hemmer

TYPO3 & double authentification

Mise en place de la 2FA sur TYPO3

2024

Introduction

La double authentification (2FA) ajoute une couche de sécurité supplémentaire à vos comptes TYPO3 en exigeant deux facteurs d'authentification lors de la connexion. Cela signifie qu'en plus de votre mot de passe, vous devrez également fournir un code supplémentaire provenant d'une application d'authentification ou d'un autre appareil. Ceci rend plus difficile pour les pirates informatiques d'accéder à vos comptes, même s'ils obtiennent votre mot de passe.

1. Prérequis

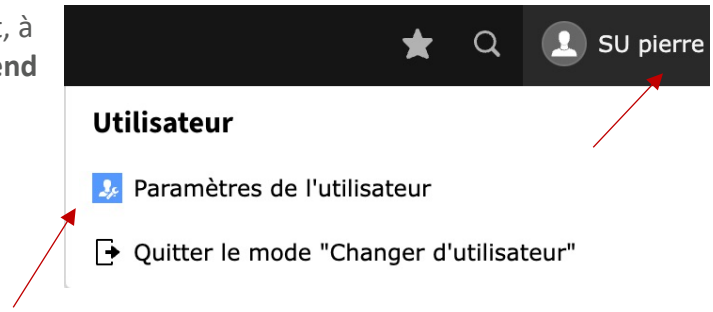
Avant de configurer la 2FA sur TYPO3, vous aurez besoin de :

- Un compte TYPO3 avec les droits d'administration
- Une application d'authentification, telle que Google Authenticator ou Microsoft Authenticator
- Un appareil mobile pour exécuter l'application d'authentification ou Bitwarden

2. Configuration de la 2FA pour un utilisateur principal

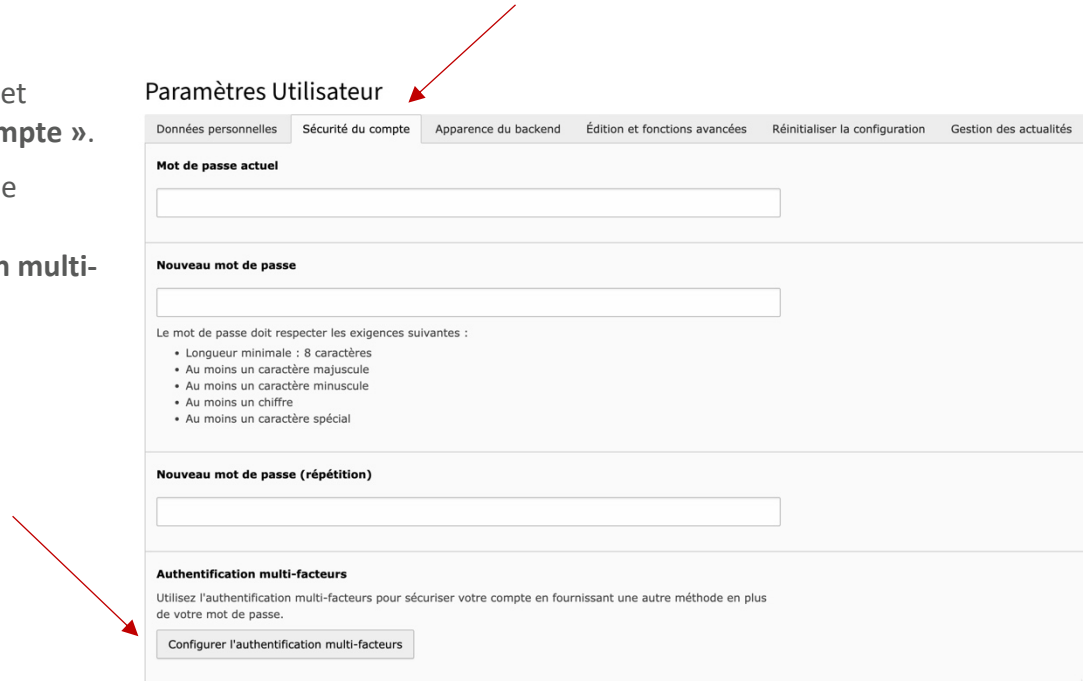
Connectez-vous à votre backend TYPO3. En haut, à droite, accédez au module **Utilisateurs du backend** en cliquant sur votre nom d'utilisateur.

Ensuite, sélectionnez l'option **« Paramètres de l'utilisateur ».**

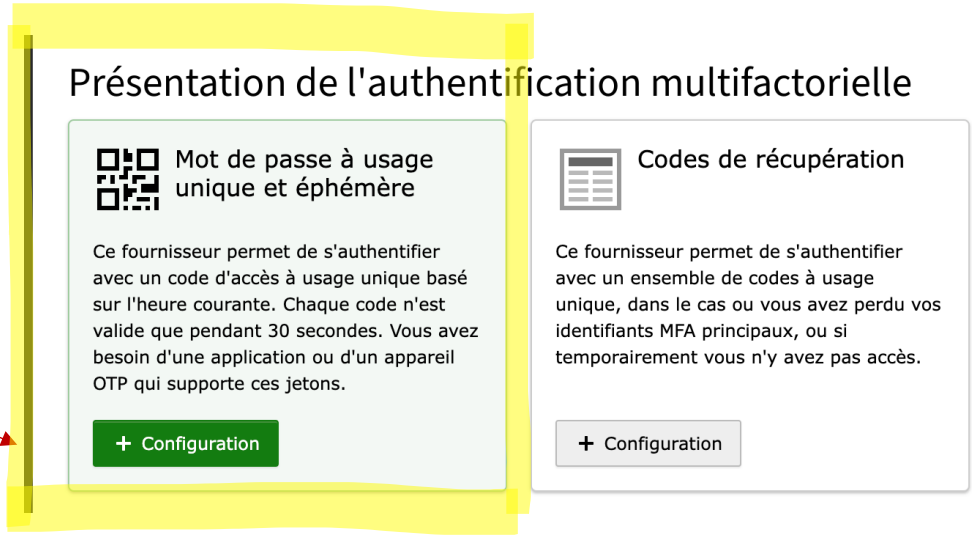


Cliquez sur l'onglet « **Sécurité du compte** ».

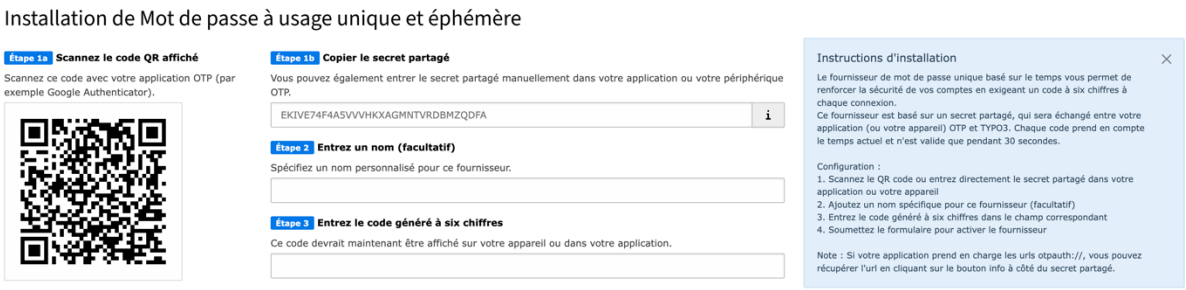
Cliquez sur la case « **Configurer l'authentification multi-facteurs** ».



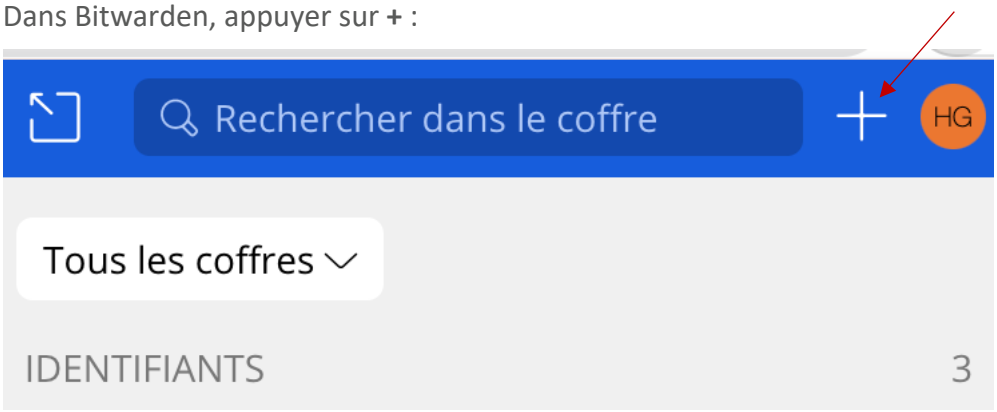
Cliquez sur la case « **Configuration** »



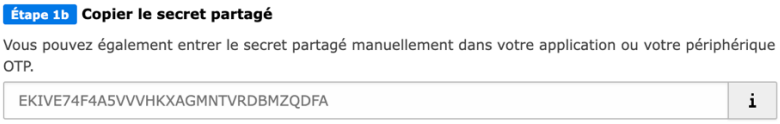
a) En cas d'utilisation de Bitwarden :



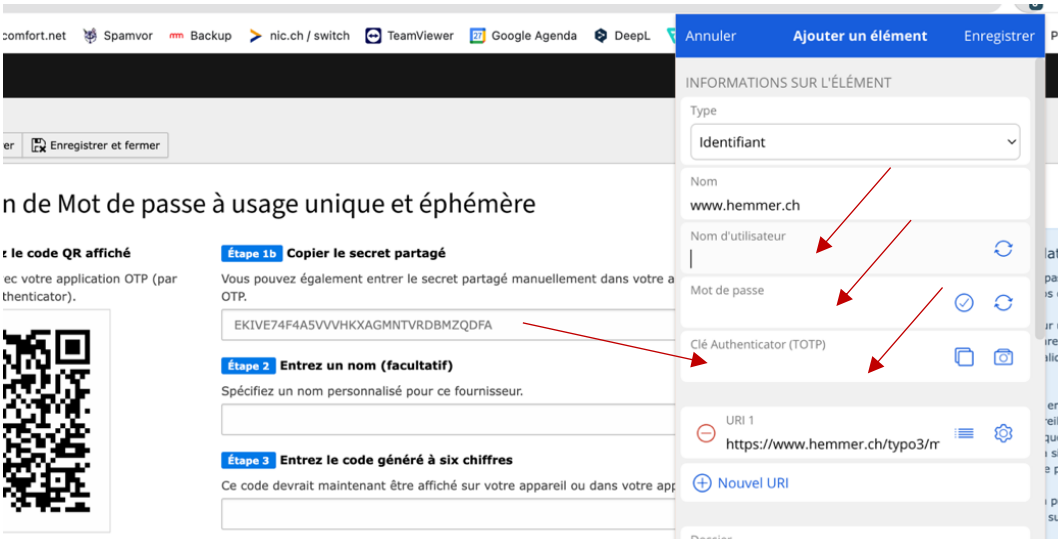
- Dans Bitwarden, appuyer sur **+** :

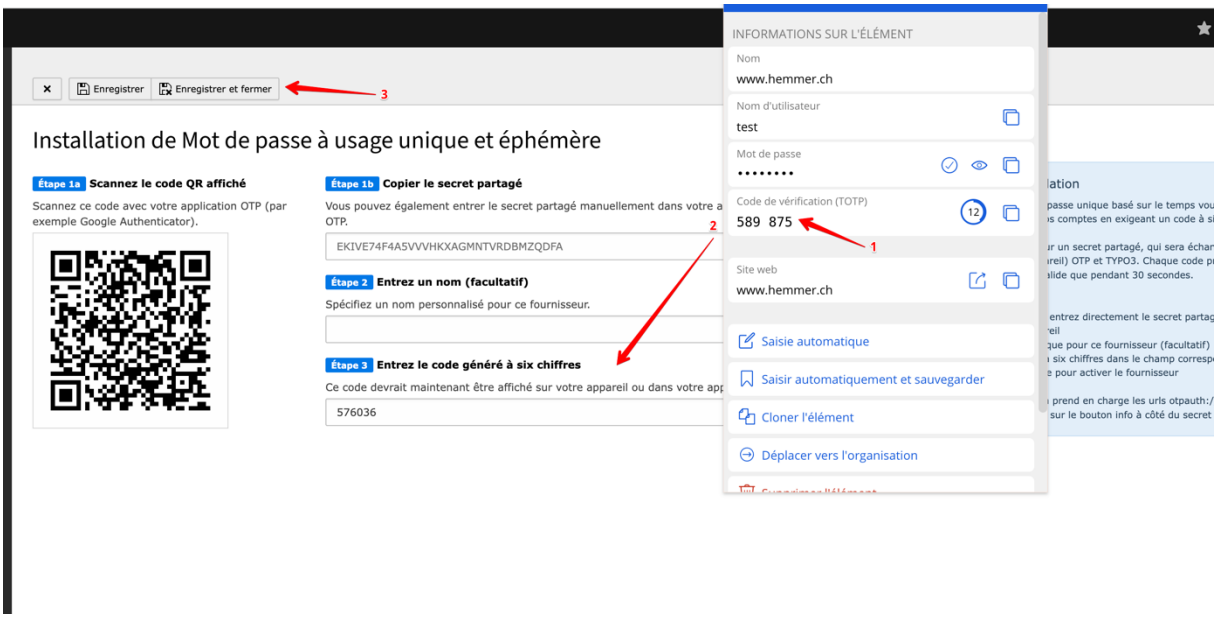


- Remplir les champs suivants : « **nom** » « **nom d'utilisateur** » « **mot de passe** de votre TYPO3 »
- Prendre manuellement la clé secrète et l'insérer dans « **Clé Authenticator (TOTP)** » et « **Enregistrer** » :



- Réouvrir Bitwarden, reprendre le « **Code de vérification (TOTP)** » et l'insérer dans TYPO3 sur « **Etape 3** » et « **Enregistrer et fermer** »





b) En cas d'utilisation de l'application d'authentification :

- Scanner le code QR et reprendre le code affiché dans l'application « **TYPO3 éditeur** »
- Il faut ensuite l'insérer dans l'étape 3 « **Entrer le code généré à six chiffres** » et « Enregistrer et fermer »

La 2FA est maintenant activée pour l'utilisateur.

3. Connexion sur TYPO3

- Entrez les champs **« nom d'utilisateur » « mot de passe »**

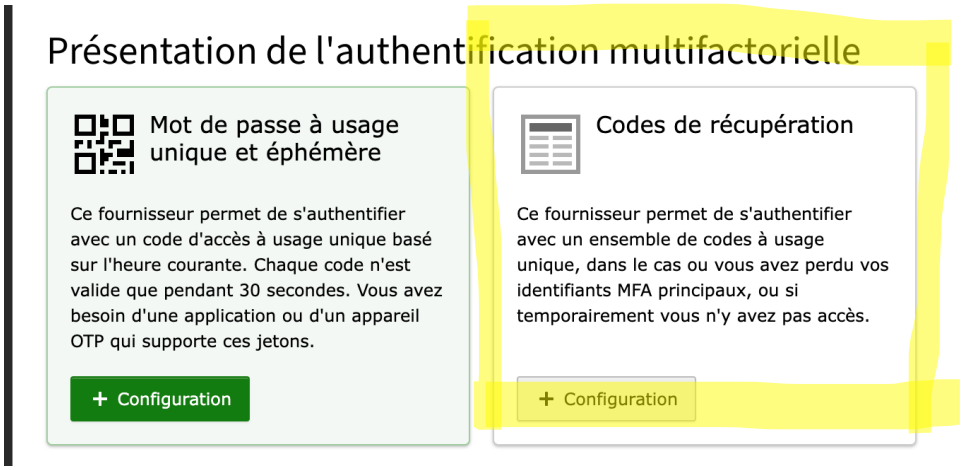
- Saisissez le code généré par l'application d'authentification dans le champ **« Entrer le code à six chiffres »**.
- Cliquez sur le bouton **« Vérifier »**

4. Installation de codes de récupération

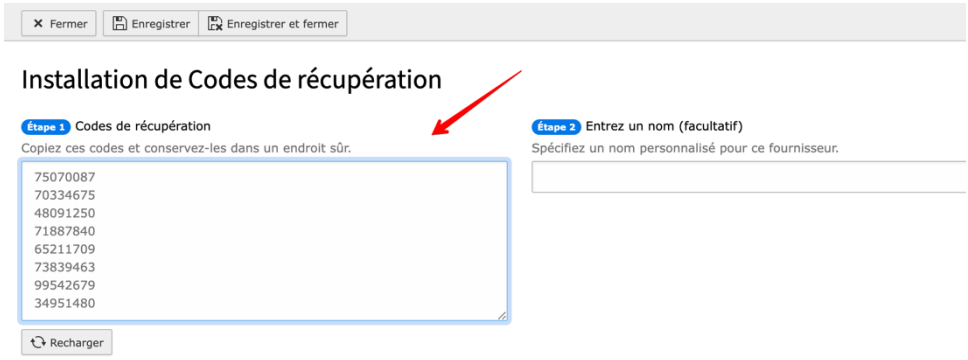
L'installation de codes de récupération permet de récupérer l'accès TYPO3 en cas de perte de l'application permettant la double authentification.

Pour ce faire :

Cliquez sur la 2ème case **« Configuration »** sous l'intitulé « Codes de récupération »



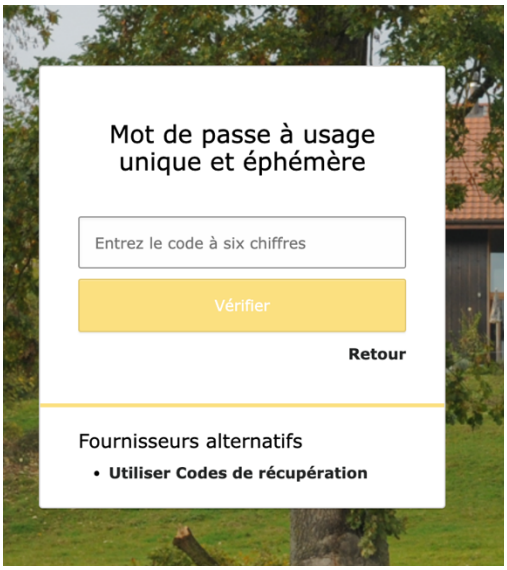
Copiez les codes donnés et conservez-les dans un endroit sûr.



En cas de perte du système de double authentification

Cliquez sur « **Utiliser Codes de récupération** » puis insérez le premier numéro de la liste.

Ce numéro ne peut être utilisé qu'une seule fois.



5. Conseils supplémentaires

Il est recommandé de sauvegarder votre clé secrète en lieu sûr. En cas de perte de votre appareil mobile, vous pourrez utiliser la clé secrète pour vous connecter à votre compte TYPO3.

Vous pouvez désactiver la 2FA pour un utilisateur à tout moment en suivant les étapes ci-dessus et en décochant la case **Activer l'authentification à deux facteurs**.

Pour plus d'informations sur la configuration de la 2FA dans TYPO3, veuillez consulter la documentation officielle : https://docs.typo3.org/m/typo3/reference-coreapi/main/en-us/ApiOverview/Authentication/MultiFactorAuthentication.html

6. Conclusion

La configuration de la 2FA sur TYPO3 est un moyen simple et efficace d'améliorer la sécurité de vos comptes. En suivant les étapes décrites dans ce guide, vous pouvez protéger vos comptes contre les accès non autorisés.