# Comprendre l’authentication à deux facteurs

Professionnels des RH fournissant des technologies RH

www.hrwize.com

# Qu'est-ce que l'authentification à deux facteurs ?

L'authentification à deux facteurs (A2F) est une mesure de sécurité qui oblige les utilisateurs à vérifier leur identité à l'aide de plusieurs méthodes avant de pouvoir accéder à un système. Elle combine au moins deux facteurs d'authentification, tels que quelque chose que vous connaissez (un mot de passe) ou quelque chose que vous possédez (un smartphone ou une clé de sécurité). En exigeant plusieurs formes de vérification, la A2F réduit considérablement le risque d'accès non autorisé.

Les applications d'authentification génèrent des codes à durée limitée sur un appareil de confiance et sont moins vulnérables au phishing, au transfert ou à l'interception que les codes envoyés par e-mail.

L'authentification à deux facteurs par e-mail peut être utilisée pour l'accès de vos employés au système, mais cela dépend de la sécurité du compte de messagerie ; si la boîte de réception est compromise, le code à usage unique peut également être exposé. Par conséquent, l'application d'authentification est notre méthode la plus sûre et constitue la méthode par défaut pour les rôles à privilèges élevés (administrateurs/RH/gestionnaires).

# Qu'est-ce que l'authentification à deux facteurs ?

La mise en place de l'authentification à deux facteurs (2FA) renforce la sécurité de vos comptes en ajoutant une couche de protection supplémentaire qui va au-delà du simple mot de passe. Par exemple, même si un mot de passe venait à être compromis, un pirate devrait tout de même avoir accès à la méthode d'authentification supplémentaire, telle qu'un code envoyé sur votre téléphone ou une validation via une application d'authentification. Cela en fait un outil très efficace pour prévenir les cyberattaques et protéger les informations sensibles.

**Remarque :**

Si vous utilisez actuellement l'authentification unique (SSO) pour accéder à vos systèmes, l'authentification à deux facteurs (2FA) doit tout de même être mise en place comme point d'accès initial à votre réseau local. Cette configuration ne doit pas être effectuée au sein de votre système HCM ou de paie, comme indiqué dans le guide.

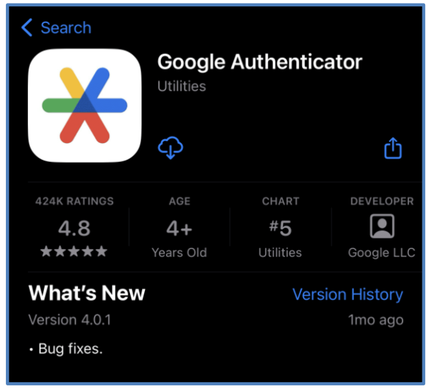
La 2FA doit plutôt être configurée au sein de votre propre environnement réseau. Nous vous recommandons vivement de consulter votre équipe informatique locale pour vous assurer que cette configuration est correcte.

# Installation et utilisation d'un authentificateur pour accéder à votre système

## Utilisation d'une application d'authentification pour accéder à votre système

La configuration et l'utilisation d'une application d'authentification sont des opérations simples qui renforcent la sécurité de votre compte. Ce guide vous explique les étapes à suivre pour configurer une application d'authentification en vue de l'authentification à deux facteurs (2FA).

## Téléchargement d'une application d'authentification sur votre appareil mobile




Vous pouvez télécharger une application d'authentification sur n'importe quel appareil intelligent, tel qu'un smartphone ou une tablette. Nous vous recommandons de télécharger une application d'authentification fiable, comme Microsoft Authenticator ou Google Authenticator. Vous pouvez les télécharger sur votre appareil mobile via les boutiques Android ou iOS, selon votre système d'exploitation.

# Enregistrez l'authentificateur pour l'utiliser avec votre profil système



Lorsqu'un employé tente de se connecter après l'activation de l'authentification à deux facteurs (2FA) dans votre système, l'écran ci-dessous s'affiche pour l'aider à configurer son application d'authentification. L'employé doit alors cliquer sur « Commencer la configuration » depuis cet écran.

# Rappel concernant l'application d'authentification


Une fois qu'ils auront sélectionné « Démarrer la configuration », un écran s'affichera pour leur rappeler de télécharger et d'installer une application d'authentification approuvée.

# Scannez le code QR et vérifiez


Le système affichera un code QR sur votre écran. Ouvrez l'application d'authentification sur votre appareil mobile et utilisez sa fonction de lecture pour scanner le code QR. Cela permettra de lier l'application à votre compte et de générer un code d'authentification unique.

# Saisissez le code d'authentification


Saisissez le code d'authentification affiché dans l'application sur le portail pour valider la configuration. Une fois la validation effectuée, votre application d'authentification sera correctement configurée et vous pourrez l'utiliser pour vous connecter en toute sécurité à l'avenir.

Une fois l'application correctement associée au système, le message ci-dessous s'affichera. Il leur suffira alors de cliquer sur le bouton « Activer l'authentification à deux facteurs » dans le message pour accéder à leur système.

# Résumé de la configuration de l'Authenticator

En suivant ces étapes, vous avez configuré avec succès une application d'authentification pour l'authentification multifactorielle. Ce niveau de sécurité supplémentaire garantit que votre compte reste protégé contre tout accès non autorisé. Chaque fois qu'un employé (Admin/RH/Gestionnaire) se connectera à votre système, il devra ouvrir l'application d'authentification et saisir le code généré dans le cadre de la procédure de connexion.

# Merci!

## CONTACT

1425 Trans-Canada Highway,
Dorval, Québec H9P 2W9,
Suite 020B

### Support

support@hrwize.com

www.hrwize.com