Authentification à deux facteurs sur la console KMC

L'authentification à deux facteurs (2FA) ajoute une couche de sécurité essentielle à votre compte. En plus de votre mot de passe, vous devrez saisir un **code temporaire** généré par une application d'authentification (comme Google Authenticator, Microsoft Authenticator ou Authy). Ce code change automatiquement toutes les 30 secondes et ne dépend pas du réseau, ce qui le rend plus fiable et plus sûr que les codes envoyés par email ou SMS.

Lors de l'activation de l'authentification à deux facteurs, vous recevez également des **codes de secours**. Ces codes sont à conserver en lieu sûr. Ils vous permettent de vous connecter à votre compte si vous perdez l'accès à votre téléphone ou à votre application d'authentification. **Chaque code ne peut être utilisé qu'une seule fois.**

En activant l'authentification à deux facteurs, vous protégez efficacement votre compte contre le vol de mot de passe, le phishing et de nombreuses formes d'usurpation d'identité, tout en conservant un accès fiable en cas d'imprévu.

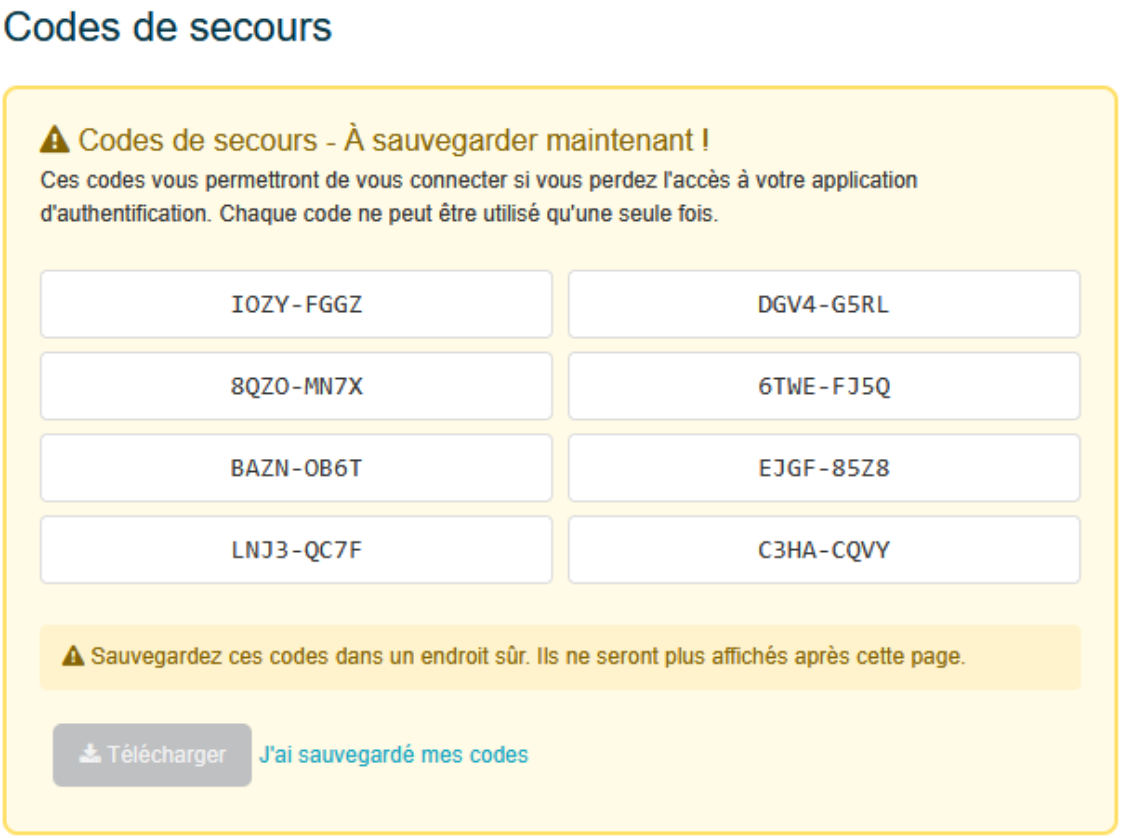
Activation de l'authentification à deux facteurs

Sur la page des utilisateurs dans la console KMC, les utilisateurs avec le rôle « Méta Administrateur » peuvent rendre l'authentification à deux facteurs obligatoire pour les administrateurs (mais pas les méta administrateurs) :

Il est également possible d'activer la 2FA pour un seul utilisateur. L'utilisateur peut l'activer pour lui-même, et les méta administrateurs peuvent l'activer pour n'importe quel autre utilisateur.

Lors de la prochaine connexion à la console KMC, l'utilisateur devra configurer l'authentification à deux facteurs. Il est possible pour l'utilisateur d'annuler la configuration, sauf si l'utilisateur est un administrateur et que la 2FA est obligatoire pour tous les administrateurs.

Une fois l'authentification à deux facteurs configurée, l'utilisateur doit sauvegarder ses codes de secours dans un endroit sûr (par exemple les imprimer et les mettre dans un emplacement sécurisé).



Si l'utilisateur n'a plus accès à l'application d'authentification, il peut utiliser un code de secours afin de pouvoir se connecter.

Le but de l'authentification à deux facteurs étant d'être résistant au piratage de mot de passe, il faut faire attention à ne pas les stocker au même endroit que le mot de passe utilisé pour la console KMC.

Lors de la prochaine connexion, après avoir entré son mot de passe, il sera demandé à l'utilisateur d'entrer le code de son application d'authentification (ou un code de secours) :

Il est possible, si l'utilisateur le souhaite, de ne plus demander de code 2FA (le mot de passe sera toujours demandé) pendant 30 jours sur le navigateur utilisé pour la connexion.

Gestion de l'authentification à deux facteurs

Une fois que l'utilisateur a configuré l'authentification à deux facteurs, il peut la gérer sur son espace utilisateur :

L'utilisateur peut :

- Regénérer les codes de secours, si les codes ont été piratés ou perdus ;
- Réinitialiser l'authentification à deux facteurs (les codes de secours actuels seront supprimés et l'utilisateur devra refaire la configuration), si l'application d'authentification a été piratée ou perdue (par exemple téléphone volé);
- Désactiver l'authentification à deux facteurs (sauf si l'utilisateur est un administrateur et que la 2FA est obligatoire pour les administrateurs).

Un méta administrateur peut également réinitialiser ou désactiver le 2FA d'un utilisateur, mais pas regénérer ses codes de secours.

Blocage de compte

Pour éviter le piratage par « force brute » où le pirate teste continuellement des codes au hasard jusqu'à en trouver un qui fonctionne, un nombre limité de tentatives est autorisé pour chaque connexion :

Le compte de l'utilisateur sera verrouillé temporairement au bout d'un certain nombre de tentatives :

L'utilisateur commence avec 5 tentatives, puis le compte est verrouillé pendant 1mn, 5mn, 15mn, puis 1h entre chaque tentative.

Un méta administrateur peut vérifier l'état de verrouillage du compte sur la console KMC, et peut débloquer le compte si besoin. Attention : si le compte est verrouillé et qu'il ne s'agit pas d'une erreur de l'utilisateur, cela peut signifier que le mot de passe de l'utilisateur a été piraté.

Authentification à deux facteurs (2FA)

État 2FA: Activé et configuré

Compte verrouillé: Trop de tentatives 2FA échouées. Déverrouillage automatique dans 230 seconde(s).

Débloquer le compte | Réinitialiser 2FA | Désactiver 2FA