

### Algemeen

**V: Wat verandert er?**

A: Het proces om in te loggen op AIG-toepassingen vereist nu meervoudige verificatie (MFA). Dit betekent dat wanneer u inlogt met uw gebruikersnaam en wachtwoord, u ook verplicht bent om de aanmelding te verifiëren via een tweede manier van verificatie van uw keuze (mobiele applicatie, SMS of telefoongesprek). Deze wijziging wordt in een gefaseerde aanpak uitgerold naar toepassingen, dus u kunt updates van de inloginterface in golven opmerken, afhankelijk van het aantal AIG-applicaties dat u opent.

**V: Waarom verandert de inlogervaring?**

A: AIG integreert een bijgewerkt authenticatiesysteem in de inlogervaring om de beveiliging van uw online accounts te verbeteren.

**V: Welke MFA-methoden zijn er voor mij beschikbaar?**

A: De MFA-opties die worden ondersteund, omvatten mobiele authenticatietoepassing (momenteel Okta Verify en Google Authenticator), SMS-verificatie of Voice Call Authentication.

**V: Welke MFA-optie raadt AIG aan?**

A: De MFA-opties die worden ondersteund via de Okta CIAM-oplossing die door AIG wordt gebruikt, omvatten mobiele authenticatietoepassing (momenteel Okta Verify en Google Authenticator), sms-authenticatie of spraakoproepauthenticatie. AIG doet geen aanbevelingen met betrekking tot authenticatiemethodes en gebruikers kunnen een van de ondersteunde methodes kiezen die aan uw behoeften voldoen. Houd er rekening mee dat de beste werkwijze voor een beveiligde verbinding is om een authenticatietoepassing te gebruiken in plaats van sms- of spraakoproepauthenticatie. Klik [hier](#) voor meer informatie over best practices voor MFA.

**V: Kan ik een andere toepassing gebruiken voor MFA dan Okta Verify of Google Authenticator?**

A: Op dit moment zijn Okta Verify en Google Authenticator de twee ondersteunde authenticatietoepassingen. U kunt er ook voor kiezen om de authenticatie te verifiëren via SMS-bericht of Voice Call-verificatie.

**V: Waar kan ik de mobiele authenticatietoepassingen downloaden (Okta Verify, Google Authenticator)?**

A: U kunt een van de mobiele authenticatietoepassingen downloaden vanuit de App Store (Apple) of Google Play Store (Android). Als u ervoor kiest om de Okta mobiele authenticator te gebruiken, moet u Okta Verify downloaden (niet Okta Mobile).

**V: Wat als ik geen smartphone heb (bijv. een ouder model omklaptelefoon)?**

A: Er zijn andere MFA-opties beschikbaar, waaronder SMS-verificatie of spraakoproepverificatie, die zonder smartphone kunnen worden gebruikt.

**V: Moet ik een app voor MFA downloaden en installeren?**

A: Een extra软件下载 is alleen nodig als u ervoor kiest om te verifiëren via OKTA Verify of Google Authenticator. U kunt er ook voor kiezen om te authenticeren via SMS-verificatie of Voice Call Authentication, waarvoor geen app-installatie nodig is.

**V: Hoe log ik in als mijn mobiele telefoon niet werkt of niet beschikbaar is?**

A: U moet elke keer een MFA gebruiken om uw aanmelding te verifiëren. Neem contact op met de juiste helpdesk om de MFA-methode opnieuw in te stellen.

**V: Moet ik meer dan één keer authenticeren als ik meerdere AIG-toepassingen gebruik?**

A: Het is niet nodig om opnieuw te authenticeren als u toegang hebt tot andere toepassingen die dezelfde MFA-methode gebruiken. Zodra u bent geauthenticeerd, hebt u toegang tot al uw toepassingen.

**V: Is het MFA-proces anders wanneer mijn wachtwoord verloopt?**

A: Nee. De MFA-methode verandert niet als het wachtwoord verloopt of opnieuw wordt ingesteld.

**V: Is het time-outproces van de aanvraag anders?**

A: De time-out van de toepassing blijft hetzelfde; u moet de aanmelding echter opnieuw authenticeren met behulp van de MFA wanneer u zich opnieuw aanmeldt.

### Toepassings specifieke informatie

**V: Wat is Okta?**

A: **Okta CIAM** is een oplossing van een derde partij die door AIG wordt gebruikt voor gebruikersauthenticatie om toegang te krijgen tot verschillende systemen en applicaties van AIG.

**Okta Verify** is een MFA-applicatie die door Okta wordt geleverd om een tweede factor te bieden om in te loggen en een betere zekerheid te verkrijgen voor uw accountbescherming. Voor meer informatie over Okta Verify.

**V: Welke persoonsgegevens verzamelt Okta?**

A: Om de identiteit van een gebruiker te verifiëren, gebruikt AIG de Okta CIAM-oplossing om de naam, het e-mailadres, telefoonnummer, unieke telefoon-ID's en IP-adressen van gebruikers te verzamelen en op te slaan. Deze informatie wordt opgeslagen in een Okta CIAM-cloudomgeving zolang een gebruiker toegang tot een toepassing nodig heeft en moet worden geauthenticeerd voor toegang. Hierdoor hoeven gebruikers die zich aanmelden bij meerdere AIG-toepassingen slechts één keer hun login te verifiëren voor alle applicaties tijdens een sessie. Ga voor informatie over de privacypraktijken van AIG naar <https://www.aig.com/privacy-policy>.

Okta Verify is een afzonderlijke toepassing die wordt beheerd door Okta en codes biedt die kunnen worden gebruikt als een tweede authenticatiefactor om in te loggen bij andere services.

**V: Welke persoonsgegevens is vereist voor Okta Verify?**

A: Okta Verify kan persoonsgegevens verzamelen als onderdeel van het authenticatieproces. AIG heeft geen toegang tot persoonsgegevens die door Okta Verify is verzameld. Voor meer informatie over het privacybeleid van Okta, zie <https://www.okta.com/privacy-policy/>.

**V: Wat is Google Authenticator?**

A: Google Authenticator is een toepassing die wordt beheerd door Google en codes biedt die kunnen worden gebruikt als een tweede authenticatiefactor om in te loggen bij andere services. Als u verificatie in 2 stappen instelt, kunt u de Google Authenticator-app gebruiken om codes te ontvangen. U kunt nog steeds codes ontvangen zonder internetverbinding of mobiele service.

**V: Welke persoonsgegevens verzamelt Google Authenticator?**

A: Google Authenticator kan persoonsgegevens verzamelen als onderdeel van het verificatieproces. AIG heeft geen toegang tot persoonsgegevens die door Google Authenticator is verzameld. Ga voor meer informatie over het privacybeleid van Google naar <https://policies.google.com/privacy>.

**V: Kan ik Okta Verify of Google Authenticator op meer dan één apparaat downloaden en activeren?**

A: Op dit moment kan Okta Verify slechts op één apparaat worden geactiveerd. Google Authenticator kan op meerdere apparaten worden gebruikt. De Google Authenticator-app moet worden gedownload op alle apparaten die u wilt gebruiken.

**V: Gebruikt Okta Verify of Google Authenticator mobiele data of vereist het extra opslag?**

A: Okta Verify gebruikt weinig data – ongeveer een paar bytes. Er is geen extra opslagruimte voor nodig. Google Authenticator vereist geen internetverbinding of mobiele verbinding en vereist geen extra opslag.

**V: Welke persoonsgegevens wordt verzameld als ik SMS- of spraakauthenticatie gebruik?**

A: Als u ervoor kiest om SMS- of spraakauthenticatie te gebruiken, worden er geen persoonsgegevens verzameld door een authenticatietoepassing, maar er worden beperkte persoonsgegevens verzameld via de Okta CIAM-oplossing om uw identiteit te verifiëren, waaronder naam, e-mailadres, telefoonnummer, unieke telefoon-ID's en IP-adres.