bitwarden | Artículo del Centro de Ayuda

MI CUENTA > INICIO DE SESIÓN EN DOS PASOS

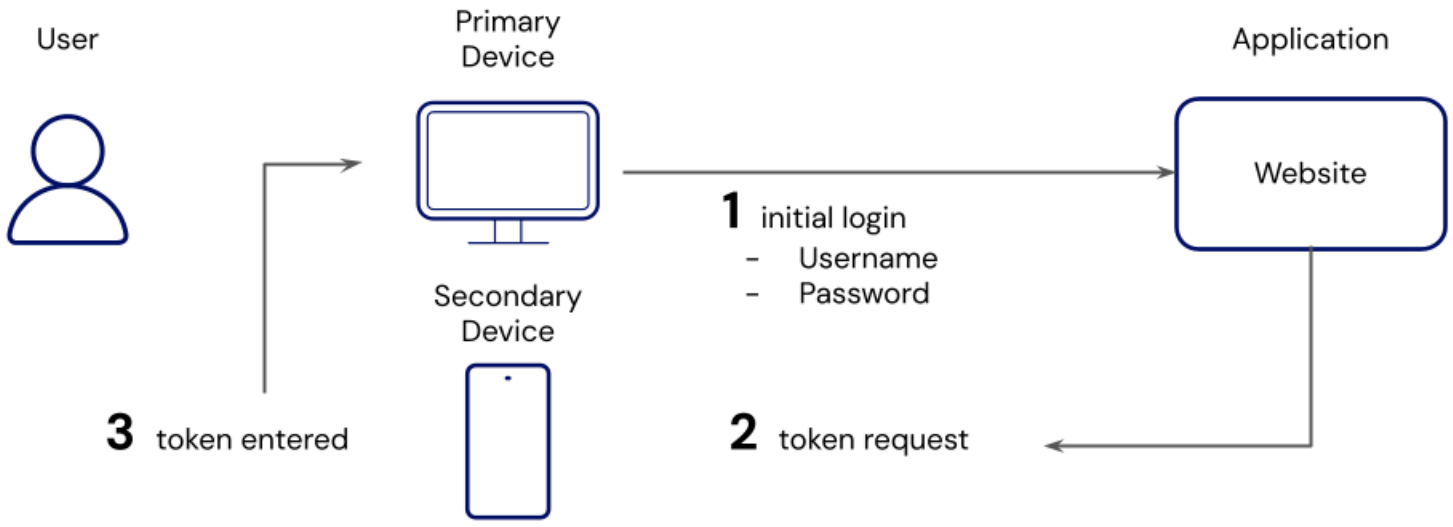
Guía de Campo para el Inicio de Sesión en Dos Pasos

Ver en el centro de ayuda:
https://bitwarden.com/help/bitwarden-field-guide-two-step-login/

Guía de Campo para el Inicio de Sesión en Dos Pasos

El inicio de sesión en dos pasos (también llamado autenticación de dos factores o 2FA) es una técnica de seguridad común utilizada por páginas web y aplicaciones para proteger tus datos sensibles. Las páginas web que utilizan inicio de sesión en dos pasos requieren que verifiques tu identidad ingresando un "token" adicional (también llamado código de verificación o contraseña de un solo uso (OTP)) además del nombre de usuario y la contraseña, generalmente obtenido de un dispositivo diferente.

Sin acceso físico al token de tu dispositivo secundario, un actor malintencionado no podría acceder a la página web, incluso si descubren tu nombre de usuario y contraseña:



Flujo básico de inicio de sesión en dos pasos

Comúnmente, las páginas web o aplicaciones con datos sensibles (por ejemplo, tu cuenta bancaria en línea) intentarán verificar tu identidad fuera de la pantalla de inicio de sesión mediante:

- Enviando un token en un SMS / mensaje de texto al dispositivo móvil en archivo.
- Solicitando un token generado por una aplicación de autenticación (por ejemplo, Authy) en tu dispositivo móvil.
- Buscando un token de una clave de seguridad física (por ejemplo, YubiKey).

¿Cómo debería usar el inicio de sesión de dos pasos?

La seguridad a menudo implica un compromiso entre protección y comodidad, ¡así que finalmente depende de ti! Generalmente, las dos formas más críticas de usar el inicio de sesión de dos pasos son:

1. Para asegurar Bitwarden

Asegure todos los datos de la caja fuerte requiriendo un paso secundario cada vez que inicie sesión en Bitwarden, además de ingresar su contraseña maestra.

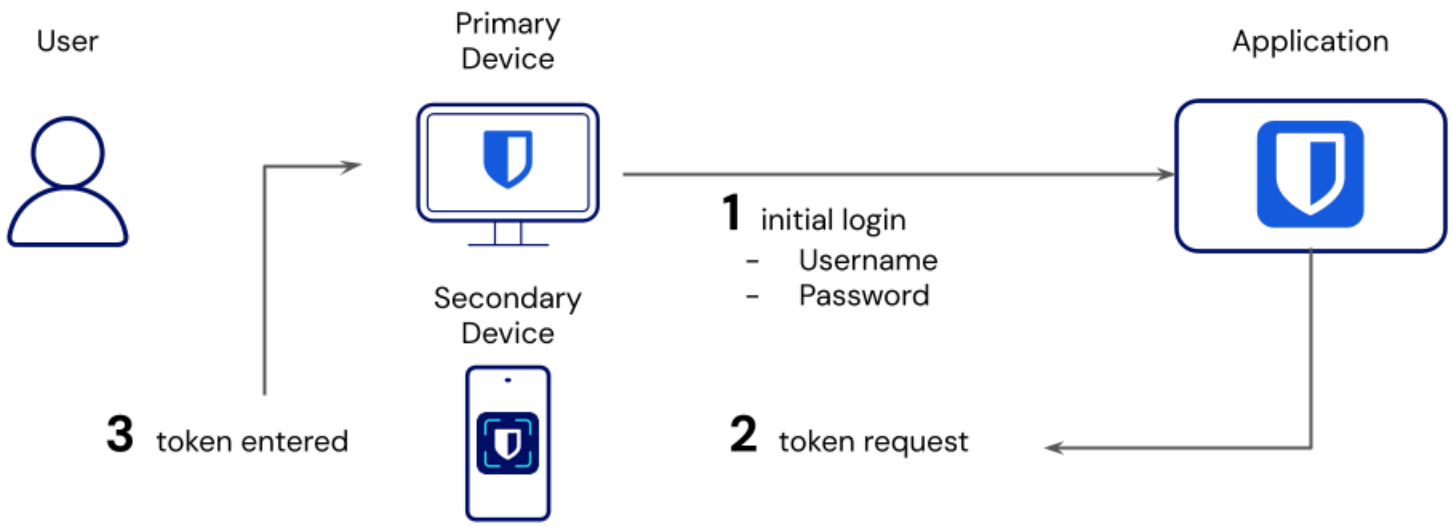
2. Para asegurar páginas web importantes

   Asegure una página web individual requiriendo una contraseña de un solo uso temporal (TOTP) cuando inicie sesión. Puedes almacenar y generar TOTPs con Bitwarden.

Asegurando Bitwarden

Dado que tu administrador de contraseñas almacena todos tus inicios de sesión, te recomendamos encarecidamente que lo asegures con inicio de sesión en dos pasos. Hacerlo protege todos tus inicios de sesión al prevenir que un actor malintencionado acceda a tu caja fuerte, incluso si descubren tu contraseña maestra.

Habilitar el inicio de sesión en dos pasos requerirá que completes un paso secundario cada vez que inicies sesión, además de tu método principal de inicio de sesión (contraseña maestra). No necesitarás completar tu segundo paso para desbloquear tu caja fuerte, solo para iniciar sesión.



Inicio de sesión de dos pasos para acceder a Bitwarden

Bitwarden ofrece varios métodos de inicio de sesión en dos pasos gratis, incluyendo:

- FIDO (cualquier llave certificada por FIDO2 WebAuthn)
- a través de una aplicación de autenticación (por ejemplo, 2FAS, Ravio, o Aegis)
- vía correo electrónico

Para los usuarios Premium, Bitwarden ofrece varios métodos avanzados de inicio de sesión en dos pasos:

- Duo Security con Duo Push, SMS, llamada telefónica y claves de seguridad
- YubiKey (cualquier dispositivo de la serie 4/5 o YubiKey NEO/NFC)

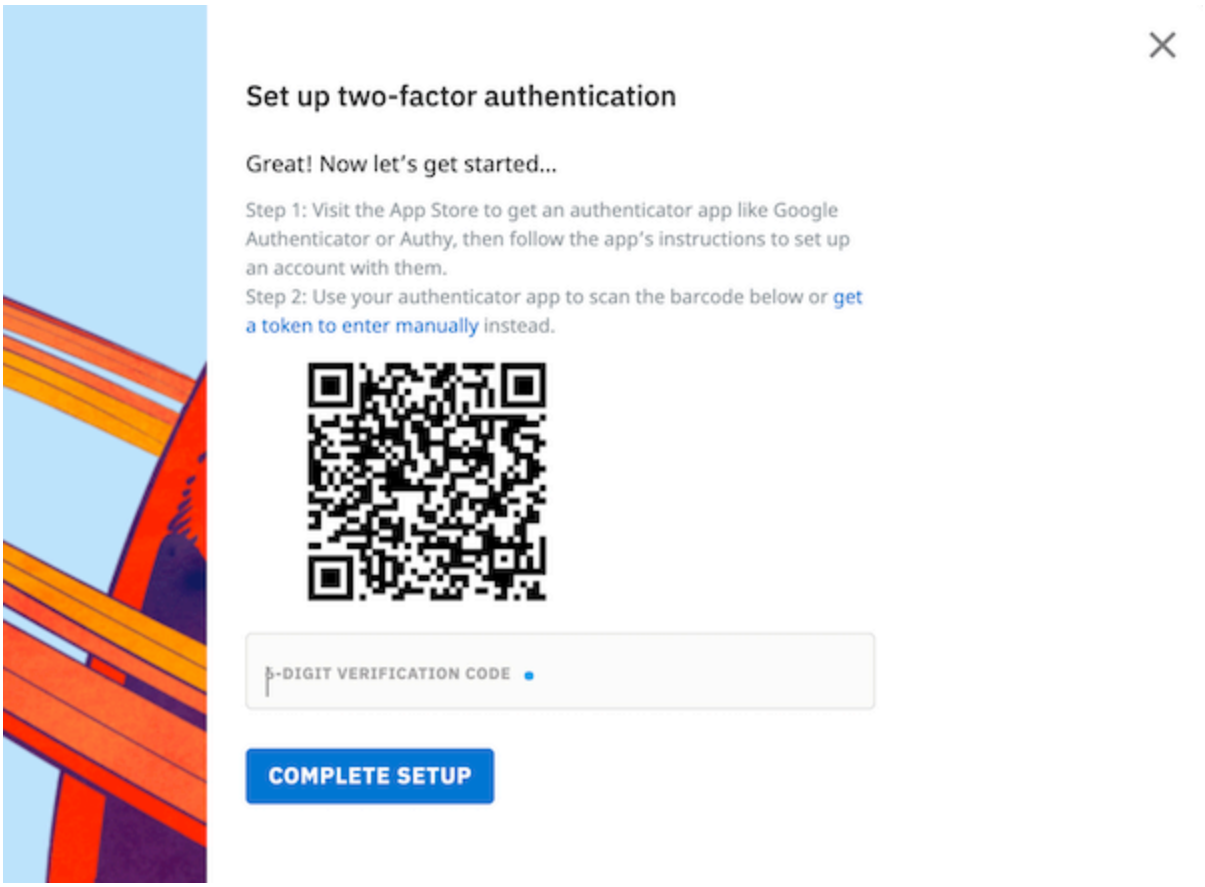
Aprende más sobre tus opciones o recibe ayuda para configurar cualquier método usando nuestras **Guías de Ajustes.**

> **Note**
> Bitwarden no admite 2FA por SMS debido a vulnerabilidades, incluyendo la usurpación de SIM. No recomendamos SMS 2FA para otras cuentas a menos que sea el único método disponible. Cualquier segundo factor es recomendado sobre no tener ninguno, pero la mayoría de las alternativas son más seguras que el 2FA SMS.

Asegurando páginas web importantes

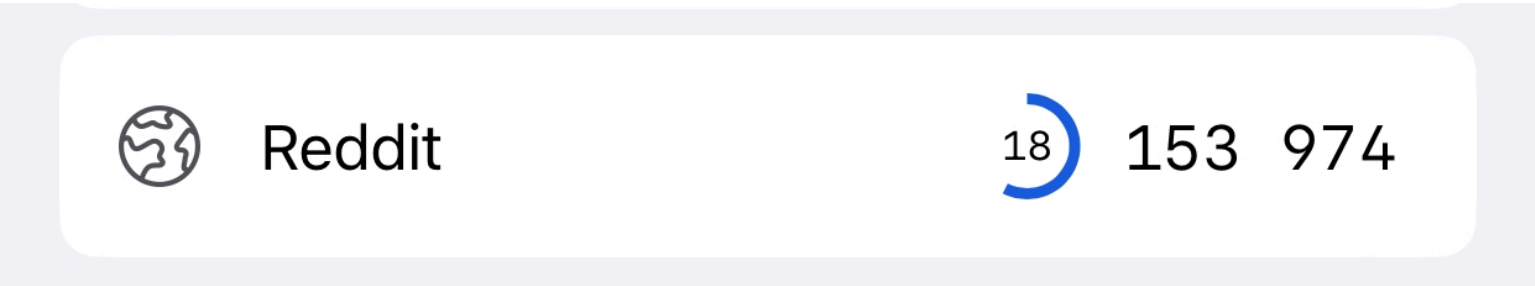
Muchas otras páginas web y aplicaciones tienen opciones de inicio de sesión en dos pasos, esto es especialmente común para páginas web que almacenan información sensible (por ejemplo, números de tarjeta de crédito o números de cuenta bancaria). La opción de inicio de sesión en dos pasos de la mayoría de las páginas web se encontrará en los menús de **Ajustes**, **Seguridad** o **Privacidad**.

La activación del inicio de sesión de dos pasos normalmente abrirá un código QR, como este ejemplo de Reddit:



Código QR de 2FA

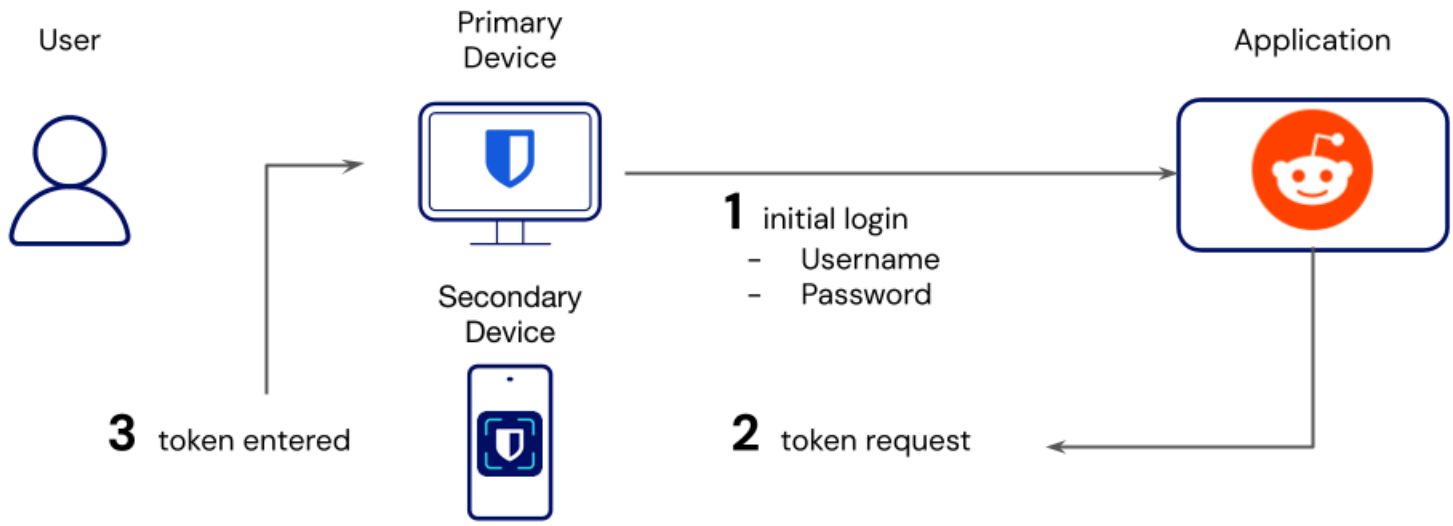
Al escanear este código con una aplicación de autenticación, la aplicación podrá generar tokens de seis dígitos rotativos que puedes usar para verificar tu identidad, como este generado por Authy:



TOTP Token

Usa Authy

Para configurar el inicio de sesión en dos pasos para Reddit usando Authy, toca el botón **Agregar Cuenta** y escanea el código QR presentado por tu página web o aplicación. Escanear el código QR generará tu token de seis dígitos. Ingrese este código en el cuadro de entrada **Código de Verificación** para terminar de configurar.



Inicio de sesión en dos pasos usando Authy

Normalmente, se te dará la opción de descargar códigos de recuperación. Descargar los códigos de recuperación es fundamental para evitar que pierdas el acceso a tus tokens de inicio de sesión de dos pasos, incluso si pierdes el dispositivo en el que está instalado Authy.

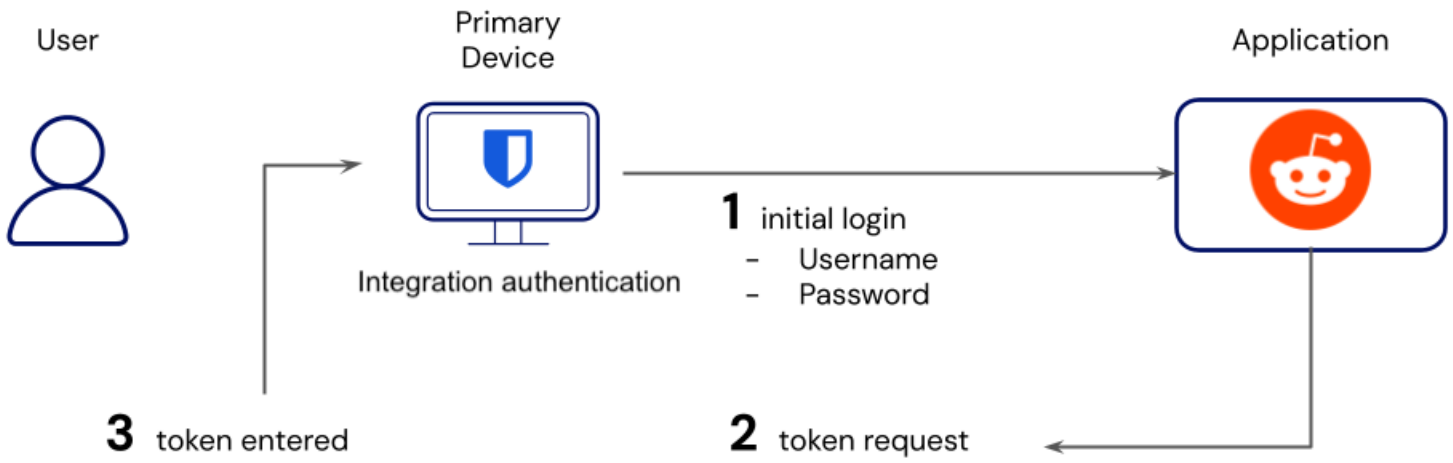
La próxima vez que inicies sesión en Reddit, se te requerirá verificar tu identidad ingresando un código de verificación de Authy. Los códigos de verificación rotan cada 30 segundos, por lo que será imposible para un actor malintencionado descubrir tu código sin acceso físico a tu dispositivo.

> **Note**
>
> Authy es nuestra aplicación de autenticación recomendada porque incluye copias de seguridad para cualquier dispositivo. Las copias de seguridad te previenen de perder acceso a tus tokens, incluso si pierdes el dispositivo en el que está instalado Authy. Activa el interruptor de **Copias de seguridad del Autenticador** en la pantalla de **Cuentas** de la aplicación Authy para usar esta funcionalidad.
>
> Otras aplicaciones de autenticación incluyen Google Authenticator y FreeOTP, y a partir del 7 de mayo de 2020, Google Authenticator incluye portabilidad de código de verificación en dispositivos Android.

Usa el autenticador de Bitwarden

Como alternativa a Authy, Bitwarden ofrece un autenticador integrado para usuarios Premium, incluyendo miembros de organizaciones pagadas (familias, Equipos o empresas).

Bitwarden para iOS y Android puede escanear códigos QR y generar tokens de seis dígitos al igual que otras aplicaciones de autenticación. Usar el autenticador de Bitwarden para asegurar una página web guardará un token rotativo de seis dígitos con ese elemento de inicio de sesión en la caja fuerte. También puedes guardar manualmente tu secreto de código de verificación en un elemento de caja fuerte desde cualquier aplicación de Bitwarden.



Inicio de sesión en dos pasos usando Bitwarden

Aprende cómo usar el autenticador de Bitwarden.

¿Por qué usar el autenticador de Bitwarden?

Comprensiblemente, algunos usuarios son escépticos acerca de usar Bitwarden para la autenticación de token. Recuerda, la seguridad a menudo implica un equilibrio entre protección y conveniencia, por lo que la mejor solución depende de ti. Generalmente, las personas

que usan el autenticador de Bitwarden lo hacen por dos razones:

1. **Conveniencia**

   Cuando usas las aplicaciones móviles de Bitwarden o las extensiones de navegador para autocompletar un nombre de usuario y contraseña, automáticamente copiará el código de verificación a tu portapapeles para facilitar su pegado.

   Si estás utilizando una extensión de navegador, puedes encadenar el atajo de teclado de inicio de sesión (Windows: `Ctrl + Shift + L` / macOS: `Cmd + Shift + L`), seguido del atajo de pegar (Windows: `Ctrl + V` / macOS: `Cmd + V`) para inicios de sesión rápidos como un rayo.

2. **Compartiendo**

   Para las organizaciones, un gran beneficio de usar el autenticador de Bitwarden para la verificación de tokens es la capacidad de compartir la generación de tokens entre los miembros del equipo. Esto permite a las organizaciones proteger sus cuentas con inicio de sesión de dos pasos sin sacrificar la capacidad para que varios usuarios accedan a esa cuenta o requieran coordinación entre dos empleados para compartir tokens de una manera insegura.

Claves de seguridad 2FA y contraseñas

Las claves de seguridad FIDO2 son una opción popular y segura para agregar 2FA a tu cuenta de Bitwarden. Si no está familiarizado con las claves de seguridad FIDO2, consulte la página web de la Alianza FIDO para obtener información adicional sobre FIDO2.

Un dispositivo YubiKey es una clave de seguridad que funciona con los protocolos de autenticación FIDO, y puede tener varios casos de uso. Dos usos son como claves de seguridad 2FA, o llaves de paso.

- **Clave de seguridad 2FA:** Usar un YubiKey como clave de seguridad 2FA actuará como un dispositivo adicional en el proceso de autenticación. Esto irá acompañado de otro método principal de autenticación (como la contraseña maestra). La clave de seguridad YubiKey debe estar físicamente conectada para proporcionar las credenciales de autenticación.

- **Clave de paso:** Una clave de paso es un par de claves criptográficas públicas-privadas que se utilizan para autenticar un inicio de sesión. En lugar de crear un nombre de usuario, contraseña y agregar 2FA a una cuenta, se utiliza la llave única. Durante la creación de la clave de acceso, la YubiKey es capaz de funcionar como el generador de claves de acceso para generar las claves públicas y privadas necesarias para el inicio de sesión de la clave de acceso. Aprende más sobre cómo usar un YubiKey como llave de paso aquí.

Con Bitwarden, el uso principal de una clave de seguridad como un dispositivo YubiKey es proporcionar autenticación 2FA.

Próximos pasos

Ahora que eres un experto en inicio de sesión de dos pasos, recomendamos:

- Configura el inicio de sesión de dos pasos
- Obtén Premium para acceder a métodos avanzados de inicio de sesión en dos pasos
- Configura el autenticador de Bitwarden
- Configura el inicio de sesión de dos pasos para Equipos y empresas