

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

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 ¹

Confidentialité

Organisations

Mot de passe

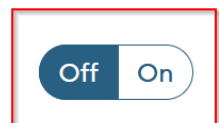
Mot de passe

Changé il y a 4 ans



Authentification multifacteur

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

²

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.

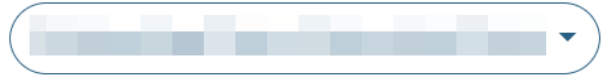
App d'authentification

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.

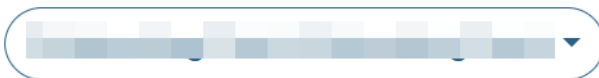
Numéro de téléphone mobile

+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.

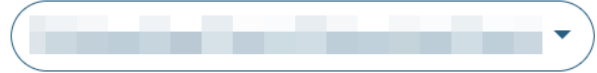
De plus en plus de gestionnaires de mot de passe offrent la possibilité de gérer à la fois vos mots de passe ainsi que le 2e facteur au sein d'une seule et unique app, comme le trousseau macOS (dernière version) ou

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

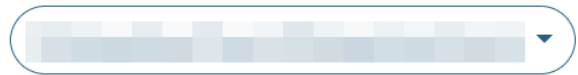
gestionnaire de mots de passe synchronisé comme BitWarden, qui permet d'utiliser la même Passkey sur plusieurs appareils.

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 includes a description and a toggle switch that is currently set to 'Off'. A red box highlights the 'Off' button, with a mouse cursor pointing to it.

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.

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 **Paskey** 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)~~

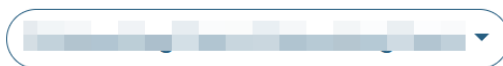
The edu-ID identity includes the use of multifactor authentication, and its activation is easy. To read the official SWITCH documentation on MFA and edu-ID, visit the following page:

<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**,



Profile

Security



Privacy

Organisations

Password

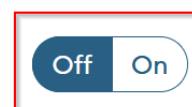
Password

Set 4 years ago



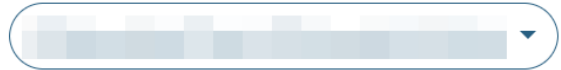
Multi-factor Authentication

Increase your account security by using a second factor.



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.



Set Up Multi-factor Authentication

Passkey

Use the passwordless login method, which uses biometric information such as fingerprint or Face ID. Passkeys replace the first and second factor of a login.

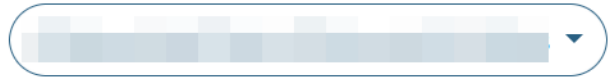
Authenticator App

Use an authenticator app like Google or Microsoft Authenticator. This method is used in combination with your password to provide a multi-factor authentication.

[More options](#)

Authenticator app

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



Mobile Number for the Multi-Factor Authentication

Please provide a mobile number which can be used in case you need to recover your account.

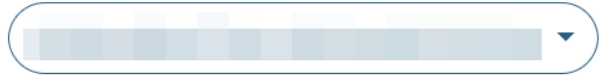
Mobile phone number

+41 79 234 56 78

Skip

Verify

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



Register your Authenticator App

1. Open your authenticator app

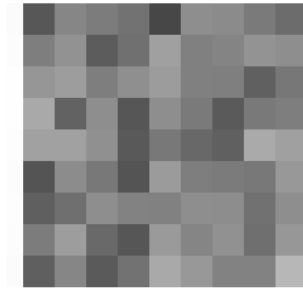
Frequently used applications:

- Google Authenticator ([iOS](#), [Android](#))
- Microsoft Authenticator ([iOS](#), [Android](#))
- Password manager

2. Add a new item

3. Scan the QR code

4. Enter the 6 digits below



Secret key



Verification code

123456

Cancel

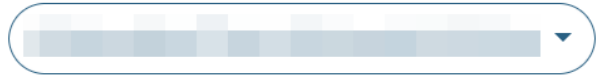
Submit

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.



Your New Recovery Code

Keep the recovery code in a **safe but retrievable place** (e.g., password manager or safety box).



I have stored it

Continue

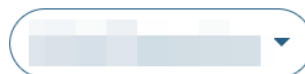
Passkey

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 find more information in the [Switch FAQ](#).

If you encounter problems or compatibility issues while configuring or using Passkeys, please report them to the [helpdesk](#).



Manage your Passkeys

Passkeys are a replacement for your password and allow a faster, easier and more secure login. Secure your account with Passkey!

⚠ We recommend registering **multiple passkeys** in order to have a spare device in case of loss.

You have no registered passkeys yet.

+ Add a Passkey

Back

Continue

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.

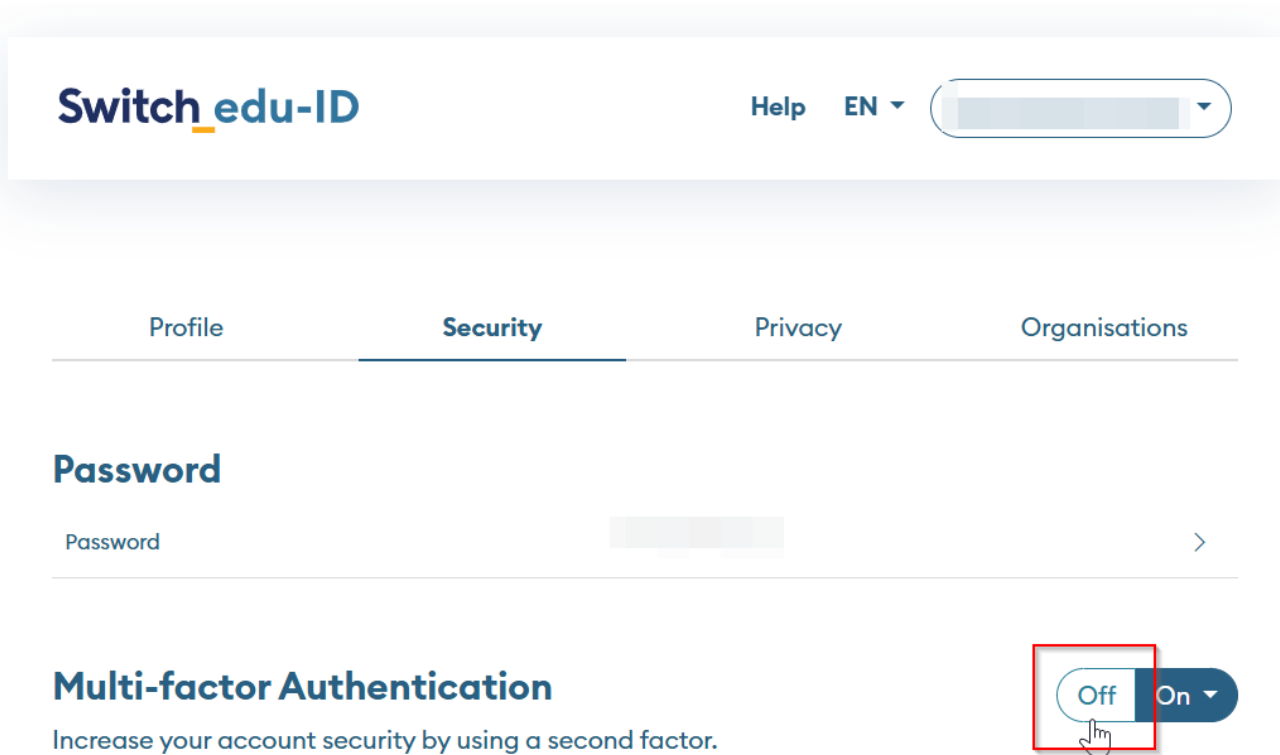
If you use a non-Swiss phone number, please be aware that certain countries and operators may limit the delivery of SMS messages, or charge for them. In this case, we recommend you use an authenticator app rather than the SMS option.

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 process 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>).



The screenshot shows the 'Switch edu-ID' account management interface. At the top, there is a navigation bar with the logo, 'Help', 'EN', and a language selector. Below this is a horizontal menu with 'Profile', 'Security', 'Privacy', and 'Organisations'. The 'Security' tab is selected. Under the 'Password' section, there is a 'Password' field with a right-pointing arrow. Below that, the 'Multi-factor Authentication' section is visible, with the text 'Increase your account security by using a second factor.' To the right of this text is a toggle switch currently set to 'Off'. A red rectangular box highlights the 'Off' button, and a mouse cursor is pointing at it.

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:

Login

E-mail

Use password

 Use a passkey

TOTP

If you choose the password, enter it

Create Account

Login

E-mail

Password

Enter your password



Forgot password?

Login

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

Login

Two-Step Login:

 Open your authenticator app to see the code.

Code

123456

Don't ask again for some time

[Reset multi-factor authentication](#)

[Login](#)

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.

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/multifacteurs?
- 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

Quel type d'utilisateur ?

ont tous un compte UNIL

Entra

- Service interne UNIL
- Groupes AD/Sylvia possibles
- 2e facteur déjà configuré
- Échange de métadonnées nécessaires
- Identifiants compte UNIL

peuvent venir de l'UNIL
et/ou d'autres institutions

Edu-ID

- Utilisateurs hors UNIL possible
- Fédération AAI Switch
- Resource Registry à configurer
- Identifiants Edu-ID
- 2e facteur à configurer par l'utilisateur si pas encore fait