bitwarden | Artículo del Centro de Ayuda

PASSWORD MANAGER > ADMINISTRACIÓN DE CÁMARAS ACORAZADAS

Informes sanitarios de las cámaras acorazadas

Ver en el centro de ayuda:
https://bitwarden.com/help/reports/

Informes sanitarios de las cámaras acorazadas

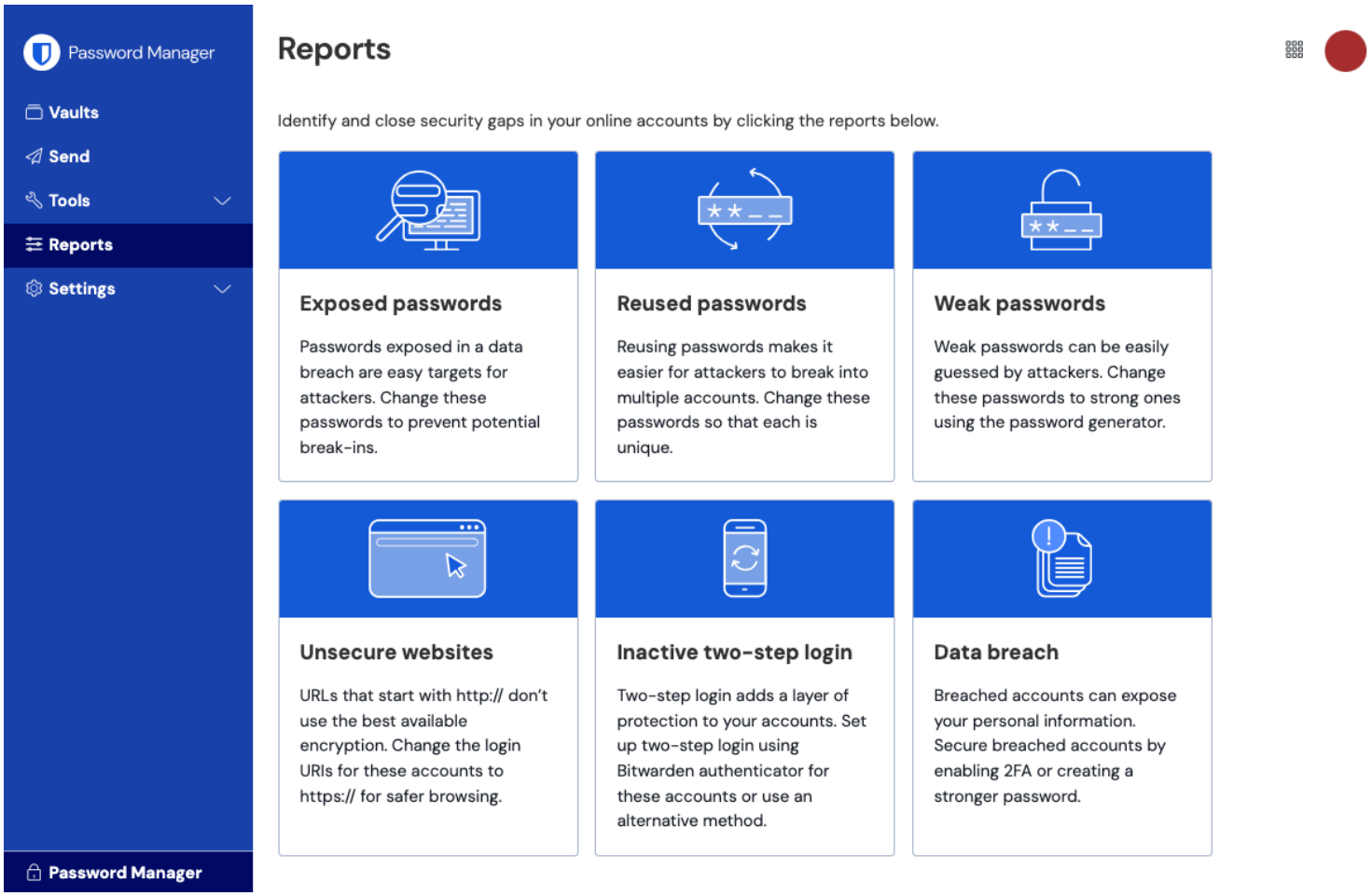
Los informes de salud de la caja fuerte pueden utilizarse para evaluar la seguridad de su caja fuerte individual o de organización de Bitwarden. Los informes, por ejemplo el informe de Contraseñas Reutilizadas y Contraseñas Débiles, se ejecutan localmente en su cliente. Esto permite identificar elementos ofensivos, sin que Bitwarden tenga nunca acceso a versiones no cifradas de estos datos.

> **Note**
>
> La mayoría de los informes de estado de la bóveda solo están disponibles para usuarios premium, incluidos los miembros de organizaciones pagas (familias, equipos o empresas), pero el informe de violación de datos es gratuito para todos los usuarios.

Ver un informe

Para ejecutar cualquier informe de salud de la caja fuerte para su **caja fuerte individual**:

1. Inicia sesión en la aplicación web y selecciona **Informes** desde la navegación:



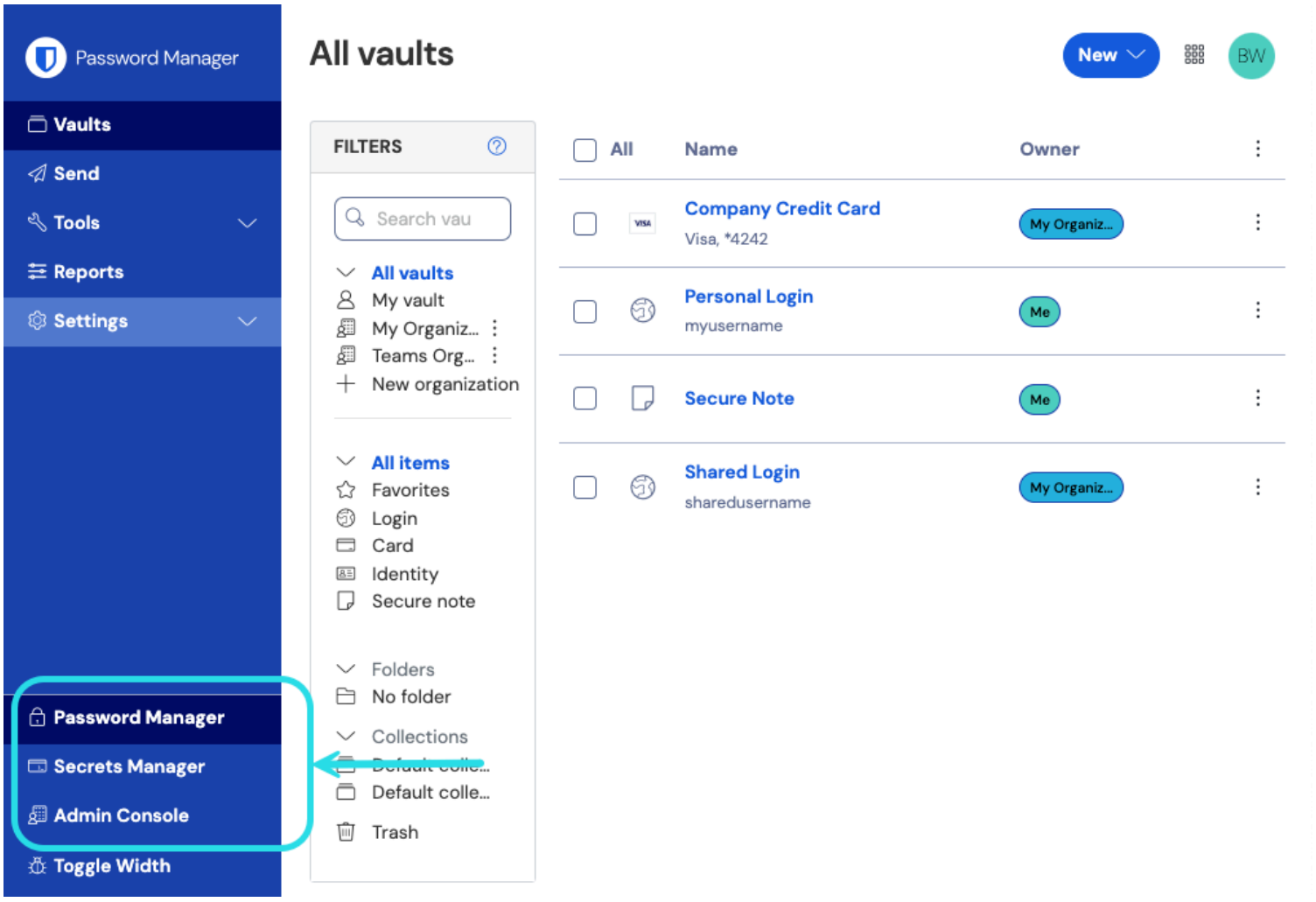
Página de informes

2. Elija un informe para ejecutar.

Para ejecutar cualquier informe de salud de la caja fuerte para la caja fuerte de su **organización**:

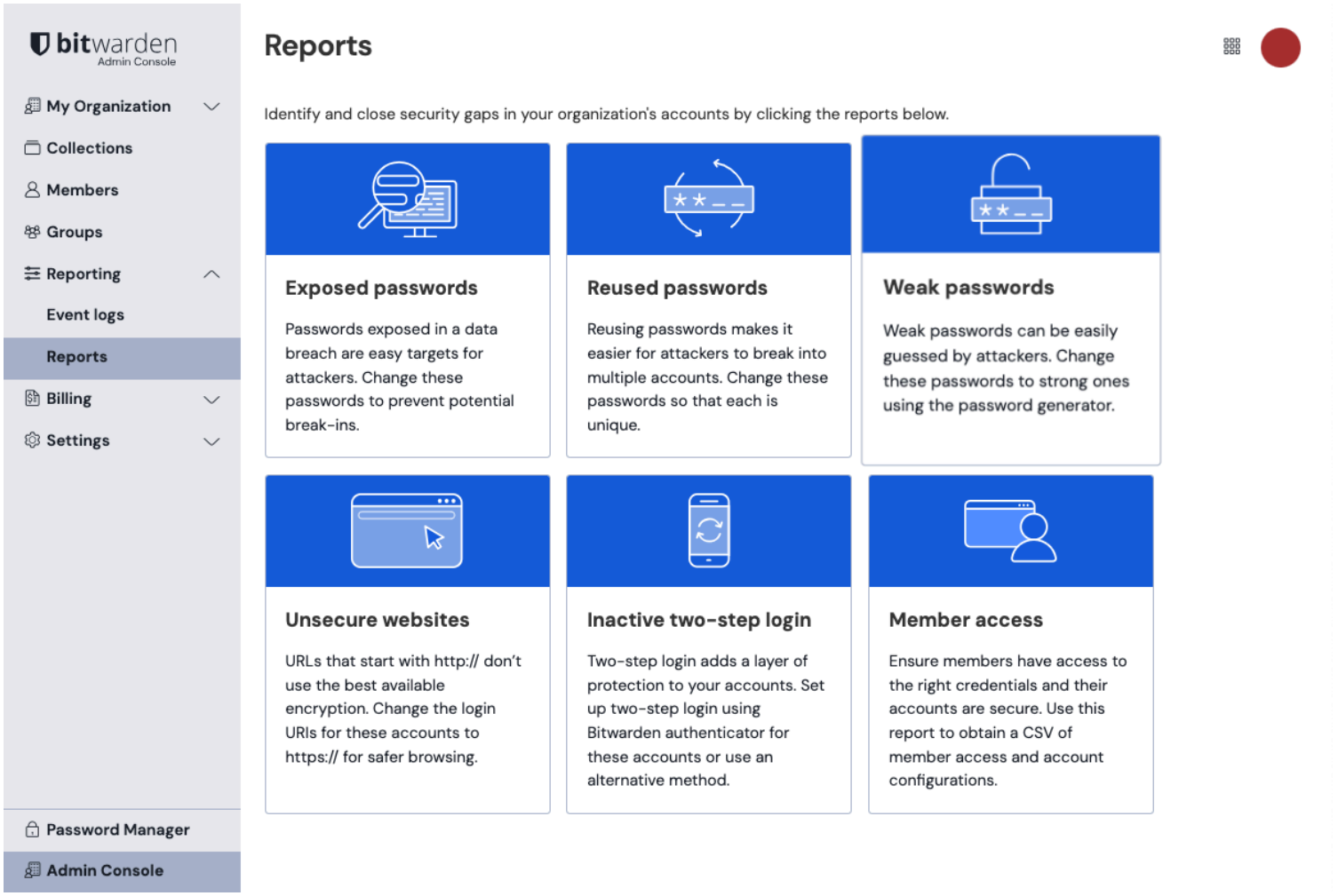
1. Inicia sesión en la aplicación web de Bitwarden.

2. Abra la Consola de Administrador utilizando el conmutador de producto (⊞):



Selector de producto

3. En su organización, seleccione **Informe** → **Informes** desde la navegación.



Informes de organización

4. Elija un informe para ejecutar.

Informes disponibles

Informe de contraseñas comprometidas

El informe de Contraseñas Comprometidas identifica contraseñas que han sido descubiertas en conocidas filtraciones de datos que fueron publicadas públicamente o vendidas en la web oscura por hackers.

Este informe utiliza un servicio web de confianza para buscar los primeros cinco dígitos del hash de todas sus contraseñas en una base de datos de contraseñas filtradas conocidas. La lista de coincidencias de hashes devuelta se compara localmente con el hash completo de tus contraseñas. Esa comparación solo se realiza localmente para preservar tu k-anonimato.

Una vez identificado, deberías crear una nueva contraseña para las cuentas o servicios ofensivos.

> **Tip**
>
> ¿Por qué usar los primeros cinco dígitos de los hashes de contraseña?
>
> Si el informe se realizó con tus contraseñas actuales, no importa si estuvieron comprometidas o no, estarías filtrándolas voluntariamente al servicio. El resultado de este informe puede no significar que su cuenta ha sido comprometida, sino que está utilizando una contraseña que se ha encontrado en estas bases de datos de contraseñas comprometidas, sin embargo, debe evitar usar contraseñas filtradas y no únicas.

Informe de contraseñas reutilizadas

El informe de Contraseñas Reutilizadas identifica contraseñas no únicas en tu caja fuerte. Reutilizar la misma contraseña para varios servicios puede permitir a los hackers obtener fácilmente acceso a más de tus cuentas en línea cuando se viola un servicio.

Una vez identificado, debes crear una contraseña única para las cuentas o servicios ofensivos.

Informe de contraseñas débiles

El informe de Contraseñas Débiles identifica contraseñas débiles que pueden ser adivinadas fácilmente por hackers y herramientas automatizadas que se utilizan para descifrar contraseñas, ordenadas por la gravedad de la debilidad. Este informe utiliza zxcvbn para el análisis de la fuerza de la contraseña.

Una vez identificado, deberías usar el generador de contraseñas de Bitwarden para generar una contraseña fuerte para las cuentas o servicios ofensivos.

Informe de sitios web no seguros

El informe de sitios web no seguros identifica elementos de inicio de sesión que utilizan esquemas no seguros (`http://`) en las URI. Es mucho más seguro usar `https://` para cifrar las comunicaciones con TLS/SSL. Para aprender más, vea usando URIs.

Una vez identificados, deberías cambiar los URI ofensivos de `http://` a `https://`.

Informe de 2FA inactivo

El informe de 2FA inactivo identifica elementos de inicio de sesión donde:

- La autenticación de dos factores (2FA) a través de TOTP está disponible desde el servicio.
- No has almacenado una clave de autenticador TOTP.

La autenticación de dos factores (2FA) es un importante paso de seguridad que ayuda a proteger tus cuentas. Si cualquier sitio web lo ofrece, siempre deberías activar el 2FA. Los elementos ofensivos se identifican al cruzar los Datos-URI con los datos de https://2fa.directory/.

Una vez identificado, configure 2FA utilizando el hipervínculo `Instrucciones` para cada elemento ofensivo:

Instrucciones del Informe

Informe de filtración de datos (solo cajas fuertes individuales)

El informe de filtración de datos identifica los datos comprometidos (direcciones de correo electrónico, contraseñas, tarjetas de crédito, fecha de nacimiento y más) en filtraciones conocidas, utilizando un servicio llamado Have I Been Pwned (HIBP).

Cuando creas una cuenta de Bitwarden, tendrás la opción de ejecutar este informe en tu contraseña maestra antes de decidir usarla. Para ejecutar este informe, se envía un hash de tu contraseña maestra a HIBP y se compara con los hashes comprometidos almacenados. Tu contraseña maestra nunca es comprometida por Bitwarden.

Una "violación" se define según HIBP como "un incidente donde los datos se exponen inadvertidamente en un sistema comprometido, generalmente debido a controles de acceso insuficientes o debilidades de seguridad en el software". Para obtener más información, consulte la documentación de preguntas frecuentes de HIBP.

ⓘ Note

Si está autoalojando Bitwarden, para ejecutar el informe de filtración de datos en su instancia, necesitará comprar una clave de suscripción HIBP que le autorizará a realizar llamadas a la API, obtenida aquí.

Una vez que tenga la clave, abra su `./bwdata/env/global.override.env` y REEMPLACE el valor de los marcadores de posición para `globalSettings__hibpApiKey` con su clave API comprada:

```Bash
globalSettings__hibpApiKey=REPLACE
```

Para obtener más información, consulte configurar variables de entorno.