Autenticazione a più fattori

Domande frequenti

Generale

D: Cosa cambia?

R: L'accesso alle applicazioni AIG richiederà ora l'autenticazione a più fattori (Multi-Factor Authentication, MFA). Ciò significa che quando si accede con il proprio nome utente e password, sarà anche necessario verificare l'accesso tramite un ulteriore strumento di verifica scelto dall'utente (applicazione mobile, SMS o chiamata telefonica). Questo cambiamento sarà applicato in maniera graduale, pertanto periodicamente è possibile notare degli aggiornamenti nell'interfaccia di accesso a seconda del numero di applicazioni AIG a cui si accede.

D: Perché cambia l'esperienza di accesso?

R: AIG sta integrando un sistema di autenticazione aggiornato nell'esperienza di accesso per migliorare la sicurezza degli account online.

D: Quali metodi di autenticazione a più fattori sono disponibili per me?

R: Le opzioni di autenticazione a più fattori supportate includono le applicazioni di autenticazione mobile (attualmente Okta Verify e Google Authenticator), l'autenticazione tramite SMS o l'autenticazione tramite chiamata vocale.

D: Quale opzione di autenticazione a più fattori consiglia AIG?

R: Le opzioni MFA supportate tramite la soluzione Okta CIAM utilizzata da AIG includono l'applicazione di autenticazione mobile (attualmente Okta Verify e Google Authenticator), l'autenticazione SMS o l'autenticazione delle chiamate vocali. AIG non fornisce raccomandazioni in merito ad alcun metodo di autenticazione e gli utenti possono selezionare uno qualsiasi dei metodi supportati che si adattano alle proprie esigenze. Tieni presente che la migliore pratica per una connessione sicura consiste nell'utilizzare un'applicazione di autenticazione anziché l'autenticazione tramite SMS o chiamata vocale. Per ulteriori informazioni sulle best practice MFA, fare clic qui.

D: Posso utilizzare un'applicazione per l'autenticazione a più fattori diversa da Okta Verify o Google Authenticator?

R: Al momento, Okta Verify e Google Authenticator sono le due applicazioni di autenticazione supportate. In alternativa, è possibile scegliere di verificare l'autenticazione tramite SMS o chiamata vocale.

D: Dove posso scaricare le applicazioni di autenticazione mobile (Okta Verify, Google Authenticator)?

R: È possibile scaricare una delle applicazioni di autenticazione mobile dall'App Store (Apple) o da Google Play Store (Android). Se si sceglie di utilizzare l'autenticatore mobile Okta, assicurarsi di scaricare Okta Verify (non Okta Mobile).

D: Come faccio se non ho uno smartphone (ad es., ho un cellulare senza dati)?

R: Sono disponibili altre opzioni di autenticazione a più fattori, tra cui l'autenticazione tramite SMS o chiamata vocale, che possono essere utilizzate anche senza uno smartphone.

D: Devo scaricare e installare un'app per l'autenticazione a più fattori?

R: È necessario scaricare un ulteriore software solo se si sceglie di verificare tramite OKTA Verify o Google Authenticator. In alternativa, è anche possibile scegliere di verificare l'autenticazione tramite SMS o chiamata vocale, che non richiede l'installazione di un'app.

D: Come posso effettuare l'accesso se il cellulare non funziona o non è disponibile?

R: Per verificare ogni accesso è necessario ricorrere all'autenticazione a più fattori. Contatta l'Help Desk appropriato per reimpostare il metodo di autenticazione a più fattori.

D: Dovrò autenticarmi più di una volta se utilizzo più applicazioni AIG?

R: Non è necessario eseguire nuovamente l'autenticazione se si accede ad altre applicazioni che utilizzano lo stesso metodo di autenticazione a più fattori. Una volta eseguita l'autenticazione, è possibile accedere a tutte le applicazioni.

D: Il processo di autenticazione a più fattori cambierà alla scadenza della mia password?

R: No. Il metodo di autenticazione a più fattori non cambierà se la password scade o viene reimpostata.

D: Il processo di timeout dell'applicazione sarà diverso?

R: Il timeout dell'applicazione rimarrà lo stesso; tuttavia, sarà necessario autenticare nuovamente l'accesso utilizzando l'autenticazione a più fattori quando si effettua nuovamente l'accesso.

Autenticazione a più fattori

Domande frequenti

Informazioni specifiche sull'applicazione

D: Cos'è Okta?

R: **Okta CIAM** è una soluzione di terze parti utilizzata da AIG per autenticare gli utenti che accedono a vari sistemi e applicazioni AIG.

Okta Verify è un'applicazione di autenticazione a più fattori fornita da Okta per fornire un secondo fattore di accesso e offrire una maggiore sicurezza per la protezione degli account. Per ulteriori informazioni su Okta Verify.

D: Quali informazioni personali raccoglie Okta?

R: Al fine di autenticare l'identità di un utente, AIG utilizza la soluzione Okta CIAM per raccogliere e archiviare il nome, l'indirizzo e-mail, il numero di telefono, gli identificatori univoci del telefono e gli indirizzi IP degli utenti. Queste informazioni vengono archiviate in un ambiente cloud di Okta CIAM fino a quando l'utente avrà bisogno di accedere a un'applicazione e dovrà quindi essere autenticato per poter accedere. Ciò consente agli utenti che accedono a più applicazioni AIG di autenticare il proprio accesso una sola volta per tutte le applicazioni durante una sessione. Sono disponibili informazioni sulle pratiche di AIG in materia di privacy all'indirizzo https://www.aig.com/privacy-policy.

Okta Verify è un'applicazione distinta gestita da Okta che fornisce codici da utilizzare come secondo fattore di autenticazione per accedere ad altri servizi.

D: Quali informazioni personali sono necessarie per Okta Verify?

R: Okta Verify può raccogliere informazioni personali come parte del processo di verifica. AIG non ha accesso alle informazioni personali raccolte da Okta Verify. Sono disponibili informazioni sulla politica sulla privacy di Okta all'indirizzo https://www.okta.com/privacy-policy/.

D: Che cos'è Google Authenticator?

R: Google Authenticator è un'applicazione gestita da Google che fornisce codici da utilizzare come secondo fattore di autenticazione per accedere ad altri servizi. Se si sceglie di impostare la verifica in 2 fasi, è possibile utilizzare l'app Google Authenticator per ricevere i codici. È possibile ricevere i codici anche senza connessione a Internet o servizio di telefonia mobile.

D: Quali informazioni personali raccoglie Google Authenticator?

R: Google Authenticator può raccogliere informazioni personali come parte del processo di verifica. AIG non ha accesso alle informazioni personali raccolte da Google Authenticator. Sono disponibili informazioni sulla politica sulla privacy di Google all'indirizzo https://policies.google.com/privacy.

D: Posso scaricare e attivare Okta Verify o Google Authenticator su più di un dispositivo?

R: Attualmente, Okta Verify può essere attivato solo su un dispositivo. Google Authenticator può essere utilizzato su più dispositivi. L'app Google Authenticator deve essere scaricata su tutti i dispositivi che si desiderano utilizzare.

D: Okta Verify o Google Authenticator utilizzano dati mobili o richiedono ulteriore spazio di archiviazione?

R: Il consumo di dati di Okta Verify è minimo, nell'ordine di grandezza di pochi byte. Non richiede spazio di archiviazione aggiuntivo. Google Authenticator non richiede alcuna connessione a Internet o mobile e non è necessario alcuno spazio di archiviazione aggiuntivo.

D: Quali informazioni personali vengono raccolte se utilizzo l'autenticazione tramite SMS o chiamata vocale?

R: Se si sceglie di utilizzare l'autenticazione tramite SMS o chiamata vocale, non saranno raccolte informazioni personali da un'applicazione di autenticazione, ma saranno raccolte informazioni personali limitate tramite la soluzione Okta CIAM per autenticare l'identità dell'utente, come nome, indirizzo e-mail, numero di telefono, identificatori univoci del telefono e indirizzo IP.