



Guide de l'authentification multifactorielle (AMF)

Version, Datum

Version 1.4, 01.10.2025

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.

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

The screenshot shows the time2learn login interface. On the left, under 'Connexion à time2learn', there is a text input field labeled 'Nom d'utilisateur:' and a 'Suivant' button. On the right, under 'Informations', there is a section for 'Support en général' with a phone number (0848 02 55 02) and email (info@time2learn.ch). Below this is a section for 'Support SAVOIRSOCIAL' with links to ARTISET (time2learn@artiset.ch) and kibesuisse (time2learn@kibesuisse.ch), and a list of support documents: >> Documents du support, >> Exigences techniques, >> Guide d'utilisation, >> Formations et cours, >> Bulletin.

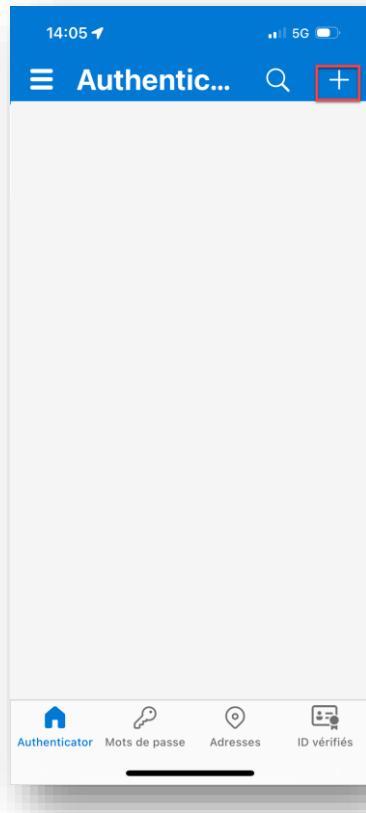
Étape 2: Connectez-vous à time2learn

The screenshot shows the 'Se connecter' (Log in) page of the time2learn application. It features a light gray header with the Swiss Learning Hub logo. Below it is a white form area with a rounded rectangle border. Inside the form, there are two input fields: 'Nom d'utilisateur' (User name) containing 'maxine.musterson' and 'Mot de passe' (Password) with a masked value. To the right of the password field is a small circular icon with a dot. Below these fields are links for 'Mot de passe oublié?' (Forgot password?) and 'Se connecter' (Log in). At the bottom left is a language selector 'Français ▾'. At the bottom center is the text 'Powered by SWISS LEARNING HUB'.

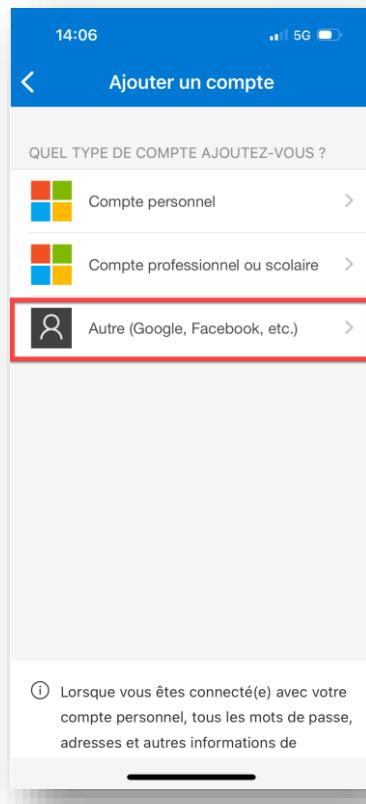
Si l'authentification multi-facteurs est active, vous verrez cet écran.

The screenshot shows the 'Configurer l'authentification multifactorielle' (Configure multi-factor authentication) page. A yellow callout box at the top states: 'Vous devez configurer l'authentification multifactorielle pour activer le compte utilisateur.' (You must configure multi-factor authentication to activate the user account.) Below this, numbered steps guide the user: 1. Install one of the following applications on your mobile device: Microsoft Authenticator, FreeOTP, Google Authenticator. 2. Open the app and scan the QR code. A large QR code is displayed in the center. 3. Enter the unique code provided by the app and click 'Soumettre'. A note below says: 'Renseignez un nom d'appareil pour faciliter la gestion de vos appareils OTP.' (Enter a device name to facilitate management of your OTP devices.) At the bottom are input fields for 'Code à usage unique *' (One-time code *) and 'Nom d'appareil' (Device name), and a blue 'Soumettre' (Submit) button. The bottom left corner shows the language selector 'Français ▾'.

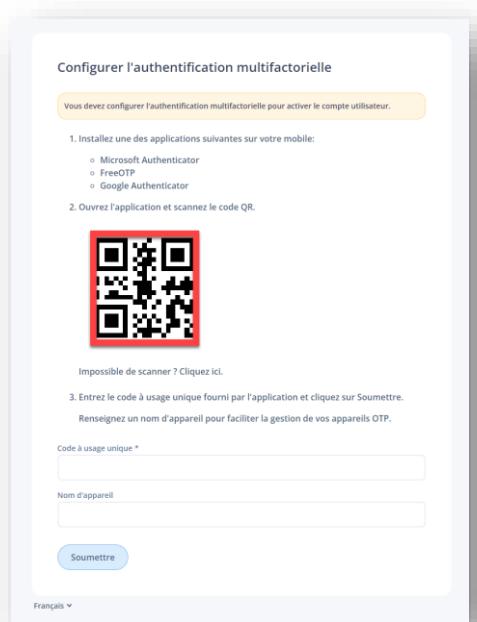
Étape 3: Ouvrez Microsoft Authenticator et sélectionnez "Ajouter un compte".



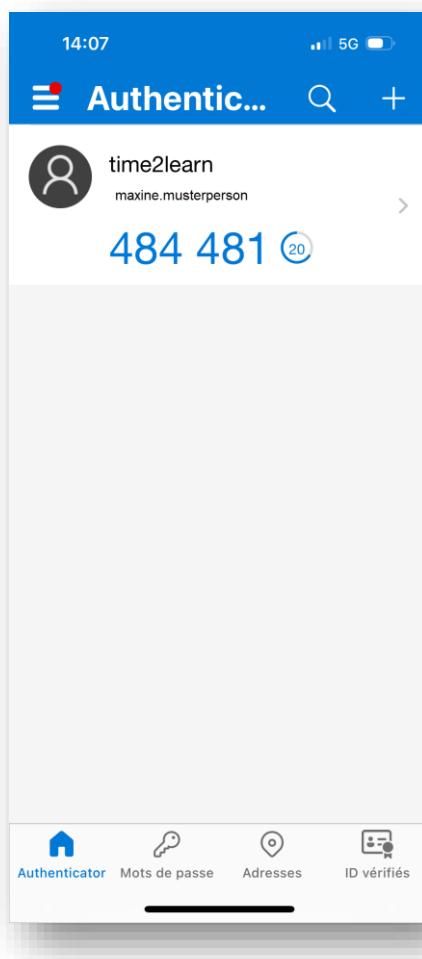
Ensuite, cliquez sur "Autre compte".



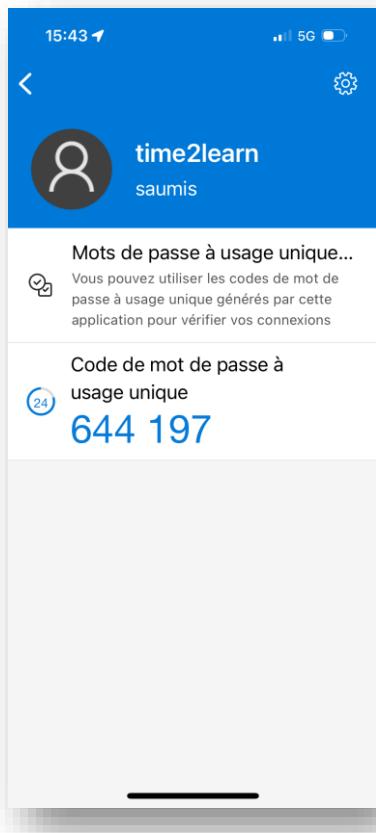
Étape 4: Maintenant, vous pouvez tout simplement scanner le code QR dans time2lean.



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.



Pour terminer la première inscription, vous pouvez encore nommer ici l'appareil avec lequel vous vous connecterez à l'avenir.

Configurer l'authentification multifactorielle

Vous devez configurer l'authentification multifactorielle pour activer le compte utilisateur.

1. Installez une des applications suivantes sur votre mobile:
 - Microsoft Authenticator
 - FreeOTP
 - Google Authenticator
2. Ouvrez l'application et scannez le code QR.



Impossible de scanner ? Cliquez ici.

3. Entrez le code à usage unique fourni par l'application et cliquez sur Soumettre.
Renseignez un nom d'appareil pour faciliter la gestion de vos appareils OTP.

Code à usage unique *	2344543
Nom d'appareil	Le téléphone portable de Maxine

Soumettre

Français ▾

Powered by ::SWISS LEARNING HUB

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

The screenshot shows the time2learn login interface. On the left, under 'Connexion à time2learn', there is a text input field labeled 'Nom d'utilisateur:' and a 'Suivant' button. On the right, the 'Informations' sidebar contains sections for general support, contact details (Hotline, E-mail), and links to various support documents.

Connexion à time2learn

Veuillez cliquer sur le bouton pour vous connecter à time2learn:

Nom d'utilisateur:

Suivant

Informations

Support en général

Hotline: 0848 02 55 02
(jours ouvrables 08:30h-12h, CHF 0.08/min)

E-mail: info@time2learn.ch

Support SAVOIRSOCIAL

ARTISET: time2learn@artiset.ch
kibesuisse: time2learn@kibesuisse.ch

>> Documents du support
>> Exigences techniques
>> Guide d'utilisation
>> Formations et cours
>> Bulletin

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

The screenshot shows the 'Se connecter' (Log in) page. It features fields for 'Nom d'utilisateur' (username) containing 'maxine.musterson' and 'Mot de passe' (password) with a redacted value. Below these are links for password recovery ('Mot de passe oublié?') and a 'Se connecter' (Log in) button. At the bottom, there is a language selection dropdown set to 'Français' and a footer note about the power source.

Se connecter

Nom d'utilisateur

maxine.musterson

Mot de passe

.....

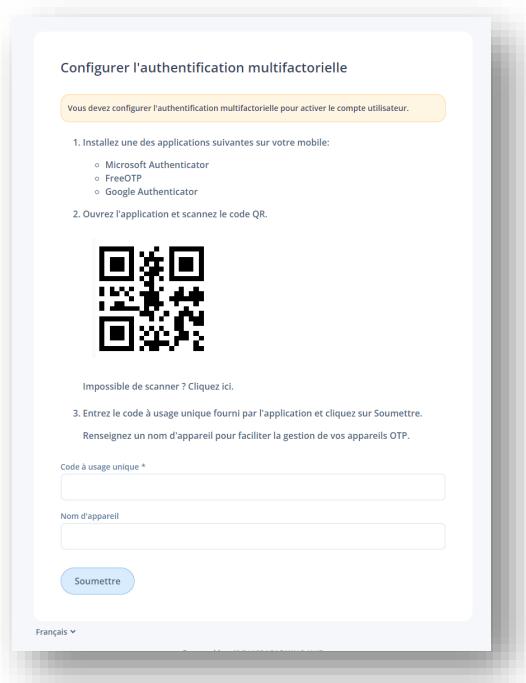
Mot de passe oublié?

Se connecter

Français ▾

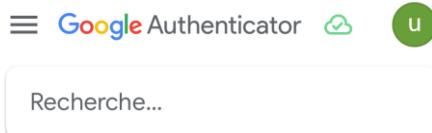
Powered by ■■ SWISS LEARNING HUB

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

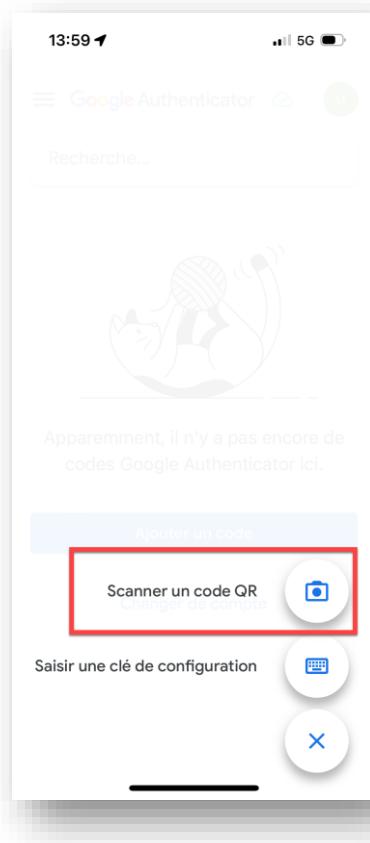


Étape 3: Ouvrez Google Authenticator, connectez-vous avec votre compte Google et sélectionnez le signe "+" pour ajouter un compte.

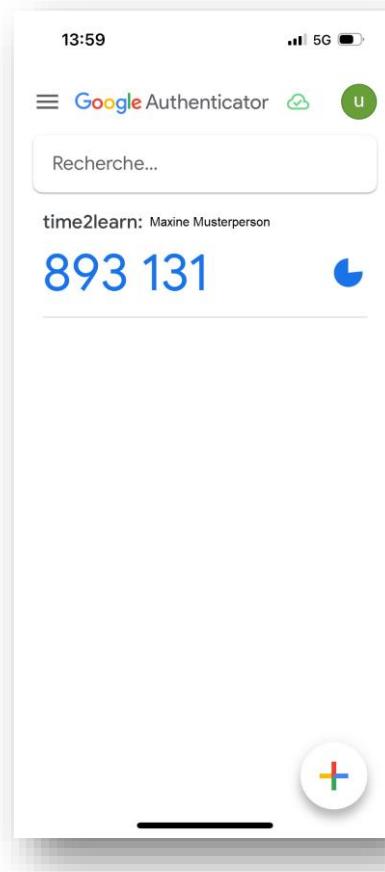
13:58 1 5G



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.



Pour terminer la première inscription, vous pouvez encore nommer ici l'appareil avec lequel vous vous connecterez à l'avenir.

Configurer l'authentification multifactorielle

Vous devez configurer l'authentification multifactorielle pour activer le compte utilisateur.

1. Installez une des applications suivantes sur votre mobile:

- Microsoft Authenticator
- FreeOTP
- Google Authenticator

2. Ouvrez l'application et scannez le code QR.



Impossible de scanner ? Cliquez ici.

3. Entrez le code à usage unique fourni par l'application et cliquez sur Soumettre.

Renseignez un nom d'appareil pour faciliter la gestion de vos appareils OTP.

Code à usage unique *

Nom d'appareil

Soumettre

Français ▾

Powered by ■■ SWISS LEARNING HUB

La configuration est maintenant terminée ! L'application Microsoft 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".

Se connecter

Nom d'utilisateur
maxine.musterson

Mot de passe
.....

Mot de passe oublié?

Se connecter

Français ▾

Powered by :: SWISS LEARNING HUB

Entrez votre code de sécurité/mot de passe

Nom d'utilisateur: maxine.musterson

Redémarrer la connexion

Code à usage unique
2223332

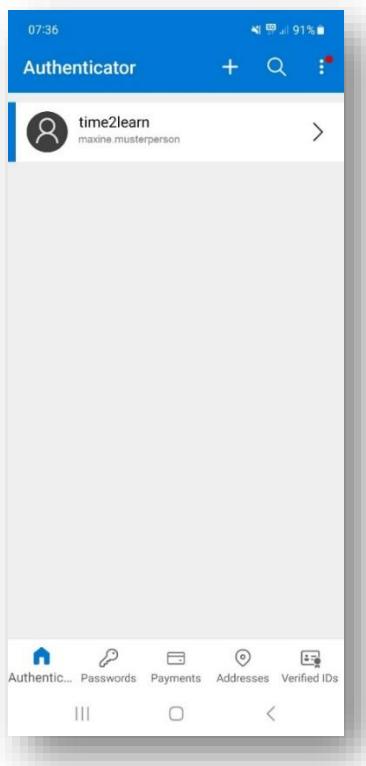
Se connecter

Français ▾

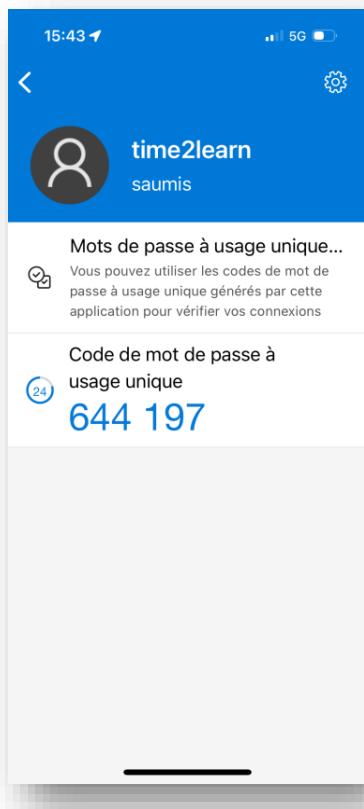
Powered by :: SWISS LEARNING HUB

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

Microsoft Authenticator

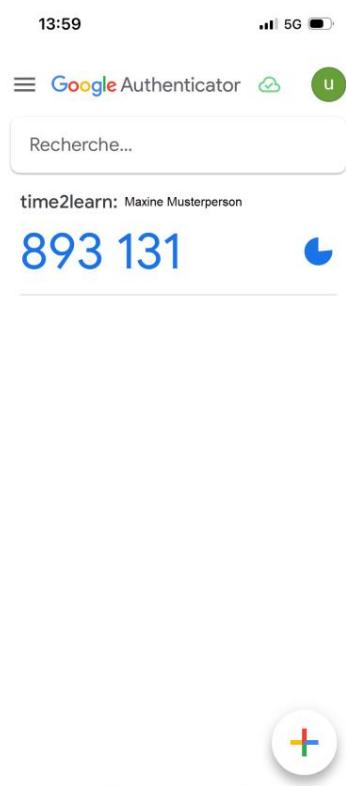


Sélectionnez time2learn



Maintenant, le code est également visible ici

Google Authenticator



Le code est directement visible ici

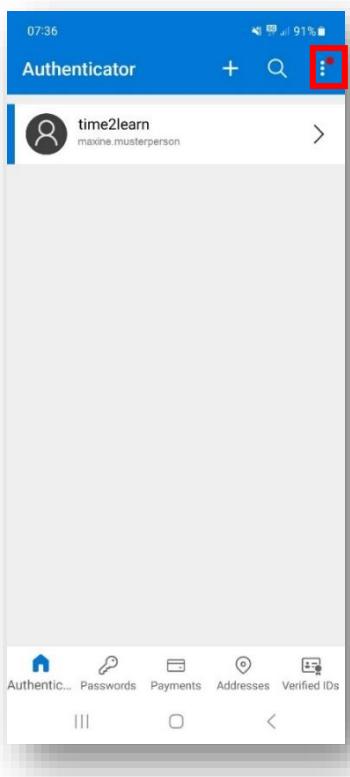
4 Cas d'assistance fréquents

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 préférions 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

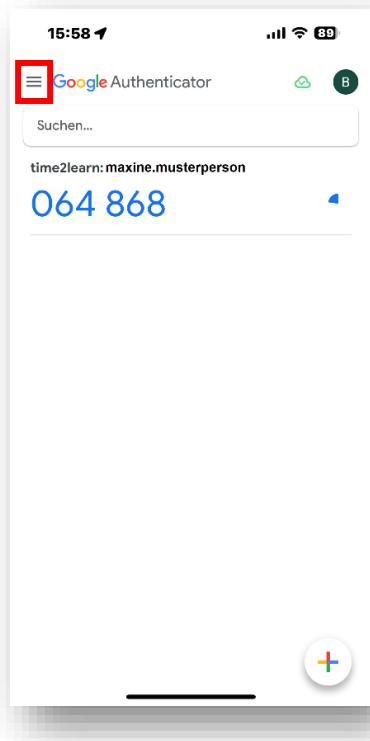
Selon l'authentificateur, il est possible d'exporter les entrées existantes dans l'authentificateur et de les réimporter sur le nouvel appareil dans l'authentificateur correspondant. Sur votre nouvel appareil, chargez déjà au préalable l'Authenticator utilisé à l'origine.

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 utilisez 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.