

Utiliser la double authentification

LANGUE Français

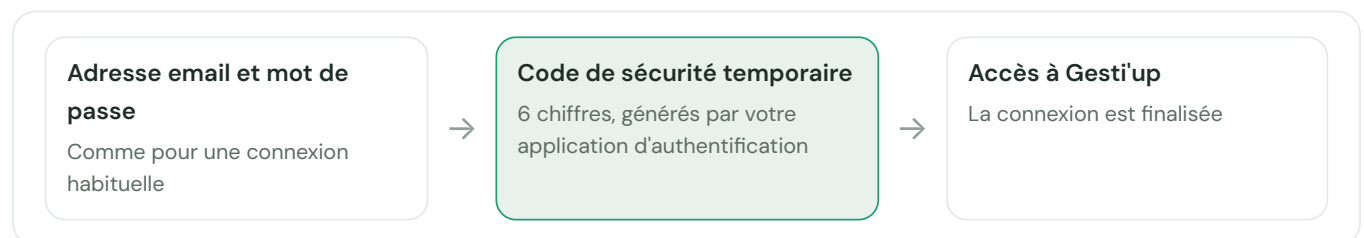
AUDIENCE Tous les utilisateurs

SECTIONS 06 ET 07 Administrateurs

La double authentification (2FA) ajoute une étape de sécurité à la connexion à votre compte Gesti'up : en plus de votre mot de passe, un code temporaire généré par votre application d'authentification est demandé.

01 Comment fonctionne la double authentification ?

La connexion se fait en deux temps. Sans le code, l'accès au compte est refusé.



02 Activer la double authentification

Quatre étapes, à faire avec votre smartphone à portée de main.

1

Cliquez sur « Activer la 2FA »

Le bouton se trouve dans la section **Double authentification (2FA)**, depuis :

Paramètres → Mon compte → Sécurité



2

Installez une application d'authentification

Si vous n'en possédez pas déjà une, installez une application compatible sur votre smartphone. Elle génère le code temporaire demandé à la connexion.

Google Authenticator

Authy

Aegis



Besoin d'aide ?

Bulle d'aide · FAQ · Ticket support · Vidéos tutorielles

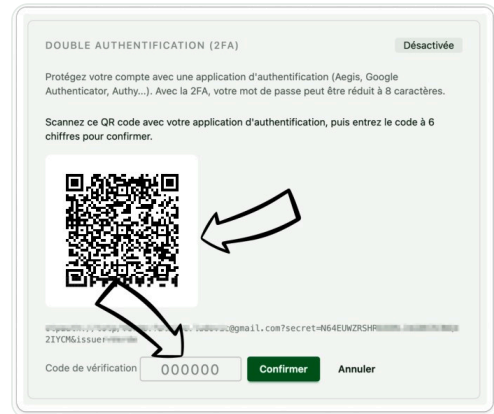
3

Associez votre compte Gesti'up à l'application

Après le clic sur « Activer la 2FA », un QR code et une clé de configuration s'affichent. Dans votre application d'authentification :

- 1 Ajoutez un nouveau compte.
- 2 **Scannez le QR code** affiché à l'écran, ou saisissez manuellement la clé fournie.

L'application génère alors un code à 6 chiffres, renouvelé automatiquement.



QR code d'exemple.

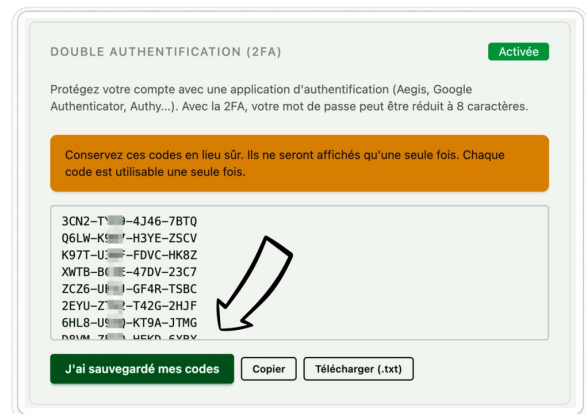
4

Confirmez l'activation et sauvegardez vos codes de secours

Saisissez le **code de vérification** affiché dans votre application, puis cliquez sur **Confirmer**.

Téléchargez ensuite vos **codes de secours** et conservez-les en lieu sûr. Ils permettent de vous connecter si vous n'avez pas votre application d'authentification.

Votre double authentification est désormais activée.



⚠ Les codes de secours ne sont affichés **qu'une seule fois**, et chaque code n'est utilisable **qu'une seule fois**.

i Avec la 2FA activée, la longueur minimale de votre mot de passe peut être réduite à 8 caractères.



Besoin d'aide ?

Bulle d'aide · FAQ · Ticket support · Vidéos tutorielles

03 Se connecter avec la 2FA activée

À chaque connexion, le code remplace une simple validation par mot de passe.

- 1 Saisissez votre **adresse email** et votre **mot de passe**.
- 2 Renseignez le **code temporaire** affiché dans votre application d'authentification.

Sans ce code, l'accès au compte est refusé. Si vous n'avez pas votre application, utilisez un code de secours.

Gesti'up↑

Double authentification

Entrez le code de votre application d'authentification pour [email redacted].com.

Code à 6 chiffres

000000

☐ Se souvenir de ce navigateur pendant 30 jours

Vérifier

[Utiliser un code de secours](#)

Dois-je saisir un code à chaque connexion ?

SITUATION	CODE 2FA DEMANDÉ
Même navigateur et même appareil, case « Se souvenir de ce navigateur pendant 30 jours » cochée	Au bout de 30 jours
Autre navigateur ou autre appareil	À chaque nouvelle connexion
Case non cochée	Une nouvelle vérification peut être demandée à la reconnexion

04 Désactiver la 2FA

Vous devez connaître votre mot de passe et disposer d'un code de votre application ou d'un code de secours.

Paramètres → Mon compte → Sécurité

1

Cliquez sur « Désactiver la 2FA »

DOUBLE AUTHENTIFICATION (2FA) **Activée**

Protégez votre compte avec une application d'authentification (Aegis, Google Authenticator, Authy...). Avec la 2FA, votre mot de passe peut être réduit à 8 caractères.

10 code(s) de secours restant(s)

[Régénérer les codes de secours](#) [Désactiver la 2FA](#)



2

Confirmez avec votre mot de passe et un code

- 1 Renseignez votre **mot de passe**.
- 2 Saisissez le **code TOTP** généré par votre application d'authentification, ou un **code de secours**.
- 3 Cliquez sur **Désactiver**.

DOUBLE AUTHENTIFICATION (2FA) Activée

Protégez votre compte avec une application d'authentification (Aegis, Google Authenticator, Authy...). Avec la 2FA, votre mot de passe peut être réduit à 8 caractères.

Entrez votre mot de passe et le code TOTP (ou un code de secours) pour désactiver la 2FA.

Mot de passe

Code TOTP ou code de secours

000000 ou XXXX-XXXX-XXXX-XXXX

Désactiver Annuler

⚠ Si votre administrateur ou le créateur du compte a rendu la double authentification obligatoire, il vous sera demandé de la configurer à nouveau lors de votre prochaine connexion.

05 J'ai changé de téléphone et je ne peux plus me connecter

La solution dépend de ce à quoi vous avez encore accès.

Cas 1 : j'ai encore accès à mon ancien téléphone

Connectez-vous à votre compte, puis ouvrez Paramètres → Mon compte → Sécurité. Désactivez la double authentification, puis activez-la à nouveau et scannez le nouveau QR code avec l'application d'authentification de votre nouvel appareil.

Cas 2 : je n'ai plus accès à mon ancien téléphone

Si vous avez conservé vos codes de secours, utilisez-en un pour accéder à votre compte. Chaque code ne peut être utilisé qu'une seule fois.

Cas 3 : je n'ai plus accès à mon téléphone ni à mes codes de secours

Demandez à votre administrateur ou au créateur du compte de désactiver temporairement la 2FA sur votre accès (voir la section 06). Vous pourrez alors vous connecter normalement, puis la réactiver.

**Besoin d'aide ?**

Bulle d'aide · FAQ · Ticket support · Vidéos tutorielles

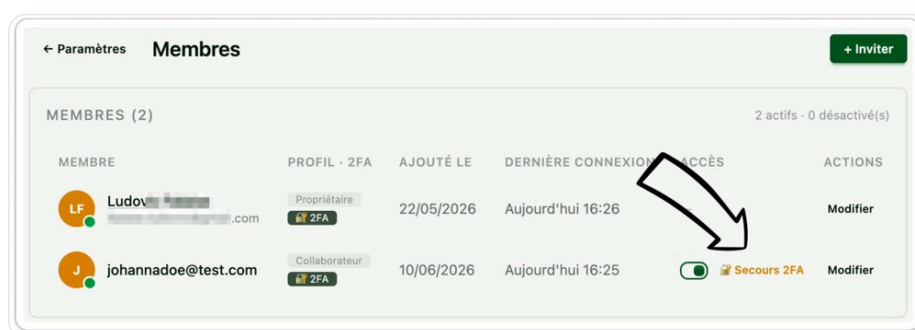
06 Désactiver la 2FA d'un utilisateur ou d'un collaborateur

Administrateur ou créateur du compte

Cette fonctionnalité permet d'aider un utilisateur qui n'a plus accès à son application d'authentification (changement de téléphone, perte d'appareil, suppression de l'application). Il retrouve l'accès à son compte et peut reconfigurer sa double authentification.

Paramètres → Équipe → Membres

- 1 Recherchez l'utilisateur concerné dans la liste des membres.
- 2 Sur sa ligne, cliquez sur **Secours 2FA**.
- 3 Confirmez la désactivation temporaire de la double authentification.



L'utilisateur peut alors se reconnecter sans code de vérification. Cette action désactive uniquement la protection 2FA du compte concerné ; elle ne doit être utilisée que lorsque c'est nécessaire.

07 Rendre la 2FA obligatoire pour tous les utilisateurs

Administrateur

Les administrateurs peuvent rendre la double authentification obligatoire pour l'ensemble des utilisateurs du compte, depuis Paramètres → Organisation → Informations société.

[i Voir la documentation « Forcer la double authentification pour tous les utilisateurs ».](#)

08 Puis-je communiquer mon code 2FA à quelqu'un ?

Non. Votre code de double authentification est personnel.

⚠ Ne communiquez jamais votre code à un tiers, y compris à une personne se présentant comme membre du support Gesti'up. Gesti'up ne vous demandera jamais votre mot de passe ni votre code de double authentification.



Besoin d'aide ?

Bulle d'aide · FAQ · Ticket support · Vidéos tutorielles

© 2026 Gesti'up · PROC-SUP-V1FR-Q2-PUB · Mise à jour : octobre 2026

Français · Tous les utilisateurs · 5/5