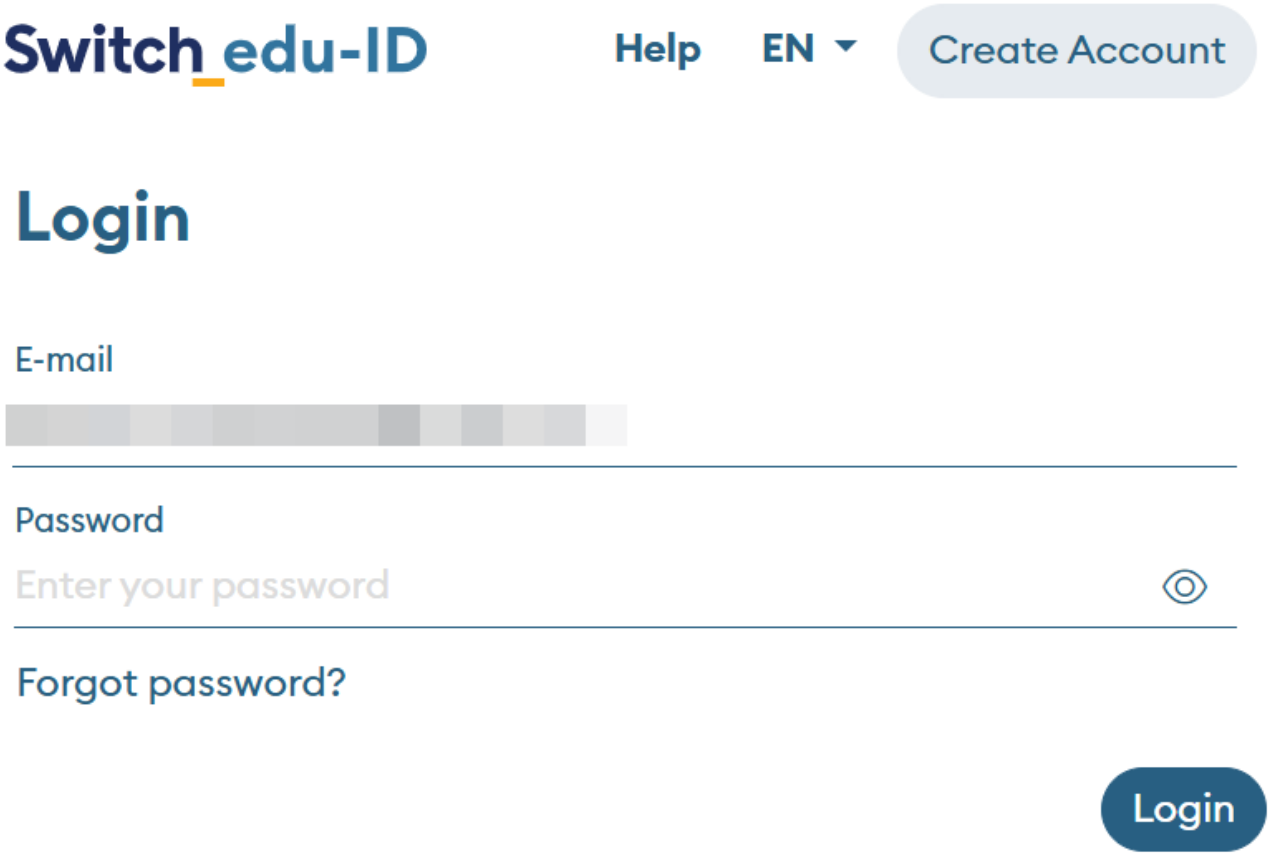
Login

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:

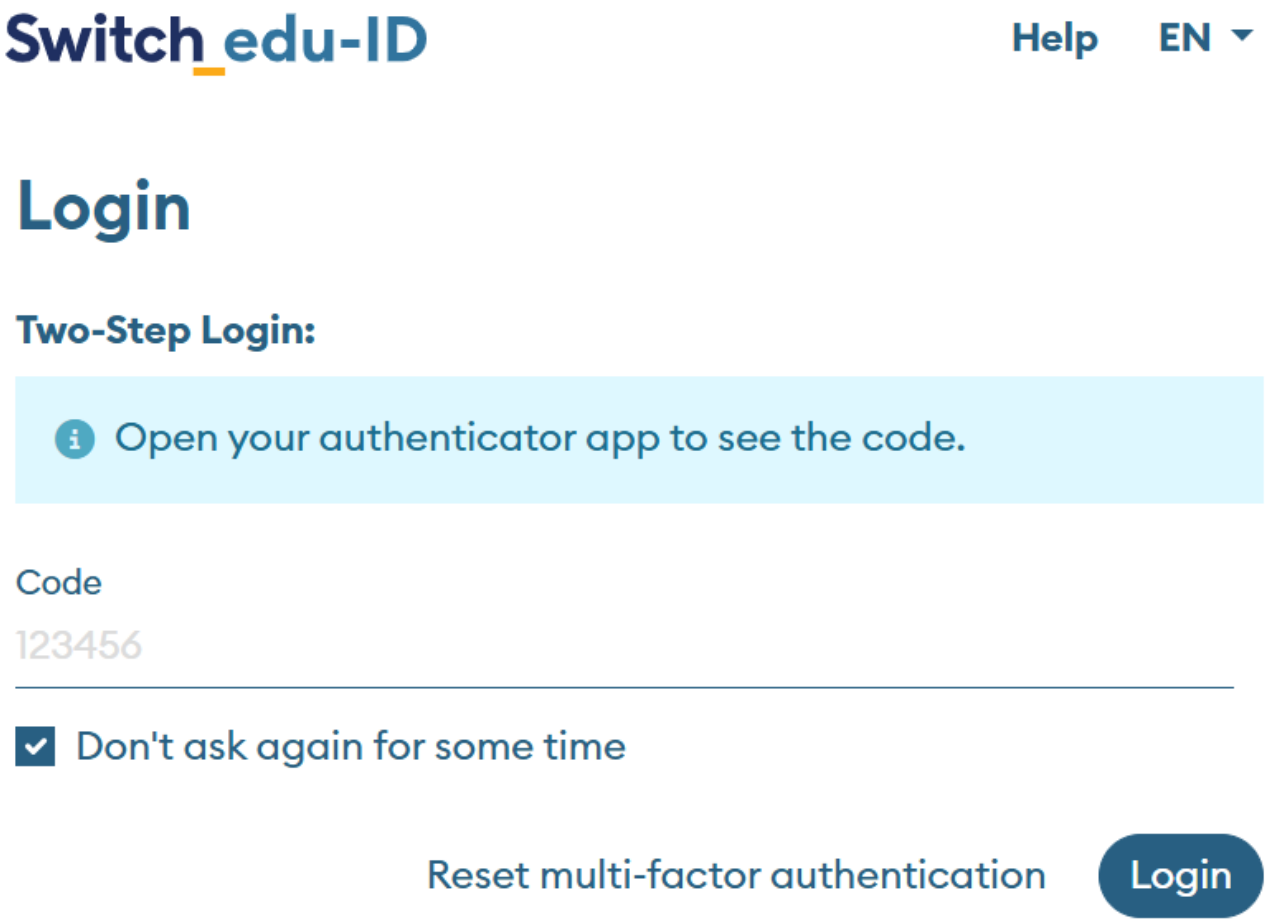


TOTP

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#two-step-login

I lost my second factor, what should I do?

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

Doc publique

Comment intégrer le SSO dans mon service?

Intégrer une solution SSO à votre service

Avant de commencer l'intégration, il vous faut être au clair sur:

- qui va se connecter à votre service (quel(s) institution(s)? Si Unil uniquement, est-ce un service ouvert à tous? Ou destiné qu'à un groupe d'utilisateurs?),
- par quel biais (uniquement un navigateur web? Ou une app?),
- est-ce un service qui nécessite une authentification forte/mutifacteurs?
- est-ce que votre service est bien compatible SAML ou OIDC?
- quelles informations (attributs) sont nécessaires pour s'authentifier à votre service?

Quel type d'authentification selon le type d'utilisateur

Cela dépend qui doit se connecter à votre service.

Si les personnes qui s'y connectent:

- ont tous un compte informatique Unil -> **Entra**
- peuvent provenir d'autres institutions, ou à titre privé -> **edu-ID**

Les protocoles pris en charge sont:

- Le SAML (plus adapté pour les services web-based)
- ou OIDC

Entra

- Adapté pour une utilisation interne, où tous les utilisateurs ont un compte Unil. On peut limiter l'accès à un groupe d'utilisateurs (groupe AD/Sylvia), et demander un 2e facteur.
- Utilise les identifiants Unil.

- Nécessite un échange de métadonnées, et l'intervention d'un admin MS365. Merci de contacter helpdesk@unil.ch

Edu-ID

- Adapté si les utilisateurs se connectent depuis l'Unil ainsi que des institutions hors Unil, ou à titre privé.
- Cela se repose sur la fédération AAI, gérée par Switch. Documentation: https://help.switch.ch/aai/about/
- Utilise les identifiants Switch Edu-ID.
- Nécessite de configurer une ressource dans le Resource Registry de Switch: https://rr.aai.switch.ch/. Les membres de l'Unil peuvent normalement soumettre une demande directement, qui sera ensuite validée par l'un des admins AAI de l'Unil.
- Métadonnées de notre Idp: https://rr.aai.switch.ch/gen_saml2md_entity.php?homeOrg=137

Questions? Contactez aai@unil.ch

Intégration d'un service géré par des tiers

Si vous souhaitez intégrer une authentification edu-ID à un service géré par des tiers, il faut voir si cette intégration sera un "one shot" ou si cet intégrateur tiers souhaite offrir ce service à la fédération AAI entière. Si c'est une intégration unique avec l'Unil, contactez-nous avec les métadonnées et les attributs nécessaires, et nous rajouterons le nécessaire au Resource Registry. Si le service tiers souhaite être accessible à la fédération entière, il faut devenir un Switch edu-ID Federation Partner: https://help.switch.ch/aai/join/partners/

Arbre décisionnel

Intégrer une solution SSO à votre service

