Authentification multifacteur

Foire aux questions

Général

Q : Qu'est-ce qui change?

R : Le processus de connexion aux applications d'AIG nécessitera désormais une authentification multifacteur (AMF). Cela signifie que lorsque vous vous connecterez avec votre nom d'utilisateur et votre mot de passe, vous devrez également vérifier la connexion par un moyen de vérification secondaire de votre choix (application mobile, SMS ou appel téléphonique). Cette modification sera déployée dans les applications à l'aide d'une approche progressive, alors vous pourrez remarquer des mises à jour d'interface de connexion par vagues selon le nombre d'applications d'AIG auxquelles vous accédez.

Q : Pourquoi l'expérience de connexion change-t-elle?

R : AIG intègre un système d'authentification mis à jour dans l'expérience de connexion pour améliorer la sécurité de vos comptes en ligne.

Q : Quelles sont les méthodes d'AMF qui me sont offertes?

R : Les options d'AMF prises en charge comprennent une application d'authentification mobile (actuellement, Okta Verify et Google Authenticator), une authentification par SMS ou une authentification par appel vocal.

Q : Quelle option d'AMF AIG recommande-t-elle?

R : Les options d'AMF prises en charge par l'intermédiaire de la solution CIAM d'Otka utilisée par AIG comprennent une application d'authentification mobile (actuellement, Okta Verify et Google Authenticator), une authentification par SMS ou une authentification par appel vocal. AIG ne fait pas de recommandations concernant une méthode d'authentification et les utilisateurs peuvent choisir l'une des méthodes prises en charge qui répondent à leurs besoins.

Q : Puis-je utiliser une autre application qu'Okta Verify ou Google Authenticator pour l'AMF?

R : Pour le moment, Okta Verify et Google Authenticator sont les deux applications d'authentification prises en charge. Vous pouvez également choisir de vérifier l'authentification par SMS ou par appel vocal.

Q : Où puis-je télécharger les applications d'authentification mobile (Okta Verify et Google Authenticator)?

R : Vous pouvez télécharger l'une des applications d'authentification mobile à partir de l'App Store (Apple) ou de Google Play Store (Android). Si vous choisissez d'utiliser l'authentificateur mobile Okta, assurez-vous de télécharger Okta Verify (et non Okta Mobile).

Q : Que dois-je faire si je n'ai pas de téléphone intelligent (p. ex., j'ai un téléphone pliable)?

R : Il existe d'autres options d'AMF disponibles, ce qui comprend l'authentification par SMS ou l'authentification par appel vocal, qui peuvent être utilisées sans téléphone intelligent.

Q : Dois-je télécharger et installer une application pour l'AMF?

R : Un téléchargement de logiciel supplémentaire n'est nécessaire que si vous choisissez d'effectuer la vérification par l'intermédiaire d'OKTA Verify ou de Google Authenticator. Vous pouvez également choisir de vérifier l'authentification par SMS ou par appel vocal, ce qui ne nécessite pas l'installation d'une application.

Q : Comment vais-je me connecter si mon téléphone cellulaire ne fonctionne pas ou si je n'y ai pas accès?

R : Vous devrez utiliser une AMF pour vérifier votre connexion chaque fois. Communiquez avec le centre d'assistance approprié pour réinitialiser la méthode d'AMF.

Q : Devrai-je m'authentifier plus d'une fois si j'utilise plusieurs applications d'AIG?

R : Il n'est pas nécessaire de vous authentifier de nouveau si vous accédez à d'autres applications qui utilisent la même méthode d'AMF. Lorsque vous vous serez authentifié(e), vous pourrez accéder à toutes vos applications.

Q : Le processus d'AMF changera-t-il lorsque mon mot de passe expirera?

R : Non. La méthode d'AMF ne changera pas si le mot de passe expire ou est réinitialisé.

Q : Est-ce que le processus relatif au délai d'inactivité de l'application sera différent?

R : Le délai d'inactivité de l'application restera le même; cependant, vous devrez vous authentifier de nouveau en utilisant l'AMF lorsque vous vous reconnecterez.

Authentification multifacteur

Foire aux questions

Renseignements spécifiques à l'application

Q : Qu'est-ce qu'Okta?

R : **CIAM d'Okta** est une solution tierce utilisée par AIG pour l'authentification des utilisateurs afin d'accéder à divers systèmes et applications d'AIG.

Okta Verify est une application d'AMF offerte par Okta pour fournir un deuxième facteur afin de se connecter et établir une assurance plus solide pour la protection de votre compte. Pour plus de renseignements sur Okta Verify.

Q : Quels renseignements personnels Okta recueille-t-elle?

R : Pour authentifier l'identité d'un utilisateur, AIG utilise la solution de CIAM d'Okta pour recueillir et stocker le nom, l'adresse courriel, le numéro de téléphone, les identifiants de téléphone uniques et les adresses IP des utilisateurs. Ces renseignements sont stockés dans un environnement infonuagique de CIAM d'Okta tant qu'un utilisateur aura besoin d'accéder à une application et qu'il devra être authentifié pour y accéder. Cela permet aux utilisateurs qui se connectent à plusieurs applications d'AIG de ne devoir authentifier leur connexion qu'une seule fois pour toutes les applications pendant une session. Pour obtenir des renseignements sur les pratiques en matière de protection des renseignements personnels d'AIG, visitez le site Web https://www.aig.com/privacy-policy.

Okta Verify est une application distincte gérée par Okta qui fournit des codes qui peuvent être utilisés comme deuxième facteur d'authentification pour se connecter à d'autres services.

Q : Quels renseignements personnels sont requis pour Okta Verify?

R : Okta Verify peut recueillir des renseignements personnels dans le cadre du processus de vérification. AIG n'a pas accès aux renseignements personnels recueillis par Okta Verify. Pour plus d'informations sur la politique de confidentialité d'Okta, consultez le site Web https://www.okta.com/privacy-policy/.

Q : Qu'est-ce que Google Authenticator?

R : Google Authenticator est une application gérée par Google qui fournit des codes qui peuvent être utilisés comme deuxième facteur d'authentification pour se connecter à d'autres services. Si vous configurez la vérification en deux étapes, vous pouvez utiliser l'application Google Authenticator pour recevoir les codes. Vous pouvez toujours recevoir des codes sans connexion Internet ou sans service mobile.

Q : Quels renseignements personnels Google Authenticator recueille-t-elle?

R : Google Authenticator peut recueillir des renseignements personnels dans le cadre du processus de vérification. AIG n'a pas accès aux renseignements personnels recueillis par Google Authenticator. Pour plus d'informations sur la politique de Google, consultez le site Web https://policies.google.com/privacy.

Q : Puis-je télécharger et activer Okta Verify ou Google Authenticator sur plus d'un appareil?

R : Actuellement, Okta Verify ne peut être activé que sur un seul appareil. Google Authenticator peut être utilisé sur plusieurs appareils. L'application Google Authenticator doit être téléchargée sur tous les appareils que vous souhaitez utiliser.

Q : Est-ce que Google Authenticator ou Otka Verify utilisent des données mobiles ou nécessitent un espace de stockage supplémentaire?

R : Okta Verify utilise un minimum de données (environ quelques octets). Elle ne nécessite aucun stockage supplémentaire. Google Authenticator ne nécessite aucune connexion Internet ou mobile et ne nécessite aucun stockage supplémentaire.

Q : Quels renseignements personnels sont recueillis si j'utilise l'authentification par SMS ou par appel vocal?

R : Si vous choisissez d'utiliser l'authentification par SMS ou par appel vocal, aucun renseignement personnel ne sera recueilli par une application d'authentification, mais un certain nombre de renseignements personnels seront recueillis par l'entremise de la solution de CIAM d'Okta pour authentifier votre identité, ce qui comprend votre nom, votre adresse courriel, votre numéro de téléphone, vos identifiants téléphoniques uniques et votre adresse IP.