

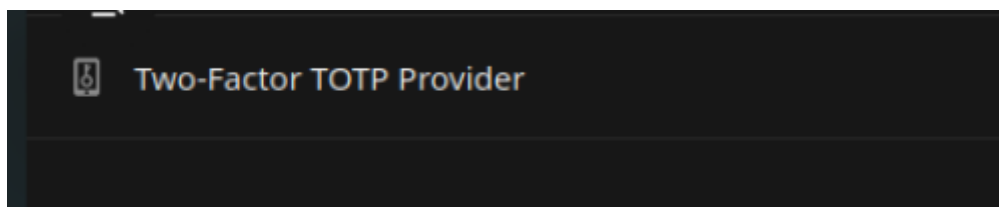
Configuration de la 2FA (authentification a deux facteurs)

Installation de l'application

Nextcloud n'a pas d'application de base permettant de générer l'authentification à doubles facteurs.

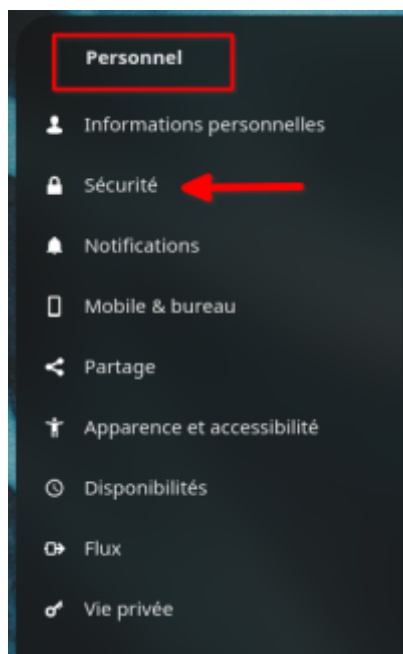
Il faut installé une application **Nextcloud**, l'application **TOTP** est très **utilisé**, **tester** sur plusieurs applications de **MFA** et a un **Github** actif.

Dans le menu **+applications** rechercher **TOTP** puis **installer et activer**.



Configuration utilisateur

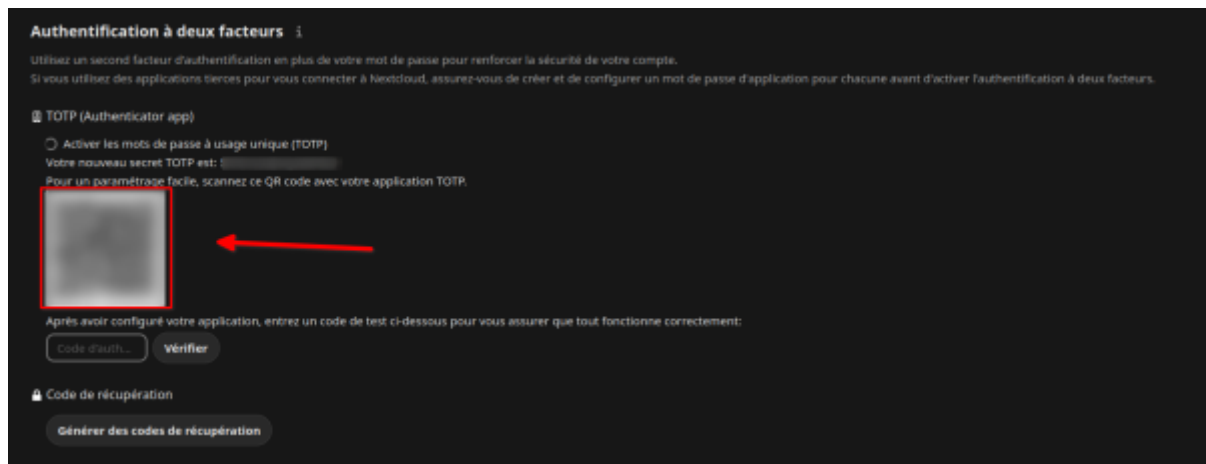
Pour configurer le **2FA**, se rendre dans les paramètres **personnel** dans l'onglet **sécurité**.



La parti authentification à deux facteurs devrait apparaître.

Cocher **Activer les mots de passe à usage unique (TOTP)**

Un QR code apparaîtra, le scanner sur une application de MFA(Aegis, Authy, Google authenticator ou autres).



Une fois scanner et rajouter, taper le code de vérification de l'application **MFA** juste en dessous du QR code puis cliquer sur **Vérifier**.

A la prochaine connexion voici la page de TOTP.

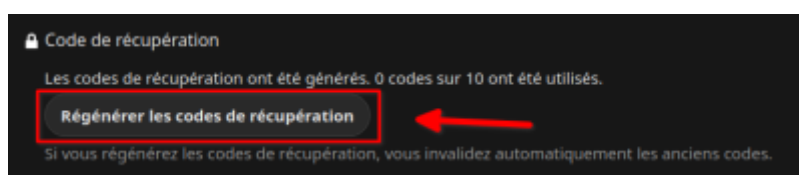


La double authentification est désormais **activer**.

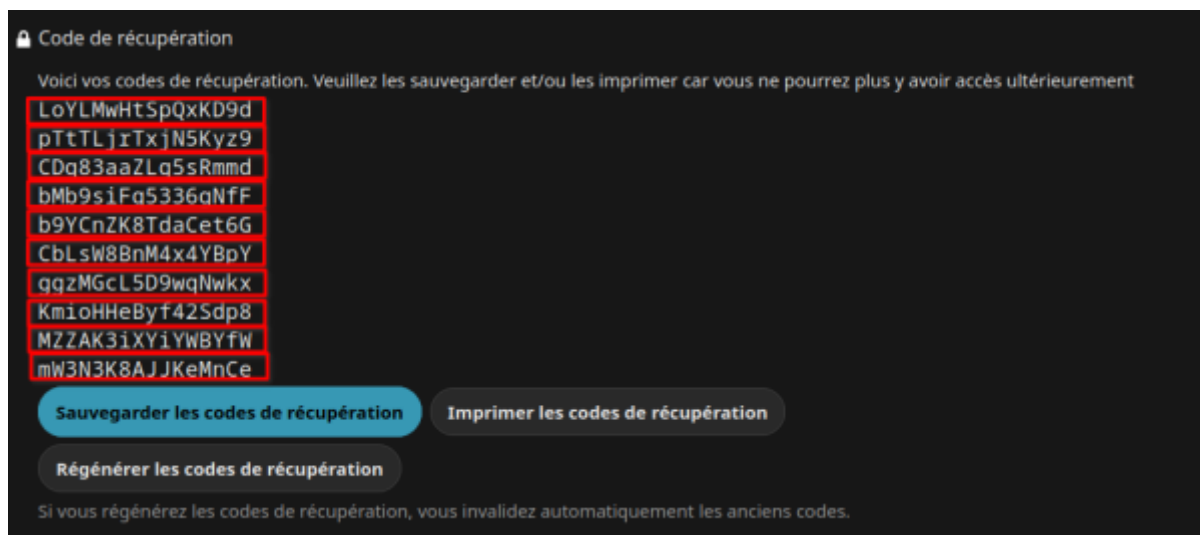
Codes de récupération

Si l'application **MFA** est indisponible, un contournement existe il s'agit des codes de récupération. Ces codes sont à **usages uniques** et permettent de contourner la **2FA** si besoin.

Toujours dans l'onglet **sécurité personnel**, cliqué sur **Générer les codes de récupérations**



10 codes à usage unique seront affichés avec possibilité de les sauvegarder dans un fichier .TXT ou les imprimer.

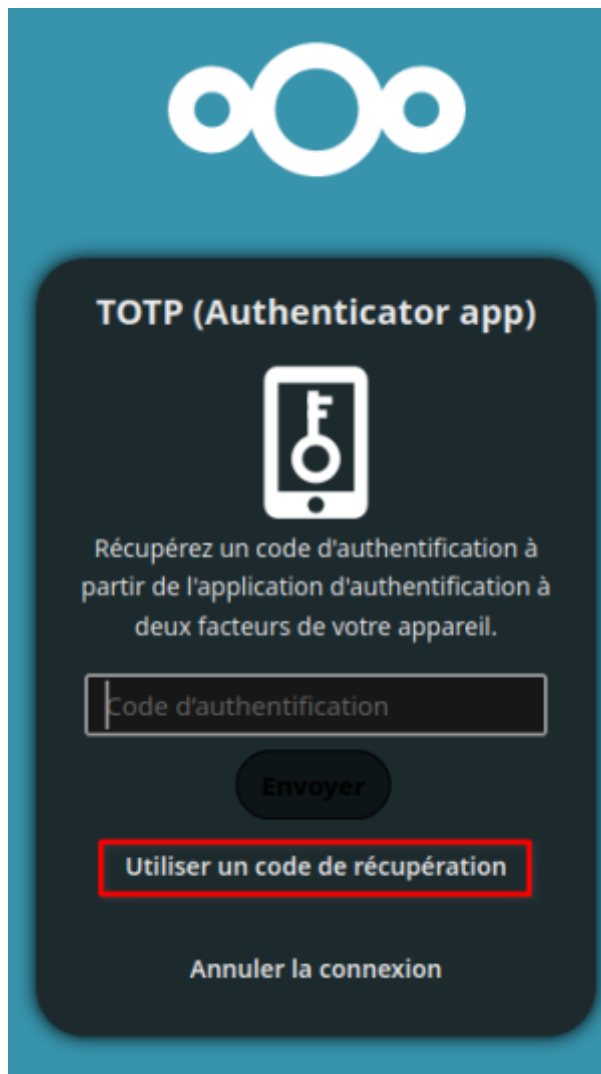


Le bouton **Régénérer tous les codes de récupération** en générera 10 autres et **invalideront** les précédents.



Les codes disparaîtront de la page dès son **rafraîchissement**.

Les codes sont utilisables dès la demande de code MFA.



Imposer la double authentification



Avant d'imposer la double authentification, **vérifier** qu'au moins un administrateur est **TOTP** configuré. Sinon après la manipulation **l'authentification par le web ne sera plus possible.**

Dans les paramètres d'administration du serveur, dans l'onglet Sécurité, cocher le bouton **“Imposer l'authentification à deux facteurs”**

Authentification à deux facteurs

L'authentification à deux facteurs peut être forcée pour tous les utilisateurs et des groupes spécifiques. S'ils n'ont pas un fournisseur de deux facteurs configuré, ils ne seront pas capables de s'authentifier sur le système.

☒ Imposer l'authentification à deux facteurs

Limiter aux groupes

L'authentification à deux facteurs peut être imposée à certains groupes seulement.

L'authentification à deux facteurs est forcée pour tous les membres des groupes suivants :

Groupes forcés : admin X

L'authentification à deux facteurs n'est pas forcée pour les membres des groupes suivants :

Groupes exclus :

Lorsque des groupes sont forcés/exclus, la logique suivante est utilisée pour déterminer si l'authentification à double facteur (ADF) est imposée à un utilisateur. Si aucun groupe n'est forcé, l'authentification à double facteur est activée pour tous sauf pour les membres des groupes exclus. Si des groupes sont forcés, l'authentification à double facteur est exigée pour tous les membres de ces groupes. Si un utilisateur est à la fois dans un groupe forcé et exclu, c'est le groupe forcé qui prime et l'authentification double facteur est imposée.

Enregistrer les modifications

Puis choisir les groupes **forcés** à l'utiliser puis les **exclus** qui ne seront pas imposés.

Désactiver la 2FA par CLI

En cas de besoin voici comment désactiver la **2FA** en CLI.

```
sudo -u#33 php occ config:system:set twofactor_enforced disable
```

From:
<https://www.hugo-mattaliano.fr/wiki/> - Gogo Wiki

Permanent link:
https://www.hugo-mattaliano.fr/wiki/doku.php?id=wiki:nextcloud:nextcloud_2fa&rev=1720475358

Last update: 2024/08/21 14:20

