DOCUMENTATION / SUPPORT DE FORMATION

Table des matières

Accueil - Authentification sécurisée

Généralités

Dans l'application il est possible d'ajouter une étape complémentaire de sécurisation pour vous connecter à votre compte en plus de l'identifiant et mot de passe.

Ce contrôle doit être activé par l'utilisateur lui-même. Il ne peut pas être fait par un administrateur pour tous les collaborateurs. Par ailleurs, ce système ne peut être mis en place que pour des authentifications internes. Il ne fonctionne pas avec Microsoft Office 365 et Google Apps.

Conseil : Si vous souhaitez le mettre en place pour tous les collaborateurs, vous pouvez repartir de ce zoom pour faire une communication en interne sur son fonctionnement et sa mise en place.

Comment fonctionne l'authentification double facteur ?

Le contrôle qui s'ajoute se fait via un OTP (One-time password). Il s'agit d'un code unique qui est auto généré à intervalle régulier par une application spécifique.

Google Authenticator est l'application la plus simple d'utilisation, c'est celle que nous vous conseillons d'installer. Vous la retrouverez sur Google Play et Apple store. Elle est compatible avec le terminaux Android (version 2.1 ou supérieur) et les terminaux Apple (iPhone, iPad ou iPod Touch, iOS 5.0 ou supérieur)

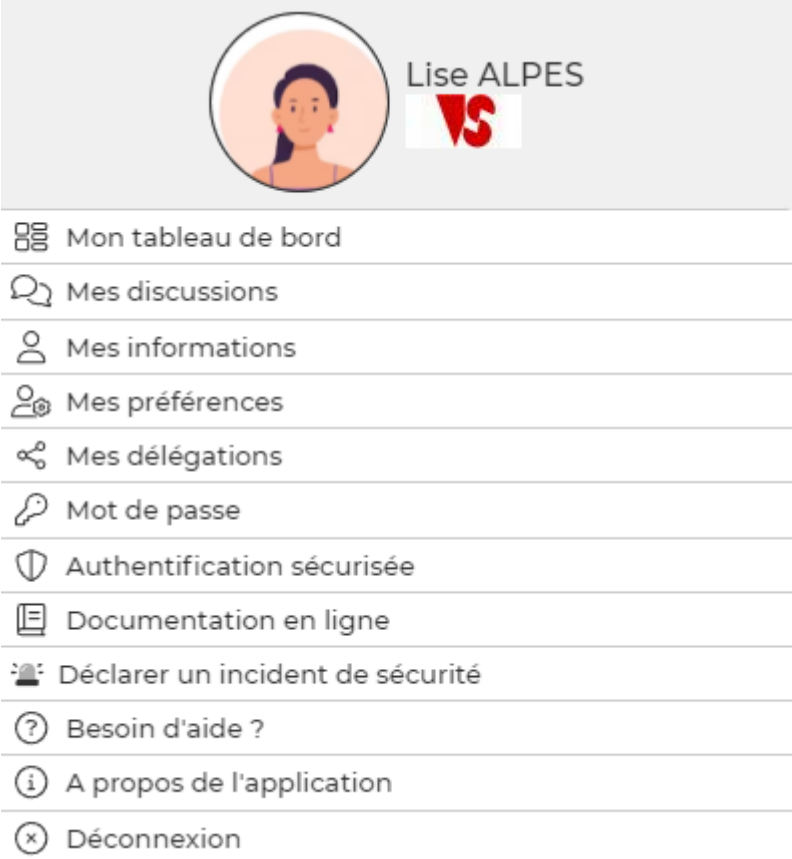
Etape 1 : Activation d'un droit (action à faire par l'administrateur ERP)

Pour que les collaborateurs puisse activer cette double authentification, vous devez activer un droit dans les groupes de sécurité concernés.

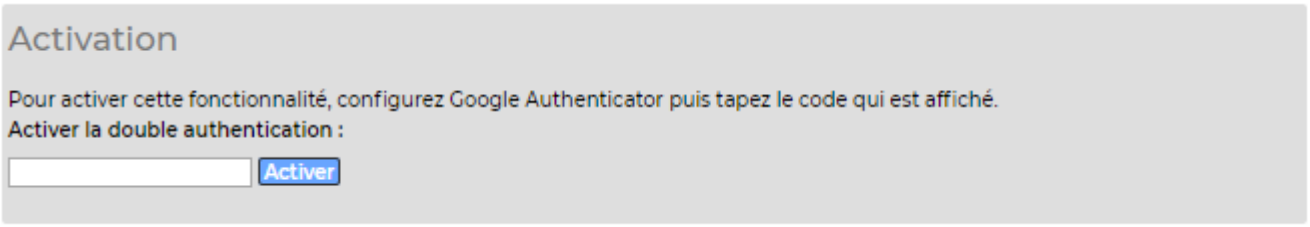
Fonctions transverses > Authentification sécurisée

Etape 2 : Activation de la double authentification par le collaborateur

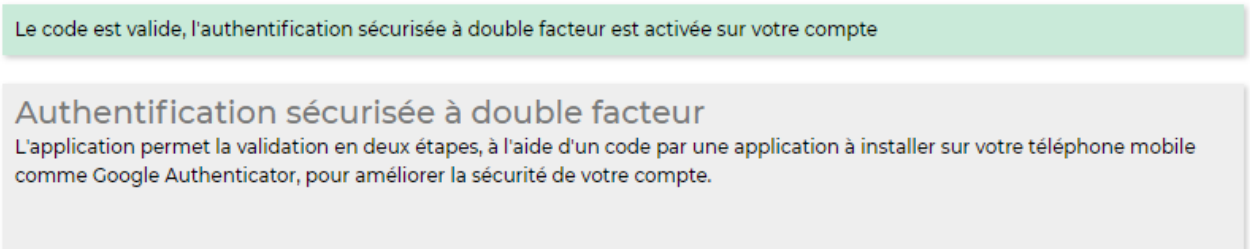
Une fois l'application Google Authenticator installée, vous devrez ensuite aller dans votre *espace personnel > Authentification sécurisée*



Cliquez ensuite sur Afficher le QR Code
Depuis votre application Google Authenticator, scannez ce QR code.
Une ligne de code à 6 chiffres apparaîtra.
C'est ce code que vous devrez rentrer dans la partie Activation de votre écran pour finaliser l'installation.

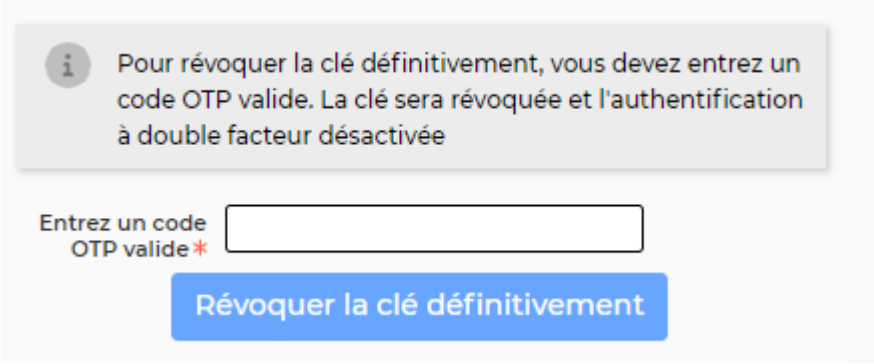


Un message de confirmation, que l'authentification sécurisée s'applique bien sur votre compte apparaitra en haut de l'écran.



Besoin de révoquer la clé ?

Il vous est possible de changer le QR code qui a été précédemment généré.
Pour cela cliquez sur Révoquer la clé
Vous devrez renseigner le code à 6 chiffres disponible dans Google Authenticator.



Un message s'affichera pour vous informer que la révocation s'est bien faite.

Une fois l'action terminée, un nouveau QR code sera disponible pour vous permettre de remettre en place l'authentification sécurisée.

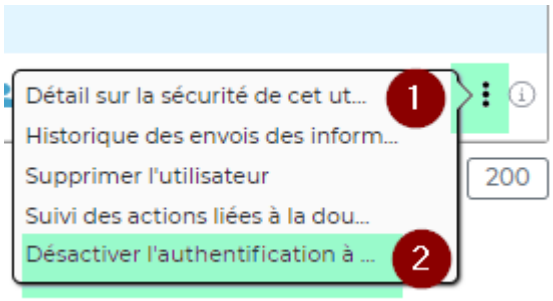
Conseil : Pensez à bien supprimer la ligne de code précédemment révoquée avant de réactiver un nouveau code.

Comment désactiver l'authentification sécurisée ?

Le collaborateur lui même a la possibilité de désactiver cette authentification.

Il lui suffira de rentrer le code OTP dans la partie désactivation.

Cependant si vous souhaitez qu'un administrateur vienne le faire à sa place, il faudra ajouter un droit dans le groupe de sécurité concerné. (*Administration > Gestion des utilisateurs > Possibilité de désactiver l'authentification à double facteur*) Le fait qu'un administrateur vienne desactiver l'authentification double facteur révoquera automatiquement la clé.
Cette action est disponible en action de ligne sur chaque collaborateur qui a l'authentification double facteur activée.



Que se passe t'il quand un collaborateur quitte la société ?

Le fait de désactiver le compte de l'utilisateur dans l'application suffit pour bloquer sa connexion. Ainsi aucune autre action ne sera nécessaire.