

Guide de l'authentification à deux facteurs (2FA)

Activation, connexion et gestion des méthodes de validation

Document destiné aux utilisateurs finaux

Objectif du document

Ce guide explique simplement comment fonctionne l'authentification à deux facteurs dans l'application : première connexion, réception des codes, choix de la méthode préférée et modification des coordonnées de validation.

1. Pourquoi activer le 2FA ?

L'authentification à deux facteurs, aussi appelée 2FA, renforce la sécurité de votre compte dans l'application.

En plus de votre mot de passe habituel, un code de validation peut être demandé lors de la connexion. Ce code est envoyé vers l'adresse e-mail ou le numéro de téléphone associé à votre compte.

Cette vérification supplémentaire permet de mieux protéger l'accès à vos données, même si votre mot de passe venait à être connu par une personne non autorisée.

À retenir

Le 2FA ajoute une étape de sécurité lors de la connexion, mais son fonctionnement reste simple : vous vous connectez, vous recevez un code, puis vous validez l'accès.

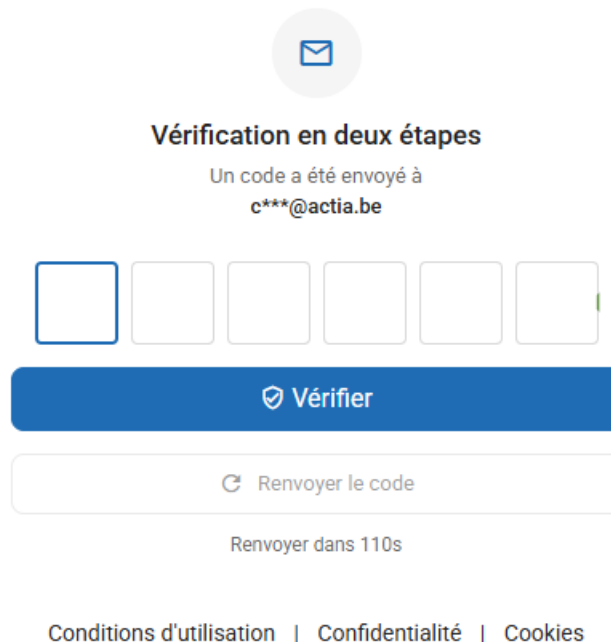
2. Activation du 2FA

L'activation du 2FA est effectuée soit par un administrateur de votre organisation, soit par vous-même si la configuration de l'organisation le permet.

3. Première connexion après activation

Lors de votre première connexion après activation du 2FA :

1. Connectez-vous avec votre identifiant et votre mot de passe habituels.
2. Un code de validation est envoyé par e-mail, méthode utilisée par défaut lors de la première connexion.
3. Saisissez le code reçu dans l'écran prévu à cet effet.
4. La connexion est alors validée.



The image shows a two-step verification interface. At the top, there is a circular icon with an envelope. Below it, the text 'Vérification en deux étapes' is displayed. Underneath, it says 'Un code a été envoyé à' followed by the email address 'c***@actia.be'. There are six input boxes for the verification code. Below the input boxes is a blue button with a shield icon and the text 'Vérifier'. Below that is a light gray button with a circular arrow icon and the text 'Renvoyer le code'. At the bottom, it says 'Renvoyer dans 110s'. At the very bottom, there are links for 'Conditions d'utilisation', 'Confidentialité', and 'Cookies'.

Vérification en deux étapes

Un code a été envoyé à
c***@actia.be

Vérifier

Renvoyer le code

Renvoyer dans 110s

[Conditions d'utilisation](#) | [Confidentialité](#) | [Cookies](#)

Exemple d'écran de validation du code 2FA.

4. Connexions suivantes

Après une authentification réussie, l'application peut mémoriser la validation pendant 10 jours.

À l'issue de cette période, un nouveau code de validation pourra être demandé. Si plusieurs méthodes sont configurées, la méthode préférée sera sélectionnée par défaut, mais une autre méthode active pourra être utilisée si nécessaire.

5. Gérer vos coordonnées de validation

Les coordonnées utilisées pour recevoir les codes peuvent être consultées et mises à jour depuis les paramètres de l'utilisateur.

Ces informations sont disponibles dans l'écran Paramètres Généraux.

Gérer votre compte

- Paramètres généraux
- Sécurité
- Paramètres d'affichage

Paramètres généraux

Mon profil

Nom	2fa	Prénom	test
Langue	Français	Page d'accueil	Suivi d'assets

Ces champs sont protégés par vérification en deux étapes et se modifient séparément.

E-mail *

Téléphone

Exemple d'accès aux informations du profil utilisateur.

6. Choisir la méthode de validation préférée

La méthode utilisée par défaut se configure depuis l'écran Sécurité des paramètres utilisateur.

Selon les informations renseignées sur le compte, plusieurs méthodes peuvent être disponibles, par exemple l'e-mail ou le téléphone.

Gérer votre compte

- Paramètres généraux
- Sécurité**
- Paramètres d'affichage

Sécurité

Mot de passe

Règles pour le mot de passe

- ☐ Minimum 8 caractères
- ☐ Au moins une majuscule
- ☐ Au moins un caractère spécial
- ☐ Au moins un chiffre
- ☐ Ne peut pas être identique à un mot de passe précédent

Mot de passe actuel *

Nouveau mot de passe *

Confirmation *

Modifier le mot de passe

Double authentification

Sécurisez votre compte en exigeant un code en plus de votre mot de passe lors de la connexion. Vous pouvez activer ou désactiver les méthodes à tout moment.

SMS
+32495557570 ☆ Définir favori ☐

E-mail
frederic.ludwig@perso.be ★ Favori ☒

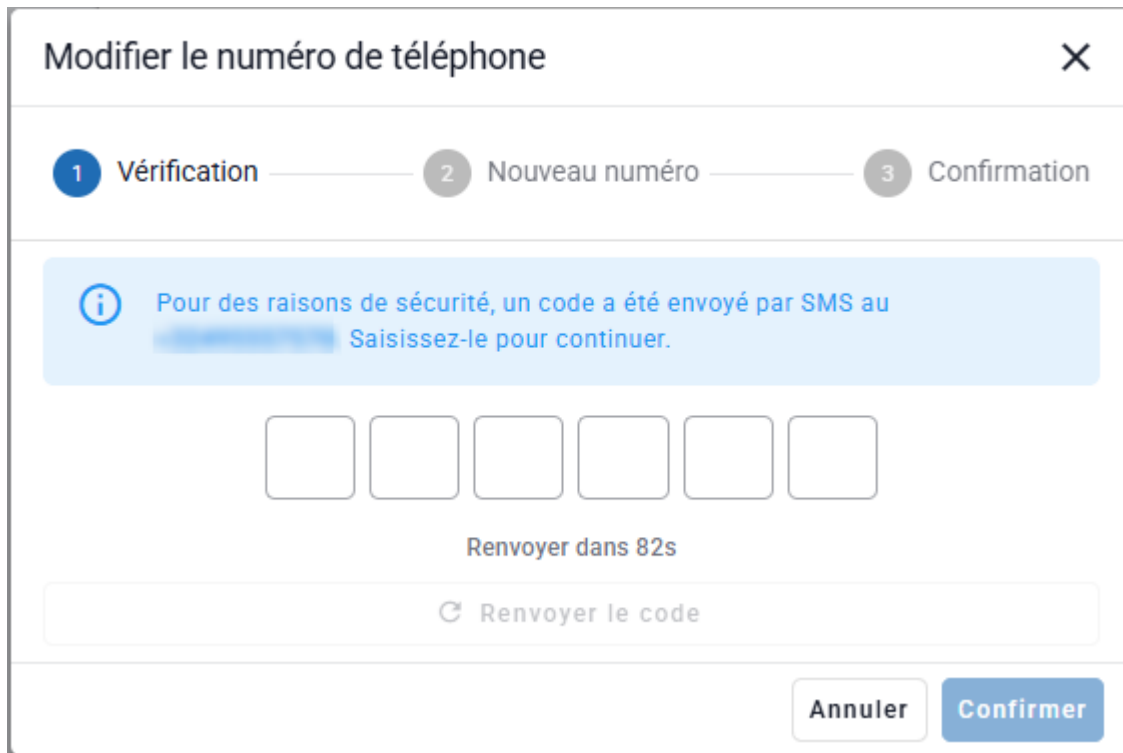
★ La méthode favorite est utilisée par défaut lors de la connexion.

Exemple d'écran de configuration des méthodes de sécurité.

7. Modifier une adresse e-mail ou un numéro de téléphone

Pour protéger votre compte, la modification d'une adresse e-mail ou d'un numéro de téléphone doit être confirmée.

Lorsqu'une méthode de validation existe déjà, un code sera envoyé vers l'ancienne méthode. Une fois la nouvelle valeur renseignée, un code est envoyé vers cette nouvelle adresse ou ce nouveau numéro afin de confirmer la modification.



Exemple de modification d'une coordonnée de validation.

8. Ajouter ou désactiver une méthode

Pour activer une méthode d'authentification, commencez par renseigner les informations nécessaires dans votre profil utilisateur (par exemple, un numéro de téléphone ou une adresse e-mail). Une fois ces informations enregistrées, activez l'**interrupteur à bascule** (switch) correspondant à la méthode souhaitée, puis saisissez le code de validation reçu afin de confirmer l'activation.

Pour désactiver une méthode d'authentification, il suffit de désactiver l'**interrupteur à bascule** situé en regard de la méthode concernée. La méthode ne sera alors plus disponible pour la double authentification.

Bon à savoir

Au moins une méthode d'authentification doit rester active pour garantir la sécurité de votre compte.

9. Résumé pratique

Situation	Ce qu'il faut faire
Première connexion après activation	Se connecter normalement, puis saisir le code reçu par e-mail ou téléphone.
Code demandé après quelques jours	Saisir le code reçu sur la méthode de validation préférée.
Numéro ou e-mail à modifier	Mettre à jour la donnée dans le profil, puis confirmer la modification avec le code reçu.
Méthode préférée à changer	Aller dans l'écran Sécurité et sélectionner la méthode souhaitée.
Méthode à supprimer	Cliquer pour désactiver l'interrupteur à bascule.
Besoin d'aide ? En cas de difficulté lors de la connexion, de la réception du code ou de la modification d'une méthode de validation, contactez votre administrateur ou le support.	