Table des matières

Public : utilisateurs du serveur de messagerie interne, domaine `@cnam.fr`

Configurer l'authentification à deux facteurs sur webmail.cnam.fr

← cnam.fr

Les utilisateurs de la messagerie du domaine `cnam.fr` peuvent utiliser l'application https://webmail.cnam.fr pour accéder à leurs courriers.

Les utilisateurs sont vivement invités à renforcer la sécurité en activant l'authentification à deux facteurs. En l'occurrence, il s'agit d'un second facteur dit TOTP (pour *Time based One Time Password*).

Authentification

On peut authentifier un individu avec :

- ce qu'il sait (un mot de passe)
- ce qu'il a (un jeton matériel ou un téléphone)
- ce qu'il est (son empreinte rétinienne ou digitale)

Le mot de passe n'est pas un moyen sûr, il se divulgue, se copie…

Pour palier à cette faiblesse majeure des mots de passe, l'authentification à plusieurs facteurs se généralise.

Pour deux facteurs, les anglo-saxons parlent de 2FA pour *2 factors authentication* ou de MFA pour *multi factors authentication*.

TOTP

Le serveur et l'utilisateur partagent un secret (une chaîne de caractères aléatoires). L'échange initial (et unique) se fait par QR code pour faciliter le transfert. Ce secret et l'heure permettent de générer un second secret qui est haché pour produire une suite de six chiffres. Ces six chiffres sont valables trente secondes.

Le secret peut être stocké dans un jeton matériel comme les Yubikey ou à l'aide d'une application *ad hoc* sur un *smartphone* (voir par exemple FreeOTP, disponible sur Android et iOS ou Google Authenticator, disponible sur Android et iOS) ou avec KeePassXC sur son poste de travail.

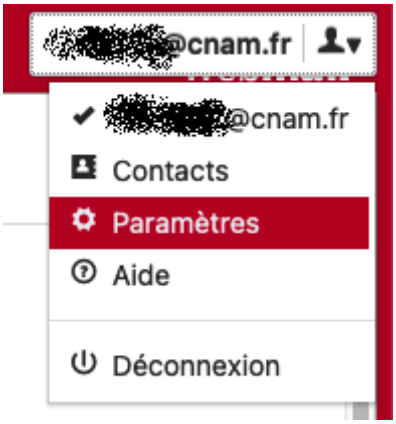
Attention : le QR code contient le secret partagé, il doit rester secret !

En plus du secret partagé, des codes de récupération à usage unique sont aussi fournis en cas de perte de l'équipement contenant le secret partagé.

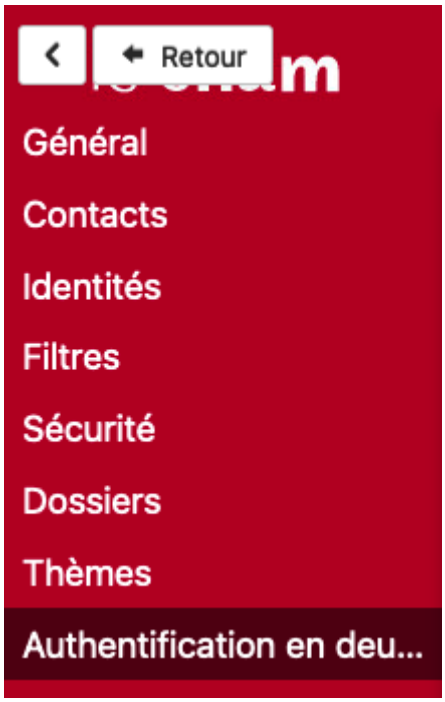
Attention : ces codes de récupération doivent eux aussi rester secrets !

Paramétrage du webmail

Ouvrir le menu en haut à droite pour cliquer sur « Paramètres » :



Suivre « Authentification à deux facteurs » :

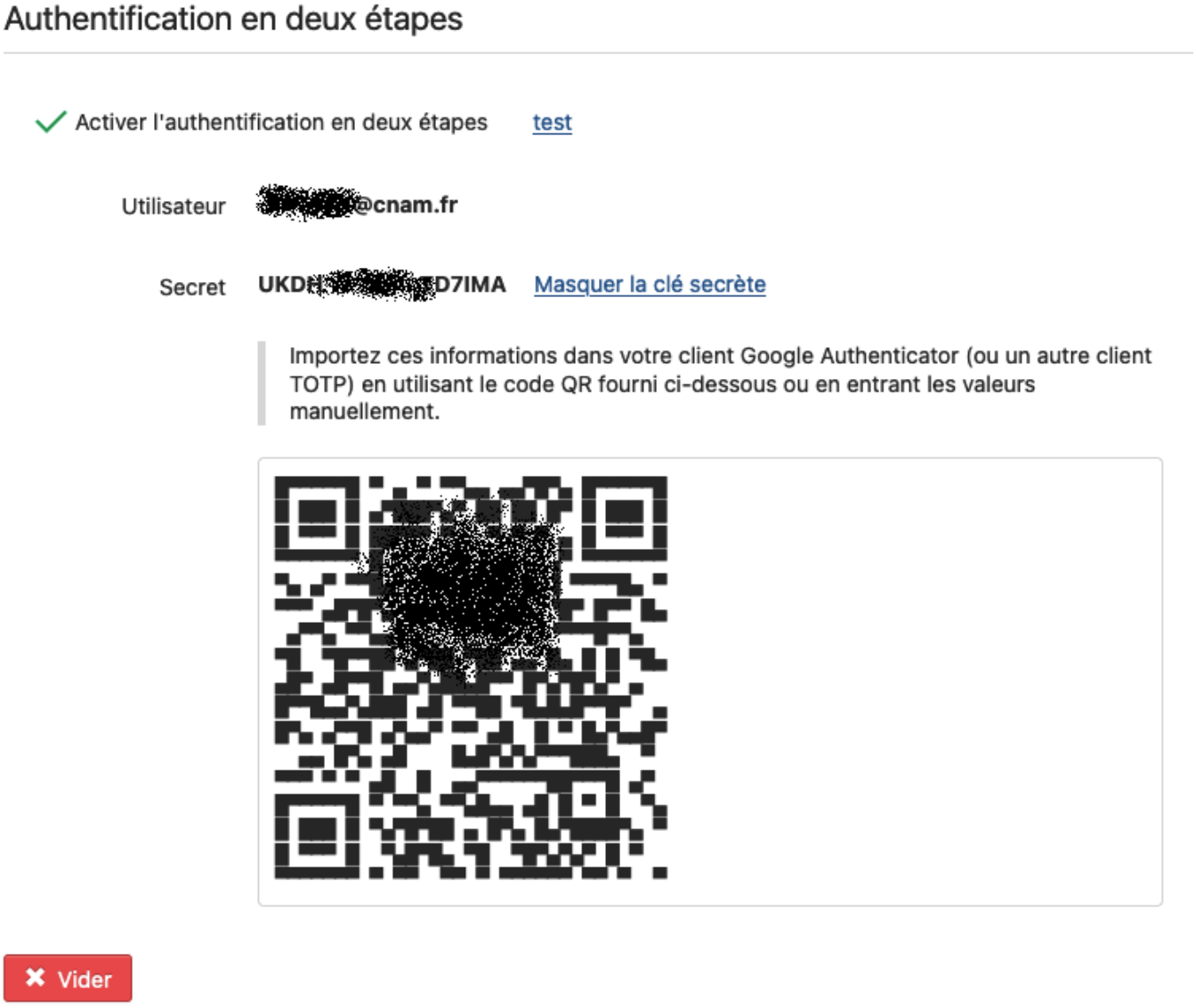


La fenêtre suivante s'affiche :

Consigner très soigneusement les codes de récupération, par exemple dans un gestionnaire de mots de passe comme KeepassXC et partager le secret avec l'application TOTP retenue.

Avant l'activation, une phase de test est indispensable.

Si le test est positif, c'est en place :



Lors de prochaine authentification, il faudrait saisir, outre le *login* et le mot de passe traditionnel, le code sur six chiffres fourni par l'application.

Nota Bene : le bouton « Vider » permet de supprimer cette configuration.

← cnam.fr