



AUTHENTIFICATION MULTIFACTORIELLE (AMF)

Application Google Authenticator Guide d'installation



Lorsque vous ouvrirez une session pour la première fois dans le Portail client, vous serez invité à installer une méthode d'authentification multifacteur (AMF).

Pour installer cette méthode d'authentification, vous devez télécharger l'application Google Authenticator sur votre appareil mobile. Une fois l'application téléchargée, suivez les étapes ci-dessous.





L'ACTIVATION NE PREND QUE QUELQUES MINUTES

Étape 1

Entrez votre nom d'utilisateur et cliquez sur Suivant, puis entrez votre mot de passe et cliquez sur Suivant.

PORTAIL CLIENT	PORTAIL CLIENT
 Les changements visuels que nous avons apportés n'affectent pas votre expérience en ligne. Connectez-vous en utilisant votre nom d'utilisateur et mot de passe habituels. Pour obtenir de l'assistance pour vous connecter à votre compte, veuillez consulter la section Besoin d'aide. 	Client_test Mot de passe
Nom d'utilisateur	Suivant Mot de passe oublié?
Suivant	Retour à la page de connexion
Nom d'utilisateur oublié?	
Créer un compte	

Étape 2

Cliquez sur le bouton **Choisir** sous l'option Google Authenticator.

•		
Vous devez activer un facteur d'authentification afin d'ajouter une couche de sécurité supplémentaire lors de la connexion à votre compte.		
★→	Google Authenticator Utiliser l'application mobile Google Authenticator pour vous authentifier.	
Ø	Okta Verify Utiliser l'application mobile Okta Verify pour vous authentifier. Choisir	
C	Téléphone Vérification via un code envoyé sur votre téléphone.	

Étape 3

Sur votre appareil mobile, lancez l'application Google Authenticator et numérisez le code QR. Note : si l'application Google Authenticator n'est pas téléchargée sur votre appareil, vous devrez la télécharger à partir de App Store (iPhone et iPad) ou de Google Play (appareils Android).

Après avoir numérisé le code QR cliquez sur **Suivant**.



Étape 4

Vous verrez un **code temporaire à 6 chiffres** que vous devrez saisir dans l'écran d'authentification dans le Portail client. Cliquez ensuite sur **Vérifier**.

11:44	.al 🕈 🗷
≡	
→ 272 232	٩
	_



Étape 5

Vous avez maintenant complété l'installation de la méthode d'authentification Google Authenticator et vous serez ramené à la page de configuration. Vous pouvez choisir d'installer une deuxième méthode d'authentification multifacteur, ou cliquer sur **Configurer plus tard** pour continuer dans votre Portail client.

On vous demandera si vous voulez que le système mémorise votre préférence d'authentification multifacteur en sélectionnant **Ne pas demander de code de vérification** ou **Demander un code à chaque connexion**. Si vous sélectionnez **Demander un code à chaque connexion**, la méthode d'authentification multifacteur que vous avez choisie s'affichera chaque fois et on vous demandera de vous authentifier avant que vous puissiez ouvrir une session.





Vous devez conserver l'application Google Authenticator sur votre appareil mobile pour de futures connexions dans le Portail client, car on pourrait vous demander de fournir un code de sécurité unique, qui sera généré dans l'application Google Authenticator.



ON S'INVESTIT, POUR VOUS.

iA Gestion privée de patrimoine est membre du Fonds canadien de protection des épargnants et de l'Organisme canadien de réglementation du commerce des valeurs mobilières. iA Gestion privée de patrimoine est une marque de commerce et un autre nom sous lequel **iA Gestion privée de patrimoine inc.** exerce ses activités.