

Authentification par app mobile | Guide pratique pour smartphones sous Android

Certains domaines de l'Administration cantonale nécessitent une authentification forte - ou multifacteur (MFA) - pour y accéder. Il s'agit concrètement d'une vérification en plusieurs étapes : en plus du mot de passe, nous devons introduire un code que nous recevons sur notre smartphone - lui-même protégé par nos propres moyens d'identification.

Dorénavant, ce code ne nous parviendra plus par SMS mais via une application à installer préalablement sur notre téléphone mobile.

Pour passer du SMS à l'application, il nous faut reconfigurer notre Profil IAM selon la procédure décrite ci-dessous.

Configuration de l'authentification forte via l'application Google Authenticator

1. Ouvrez votre smartphone, allez dans le centre de téléchargement d'applications [Google Play Store](#).
2. Recherchez et installez l'app **Google Authenticator** de Google à l'aide de ce code QR :

Vous rencontrez des problèmes avec le code QR ?
À l'aide de votre appareil mobile, accédez à [Google Play Store](#) pour obtenir l'application mobile **Google Authenticator**.

Notez que cette application de Google est **gratuite** et se présente avec cette icône :



3. Depuis votre ordinateur, ouvrez votre navigateur internet et allez sur le Portail IAM. Au besoin, connectez-vous avec votre nom d'utilisateur et votre mot de passe.
4. Une fois sur la page d'accueil du Portail IAM, sur la partie droite de la fenêtre, cliquez sur le menu « **Mon Profil** ».
5. Cliquez sur « **Authentification forte** ».
6. Dans la rubrique Gestion de l'app mobile, cliquez sur le bouton « **CONFIGURER** ».
7. Sur votre smartphone : ouvrez l'application d'authentification mobile **Google Authenticator**, puis scannez le QR code qui générera un code à six chiffres sur votre app mobile, à reporter directement sur votre Profil IAM.
8. Enregistrez, la configuration est désormais terminée !

Remarque

Il existe plusieurs applications mobiles capables de répondre à cette problématique, telles Microsoft Authenticator, Proton Authenticator ou TrustID Authenticator. Cependant, les équipes de support de la Police Cantonale Vaudoise recommandent l'utilisation de Google Authenticator, afin de standardiser au maximum ce processus, ainsi que faciliter toute assistance.

Remarque

Pour des raisons pratiques, vous pouvez éviter de devoir récupérer systématiquement un code sur l'application mobile Authenticator à chaque nouvelle connexion en cochant simplement la case présente en dessous du champ d'insertion du code, comme l'indique l'image suivante :

☐ Je souhaite sauter cette étape pour mes futures connexions à partir de cet appareil.

Cette astuce est valable pendant une durée de 3 mois, à condition que vous utilisiez le même ordinateur, le même navigateur sans le mode privé et que le cache internet n'ait pas été supprimé.

Lien intéressant

N'hésitez pas à consulter la [page d'aide dédiée](#), ainsi que la liste des questions les plus fréquemment posées.

Aide et conseil

En cas de perte, casse ou simplement un remplacement de votre téléphone, veuillez contacter le Helpdesk pour réinitialiser la configuration de l'authentification forte de votre profil IAM.

Le Helpdesk informatique se tient également à votre disposition pour toute demande d'assistance technique ou toute question concernant les fonctionnalités de votre poste de travail.

Helpdesk Informatique – helpdesk@vd.ch – tél. : 021 316 26 60

Département de l'agriculture, de la durabilité, du climat et du numérique
Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
vd.ch/dgnsi

VD.CH

Direction générale certifiée ISO 9001, 27001 et labellisée Numérique Responsable niveau 2