

# 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**
- (~~ou reçu via SMS, mais ce dernier est déconseillé pour des raisons de fiabilité!~~). (à partir de 2026, le SMS ne sera plus accepté comme 2e facteur)

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://help.switch.ch/fr/eduid/docs/services/login/two-step-login/> (en anglais).

## 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](#)**,

Profil

Sécurité <sup>1</sup>

Confidentialité

Organisations

## Mot de passe

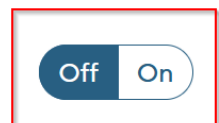
Mot de passe

Changé il y a 4 ans



## Authentification multifacteur

Augmentez la sécurité de votre compte en utilisant un deuxième facteur.

<sup>2</sup>

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.



## Configurer l'authentification multifacteur

### Passkey

Utilisez la méthode de connexion sans mot de passe, qui utilise des informations biométriques telles que l'empreinte digitale ou Face ID. Les passkeys remplacent le premier et le deuxième facteur d'une connexion.

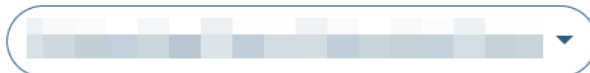
### App d'authentification

Utilisez une application d'authentification comme Google ou Microsoft Authenticator. Cette méthode est utilisée en combinaison avec votre mot de passe pour fournir une authentification multifacteur.

[Plus d'options](#)

## App d'authentification

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



## Numéro de téléphone mobile pour l'authentification multifacteur

Veillez fournir un numéro de téléphone mobile qui peut être utilisé au cas où vous auriez besoin de récupérer votre compte.

Numéro de téléphone mobile

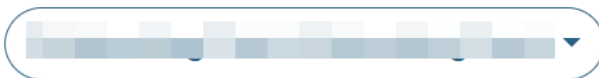
+41 79 234 56 78

---

Sauter

Vérifier

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



## Enregistrez votre app d'authentification

### 1. Ouvrez votre app d'authentification

Applications fréquemment utilisées :

- [Google Authenticator](#) ([iOS](#), [Android](#))
- [Microsoft Authenticator](#) ([iOS](#), [Android](#))
- [Gestionnaire de mots de passe](#)

### 2. Ajoutez un nouvel élément

### 3. Scannez le code QR

### 4. Saisissez les 6 chiffres ci-dessous



Secret key



Code de vérification

123456

Annuler

Soumettre

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.

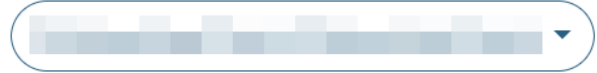
De plus en plus de gestionnaires de mot de passe offrent la possibilité de gérer à la fois vos mots de passe ainsi que le 2e facteur au sein d'une seule et unique app, comme le trousseau macOS (dernière version) ou

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.**

Switch **edu-ID**

Aide FR ▾



## Votre nouveau code de secours

Conservez le code de secours dans un endroit **sûr mais récupérable** (par exemple, un gestionnaire de mots de passe ou une boîte de sécurité).



Je l'ai enregistré

Continuer

## 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://help.switch.ch/fr/eduid/docs/services/login/auth/passkey/>

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

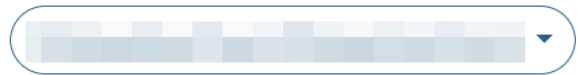
gestionnaire de mots de passe synchronisé comme BitWarden, qui permet d'utiliser la même Passkey sur plusieurs appareils.

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](#).


Switch edu-ID

Aide FR ▾



## Gérez vos passkeys

Les passkeys remplacent votre mot de passe et permettent une connexion plus rapide, plus facile et plus sûre. Sécurisez votre compte avec des passkeys !

 Nous recommandons d'enregistrer plusieurs passkeys afin d'avoir un dispositif de rechange en cas de perte

Vous n'avez pas encore de passkey enregistrée

[+ Ajouter une passkey](#)

Continuer

## SMS

**À partir de 2026, le SMS ne sera plus configurable comme 2e facteur à l'UNIL. Il vous faut configurer une [application d'authentification TOTP](#) ou des [Passkey](#).**

La dernière option, **que nous déconseillons fortement pour une raison de fiabilité** et qui sera peu à peu retirée, est d'utiliser le SMS. Un code vous sera envoyé à chaque connexion nécessitant un 2e facteur.

Si vous utilisez un numéro de téléphone non suisse, sachez que certains pays ou opérateurs peuvent limiter la réception de SMS, ou vous les faire payer. Nous vous recommandant dans ce cas de passer par une application d'authentification plutôt que le SMS.

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>).

The screenshot shows the 'Switch edu-ID' account management interface. At the top, there is a navigation bar with the logo, 'Aide', 'FR', and a user profile dropdown. Below this are four tabs: 'Profil', 'Sécurité', 'Confidentialité', and 'Organisations'. The 'Sécurité' tab is active. Underneath, there are sections for 'Mot de passe' and 'Authentification multifacteur'. The 'Authentification multifacteur' section has a red box around a toggle switch that is currently in the 'Off' position. A mouse cursor is pointing at the 'Off' button. Below the toggle, there is a descriptive text: 'Augmentez la sécurité de votre compte en utilisant un deuxième facteur.'

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 :

## Connexion

E-mail

Avec mot de passe

 Avec une passkey

## TOTP

Si vous utilisez un mot de passe, renseignez-le

# Connexion

E-mail

Mot de passe

Entrez votre mot de passe



Mot de passe oublié ?


Connexion



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

# Connexion

## Login en deux étapes:

 Ouvrez votre app d'authentification pour voir le code.

Code

123456

---

Ne plus me demander pendant un certain temps

Réinitialiser l'authentification multifacteur

Connexion

## 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-accordion>

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

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

---

Révision #67

Créé 8 avril 2021 06:42:16 par Chr Gr

Mis à jour 12 février 2026 15:21:41 par Chr Gr