Autenticación multifactor

Preguntas frecuentes

Generalidades

P: ¿Qué va a cambiar?

R: El proceso de inicio de sesión en las aplicaciones de AIG requerirá ahora autenticación multifactor (multi-factor authentication, MFA). Esto significa que cuando inicia sesión con su nombre de usuario y contraseña, también se le pedirá que verifique el inicio de sesión a través de un medio secundario de verificación de su elección (aplicación móvil, SMS o llamada telefónica). Este cambio se implementará en las aplicaciones con una estrategia por fases, por lo que podrá notar actualizaciones de la interfaz de inicio de sesión en oleadas dependiendo del número de aplicaciones de AIG a las que acceda.

P: ¿Por qué va a cambiar la experiencia de inicio de sesión?

R: AIG está integrando un sistema de autenticación actualizado en la experiencia de inicio de sesión para mejorar la seguridad de sus cuentas en línea.

P: ¿Qué métodos de MFA tengo a mi disposición?

R: Las opciones de MFA compatibles incluyen la aplicación de autenticación móvil (actualmente, Okta Verify y Google Authenticator), la autenticación por SMS o la autenticación mediante llamada de voz.

P: ¿Qué opción de MFA recomienda AIG?

R: Las opciones de MFA compatibles con la solución Okta CIAM que utiliza AIG incluyen la aplicación de autenticación móvil (actualmente, Okta Verify y Google Authenticator), autenticación por SMS o autenticación mediante llamada de voz. AIG no hace recomendaciones sobre ningún método de autenticación y los usuarios pueden seleccionar cualquiera de los métodos admitidos que se ajusten a sus necesidades. 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.

P: ¿Puedo utilizar una aplicación diferente para MFA distinta de Okta Verify o Google Authenticator?

R: En este momento, Okta Verify y Google Authenticator son las dos aplicaciones de autenticación compatibles. Como alternativa, puede seleccionar verificar la autenticación mediante mensaje SMS o una llamada de voz.

P: ¿Dónde puedo descargar las aplicaciones de autenticación móvil (Okta Verify, Google Authenticator)?

R: Puede descargar cualquiera de las aplicaciones de autenticación móvil desde App Store (apple) o Google Play Store (android). Si decide utilizar el autenticador móvil Okta, asegúrese de descargar Okta Verify (no Okta Mobile).

P: ¿Qué pasa si no tengo un teléfono inteligente (p. ej., tengo un teléfono «clamshell»)?

R: Hay otras opciones de MFA disponibles, incluida la autenticación por SMS o la autenticación mediante llamada de voz, que se pueden utilizar sin un teléfono inteligente.

P: ¿Necesito descargar e instalar una aplicación para MFA?

R: Solo es necesaria una descarga de software adicional si elige verificar mediante OKTA Verify o Google Authenticator. También puede optar por verificar mediante autenticación por SMS o autenticación mediante llamada de voz, que no requieren la instalación de una aplicación.

P: ¿Cómo iniciaré sesión si mi teléfono móvil no funciona o no está disponible?

R: Siempre tendrá que utilizar una MFA para verificar su inicio de sesión. Póngase en contacto con el servicio de asistencia técnica adecuado para restablecer el método de MFA.

P: ¿Tendré que autenticarme más de una vez si utilizo varias aplicaciones de AIG?

R: No hace falta volver a realizar la autenticación si accede a otras aplicaciones que utilizan el mismo método de MFA. Una vez que se haya autenticado, puede obtener acceso a todas las aplicaciones.

P: ¿Cambiará el proceso de MFA cuando caduque mi contraseña?

R: No. El método de MFA no cambiará si la contraseña caduca o se restablece.

P: ¿Será diferente el proceso de tiempo de espera de la aplicación?

R: El tiempo de espera de la aplicación seguirá siendo el mismo; sin embargo, tendrá que volver a autenticar el inicio de sesión utilizando la MFA cuando vuelva a iniciar sesión.

Información específica de la aplicación

P: ¿Qué es Okta?

R: **Okta CIAM** es una solución de terceros que AIG utiliza para la autenticación de usuarios para acceder a varios sistemas y aplicaciones de AIG.

Okta Verify es una aplicación de MFA que Okta proporciona para ofrecer un segundo factor para iniciar sesión y establecer una mayor garantía para la protección de su cuenta. Para obtener más información acerca de Okta Verify.

P: ¿Qué información personal recopila Okta?

R: Para autenticar la identidad de un usuario, AIG utiliza la solución Okta CIAM que recopila y almacena el nombre, la dirección de correo electrónico, el número de teléfono, los identificadores telefónicos únicos y las direcciones IP de los usuarios. Esta información se almacena en un entorno en la nube de Okta CIAM siempre que un usuario necesite acceder a una aplicación y que deba autenticarse para el acceso. Esto hace posible que los usuarios que inician sesión en varias aplicaciones de AIG solo necesiten autenticar su inicio de sesión una vez para todas las aplicaciones durante una sesión. Para obtener información sobre las prácticas de privacidad de AIG, visite https://www.aig.com/privacy-policy.

Okta Verify es una aplicación independiente administrada por Okta que proporciona códigos que se pueden utilizar como segundo factor de autenticación para iniciar sesión en otros servicios.

P: ¿Qué información personal se necesita para Okta Verify?

R: Okta Verify puede recopilar información personal como parte del proceso de verificación. AIG no tiene acceso a la información personal que Okta recopila. Para obtener más información sobre la Política de privacidad de Okta, consulte https://www.okta.com/privacy-policy/.

P: ¿Qué es Google Authenticator?

R: Google Authenticator es una aplicación administrada por Google que proporciona códigos que se pueden utilizar como segundo factor de autenticación para iniciar sesión en otros servicios. Si configura la verificación en dos pasos, puede utilizar la aplicación Google Authenticator para recibir códigos. Todavía puede recibir códigos sin conexión a Internet o servicio móvil.

P: ¿Qué información personal recopila Google Authenticator?

R: Google Authenticator puede recopilar información personal como parte del proceso de verificación. AIG no tiene acceso a la información personal recopilada por Google Authenticator. Para obtener más información sobre la Política de privacidad de Google, consulte https://policies.google.com/privacy.

P: ¿Puedo descargar y activar Okta Verify o Google Authenticator en más de un dispositivo?

R: Por el momento, Okta Verify solo se puede activar en un dispositivo. Se puede utilizar Google Authenticator en varios dispositivos. La aplicación Google Authenticator debe descargarse en todos los dispositivos que desee utilizar.

P: ¿Utilizan Okta Verify o Google Authenticator datos móviles o requieren almacenamiento adicional?

R: Okta Verify utiliza datos mínimos, en el orden de unos pocos bytes. No requiere almacenamiento adicional. Google Authenticator no requiere ninguna conexión a Internet o móvil y no requiere almacenamiento adicional.

P: ¿Qué información personal se recopila si utilizo la autenticación por SMS o por voz?

R: Si decide utilizar la autenticación por SMS o por voz, una aplicación de autenticación no recopilará ninguna información personal, pero se recopilará información personal limitada a través de la solución Okta CIAM para autenticar su identidad, incluido el nombre, dirección de correo electrónico, número de teléfono, identificadores telefónicos únicos y dirección IP.