bitwarden | Artículo del Centro de Ayuda

SEGURIDAD

Cifrado

Ver en el centro de ayuda:
https://bitwarden.com/help/what-encryption-is-used/

Cifrado

Bitwarden utiliza encriptación AES-CBC de 256 bits para los datos de tu caja fuerte, y PBKDF2 SHA-256 o Argon2 para derivar tu clave de encriptación.

Bitwarden **siempre** encripta y/o hashea tus datos en tu dispositivo local antes de que se envíe algo a los servidores en la nube para su almacenamiento. **Los servidores de Bitwarden solo se utilizan para almacenar datos cifrados.** Para obtener más información, consulte Almacenamiento.

Los datos de la caja fuerte solo pueden ser descifrados utilizando la clave derivada de su contraseña maestra. Bitwarden es una solución de cifrado de conocimiento cero, lo que significa que usted es la única parte con acceso a su clave y la capacidad de descifrar los datos de su caja fuerte.

> **Tip**
>
> Le animamos a visitar nuestra Página de Criptografía Interactiva para que vea por sí mismo cómo Bitwarden cifra sus datos.
>
> Si desea aprender más sobre cómo se utilizan estas claves de cifrado para proteger su caja fuerte, también puede consultar nuestro Libro Blanco de Seguridad.

AES-CBC

AES -CBC (encadenamiento de bloques de cifrado) , utilizado para cifrar datos de bóvedas, es un estándar en criptografía y lo utilizan el gobierno de EE. UU. y otras agencias gubernamentales de todo el mundo para proteger datos ultrasecretos. Con una implementación adecuada y una clave de cifrado fuerte (tu contraseña maestra), se considera que AES es irrompible.

PBKDF2

PBKDF2 SHA-256 se utiliza para derivar la clave de cifrado de su contraseña maestra, sin embargo, puede elegir Argon2 como una alternativa. Bitwarden sal y cifra su contraseña maestra con su correo electrónico **localmente**, antes de la transmisión a nuestros servidores. Una vez que un servidor de Bitwarden recibe la contraseña cifrada, se sala de nuevo con un valor aleatorio criptográficamente seguro, se cifra de nuevo y se almacena en nuestra base de datos.

El recuento de iteraciones predeterminado utilizado con PBKDF2 es de 600,001 iteraciones en el cliente (el recuento de iteraciones del lado del cliente se puede configurar desde los ajustes de su cuenta), y luego 100,000 iteraciones adicionales cuando se almacena en nuestros servidores (para un total de 700,001 iteraciones por defecto). La clave de la organización se comparte a través de RSA-2048.

> **Tip**
>
> El número de iteraciones predeterminadas utilizadas por Bitwarden se incrementó en febrero de 2023. Las cuentas creadas después de ese momento usarán 600,001, sin embargo, si creaste tu cuenta antes de entonces, deberías aumentar el recuento de iteraciones. Las instrucciones para hacerlo se pueden encontrar en la siguiente sección.

Las funciones hash utilizadas son hashes unidireccionales, lo que significa que nadie en Bitwarden puede **revertir su ingeniería** para revelar su contraseña maestra. Incluso si Bitwarden fuera hackeado, no habría ningún método por el cual se podría obtener su contraseña maestra.

Cambiando Iteraciones KDF

Bitwarden utiliza un valor predeterminado seguro, como se mencionó anteriormente, sin embargo, puedes cambiar el conteo de iteraciones desde el menú **Ajustes** → **Seguridad** → **Claves** de la caja fuerte web.

Cambiar el recuento de iteraciones puede ayudar a proteger su contraseña maestra de ser forzada bruscamente por un atacante, sin embargo, no debe ser visto como un sustituto para usar una contraseña maestra fuerte en primer lugar. Cambiar el conteo de iteraciones volverá a cifrar la clave simétrica protegida y actualizará el hash de autenticación, muy similar a un cambio normal de contraseña maestra,

pero no rotará la clave de cifrado simétrico, por lo que los datos de la caja fuerte no serán cifrados de nuevo. Vea aquí para obtener información sobre cómo volver a cifrar sus datos.

Establecer tus iteraciones KDF demasiado altas podría resultar en un rendimiento deficiente al iniciar sesión (y desbloquear) Bitwarden en dispositivos con CPUs más lentos. Recomendamos que aumente el valor en incrementos de 100,000 y luego pruebe todos sus dispositivos.

Cuando cambias el recuento de iteraciones, se cerrará sesión en todos los clientes. Aunque el riesgo involucrado en rotar su clave de cifrado no existe al cambiar el recuento de Iteraciones KDF, aún recomendamos exportar su caja fuerte de antemano.

Argon2id

Argon2, el ganador de la Competencia de Hashing de Contraseñas de 2015, está disponible como una alternativa a PBKDF2 (aprende más). Hay tres versiones del algoritmo, y Bitwarden ha implementado Argon2id como recomendado por OWASP. Argon2id es una combinación de otras versiones, utilizando una combinación de accesos a la memoria dependientes e independientes de los datos, lo que le da parte de la resistencia de Argon2i a los ataques de temporización de caché de canal lateral y gran parte de la resistencia de Argon2d a los ataques de cracking de GPU (fuente).

Por defecto, Bitwarden está configurado para asignar 64 MiB de memoria, iterar sobre ella 3 veces y hacerlo en 4 hilos. Estos valores predeterminados están por encima de las recomendaciones actuales de OWASP, pero aquí hay algunos consejos en caso de que decidas cambiar tus ajustes:

- Aumentar las **Iteraciones KDF** aumentará el tiempo de ejecución de manera lineal.
- La cantidad de **Paralelismo KDF** que puedes usar depende de la CPU de tu máquina. Generalmente, Max. Paralelismo = Número de Núcleos x 2.

> **Note**
>
> Los usuarios de Argon2id con un valor de memoria KDF superior a 48 MB recibirán un diálogo de advertencia cada vez que se inicie el relleno automático de iOS o se cree un nuevo Enviar a través de la hoja de Compartir. Para evitar este mensaje, ajuste los ajustes de Argon2id o habilite desbloquear con biométrica.

Invocadas bibliotecas criptográficas

Bitwarden no escribe ningún código criptográfico. Bitwarden solo invoca cripto de bibliotecas cripto populares y de buena reputación que están escritas y mantenidas por expertos en criptografía. Se utilizan las siguientes bibliotecas de criptografía:

- JavaScript (Caja fuerte web, extensión de navegador, escritorio, e ILC)
  - Cripto web
  - Node.js cripto
  - Herrería
- C# (Móvil)
  - CommonCrypto (iOS, Apple)
  - Javax.Crypto (Android, Oracle)
  - BouncyCastle (Android)