

# 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

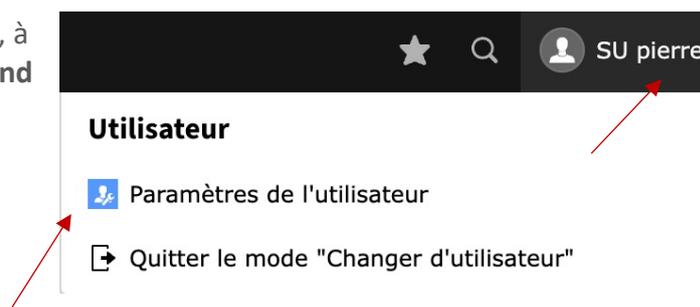
Avant de configurer la 2FA sur TYPO3, vous aurez besoin de :

- 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** ».

## Paramètres Utilisateur

Données personnelles | **Sécurité du compte** | Apparence du backend | Édition et fonctions avancées | Réinitialiser la configuration | Gestion des actualités

**Mot de passe actuel**

**Nouveau mot de passe**

Le mot de passe doit respecter les exigences suivantes :

- Longueur minimale : 8 caractères
- Au moins un caractère majuscule
- Au moins un caractère minuscule
- Au moins un chiffre
- Au moins un caractère spécial

**Nouveau mot de passe (répétition)**

**Authentification multi-facteurs**

Utilisez l'authentification multi-facteurs pour sécuriser votre compte en fournissant une autre méthode en plus de votre mot de passe.

[Configurer l'authentification multi-facteurs](#)

Cliquez sur la case  
« **Configuration** »

## Présentation de l'authentification multifactorielle



### Mot de passe à usage unique et éphémère

Ce fournisseur permet de s'authentifier avec un code d'accès à usage unique basé sur l'heure courante. Chaque code n'est valide que pendant 30 secondes. Vous avez besoin d'une application ou d'un appareil OTP qui supporte ces jetons.

[+ Configuration](#)



### Codes de récupération

Ce fournisseur permet de s'authentifier avec un ensemble de codes à usage unique, dans le cas où vous avez perdu vos identifiants MFA principaux, ou si temporairement vous n'y avez pas accès.

[+ Configuration](#)

a) En cas d'utilisation de Bitwarden :

Installation de Mot de passe à usage unique et éphémère

**Étape 1a** Scannez le code QR affiché

Scannez ce code avec votre application OTP (par exemple Google Authenticator).



**Étape 1b** Copier le secret partagé

Vous pouvez également entrer le secret partagé manuellement dans votre application ou votre périphérique OTP.

EKIVE74F4A5VVVHKXAGMNTVRDBMZQDFA

**Étape 2** Entrez un nom (facultatif)

Spécifiez un nom personnalisé pour ce fournisseur.

**Étape 3** Entrez le code généré à six chiffres

Ce code devrait maintenant être affiché sur votre appareil ou dans votre application.

**Instructions d'installation**

Le fournisseur de mot de passe unique basé sur le temps vous permet de renforcer la sécurité de vos comptes en exigeant un code à six chiffres à chaque connexion.

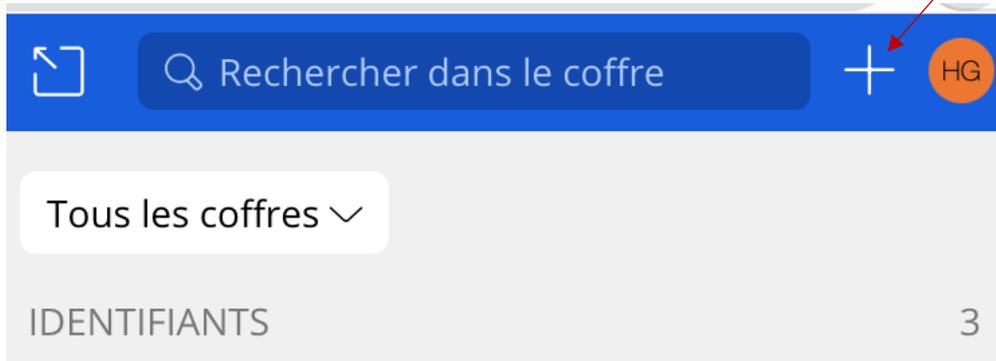
Ce fournisseur est basé sur un secret partagé, qui sera échangé entre votre application (ou votre appareil) OTP et TYPO3. Chaque code prend en compte le temps actuel et n'est valide que pendant 30 secondes.

**Configuration :**

1. Scannez le QR code ou entrez directement le secret partagé dans votre application ou votre appareil
2. Ajoutez un nom spécifique pour ce fournisseur (facultatif)
3. Entrez le code généré à six chiffres dans le champ correspondant
4. Soumettez le formulaire pour activer le fournisseur

**Note :** Si votre application prend en charge les urls otpauth://, vous pouvez récupérer l'uri en cliquant sur le bouton info à côté du secret partagé.

- Dans Bitwarden, appuyer sur + :



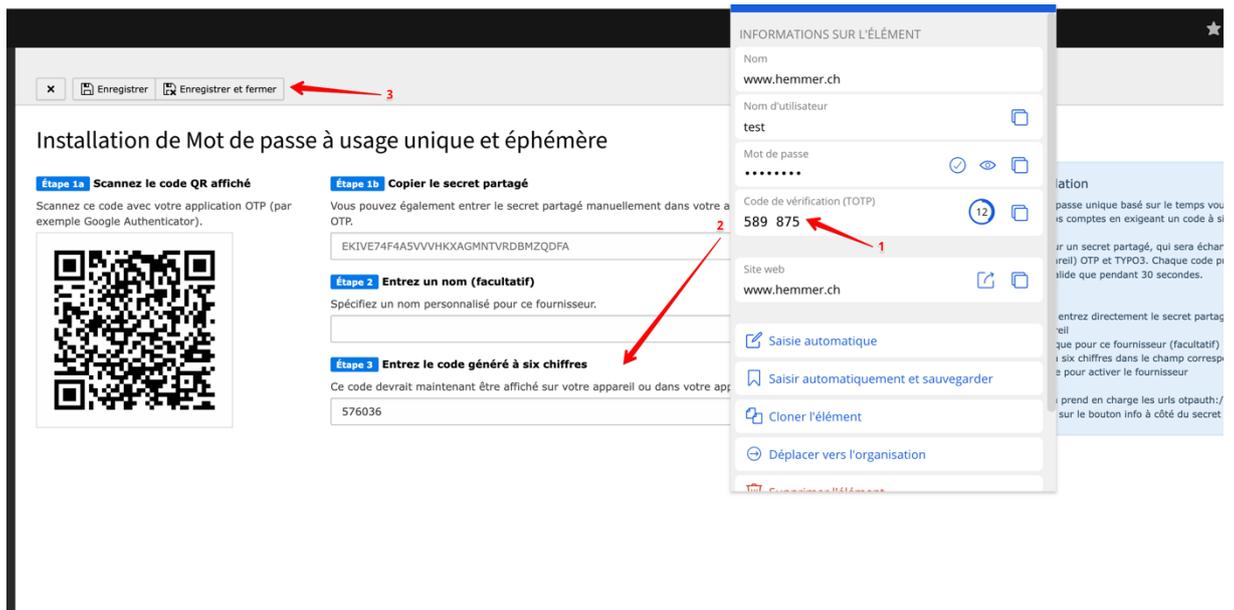
- Remplir les champs suivants : « nom » « nom d'utilisateur » « mot de passe de votre TYPO3 »
- Prendre manuellement la clé secrète et l'insérer dans « Clé Authenticator (TOTP) » et « Enregistrer » :

**Étape 1b** Copier le secret partagé

Vous pouvez également entrer le secret partagé manuellement dans votre application ou votre périphérique OTP.

EKIVE74F4A5VVVHKXAGMNTVRDBMZQDFA

- 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 :

### Installation de Mot de passe à usage unique et éphémère

**Étape 1a Scannez le code QR affiché**  
Scannez ce code avec votre application OTP (par exemple Google Authenticator).



**Étape 1b Copier le secret partagé**  
Vous pouvez également entrer le secret partagé manuellement dans votre application ou votre périphérique OTP.

**Étape 2 Entrez un nom (facultatif)**  
Spécifiez un nom personnalisé pour ce fournisseur.

**Étape 3 Entrez le code généré à six chiffres**  
Ce code devrait maintenant être affiché sur votre appareil ou dans votre application.

**Instructions d'installation**

Le fournisseur de mot de passe unique basé sur le temps vous permet de renforcer la sécurité de vos comptes en exigeant un code à six chiffres à chaque connexion.

Ce fournisseur est basé sur un secret partagé, qui sera échangé entre votre application (ou votre appareil) OTP et TYPO3. Chaque code prend en compte le temps actuel et n'est valide que pendant 30 secondes.

Configuration :

1. Scannez le QR code ou entrez directement le secret partagé dans votre application ou votre appareil
2. Ajoutez un nom spécifique pour ce fournisseur (facultatif)
3. Entrez le code généré à six chiffres dans le champ correspondant
4. Soumettez le formulaire pour activer le fournisseur

Note : Si votre application prend en charge les uris otpauth://, vous pouvez récupérer l'uri en cliquant sur le bouton info à côté du secret partagé.

- Scanner le code QR et reprendre le code affiché dans l'application « **TYPO3 éditeur** »
- Il faut ensuite l'insérer dans l'étape 3 « **Entrez 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** »



mm

Nom d'utilisateur

Mot de passe

Connexion

Mot de passe oublié ?

En savoir plus sur TYPO3

TYPO3

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



Mot de passe à usage unique et éphémère

Entrez le code à six chiffres

Vérifier

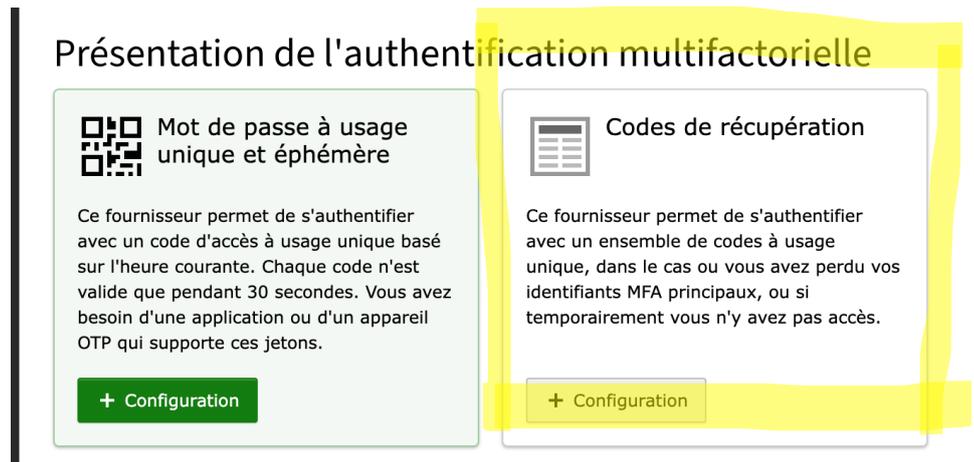
Retour

## 4. Installation de codes de récupération

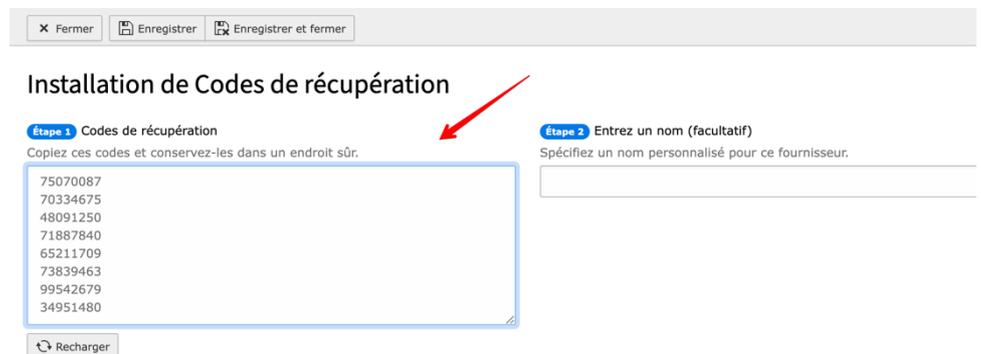
L'installation de codes de récupération permet de récupérer l'accès TYPO3 en cas de perte de l'application permettant la double authentification.

Pour ce faire :

Cliquez sur la 2<sup>ème</sup> 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.