Authentification multi-facteurs

Foire aux questions

Généralités

Q : Qu'est-ce qui change ?

R : Le processus de connexion aux applications AIG nécessite désormais une authentification multi-facteurs (AMF). Cela signifie que lorsque vous vous connectez en utilisant votre identifiant et votre mot de passe, vous serez également invité à vérifier la connexion via un moyen de vérification secondaire de votre choix (application mobile, SMS ou appel téléphonique). Ce changement sera progressivement mis en place dans les applications. Vous pourrez donc constater des mises à jour de l'interface de connexion par vagues, en fonction du nombre d'applications AIG auxquelles vous avez accès.

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

R : AIG intègre un nouveau système d'authentification dans l'expérience de connexion afin d'améliorer la sécurité de vos comptes en ligne.

Q : Quelles sont les méthodes AMF à ma disposition ?

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

Q : Quelle est l'option AMF recommandée par AIG ?

R : Les options AMF prises en charge via la solution Okta CIAM utilisée par AIG comprennent l'application d'authentification mobile (actuellement Okta Verify et Google Authenticator), l'authentification par SMS ou l'authentification par appel vocal. AIG ne recommande aucune méthode d'authentification particulière. De plus, les utilisateurs peuvent sélectionner librement l'une des méthodes prises en charge. Tenga en cuenta que la mejor práctica para una conexión segura es utilizar una aplicación de autenticación en lugar de SMS o Autenticación de llamadas de voz. Para obtener más información sobre las mejores prácticas de MFA, haga clic aquí.

Q : Puis-je utiliser une application différente d'Okta Verify ou de Google Authenticator pour l'AMF ?

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

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

R : Ces applications d'authentification mobile sont disponibles sur l'App Store (Apple) ou sur le Google Play Store (Android). Si vous choisissez d'utiliser Okta, veillez à télécharger Okta Verify (pas Okta Mobile).

Q : Que faire si je n'ai pas de smartphone (par exemple, si j'ai un téléphone à clapet) ?

R : Il existe d'autres options AMF, notamment l'authentification par SMS ou par appel vocal, qui ne requièrent pas de smartphone.

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

R : Le téléchargement d'un logiciel supplémentaire n'est nécessaire que si vous choisissez d'effectuer des vérifications via OKTA Verify ou Google Authenticator. Sinon, vous pouvez choisir l'authentification par SMS ou par appel vocal, qui ne nécessitent pas l'installation d'une application.

Q : Comment puis-je me connecter si mon téléphone portable ne fonctionne pas ou n'est pas disponible ?

R : Pour chaque connexion, vous devrez recourir à une AMF. Contactez le service d'assistance approprié pour réinitialiser la méthode AMF.

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

R : Il n'est pas nécessaire de vous authentifier à nouveau si vous accédez à d'autres applications qui utilisent la même méthode AMF. Une fois que vous vous êtes authentifié, vous pouvez accéder à toutes vos applications.

Q : Le processus AMF changera-t-il lorsque mon mot de passe expirera ?

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

Q : Le processus d'expiration de l'application sera-t-il différent ?

R : Le délai d'expiration de l'application restera le même ; cependant, vous devrez authentifier à nouveau la connexion à l'aide de méthode AMF lorsque vous vous connecterez à nouveau.

Authentification multi-facteurs

Foire aux questions

Informations spécifiques aux applications

Q : Qu'est-ce que Okta ?

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

Okta Verify est une application AMF fournie par Okta pour servir de deuxième facteur de connexion et protéger plus efficacement votre compte. Pour plus d'informations sur Okta Verify.

Q : Quels types de données à caractère personnel Okta collecte-t-elle ?

R : Afin d'authentifier un utilisateur, AIG utilise la solution Okta CIAM pour collecter et conserver le nom, l'adresse e-mail, le numéro de téléphone, les identifiants de téléphone uniques et les adresses IP des utilisateurs. Ces informations sont stockées dans le cloud d'Okta CIAM aussi longtemps qu'un utilisateur aura besoin d'accéder à une application et devra être authentifié pour y accéder. Cela permet aux utilisateurs qui se connectent à plusieurs applications AIG d'authentifier leur connexion une seule fois pour toutes les applications au cours d'une session. Pour en savoir plus sur les pratiques d'AIG en matière de confidentialité, rendez-vous sur https://www.aig.com/privacy-policy.

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

Q : Quelles sont les données à caractère personnel requises par Okta Verify ?

R : Okta Verify peut collecter des données à caractère personnel dans le cadre du processus de vérification. AIG n'a pas accès aux données à caractère personnel collectées par Okta Verify. Pour plus d'informations sur la politique de confidentialité d'Okta, rendez-vous sur 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 pouvant être utilisés comme deuxième facteur d'authentification pour se connecter à d'autres services. Si vous avez choisi la vérification en deux étapes, vous pouvez utiliser l'application Google Authenticator pour recevoir des codes. Vous pouvez recevoir des codes sans connexion Internet ou service mobile.

Q : Quels types de données à caractère personnel Google Authenticator collecte-t-elle ?

R : Google Authenticator peut collecter des données à caractère personnel dans le cadre du processus de vérification. AIG n'a pas accès aux données à caractère personnel collectées par Google Authenticator. Pour plus d'informations sur la politique de confidentialité de Google, rendez-vous sur https://policies.google.com/privacy.

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

R : Pour l'instant, 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 : Okta Verify ou Google Authenticator utilisent-t-elles des données mobiles ou nécessitent-t-elles un espace de stockage supplémentaire ?

R : Okta Verify utilise un minimum de données (quelques octets). Elle ne nécessite pas d'espace de stockage supplémentaire. Google Authenticator ne nécessite pas de connexion Internet ou mobile ni d'espace de stockage supplémentaire.

Q : Quels types de données à caractère personnel sont collectés si j'utilise l'authentification par SMS ou appel vocal ?

R : Si vous choisissez de recourir à l'authentification par SMS ou appel vocal, aucune donnée à caractère personnel ne sera collectée par une application d'authentification, mais des données à caractère personnel limitées seront collectées via la solution Okta CIAM pour vous authentifier, y compris votre nom, adresse e-mail, numéro de téléphone, identifiants de téléphone uniques et adresse IP.