SWISS LEARNING HUB

time2learn
Young Talents

Guide de l'authentification multifactorielle (AMF)

Version, Datum
Version 1.4, 13.08.2026

Copyright
© Swiss Learning Hub AG

Ce document et son contenu sont la propriété du Swiss Learning Hub SA et ne peuvent être copiés, reproduits, transmis ou utilisés pour l'exécution sans autorisation écrite.

Swiss Learning Hub AG
Rosengartenstrasse 4
CH-8608 Bubikon

www.swisslearninghub.com

Inhaltsverzeichnis

1 Pourquoi l'authentification multifactorielle (AMF)? 3

2 Configuration initiale de l'authentification multifactorielle 3

2.1 Configuration avec Microsoft Authenticator 3

2.2 Configuration avec Google Authenticator 9

3 Utilisation de l'AMF à chaque connexion 13

4 Cas d'assistance fréquents 15

4.1 Nouvel appareil mobile acquis 15

4.1.1 Microsoft Authenticator 15

4.1.2 Google Authenticator 16

4.2 Appareil mobile défectueux ou perdu 16

4.3 Aucun code n'apparaît sur votre appareil actuel 16

4.4 Nouvel enregistrement et le code scanné n’est pas valable 17

1 Pourquoi l'authentification multifactorielle (AMF)?

Dans un monde de plus en plus numérisé, la sécurité de nos activités en ligne devient de plus en plus importante. Une méthode efficace pour garantir la confidentialité de vos comptes numériques est l'authentification multifactorielle (MFA). Cette pratique de sécurité avancée exige plus qu'un simple mot de passe pour accéder aux comptes et joue donc un rôle essentiel pour garantir la sécurité des comptes d'utilisateurs à long terme.

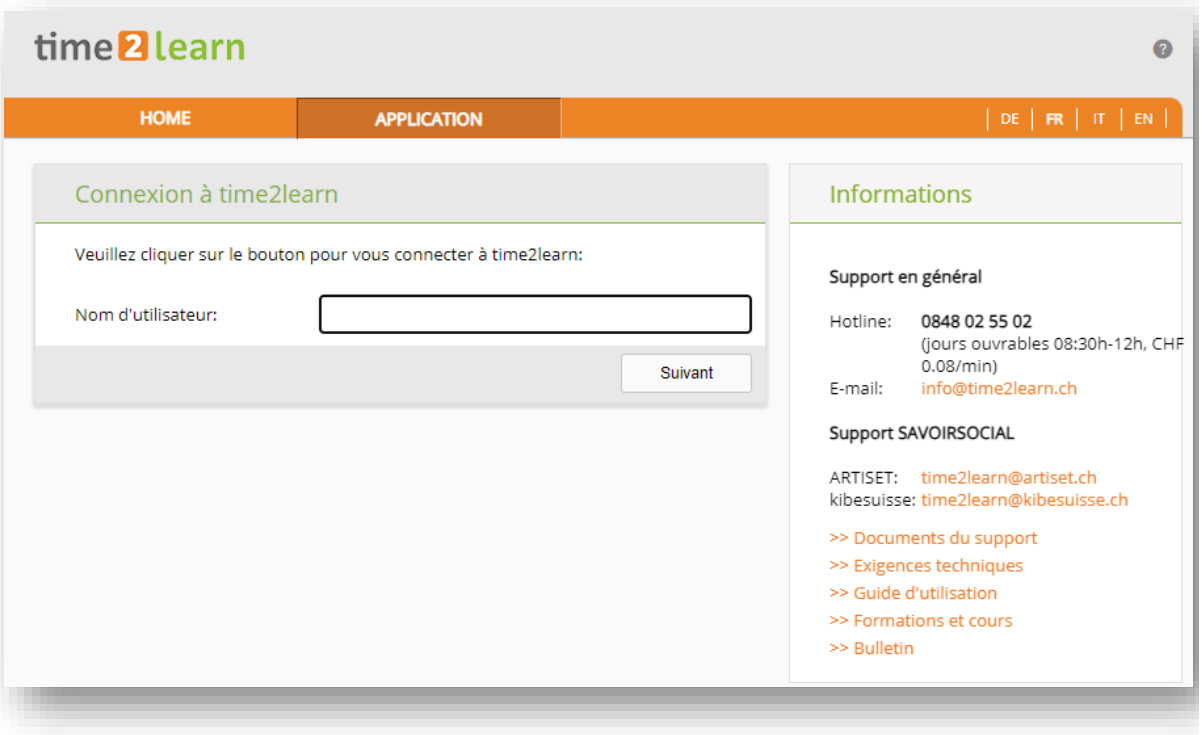
2 Configuration initiale de l'authentification multifactorielle

La configuration de AMF pour time2learn est simple et peut être effectuée en quelques étapes. Vous pouvez décider librement si vous souhaitez vous connecter avec le **Microsoft Authenticator** ou le **Google Authenticator**. Les deux peuvent être téléchargés gratuitement dans Google Playstore (Android), ou dans l'Appstore (IOS).

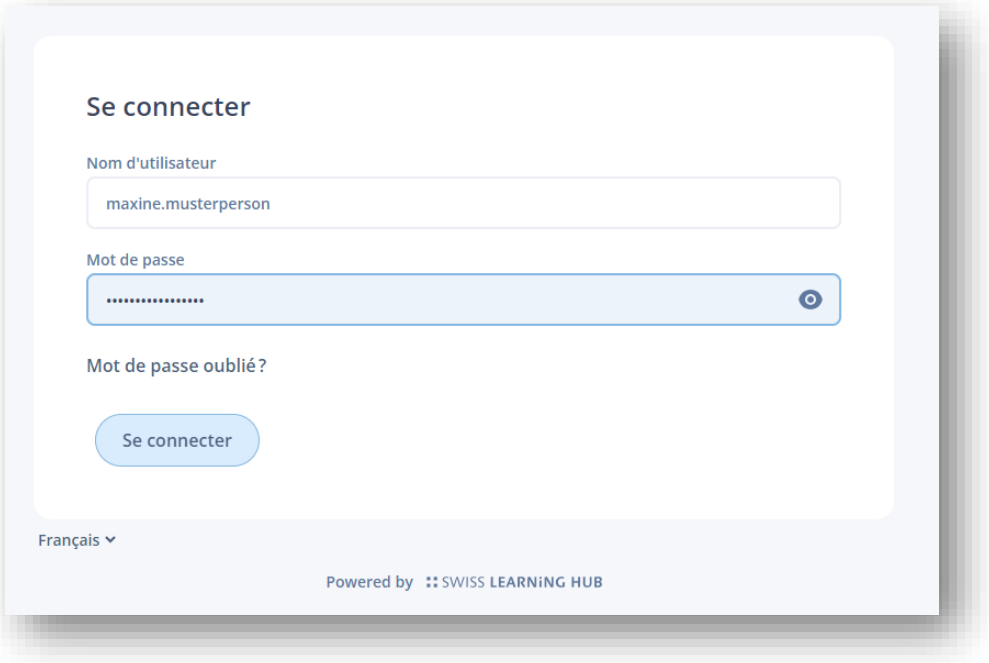
Remarque: la première configuration doit être effectuée sur un PC, un MAC ou un ordinateur portable. La première installation sur un appareil mobile n'est pas recommandée!

2.1 Configuration avec Microsoft Authenticator

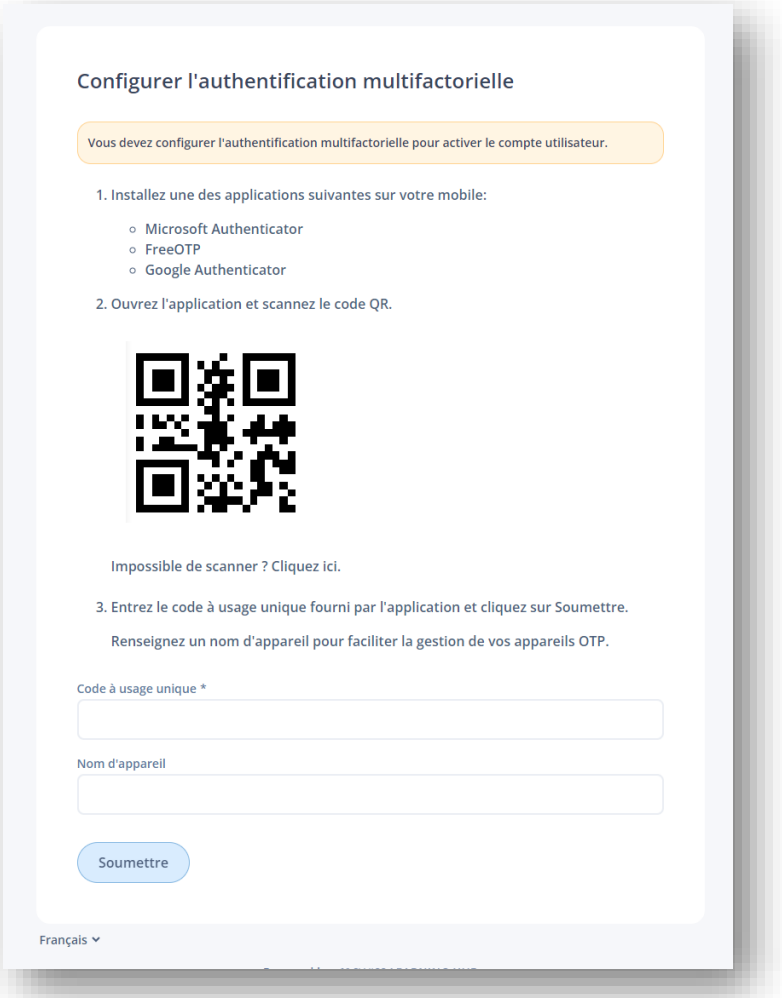
Étape 1: Saisir le nom d'utilisateur sur la page de connexion de time2learn



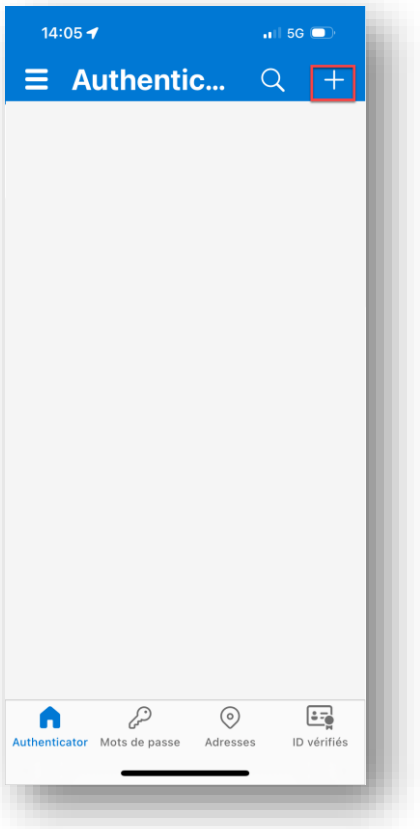
Étape 2: Connectez-vous à time2learn



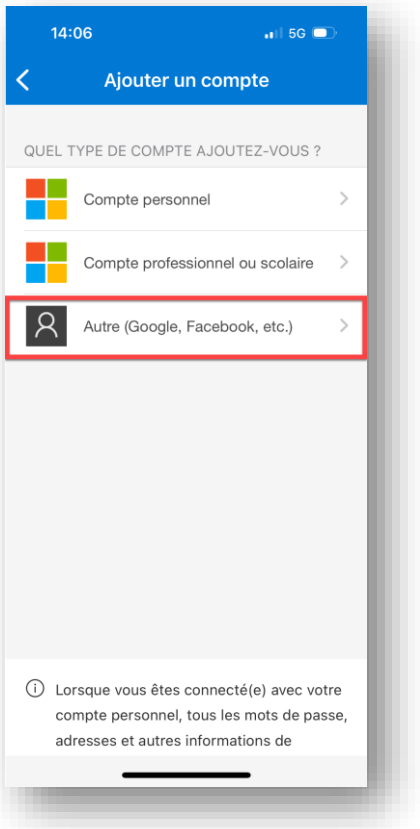
Si l'authentification multi-facteurs est active, vous verrez cet écran.



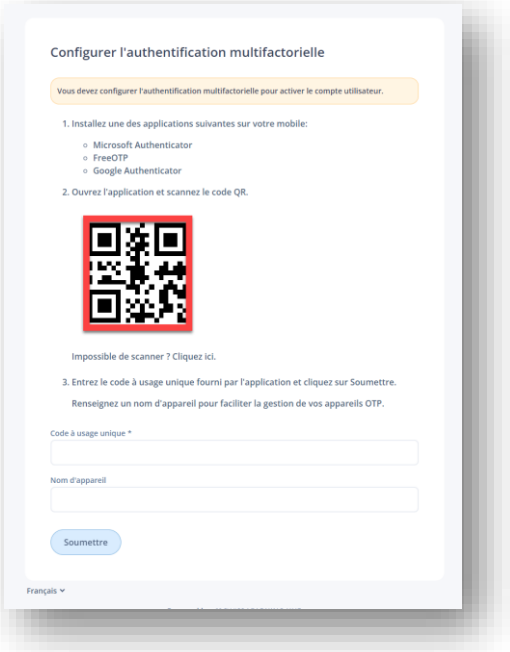
Étape 3: Ouvrez Microsoft Authenticator et sélectionnez "Ajouter un compte".



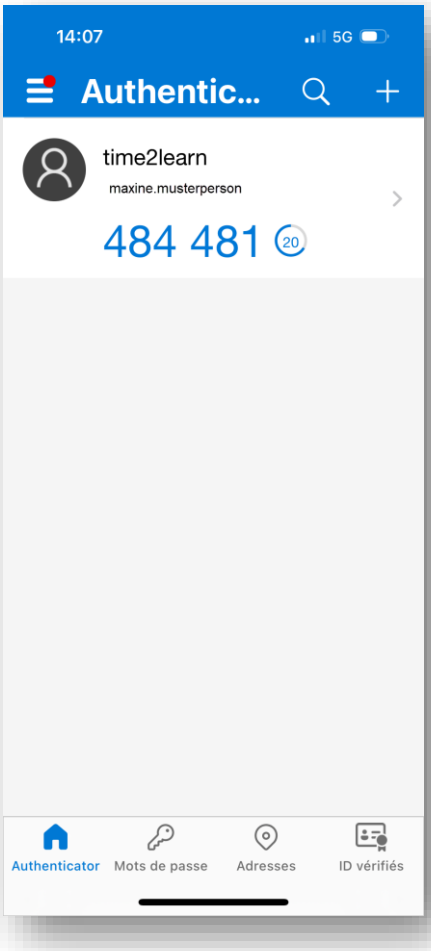
Ensuite, cliquez sur "Autre compte".



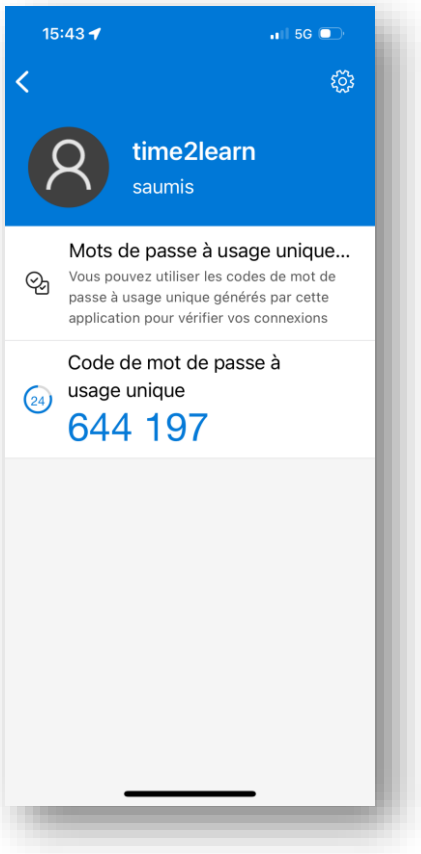
Étape 4: Maintenant, vous pouvez tout simplement scanner le code QR dans time2lean.

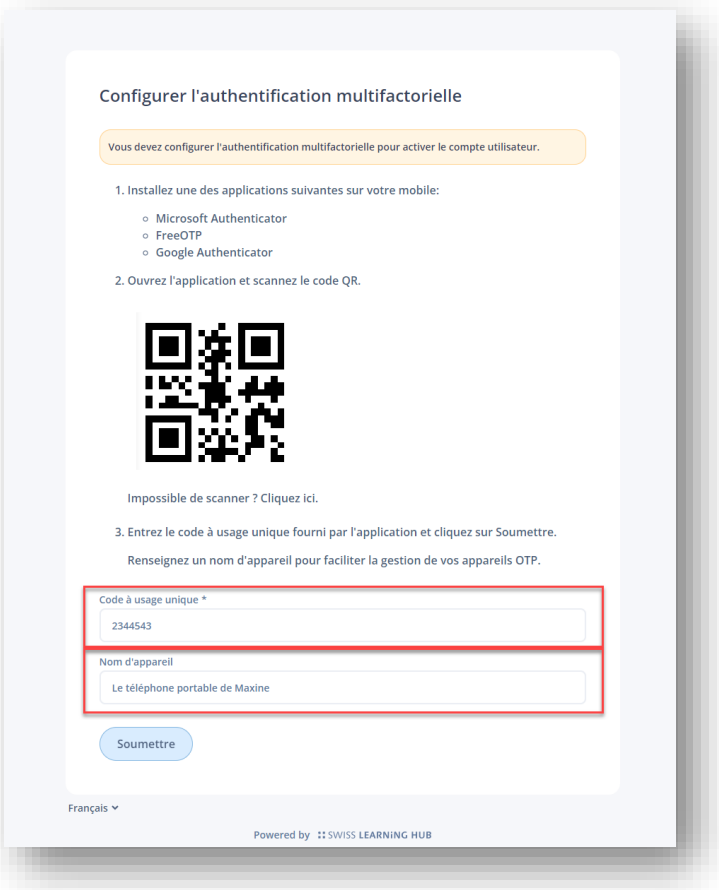


Étape 5: Vous voyez maintenant time2learn sur la page d'accueil de l'authentificateur



Étape 6: Sélectionnez time2learn et un code à usage unique s'affichera, que vous pouvez maintenant saisir sur la page de connexion.





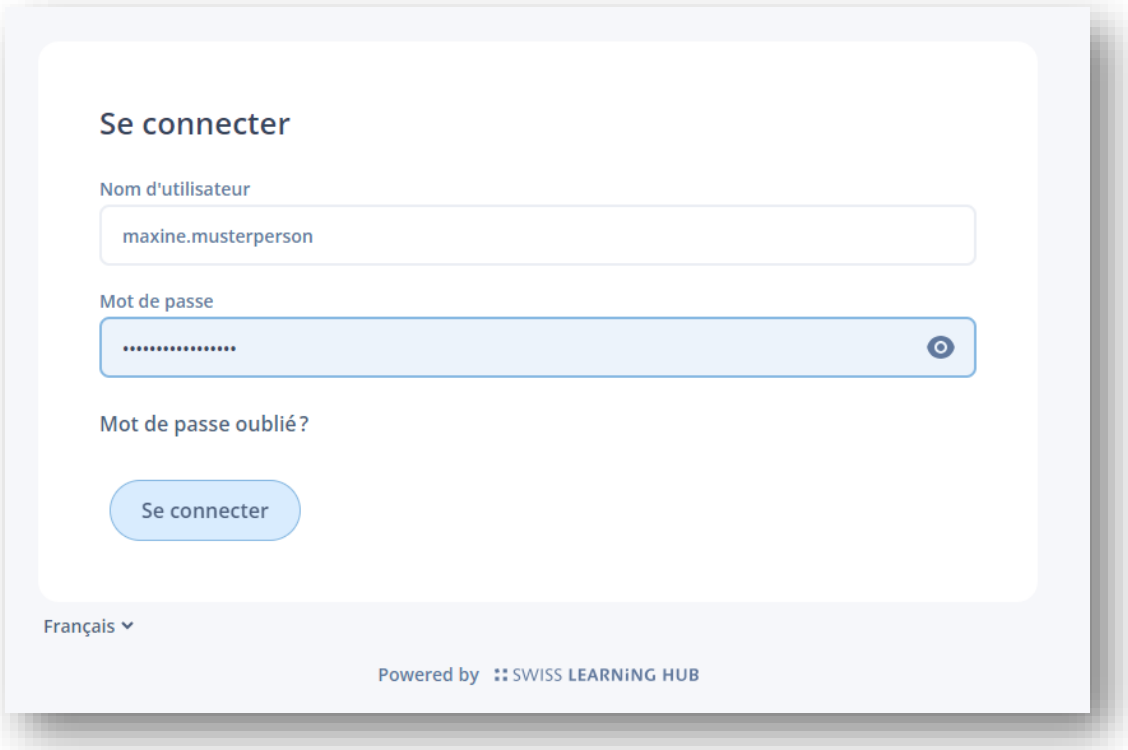
Nom de l’appareil (facultatif) : sert à identifier l’appareil utilisé. Le champ peut être laissé vide.

La configuration est maintenant terminée ! L'application Microsoft Authenticator est maintenant utilisée pour générer des codes de sécurité supplémentaires lorsque vous vous connectez à votre compte.

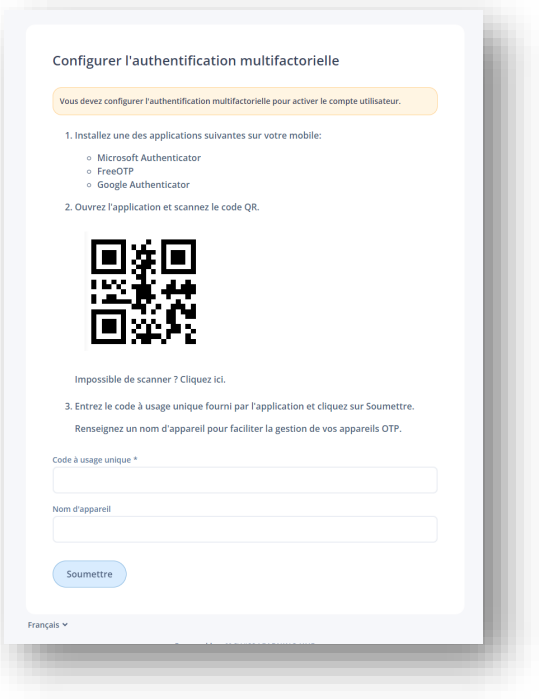
2.2 Configuration avec Google Authenticator

Étape 1: Saisir le nom d'utilisateur sur la page de connexion de time2learn

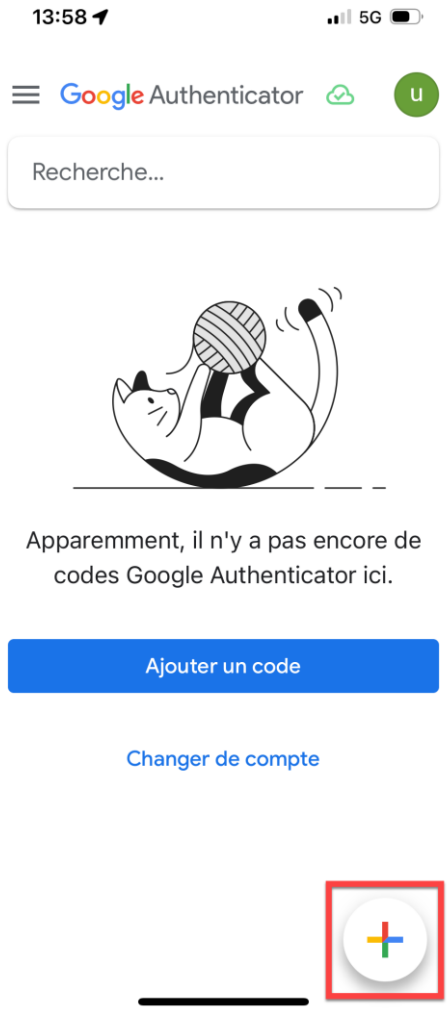
Étape 2: Connectez-vous à time2learn comme d'habitude.



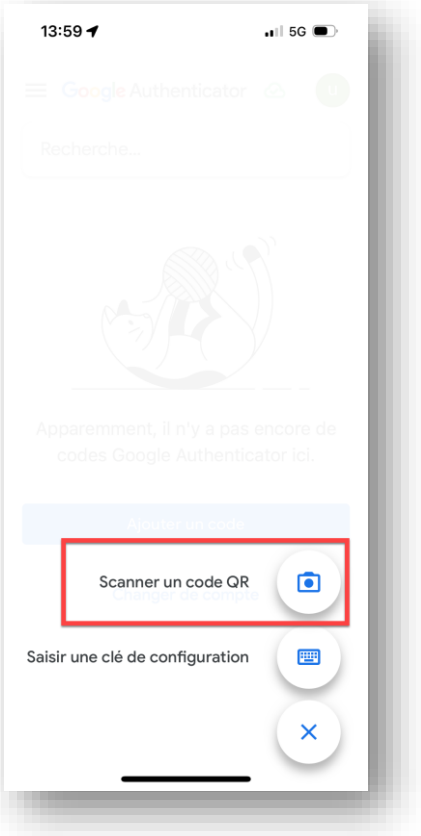
Si l'authentification multi-facteurs est active, vous verrez cet écran.



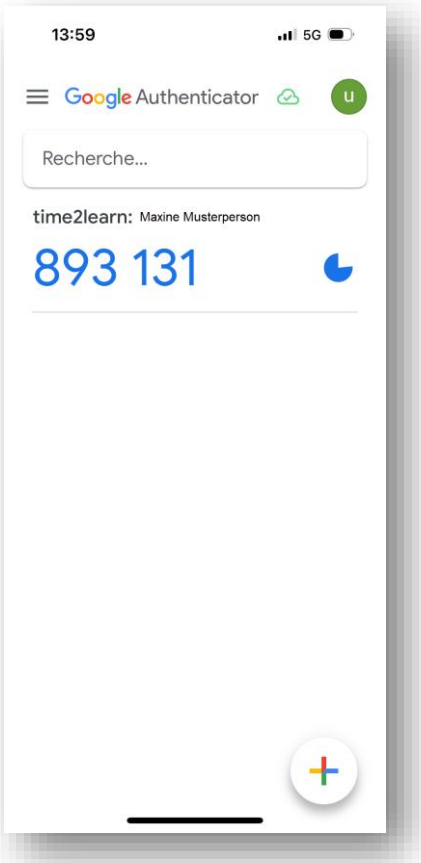
Étape 3: Ouvrez Google Authenticator, connectez-vous avec votre compte Google et sélectionnez le signe "+" pour ajouter un compte.

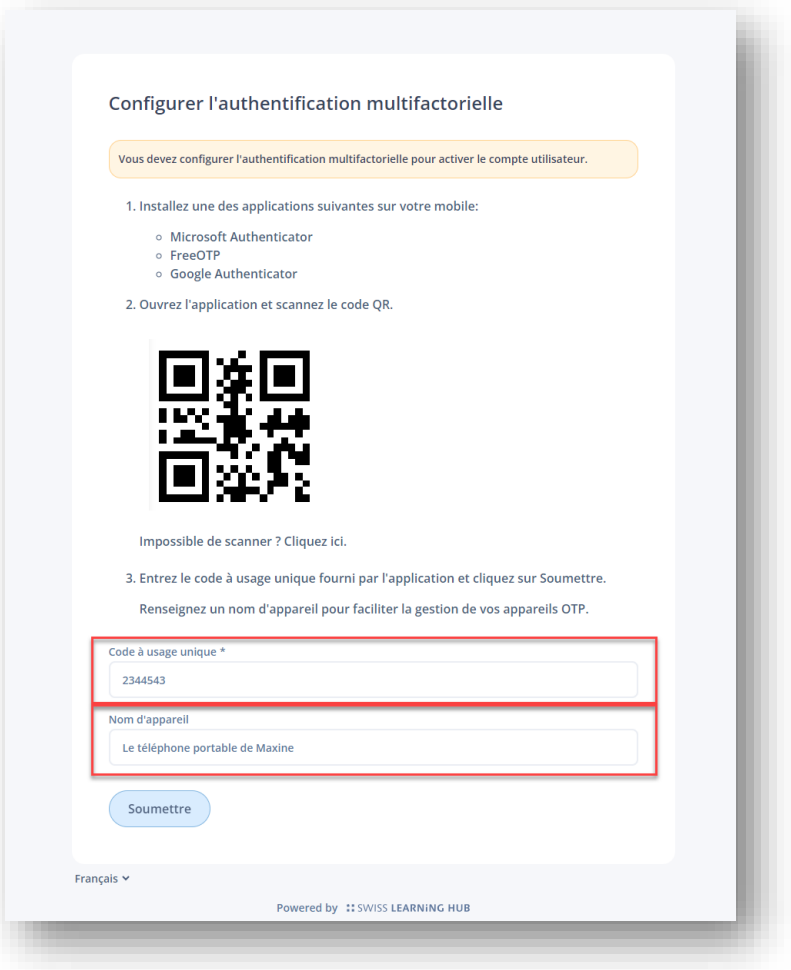


Étape 4: Maintenant, vous pouvez tout simplement scanner le code QR dans time2lean.



Étape 5: Un code à usage unique s'affiche maintenant, que vous pouvez saisir dans time2learn.



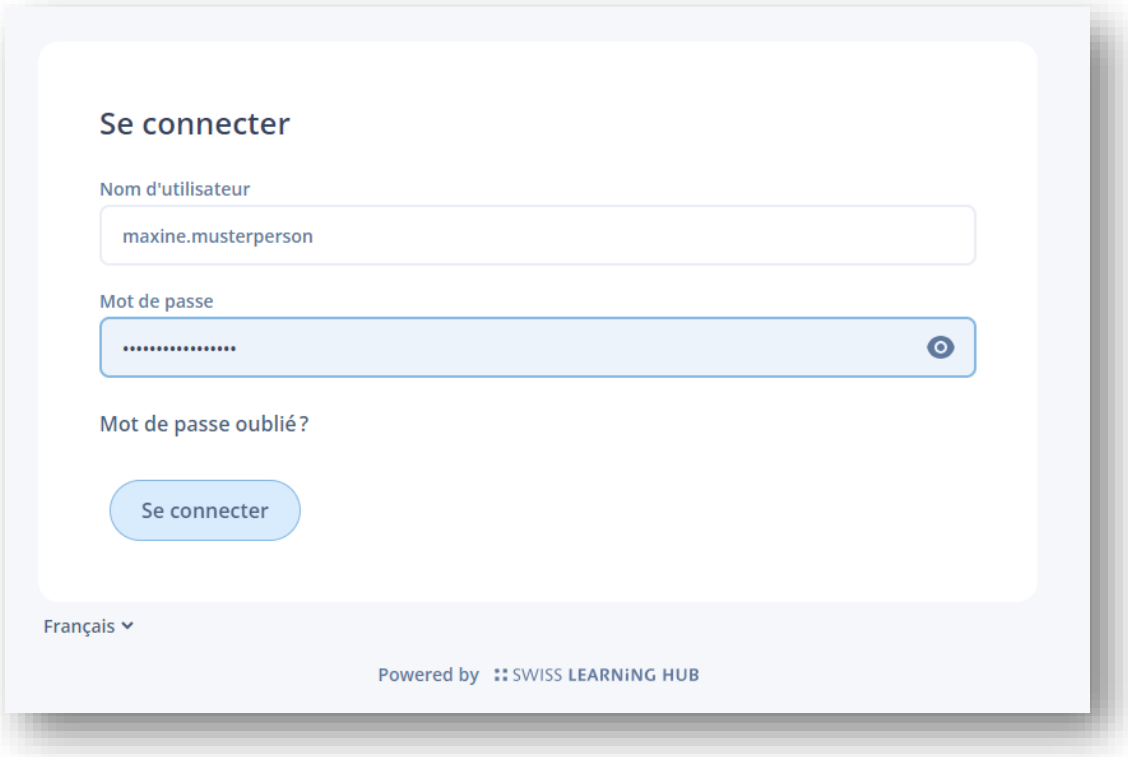


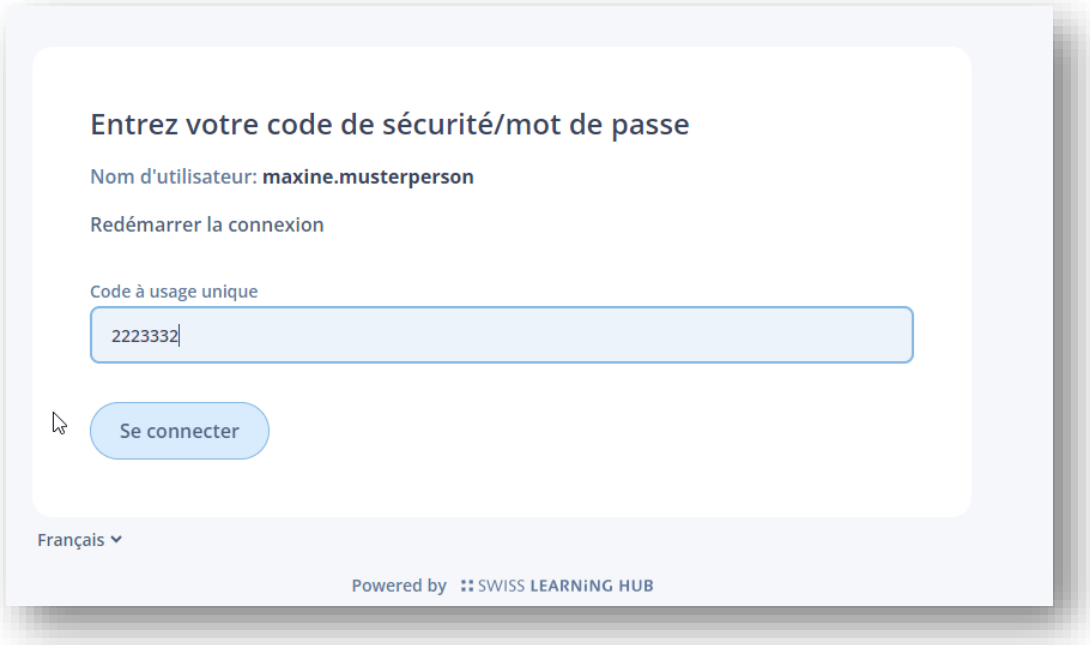
Nom de l’appareil (facultatif) : sert à identifier l’appareil utilisé. Le champ peut être laissé vide.

La configuration est maintenant terminée ! L'application Google Authenticator est désormais utilisée pour générer des codes de sécurité supplémentaires lorsque vous vous connectez à votre compte.

3 Utilisation de l'AMF à chaque connexion

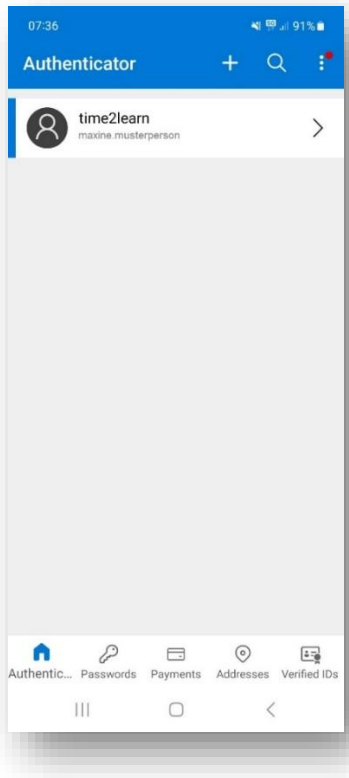
Lors de la connexion régulière à time2learn, il vous sera demandé de saisir votre nom d'utilisateur et votre mot de passe, puis un "code à usage unique".





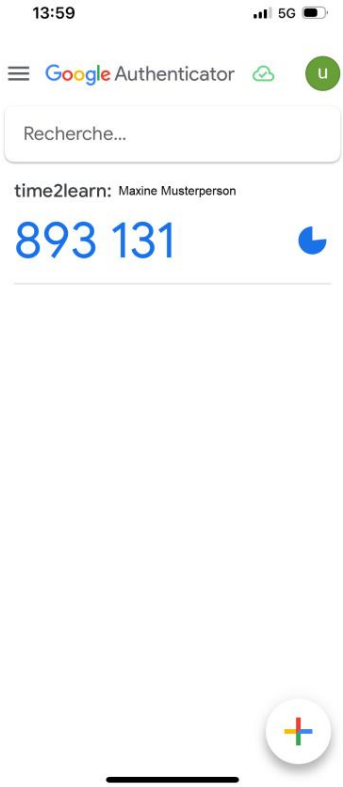
Ouvrez maintenant votre application Authenticator préférée et saisissez vos données de connexion.

Microsoft Authenticator

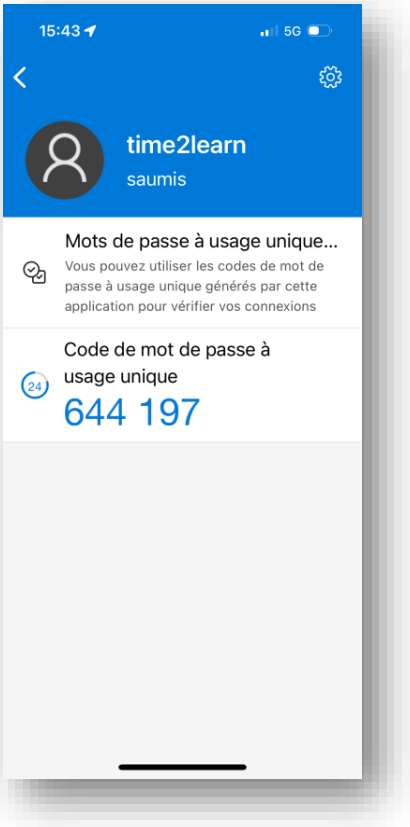


Sélectionnez time2learn

Google Authenticator



Le code est directement visible ici



Maintenant, le code est également visible ici

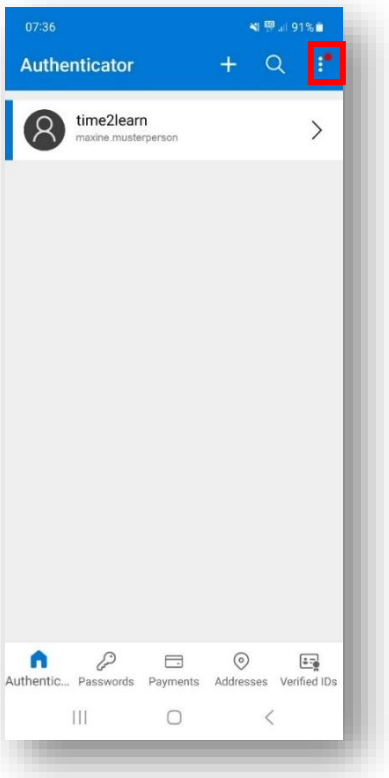
4 Cas d'assistance fréquents

Vous avez acheté un nouveau mobile, vous avez perdu votre mobile enregistré ou il est défectueux, vous n'avez pas reçu le code d'enregistrement ? Vous trouverez ici de l'aide pour les cas d'assistance les plus fréquents. Nous préférons que vous nous contactiez par e-mail. Les informations concernant le nom d'utilisateur, la raison de la réinitialisation et éventuellement une capture d'écran du message d'erreur permettent de résoudre le cas plus rapidement.

4.1 Nouvel appareil mobile acquis

Selon l'authentificateur, il est possible d'exporter les entrées existantes dans l'authentificateur et de les réimporter sur le nouvel appareil dans l'authentificateur correspondant. Sur votre nouvel appareil, chargez déjà au préalable l'Authenticator utilisé à l'origine.

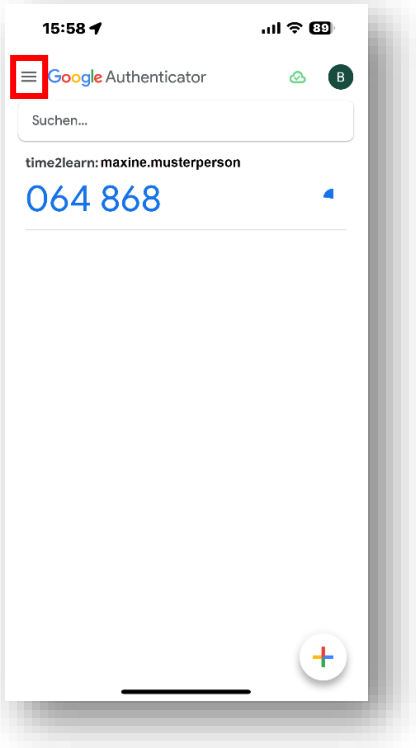
4.1.1 Microsoft Authenticator



- Tapez sur les trois points dans le coin supérieur droit et sélectionnez « Paramètres ».
- Tapez sur « Sauvegarde ».
- Activez la sauvegarde si elle n'est pas encore activée. Pour cela, vous devez être connecté à votre compte Microsoft.

- Téléchargez maintenant l'application Microsoft Authenticator depuis l'App Store (iOS) ou Google Play Store (Android) sur votre nouveau téléphone et installez-la.
- Ouvrez l'application sur votre nouveau téléphone.
- Pour transférer les entrées vers votre nouveau téléphone, vous devez restaurer la sauvegarde dans le nuage. Pour ce faire, connectez-vous avec le même compte Microsoft que celui que vous utilisiez sur votre ancien téléphone.
- L'application recherchera automatiquement les sauvegardes existantes et vous donnera la possibilité de restaurer la sauvegarde.

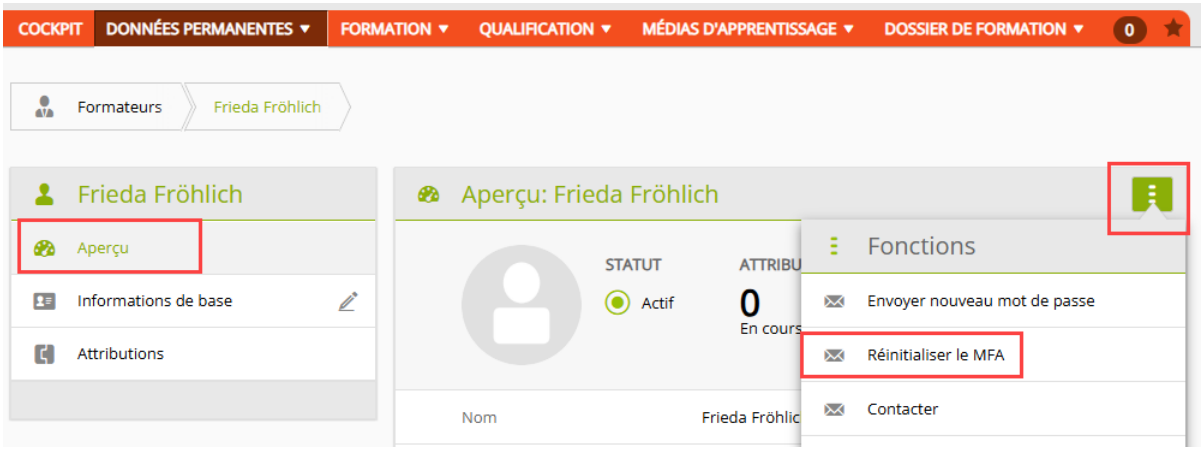
4.1.2 Google Authenticator



- Sélectionnez Menu
- Transférer des comptes
- Exposez vos comptes
- Sélectionner les comptes que vous souhaitez exporter
- Le code QR de transmission apparaît
- Scannez ce code QR sur le nouvel appareil
- Toutes les entrées sélectionnées sont reprises
- Sur l'ancien appareil, vous pouvez alors choisir de supprimer ou de conserver ces entrées

4.2 Appareil mobile défectueux ou perdu - nouvel appareil mobile

Les administrateurs au sein de l'entreprise qui créent de nouveaux profils et réinitialisent les mots de passe des utilisateurs peuvent également réinitialiser le paramètre MFA.



Lors de la prochaine connexion, un nouveau code QR apparaîtra et vous pourrez réenregistrer votre appareil mobile. Le code s'affichera ensuite sur le nouvel appareil.

4.3 Aucun code n'apparaît sur votre appareil actuel

Les administrateurs au sein de l'entreprise, qui créent également de nouveaux profils et réinitialisent les mots de passe des utilisateurs, peuvent également réinitialiser le paramètre MFA (voir ci-dessus). Ensuite, lorsque vous vous connecterez à nouveau, vous recevrez à nouveau un code QR qui vous permettra de créer une nouvelle entrée et d'enregistrer votre mobile. Il est

recommandé de supprimer au préalable une entrée déjà existante concernant time2learn dans l'Authenticator que vous utilisez.

4.4 Nouvel enregistrement et le code scanné n’est pas valable

1. Supprimez les éventuels comptes déjà créés pour time2learn dans votre application Authenticator
2. Connectez-vous à nouveau à time2learn avec votre nom d'utilisateur / mot de passe
3. Créez une nouvelle entrée pour time2learn dans votre application Authenticator en scannant le code-barres et en saisissant le code unique qui s'affiche.

IMPORTANT: Si vous ne saisissez pas de code unique ou si vous saisissez un code erroné, vous devez impérativement recommencer l'étape 1 afin que le code-barres puisse être scanné à nouveau et qu'une nouvelle entrée soit créée dans l'application.