Multi-Faktor-Authentifizierung

Häufig gestellte Fragen

Allgemeines

F: Was ändert sich?

A: Für die Anmeldung bei einigen AIG-Anwendungen ist nun eine Multi-Faktor-Authentifizierung (MFA) erforderlich. Das bedeutet, dass Sie, wenn Sie sich mit Ihrem Benutzer-Login und Passwort anmelden, auch aufgefordert werden, die Anmeldung durch ein zweites Verifizierungsmittel Ihrer Wahl (mobile Anwendung, SMS oder Telefonanruf) zu bestätigen. Diese Änderung wird schrittweise auf die Anwendungen ausgerollt, sodass Sie je nach Anzahl der AIG-Anwendungen, auf die Sie zugreifen, die schrittweise Aktualisierung der Anmeldeoberfläche bemerken können.

F: Warum ändert sich das Anmeldeverfahren?

A: AIG integriert ein aktualisiertes Authentifizierungssystem in den Login-Prozess, um die Sicherheit für Ihre Online-Konten zu erhöhen.

F: Welche MFA-Methoden stehen mir zur Verfügung?

A: Zu den unterstützten MFA-Optionen gehören mobile Authentifizierungsanwendungen (derzeit Okta Verify und Google Authenticator), die SMS-Authentifizierung oder die Sprachanruf-Authentifizierung.

F: Welche MFA-Option wird von AIG empfohlen?

A: Zu den über die von AIG verwendete Okta CIAM-Lösung unterstützten MFA-Optionen gehören mobile Authentifizierungsanwendungen (derzeit Okta Verify und Google Authenticator), die SMS-Authentifizierung oder die Sprachanruf-Authentifizierung. AIG gibt keine Empfehlungen bezüglich einer Authentifizierungsmethode ab, und Benutzer können jede der unterstützten Methoden wählen, die ihren Bedürfnissen entspricht. Bitte beachten Sie, dass die beste Vorgehensweise für eine sichere Verbindung darin besteht, eine Authentifizierungsanwendung anstelle einer SMS- oder Sprachanrufauthentifizierung zu verwenden. Weitere Informationen zu Best Practices für MFA finden Sie hier.

F: Kann ich eine andere Anwendung für MFA als Okta Verify oder Google Authenticator verwenden?

A: Zurzeit sind nur Okta Verify und Google Authenticator unterstützte Authentifizierungsanwendungen. Alternativ können Sie die Authentifizierung durch eine SMS-Nachricht oder einen Sprachanruf vornehmen.

F: Wo kann ich die mobilen Authentifizierungsanwendungen (Okta Verify, Google Authenticator) herunterladen?

A: Die beiden möglichen mobilen Authentifizierungsanwendungen können Sie aus dem App Store (Apple) oder dem Google Play Store (Android) herunterladen. Wenn Sie sich für den mobilen Okta-Authentifikator entscheiden, stellen Sie sicher, dass Sie Okta Verify herunterladen (nicht Okta Mobile).

F: Was ist, wenn ich kein Smartphone habe (sondern zum Beispiel ein Klapphandy)?

A: Es gibt noch andere MFA-Optionen wie SMS- oder Sprachanruf-Authentifizierung, die auch ohne Smartphone angewendet werden können.

F: Muss ich für MFA eine App herunterladen und installieren?

A: Ein zusätzlicher Software-Download ist nur notwendig, wenn Sie sich für die Verifizierung durch OKTA Verify oder Google Authenticator entscheiden. Alternativ können Sie sich auch für die Verifizierung per SMS- oder Sprachanruf-Authentifizierung entscheiden, die keine App-Installation erfordern.

F: Wie logge ich mich ein, wenn mein Mobiltelefon nicht funktioniert oder nicht verfügbar ist?

A: Sie müssen jedes Mal eine MFA verwenden, um Ihre Anmeldung zu verifizieren. Wenden Sie sich an den zuständigen Helpdesk, um die MFA-Methode zurückzusetzen.

F: Muss ich mich mehr als einmal authentifizieren, wenn ich mehrere AIG-Anwendungen verwende?

A: Sie müssen sich nicht erneut authentifizieren, wenn Sie auf andere Anwendungen zugreifen, die die gleiche MFA-Methode verwenden. Sobald Sie sich authentifiziert haben, können Sie auf alle Ihre Anwendungen zugreifen.

F: Ändert sich der MFA-Prozess, wenn mein Passwort abläuft?

A: Nein. Das MFA-Verfahren wird sich nicht ändern, wenn das Passwort abläuft oder zurückgesetzt wird.

F: Ändert sich etwas am Applikations-Timeout-Prozess?

A: Am Applikations-Timeout ändert sich nichts. Allerdings müssen Sie die Anmeldung mit der MFA neu authentifizieren, wenn Sie sich erneut anmelden.

Anwendungsspezifische Informationen

F: Was ist Okta?

A: Okta CIAM ist eine Drittpartei-Lösung, die von AIG zur Benutzerauthentifizierung für den Zugriff auf verschiedene AIG-Systeme und -Anwendungen verwendet wird.

Okta Verify ist eine MFA-Anwendung von Okta, um einen zweiten Faktor für die Anmeldung bereitzustellen und eine stärkere Sicherheit für den Schutz Ihres Kontos zu gewährleisten. Für weitere Informationen über Okta Verify.

F: Welche personenbezogenen Daten werden von Okta erfasst?

A: Um die Identität eines Benutzers zu authentifizieren, erfasst und speichert AIG mit der Okta CIAM-Lösung den Namen, die E-Mail-Adresse, die Telefonnummer, eindeutige Telefonkennungen und IP-Adressen der Benutzer. Diese Informationen werden in einer Okta CIAM-Cloud-Umgebung so lange gespeichert, wie ein Benutzer Zugriff auf eine Anwendung benötigt und für den Zugriff authentifiziert werden muss. Dadurch müssen Benutzer, die sich bei mehreren AIG-Anwendungen anmelden, ihre Anmeldung nur einmal für alle Anwendungen während einer Sitzung authentifizieren. Informationen über die Datenschutzverfahren von AIG finden Sie unter https://www.aig.com/privacy-policy.

Okta Verify ist eine separate, von Okta verwaltete Anwendung, die Codes bereitstellt, die als zweiter Authentifizierungsfaktor für die Anmeldung bei anderen Diensten verwendet werden können.

F: Welche personenbezogenen Daten werden für Okta Verify benötigt?

A: Okta Verify kann personenbezogene Daten als Teil des Verifizierungsprozesses erfassen. AIG hat keinen Zugriff auf personenbezogene Daten, die von Okta Verify erfasst werden. Weitere Informationen über die Datenschutzrichtlinie von Okta finden Sie unter https://www.okta.com/privacy-policy/.

F: Was ist Google Authenticator?

A: Google Authenticator ist eine von Google verwaltete Anwendung, die Codes bereitstellt, die als zweiter Authentifizierungsfaktor für die Anmeldung bei anderen Diensten verwendet werden können. Wenn Sie die 2-Schritt-Verifizierung einrichten, können Sie die Google Authenticator-App verwenden, um Codes zu erhalten. Sie können Codes auch ohne Internetverbindung oder mobilen Dienst empfangen.

F: Welche personenbezogenen Daten werden von Google Authenticator erfasst?

A: Google Authenticator kann personenbezogene Daten als Teil des Verifizierungsprozesses erfassen. AIG hat keinen Zugriff auf personenbezogene Daten, die von Google Authenticator erfasst werden. Weitere Informationen über die Datenschutzrichtlinie von Google finden Sie unter https://policies.google.com/privacy.

F: Kann ich Okta Verify oder Google Authenticator auf mehr als einem Gerät herunterladen und aktivieren?

A: Derzeit kann Okta Verify nur auf einem Gerät aktiviert werden. Google Authenticator kann auf mehreren Geräten verwendet werden. Die Google Authenticator-App muss auf allen Geräten, die Sie verwenden möchten, heruntergeladen werden.

F: Verbrauchen Okta Verify oder Google Authenticator mobile Daten oder benötigen zusätzlichen Speicherplatz?

A: Okta Verify verwendet minimale Daten - in der Größenordnung von ein paar Bytes. Es benötigt keinen zusätzlichen Speicherplatz. Google Authenticator benötigt keine Internet- oder Mobilfunkverbindung und keinen zusätzlichen Speicherplatz.

F: Welche personenbezogenen Daten werden erfasst, wenn ich SMS- oder Sprachauthentifizierung verwende?

A: Wenn Sie sich für die SMS- oder Sprachauthentifizierung entscheiden, werden keine personenbezogenen Daten von einer Authentifizierungsanwendung erfasst, aber begrenzte personenbezogene Daten werden über die Okta CIAM-Lösung erfasst, um Ihre Identität zu authentifizieren, einschließlich Name, E-Mail-Adresse, Telefonnummer, eindeutige Telefonkennungen und IP-Adresse.