

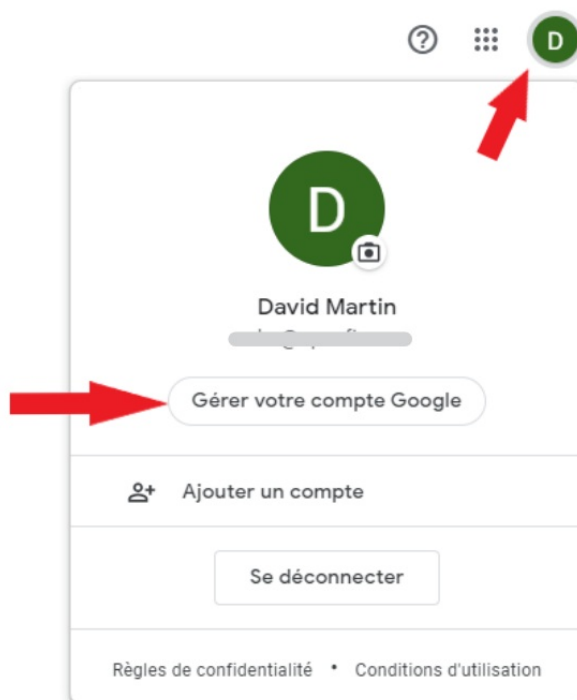
## Mails en erreurs sur Gmail (SMTP 535)

Le problème vient généralement du fait que Gmail a durci sa politique de sécurité. Dorénavant, il ne faut plus saisir votre "vrai" mot de passe gmail dans OpenFire mais un mot de passe généré par google spécifiquement pour OpenFire.

Voici comment procéder:

### Etape 1: Activation de la double validation

Connectez-vous à votre compte Gmail et cliquez sur votre profil en haut à droite. Cliquez ensuite sur "Gérer votre compte Google".



Rendez-vous ensuite dans l'onglet "Sécurité" et activez la validation en deux étapes (dans la partie "Connexion à Google").

Google Compte  Action requise

Accueil  
Informations personnelles  
Données et confidentialité  
**Sécurité**  
Contacts et partage  
Paiements et abonnements  
À propos

Examiner l'activité liée à la sécurité (9)


### Connexion à Google

Mot de passe	Dernière modification : 30 nov. 2021	>
Validation en deux étapes	<input type="checkbox"/> Désactivé	>
Mots de passe des applications	Aucun	>

Cliquez sur [commencer](#) et suivez les instructions.



Renseignez bien votre numéro de téléphone portable lorsque cela vous le sera demandé, car des codes de vérification Google vous seront par sms.

## ← Validation en deux étapes



### Protégez votre compte avec la validation en deux étapes

Empêchez les pirates informatiques d'accéder à votre compte avec un niveau de sécurité supplémentaire. Lorsque vous vous connectez, la validation en deux étapes contribue à assurer la confidentialité et la sécurité de vos informations personnelles.

-  **La sécurité en toute simplicité**  
La validation en deux étapes est une seconde étape rapide, en plus de votre mot de passe, pour vérifier qu'il s'agit bien de vous.
-  **Utilisez la validation en deux étapes pour tous vos comptes en ligne**  
La validation en deux étapes est un moyen éprouvé de se protéger contre les cyberattaques courantes. Activez-la lorsqu'elle est disponible afin de protéger tous vos comptes en ligne.

Safer with Google

[COMMENCER](#)

## Etape 2: Activation des mots de passe des applications

Lorsque cela est terminé, retournez dans l'onglet "Sécurité" de votre compte Google et cliquez de nouveau sur "Validation en 2 étapes".

Tout en bas de la page, il faut cliquer sur “Mots de passe des applications”.

Vous n'êtes actuellement connecté à aucun appareil compatible avec les tentes.

← Validation en deux étapes Configurer

Utilisez l'appli Authenticator pour recevoir sans frais des codes de validation, même si votre téléphone est hors connexion. Disponible pour Android et iPhone.

**Clé de sécurité**  
Une clé de sécurité est une méthode de validation qui vous permet de vous connecter de manière sécurisée. Elle peut être intégrée à votre téléphone, utiliser le Bluetooth ou se brancher directement sur le port USB de votre ordinateur.

**Appareils sur lesquels une deuxième étape n'est pas nécessaire**  
Vous pouvez ignorer la deuxième étape sur les appareils que vous jugez suffisamment fiables, comme votre ordinateur personnel.

**Appareils fiables**  
Révoquez le statut d'appareil vérifié pour les appareils sur lesquels la validation en deux étapes est ignorée.

[TOUT ANNULER](#)

**Mots de passe des applications**  
Les mots de passe d'application ne sont pas recommandés et sont inutiles dans la plupart des cas. Pour sécuriser votre compte Google, utilisez [Se connecter avec Google](#) pour y associer des applis.

**Mots de passe des applications**  
Aucun

Ensuite, il faut créer un mot de passe pour l'application OpenFire.

Pour cela, créez une application en sélectionnant “autre”, nommez “Openfire” et cliquez sur le bouton “Générer”. Cela générera un mot de passe à 16 caractères qu'il faudra noter.

← Mots de passe des applications

Les mots de passe d'application vous permettent de vous connecter à votre compte Google à partir d'applications sur des appareils non compatibles avec la validation en deux étapes. Comme vous ne devez saisir le mot de passe qu'une fois, vous n'avez pas besoin de le mémoriser. [En savoir plus](#)

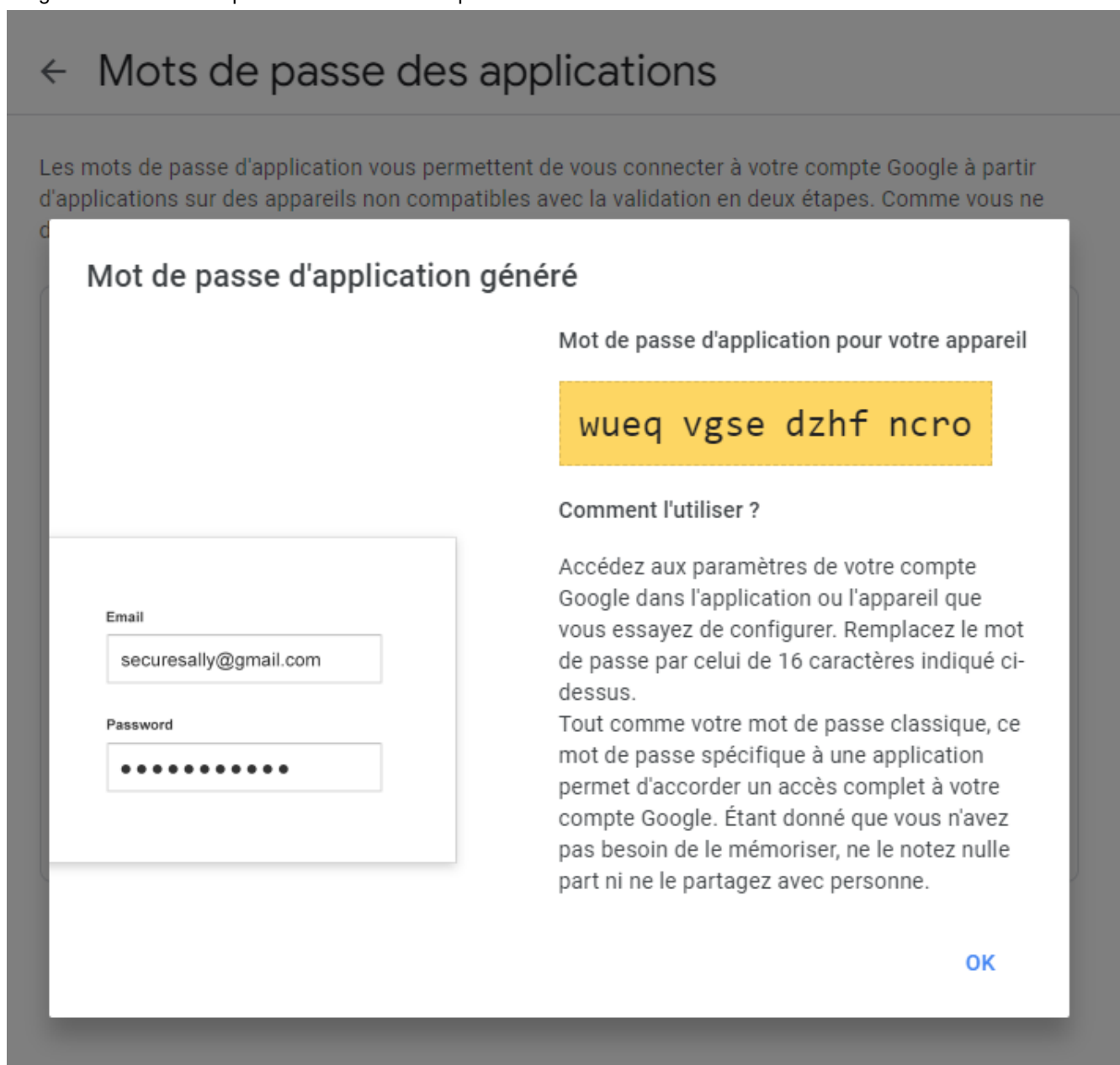
Vous n'avez aucun mot de passe d'application.

Sélectionnez l'application et l'appareil pour lesquels vous souhaitez générer le mot de passe d'application.

OpenFire

[GÉNÉRER](#)

Cela générera un mot de passe à 16 caractères qu'il faudra noter.



← Mots de passe des applications

Les mots de passe d'application vous permettent de vous connecter à votre compte Google à partir d'applications sur des appareils non compatibles avec la validation en deux étapes. Comme vous ne pouvez pas les mémoriser, Google vous en génère un à 16 caractères.

### Mot de passe d'application généré

Mot de passe d'application pour votre appareil

**wueq vgse dzhf ncro**

Comment l'utiliser ?

Accédez aux paramètres de votre compte Google dans l'application ou l'appareil que vous essayez de configurer. Remplacez le mot de passe par celui de 16 caractères indiqué ci-dessus.

Tout comme votre mot de passe classique, ce mot de passe spécifique à une application permet d'accorder un accès complet à votre compte Google. Étant donné que vous n'avez pas besoin de le mémoriser, ne le notez nulle part ni ne le partagez avec personne.

OK

**Email**  
securesally@gmail.com

**Password**  
••••••••••••••

Connectez-vous enfin à votre base Openfire (assurez-vous d'être sur un profil disposant des droits de configuration) et cliquez sur "activer le mode développeur" tout en bas à droite. Une fois la page rechargée, rendez-vous de nouveau dans l'onglet **Configuration > Technique > serveurs de courriel** sortant

Cliquez sur le serveur correspondant à votre adresse Gmail pour laquelle vous venez de configurer votre compte.

Modifiez ensuite le mot de passe pour y entrer les 16 caractères préalablement transmis par Google et cliquez sur "test de connexion" pour vérifier que tout fonctionne correctement.

