

Présentation

Le processus de connexion à certaines applications AIG nécessite désormais une authentification multi-facteurs (AMF). Cela signifie que chaque connexion doit être contrôlée via un moyen de vérification secondaire (application mobile, SMS ou appel téléphonique).

REMARQUE : Les écrans présentés dans ce guide reflètent la conception standard, mais l'apparence peut varier légèrement en fonction de l'application.

REMARQUE : Si vous avez des questions relatives au déploiement de l'authentification multi-facteurs, y compris des questions relatives à la confidentialité, consultez la [FAQ](#).

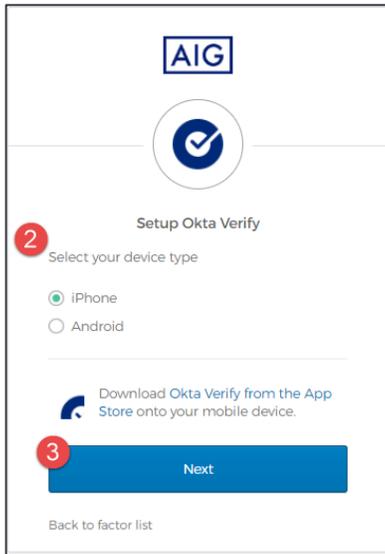
Configuration d'Okta Verify

Les utilisateurs peuvent, à leur discrétion, choisir parmi quatre méthodes actuellement prises en charge pour effectuer une authentification multi-facteurs. Bien qu'une seule méthode soit nécessaire pour authentifier la connexion, les utilisateurs peuvent choisir plusieurs méthodes AMF s'ils le souhaitent, et peuvent également modifier leur méthode AMF à tout moment en contactant le centre de contact.

Okta Verify envoie une vérification automatique sur l'appareil mobile de l'utilisateur (professionnel ou personnel), ce qui permet à l'utilisateur d'appuyer simplement sur une notification pour vérifier la connexion. Pour pouvoir utiliser cette méthode de vérification, l'application Okta Verify doit être installée sur l'appareil mobile de l'utilisateur.

Pour configurer Okta Verify :

1. Cliquez sur le bouton **Setup** (Configuration) dans l'option Okta Verify.
2. Cliquez sur le bouton radio **iPhone** ou **Android** pour configurer le type de périphérique approprié.
3. Cliquez sur le bouton **Next** (Suivant).



Pour configurer **Okta Verify** sur un appareil mobile :

1. Installez Okta Verify en cliquant sur les liens ci-dessous.
 - [iOS](#)
 - [Android](#)
2. Démarrez **Okta Verify** sur l'appareil mobile.
3. Sélectionnez **Organization** (Organisation) sur l'écran **Choose account type** (Choisir le type de compte).
4. Appuyez sur **Scan a QR code** (Scanner un code QR). Le scanner de code QR s'ouvre.

REMARQUE : Il peut être nécessaire d'autoriser l'application à accéder à la caméra de l'appareil pour continuer.

5. Utilisez l'appareil mobile pour scanner le **code QR** sur l'écran de l'ordinateur. Le compte sera ajouté à Okta Verify.
6. Cliquez sur le bouton **Next** (Suivant) sur l'écran **Setup Okta Verify** (Configurer Okta Verify).

Si le code QR ne fonctionne pas, cliquez sur **Can't scan?** (Impossible de scanner ?) sous le code QR pour activer Okta Verify par e-mail, SMS ou manuellement sans nécessité une authentification par notification push. Suivez les instructions ci-dessous selon la méthode d'activation choisie :

E-mail

1. Sélectionnez **Send activation link via Email** (Envoyer le lien d'activation par e-mail), puis appuyez sur **Next** (Suivant).
2. Ouvrez l'e-mail d'Okta sur votre appareil mobile.
3. Appuyez sur **Activate Okta Verify Push** (Activer la notification push d'Okta Verify) dans l'e-mail. L'application Okta Verify s'ouvre et le message **Enrolled in Push Authentication** (Inscription à l'authentification par notification push) s'affiche.
4. Retournez à la page de configuration et assurez-vous que Okta Verify est affiché sous **Enrolled Factors** (Facteurs inscrits).
5. Appuyez sur **Finish** (Terminer) sur l'appareil mobile pour terminer le processus.

SMS

1. Sélectionnez **Send activation link via SMS** (Envoyer le lien d'activation par SMS).
2. Entrez votre numéro de téléphone mobile dans le champ **Phone number** (Numéro de téléphone).
3. Appuyez sur **Next** (Suivant).
4. Vous recevrez un message d'Okta. Ouvrez ce message et appuyez sur le lien qu'il contient.
5. L'application Okta Verify s'ouvre, et le message **Enrolled in Push Authentication** (Inscription à l'authentification par notification push) devrait s'afficher.
6. Retournez à la page de configuration et assurez-vous que Okta Verify est affiché sous **Enrolled Factors** (Facteurs inscrits).
7. Appuyez sur **Finish** (Terminer) pour terminer le processus.

Configuration manuelle sans authentification par notification push (non recommandée)

1. Sélectionnez **Setup manually without Push Authentication** (Configuration manuelle sans authentification par notification push). La clé secrète que vous utiliserez pour configurer l'application apparaîtra.
2. Ouvrez l'application Okta Verify.
3. Appuyez sur le bouton **+**.
4. Appuyez sur **No Barcode?** (Aucun code-barres ?).
5. Entrez le nom d'utilisateur de votre compte Okta et la clé secrète affichée sur l'écran de configuration.
6. Cliquez sur **Add Account** (Ajouter un compte).
7. Sur la page de configuration, appuyez sur **Next** (Suivant).
8. Cliquez sur le code affiché dans l'application Okta Verify pour le copier, puis collez-le dans le champ **Enter code** (Entrer le code).
9. Appuyez sur **Verify** (Vérifier).
10. Assurez-vous que Okta Verify est à présent affiché sous **Enrolled Factors** (Facteurs inscrits).
11. Appuyez sur **Finish** (Terminer) pour terminer le processus.

Informations supplémentaires

Cliquez [ici](#) pour obtenir des informations supplémentaires sur l'application Okta Verify, y compris des données à caractère personnel collectées par Okta Verify. Okta Verify est une application tierce, et AIG ne gère pas ni n'a accès à aucune donnée à caractère personnel pouvant être collectée par l'application Okta Verify.