

Paramétrer un serveur mail

Il est possible de connecter OpenFire à votre compte de messagerie de telle sorte qu'OpenFire puisse émettre des mails depuis votre serveur de messagerie.

Dans un premier temps notez que l'utilisation d'un hébergeur mail destiné aux particuliers n'est ni recommandé, ni supporté par Openfire.

En effet cet usage est souvent limité ou bloqué par les fournisseurs tels que Gmail, Microsoft, Yahoo, etc.

Les manipulations énoncées sur cet articles peuvent fonctionner au moment de la configuration avec un service destiné aux particuliers, mais nous ne pouvons vous apporter aucune garantie sur la pérennité de cette solution.



Activation du mode Debug

La configuration des envois d'email se fait depuis le menu configuration et nécessite l'activation du mode Développeur.

Pour cela, rendez-vous dans l'onglet **Configuration** puis cliquez sur l'option Activer le mode développeur à droite :



Après le chargement de la page, retournez dans le menuConfiguration. Cliquez ensuite sur **Technique >** Serveurs de courriel sortant



Ces différents menus vous permettent de piloter votre envoi de mail.

Configuration des serveurs Mails

Cliquez sur Créer, puis renseignez les différents paramètres demandés.

Par exemple, pour une adresse Gmail, renseignez les champs comme suit :

- Serveur SMTP : smtp.gmail.com
- Port SMTP : 465
- Sécurité de la connexion : SSL/TLS
- Puis renseigner l'adresse et le mot de passe nécessaire.

Documentation éditée par Openfire. Documentation disponible sur documentation.openfire.fr Page: 2 / 9



Serveurs de courriel sortant / (Gmail)							
SAUVEGARDER ANNULER							
Description	Gmail	Priorité	10				
In fame attack							
Informations	sur la connexion						
Serveur SMTP	smtp.gmail.com	Port SMTP	465				
Débogage							
Sécurité et Authentification							
Sécurité de la connexion	Sécurité de la connexion						
Nom d'utilisateur	xxxxx@gmail.com						
Mot de passe							
C Test de connexion							

Pour OVH, le serveur est généralement ssl0.ovh.net et le port à utiliser est le 587.

Pour un compte Office365, le serveur est généralement *smtp.office365.com* et le port à utiliser est le 587.

Après avoir saisis les différents paramètres de votre compte, vous pouvez vérifier que tout fonctionne en cliquant sur le bouton "Test de connexion".

Description	Gmail					
Informatio	ons sur la connexion					
Serveur SMTP	smtp.gmail.com					
Débogago						

Sécurité et Authentification

Sécurité de la connexion					
Nom d'utilisateur					
Mot de passe					
🖵 Test de connexion					

Si tout est correct, vous obtenez le message suivant:

Odoo Avertissement - Avertissement	×	ic
Test de connexion réussi ! Tout semble correctement configuré !		
ок	_	

Documentation éditée par Openfire. Documentation disponible sur documentation.openfire.fr Page: 3 / 9



Erreurs Possibles

Erreur SMTP 40X:

Les codes erreurs SMTP 40X correspondent à des erreurs temporaires, exemple 421 Try again later. Ces erreurs sont remontées par le serveur expéditeur. Cela peut être un problème d'indisponibilité temporaire, ou encore un problème de quota de mail.

Erreur SMTP 534 et/ou SMTP 535:

Le problème vient généralement du fait que Gmail a durci sa politique de sécurité. Dorénavant, il ne faut plus saisir le mot de passe de votre adresse 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".



Documentation éditée par Openfire. Documentation disponible sur documentation.openfire.fr Page: 4 / 9



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

Goo	ogle Compte	Q	Rechercher dans le compte Google			>
۲	Accueil			Examiner l'activité liée à la sécurité (9)		
	Informations personne	lles				
۲	Données et confidentia	lité		Connexion à Google		
⋳	Sécurité					
6	Contacts et partage					
	Paiements et abonnem	ents		Mot de passe	Dernière modification : 30 nov. 2021	>
i	À propos			Validation en deux étapes	Césactivé	>
				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 transmis par sms.

← Validation en deux étapes

	G C	
Protégez	z votre compte avec la validation en deux étapes	i -
Empêchez le supplément la confident	ies pirates informatiques d'accèder à votre compte avec un niveau de taire. Lorsque vous vous connectez, la validation en deux étapes con tialité et la sécurité de vos informations personnelles.	sécurité tribue à assurer
	La sécurité en toute simplicité	
-7	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.	
6	Utilisez la validation en deux étapes pour tous vos comptes en ligne	I
	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.	
	ß	
	Safer with Google	
		COMMENCER

Etape 2: Activation des mots de passe des applications

Documentation éditée par Openfire. Documentation disponible sur documentation.openfire.fr Page: 5 / 9



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

Vérifiez que la validation en 2 étapes est bien activée :



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



	Utilisez l'appli Authenticator pour recevoir sans frais des codes de validation, même si votre téléphone est hors connexion. Disponible pour Android et iPhone.
От	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 s /ous pouve: /otre ordina	sur lesquels une deuxième étape n'est pas nécessaire z ignorer la deuxième étape sur les appareils que vous jugez suffisamment fiables, comme tour parcenzel
	eur personne.
	Appareils fiables Révoquez le statut d'appareil vérifié pour les appareils sur lesquels la validation en deux étapes est ignorée. TOUT ANNULER
Mots de pa Les mots de Pour sécuris	Appareils fiables Révoquez le statut d'appareil vérifié pour les appareils sur lesquels la validation en deux étapes est ignorée. TOUT ANNULER asse des applications passe d'application ne sont pas recommandés et sont inutiles dans la plupart des cas. re votre compte Google. utilisez Se connecter avec Google pour y associer des applis.

IMPORTANT : Si vous ne retrouvez pas l'emplacement "Mot de passe des applications" alors vous pouvez également faire une recherche "application" dans la barre de recherche située au dessus et sélectionner "Mot de passe des applications".

Go	ogle Compte	Q	application		×		
		2 RÉS	ULTATS				
٢	Accueil	E	Mots de passe des applications Sécurité			curité	
E	Informations personnel	Ē	Activité sur le Web et les applications			pur vous aider à protéger votre compte	
۲	Données et confidentia		bonnees et conndentiante				
₿	Sécurité	Q	Rechercher "application" dans le centre o	l'aide	>	ucune ac-	
å	Contacts et partage Paiements et abonnements			tion recommandée			
À propos				Afficher les détails			

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

Pour cela, créez une application en sélectionnant "autre", notez le nom de votre base client et cliquez sur le bouton "Générer".

Documentation éditée par Openfire. Documentation disponible sur documentation.openfire.fr Page: 7 / 9



← Mots de passe des applications

Les mots de passe d'application vous permettent de vous connecter à votre compte Google sur des applis et des services plus anciens, non compatibles avec les normes de sécurité les plus récentes.

Les mots de passe d'application sont moins sécurisés que les applis et services à jour qui utilisent les normes de sécurité les plus récentes. Avant de créer un mot de passe d'application, vous devez vérifier si votre appli en a besoin pour établir la connexion. En savoir plus



Vous allez obtenir un mot de passe à 16 caractères qu'il va falloir reporter dans Openfire.



OK

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 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 Email vous essayez de configurer. Remplacez le mot securesally@gmail.com de passe par celui de 16 caractères indiqué cidessus. Tout comme votre mot de passe classique, ce Password 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.

Connectez-vous à votre base Openfire depuis un profil ayant accès à l'application Configuration, et cliquez sur activer le mode développeur puis accédez au menu 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.

Documentation éditée par Openfire. Documentation disponible sur documentation.openfire.fr Page: 9 / 9