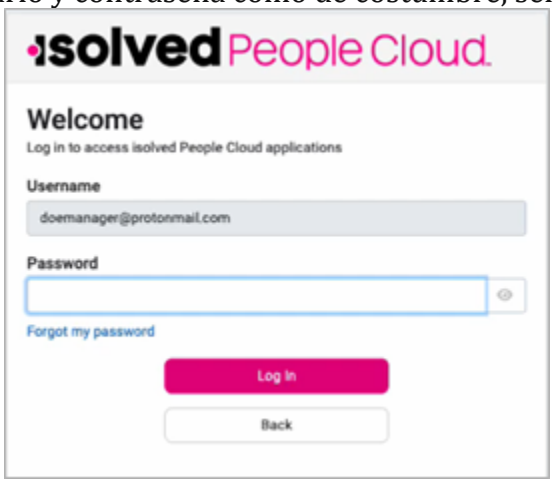
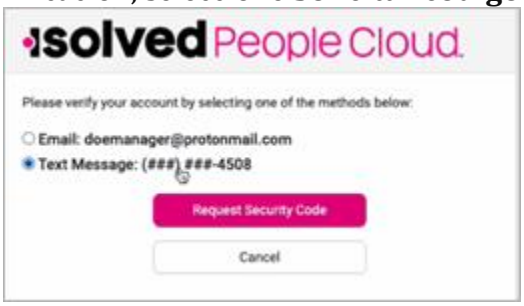
¡ATENCIÓN! El 17 de noviembre de 2023, Isolved requerirá que los usuarios utilicen una autenticación multifactor (MFA) cada vez que inicien sesión en Isolved. Esto es para proporcionar a los empleados una plataforma más segura. Por favor, lea la información importante a continuación sobre este nuevo requisito. La mayoría de los usuarios autentican su cuenta a través de correo electrónico y mensaje de texto.

Iniciar sesión

1. Ingrese su nombre de usuario y contraseña como de costumbre, seleccione **Iniciar sesión**.

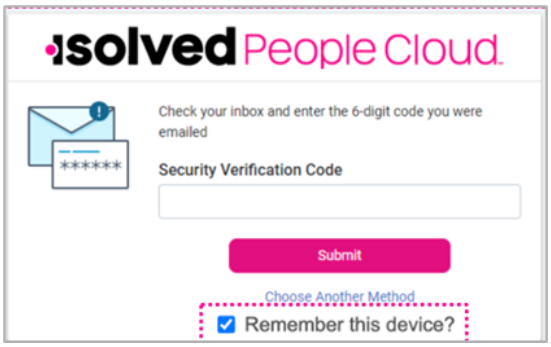


2. Seleccione una opción de verificación, seleccione **Solicitar código de seguridad.**

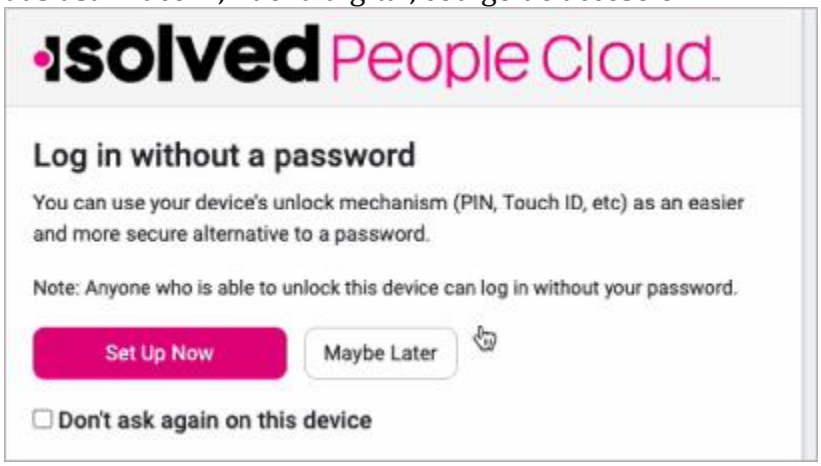


3. Use el código que recibe, o puede seleccionar **Elegir otro método** para recibir el código a la otra opción de verificación. Seleccione **Enviar**.

un. De forma predeterminada, se marcará **la opción Recordar este dispositivo**, al tener esta marcada, el sistema no requerirá MFA durante 12 horas; si no está marcada, se requerirá MFA para cada inicio de sesión



4. Haga clic en el icono **Configurar ahora** para configurar su opción sin contraseña.
   Nota: Puede realizar cambios en esto en cualquier momento cuando inicie sesión seleccionando **Mi cuenta** (**perfil** en Adaptive Employee Experience). Una vez que esto esté configurado, los inicios de sesión futuros usarán lo que ha agregado para sus opciones. Es posible que puedas usar FaceID, huella digital, código de acceso o PIN.



5. Al hacer clic en el icono **Tal vez más tarde**, podrá configurar los criterios sin contraseña más adelante. Esto no le permite omitir el proceso de autenticación multifactor.

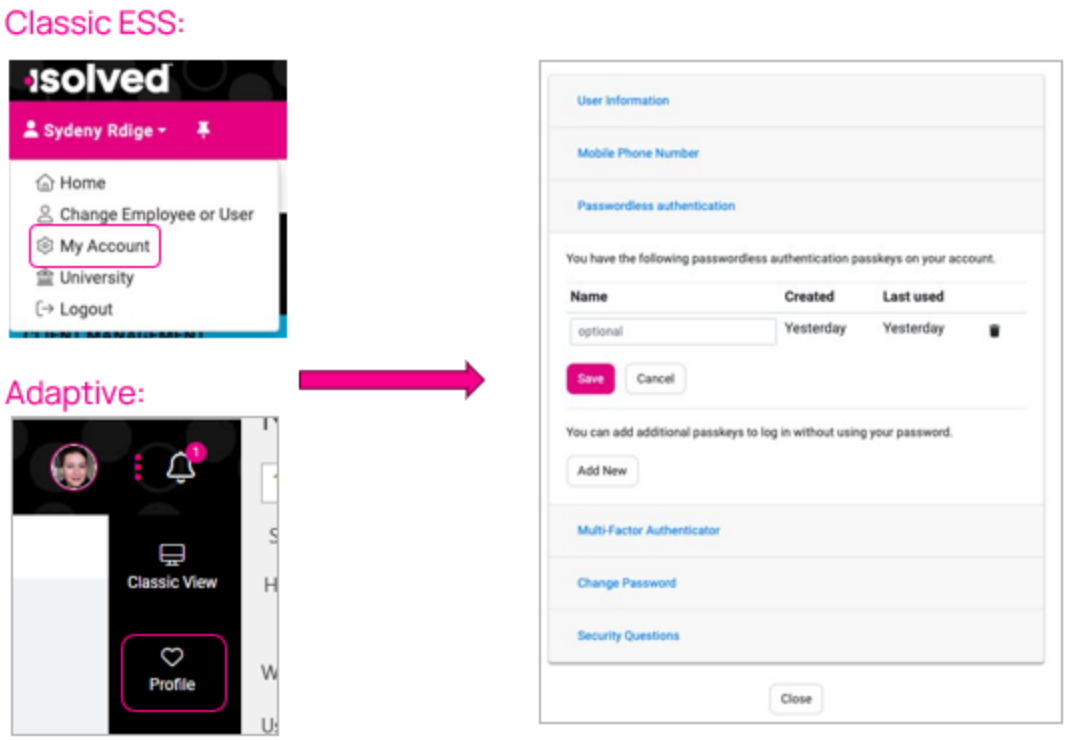
6 . **Selecciona No volver a preguntar en este dispositivo** si no quieres que este mensaje vuelva a aparecer. Esto no le permite omitir el proceso de autenticación multifactor.

7. Después de configurar su clave de acceso, cuando inicie sesión en isolved en el futuro, se le presentará la opción de usar su contraseña o usar la clave de acceso.

8. Haga clic aquí para obtener un diagrama de flujo completo de los pasos de inicio de sesión.

Gestión de MFA

Para realizar cambios, cuando haya iniciado sesión, seleccione **Mi cuenta si se encuentra en la** vista ESS clásica o Perfil si se encuentra en la experiencia adaptable del empleado.



Preguntas frecuentes

P: ¿Cuáles son las características y funcionalidades clave?

R: Ahora ofrecemos opciones de MFA fuera del correo electrónico y los mensajes de texto. MFA requiere que un usuario valide su identidad con dos o más formas de evidencia o factores cuando inicia sesión. Estamos haciendo cumplir un mínimo de dos. Un factor es algo que el usuario conoce, como su combinación de nombre de usuario y contraseña. Otros factores son los métodos de verificación que el usuario tiene en su poder.

P: ¿Puede un usuario tener acceso sin contraseña en varios dispositivos?

R: Sí, cada dispositivo permite y reconoce lo que se configuró en ese dispositivo y lo usa de forma predeterminada. Algunas opciones sin contraseña se pueden usar en varios dispositivos.

P: ¿Qué puede esperar un usuario que esto haga que no lo haga?

R: Es posible que el usuario no espere hacer esto cada vez que inicie sesión si está en el mismo dispositivo, una dirección IP registrada o ha iniciado sesión en el mismo día, sin embargo, aún debe realizar algún tipo de Preguntas frecuentes internas: Servidor de identidad de MFA independientemente. Esto podría ser diferente a lo que están acostumbrados hoy en día, dependiendo de la configuración del sistema por cliente.

P: ¿Podemos optar por no participar en la autenticación multifactor?

R: No.

P: ¿Qué es la autenticación multifactor (MFA)?

R: MFA es una forma eficaz de aumentar la protección de las cuentas de usuario contra amenazas comunes como ataques de phishing, relleno de credenciales y apropiación de cuentas.

P: ¿Cómo funciona MFA?

R: MFA agrega otra capa de seguridad a su proceso de inicio de sesión al requerir que los usuarios ingresen dos o más pruebas, o factores, para demostrar que son quienes dicen ser. Un factor es algo que el usuario conoce, como su combinación de nombre de usuario y contraseña. Otros factores son los métodos de verificación que el usuario tiene en su poder, como una aplicación de autenticación o una clave de seguridad.

P: ¿isolved requiere que los clientes habiliten MFA?

R: MFA se habilitará automáticamente para usted. Este será un requisito para todos los usuarios que accedan a isolved People Cloud.

P: ¿Por qué isolved requiere MFA?

R: No hay nada más importante que la confianza y el éxito de nuestros clientes. Entendemos que la confidencialidad, integridad y disponibilidad de los datos de cada cliente es vital para su negocio, y nos tomamos muy en serio la protección de esos datos. A medida que evoluciona el panorama global de amenazas, la implementación de estas medidas de seguridad es esencial para la seguridad y el bienestar de su empresa y sus empleados.

P: ¿Por qué isolved requiere MFA?

R: Los clientes tendrán una mayor capacidad para proteger los datos de su empresa y de sus empleados utilizando opciones adicionales para autenticarse sin problemas con una interfaz de usuario más intuitiva.

P: ¿Cuándo entra en vigor esto?

R: El requisito de MFA entra en vigor para todos los usuarios de isolved el 3 de noviembre de 2023.

P: ¿Hay algo que pueda hacer para preparar a mis empleados?

R: ¡Sí! Si bien los empleados ya tienen la opción de autenticarse usando su correo electrónico, debe alentar a TODOS los empleados a asegurarse de que también tengan un número de teléfono

registrado en su cuenta. Esto garantiza que puedan autenticarse independientemente de las nuevas opciones que hemos agregado.

P: ¿Qué impacto tendrá esto en los usuarios?

R: Ahora se pedirá a los usuarios que se autentiquen cada vez que inicien sesión, en lugar de una vez cada 30 días o cuando se identifique una nueva dirección IP.

P: ¿Cuánto duran las sesiones de usuario?

R: Si un usuario está utilizando mensajes de texto, correo electrónico o una aplicación de autenticación de terceros para MFA, en cada inicio de sesión inicial, tendrá la capacidad de "Recordar este dispositivo" u omitir MFA, durante doce (12) horas. Esto elimina la necesidad de MFA en cada inicio de sesión durante ese período de 12 horas.

NOTA: La omisión de 12 horas será la opción predeterminada, y esto no afecta a los usuarios que configuran MFA sin contraseña, ya que no se les pide que introduzcan un código. Si la omisión no está marcada, el sistema requerirá MFA después de 15 minutos de inactividad.

P: ¿Pueden los usuarios tener acceso sin contraseña en varios dispositivos?

R: Sí, cada dispositivo permite y reconoce lo que se configuró en ese dispositivo y lo usa de forma predeterminada. Algunas opciones sin contraseña se pueden usar en varios dispositivos.

P: ¿Con qué frecuencia deben los usuarios proporcionar un método de verificación al iniciar sesión directamente?

R: Como parte de esta actualización, los usuarios deberán proporcionar un método de verificación cada vez que inicien sesión en isolved.

P: ¿Qué opciones de autenticación se pueden utilizar?

Un:

- **Autenticadores de plataforma:** Verificación MFA sencilla mediante el servicio de autenticación integrado de un dispositivo móvil o de escritorio, como Windows Hello, Touch ID o Face ID.
  Nota: Cada usuario debe habilitar estas opciones nativas en el dispositivo de su elección para usarlas. Si alguien no tiene Face ID habilitado en su dispositivo, no se le pedirá que use esta opción sin fricciones.
- **Aplicaciones de autenticación de terceros:** autentícate con aplicaciones que generan códigos temporales basados en el algoritmo de contraseña de un solo uso (TOTP) basado en el tiempo de OATH. Hay muchas aplicaciones disponibles, incluidas Google Authenticator, Microsoft Authenticator y Authy.
- **Claves de seguridad de autenticación sin contraseña FIDO2:** Estos pequeños dispositivos físicos son fáciles de usar porque no hay nada que instalar ni códigos que

ingresar. Las llaves de seguridad son una gran solución si los dispositivos móviles no son una opción para los usuarios. Las llaves están disponibles en fabricantes como YubiKey.

P: ¿Afectará esto a SAML?

R: No, SAML no se ve afectado.