CONSOLA DE ADMINISTRADOR > GESTIÓN DE USUARIOS

Resumen de Incorporación y Sucesión

Resumen de Incorporación y Sucesión

> **Tip**
> Read the full paper below or download the PDF.

Gestión de contraseñas para adaptarse a su negocio

Hacer que los nuevos empleados se pongan en marcha rápidamente impulsa la productividad. Asimismo, despedirse correctamente impulsa la confianza en la seguridad de los sistemas y cuentas de su negocio. Ya sea que su negocio se incline hacia la consolidación y centralización, o prefiera un entorno flexible y dinámico, Bitwarden se adapta a sus necesidades.

Esta guía cubre el enfoque de Bitwarden para la incorporación y planificación de sucesión para los miembros de su organización, comenzando con nuestro enfoque de la relación entre los miembros y las organizaciones, luego cubriendo los casos de uso más simples para la incorporación y sucesión, y finalmente avanzando hacia las palancas y opciones a su disposición para adaptar Bitwarden a sus necesidades.

El enfoque de Bitwarden

La visión de Bitwarden es imaginar un mundo donde nadie sea hackeado. Llevamos esto adelante en nuestra misión de ayudar a individuos y empresas a gestionar su información sensible de manera fácil y segura. Bitwarden cree que:

- La gestión básica de contraseñas para individuos puede y debe ser **gratis**. Proporcionamos justo eso, una cuenta básica gratis para individuos.
- Los individuos y las familias deben desempeñar un rol activo en su seguridad utilizando TOTPs, acceso de emergencia y otras funcionalidades de seguridad de apoyo.
- Las organizaciones pueden mejorar enormemente su perfil de seguridad a través de la gestión de contraseñas organizacionales y el intercambio seguro.

> **Tip**
> For Bitwarden, different plans and options are connected and complementary, all originating in our vision of a hack-free world. Empowering everyone at work **and** at home with password management gets us one step closer to that goal.

Un aspecto clave de Bitwarden es que, a diferencia de muchas aplicaciones de software, todo en cada caja fuerte está cifrado de extremo a extremo. Para mantener este modelo de seguridad, cada persona que usa Bitwarden debe tener una cuenta única con una contraseña maestra única. Las contraseñas maestras deben ser **fuertes** y **memorables**.

Cada usuario está a cargo de su contraseña maestra. Bitwarden es una solución de cifrado de cero conocimiento, lo que significa que el equipo de Bitwarden, así como los propios sistemas de Bitwarden, no tienen conocimiento de, forma de recuperar, o forma de restablecer ninguna contraseña maestra.

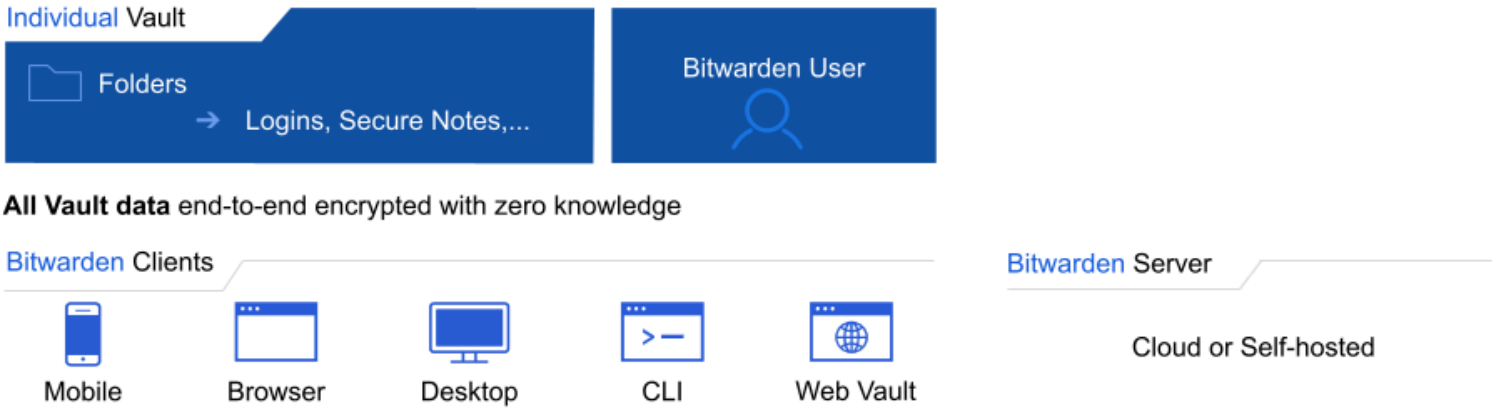
Usa Bitwarden en cualquier lugar

La seguridad en todas partes significa seguridad en cualquier lugar, por lo tanto, los mejores administradores de contraseñas proporcionan acceso en todos tus dispositivos. Bitwarden admite una gama de aplicaciones cliente, cualquiera de las cuales se puede conectar a nuestros servidores alojados en la nube o a un servidor autoalojado propio:

Bitwarden Clients/Servers

Las cajas fuertes individuales de los usuarios

Cualquiera que cree una cuenta de Bitwarden tendrá su propia caja fuerte individual. Accesible desde cualquier aplicación de cliente, las cajas fuertes individuales son únicas para cada usuario y solo ese usuario tiene la llave para acceder a ella, utilizando una combinación de su correo electrónico y contraseña maestra. Las cuentas personales, y los elementos de la caja fuerte almacenados en ellas, son responsabilidad del propietario de la cuenta. Los propietarios, administradores y gerentes de la organización no pueden ver la caja fuerte individual de ningún otro usuario por diseño, garantizando que los datos de la caja fuerte individual de alguien permanezcan siendo suyos.



Personal Vaults

Las organizaciones de Familias, Equipos y Empresa proporcionan automáticamente a los miembros individualmente con funcionalidades premium, como acceso de emergencia y almacenamiento de archivos adjuntos cifrados, que pueden elegir usar. Los datos en una caja fuerte individual pertenecen al usuario. Las bóvedas individuales no permiten compartir, las organizaciones sí .

Tip

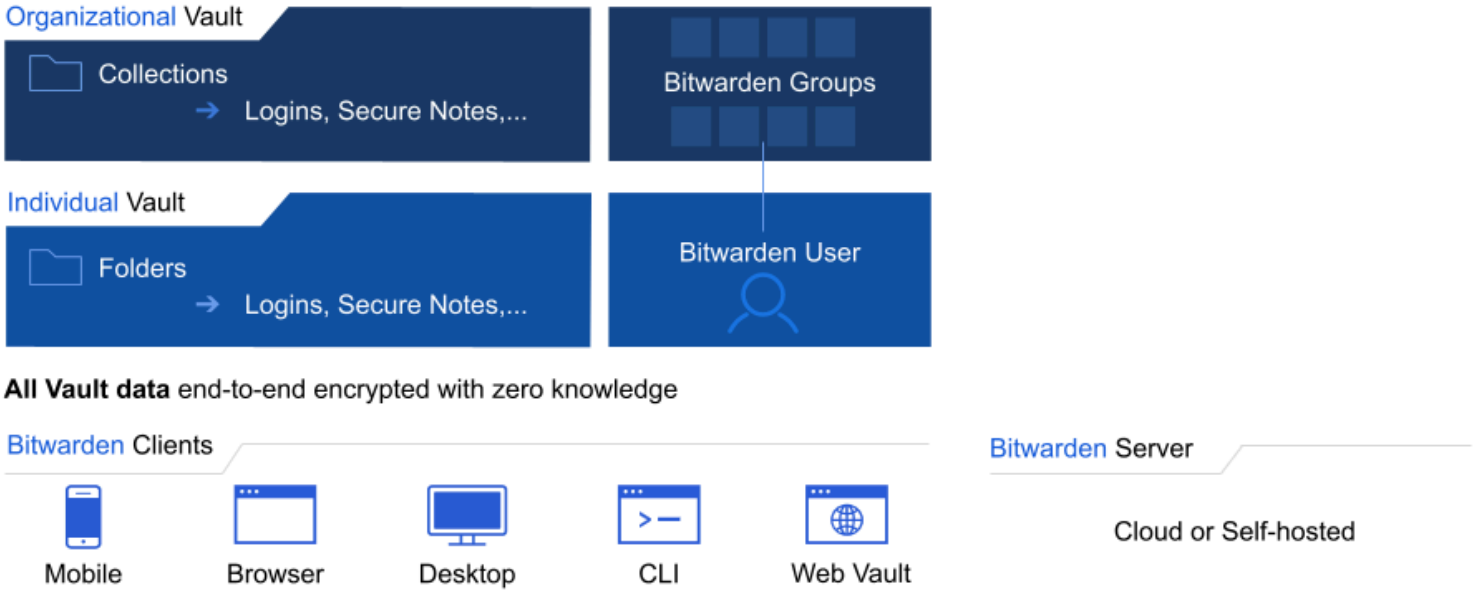
Why provide individual vaults by default?

Individual vaults are an instrumental component of the Bitwarden approach. Employees use a range of credentials every day, personally and professionally, and **habits formed in one area typically become habits in the other**. In our view, employees that use proper security practices in their personal lives will carry over that good behavior to their professional lives, **protecting your business** in the process.

Using the same tool in both areas helps that habit form faster and easier. Enterprise organizations have the option to configure policies, including to disable individual vaults.

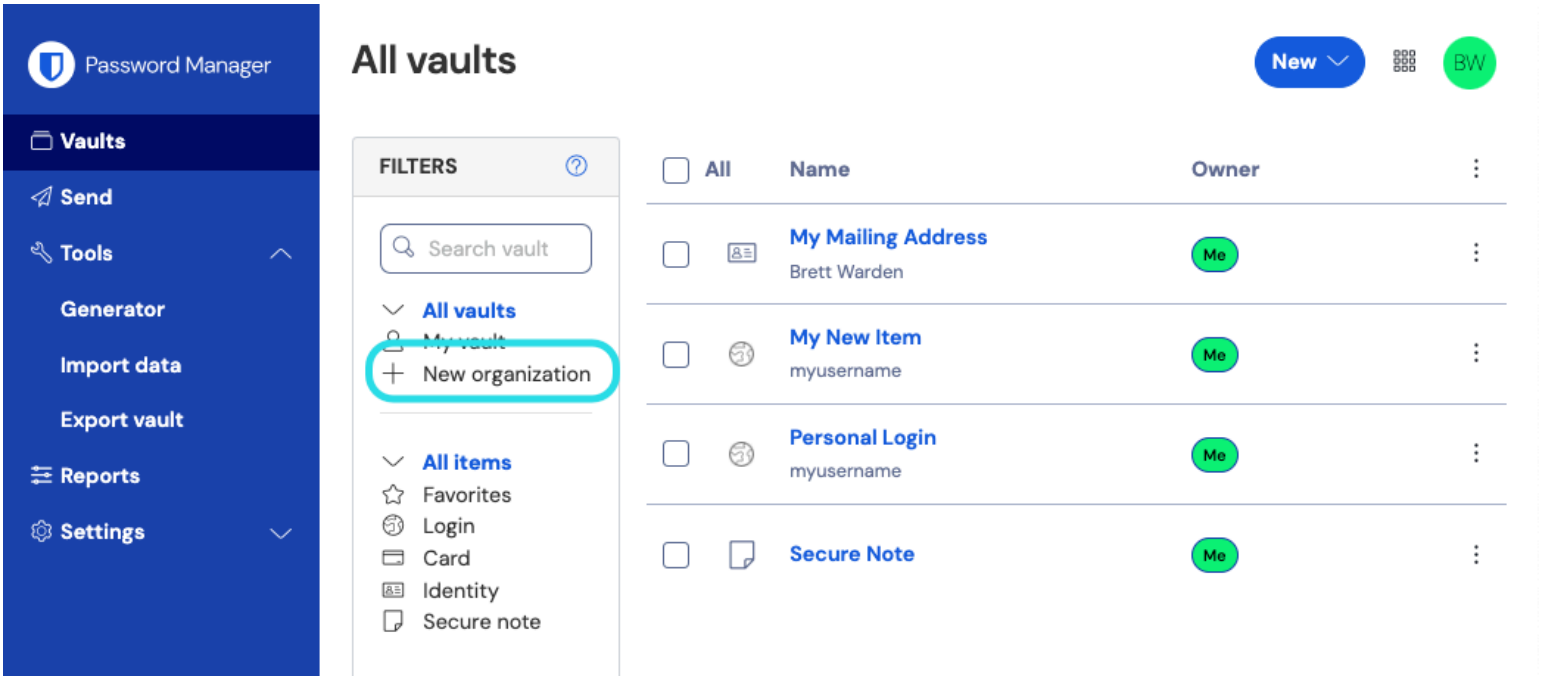
Organizaciones de Bitwarden

Las **organizaciones de Bitwarden** añaden una capa de colaboración y compartición a la gestión de contraseñas para tu equipo o empresa, permitiéndote compartir de forma segura información común como contraseñas de wifi de la oficina, credenciales en línea, o tarjetas de crédito compartidas de la empresa. La compartición segura a través de las organizaciones es segura y fácil.



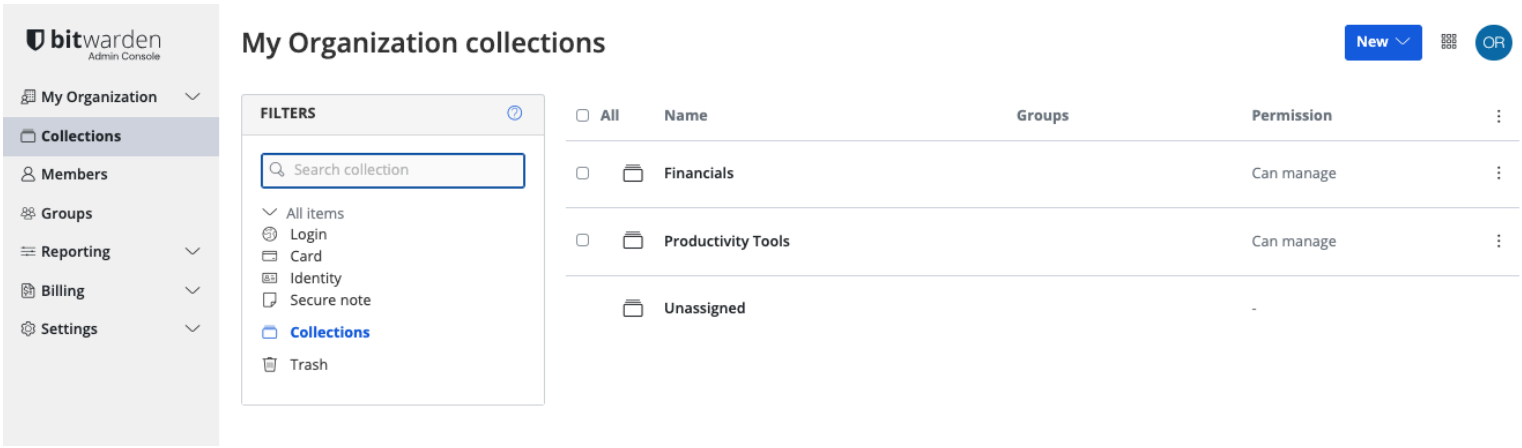
Organization Vault

Cualquiera puede iniciar una organización directamente desde la aplicación web:



Nueva organización

Una vez creado, aterrizarás en la Consola de Administrador, que es el centro neurálgico para todas las cosas relacionadas con la compartición y la administración de la organización. Quien inicie la organización será el propietario , lo que le otorgará control total para supervisar la bóveda, administrar elementos, miembros, colecciones y grupos , ejecutar informes y configurar ajustes como políticas :



Admin Console

Colecciones

Las organizaciones de Bitwarden gestionan miembros y Datos de una manera escalable y segura. Gestionar miembros y datos de manera individual es ineficiente para grandes empresas y puede dejar espacio para errores. Para solucionar esto, las organizaciones proporcionan colecciones y grupos .

Las **colecciones** agrupan inicios de sesión, notas, tarjetas e identidades para compartir de manera segura dentro de una organización:

Using Collections

Incorporación de miembros

Una vez que su organización esté establecida y las colecciones estén configuradas para almacenar sus datos, los propietarios y administradores deben invitar a nuevos miembros. Para garantizar la seguridad de su organización, Bitwarden aplica un proceso de 3 pasos para incorporar nuevos miembros, Invitar → Aceptar → Confirmar.

Los miembros pueden ser incorporados directamente desde la caja fuerte web, usando la aplicación Directory Connector para la sincronización de usuarios individuales y grupos, o a través de la provisión Just in Time (JIT) utilizando inicio de sesión con SSO.

Añadiendo miembros

En los casos más sencillos, los usuarios pueden ser añadidos a su organización directamente desde la aplicación web. Al agregar usuarios, puedes designar a qué colecciones concederles acceso, qué rol darles, y más.

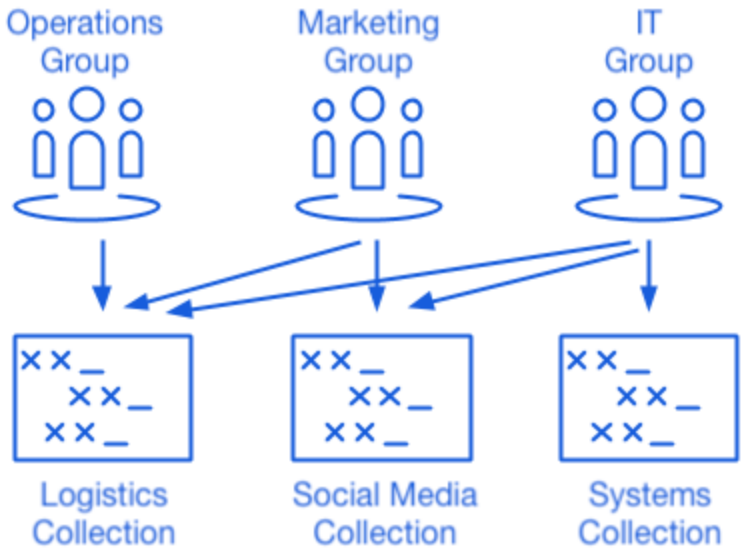
Aprende paso a paso cómo agregar usuarios a tu organización .

Una vez que los usuarios estén completamente integrados a su organización, puede asignarles acceso a los datos de la caja fuerte de su organización asignándolos a colecciones. Los Equipos y las organizaciones de Empresa pueden asignar usuarios a grupos para la asignación escalable de permisos, y construir asociaciones de grupo-colección en lugar de asignar acceso a nivel individual.

> **Tip**
> For large organizations, SCIM and Directory Connector are the best ways to onboard and offboard users at scale.

Grupos

Los grupos relacionan a los usuarios individuales y proporcionan una forma escalable de asignar permisos, incluyendo el acceso a colecciones y otros controles de acceso. Al incorporar nuevos usuarios, añádelos a un grupo para que hereden automáticamente los permisos configurados de ese grupo.



Using Collections with Groups

Controles de acceso completos basados en roles

Bitwarden adopta un enfoque amigable para la empresa para compartir a gran escala. Los miembros pueden ser agregados a la organización con un número de diferentes roles, pertenecer a diferentes grupos, y tener esos grupos asignados a varias colecciones para regular el acceso. Entre los roles disponibles se encuentra un rol personalizado para la configuración granular de permisos administrativos.

Desactivación de usuarios

En Bitwarden, vemos el compartir credenciales como un aspecto vital para realizar el trabajo de manera eficiente y segura. También reconocemos que una vez que se comparte una credencial, es *técnicamente* posible que el destinatario la conserve. Por esa razón, la incorporación segura utilizando los controles de acceso basados en roles apropiados y implementando políticas juega un rol importante en facilitar una sucesión segura.

Hay una variedad de herramientas proporcionadas por Bitwarden para personalizar tu flujo de trabajo y ejercer más control sobre la sucesión. Las siguientes secciones describirán un flujo de trabajo de sucesión básico, que no utiliza ninguna de estas herramientas, y algunas tácticas de sucesión avanzadas utilizadas frecuentemente por las organizaciones:

Desactivación básica

La desactivación de usuarios de Bitwarden implica eliminar usuarios de su organización, y al igual que la incorporación, se puede hacer directamente desde la caja fuerte web o de manera automatizada utilizando SCIM o Conector de Directorio.

Alice es una **Usuario** en su organización, que está alojada en la nube de Bitwarden y utiliza direcciones de correo electrónico de la empresa (por ejemplo, `primero-ultimo@empresa.com`). Actualmente, así es como Alice usa Bitwarden:

Área de producto	Descripción
Aplicaciones de cliente	Usa Bitwarden en móvil y una extensión de navegador personal y profesionalmente, y la caja fuerte web para trabajos ocasionales relacionados con la organización.
Correo electrónico y contraseña maestra	Inicia sesión en Bitwarden usando `alice@company.com` y `p@ssw0rD`.
Elementos personales	Almacena diversos elementos personales, incluyendo inicios de sesión y tarjetas de crédito, en su caja fuerte personal.
Autenticación en dos pasos	Utiliza Duo 2FA en toda la organización.
Colecciones	Alice tiene el permiso de "Puede Gestionar" para la colección de "Credenciales de Marketing", lo que le otorga la capacidad de gestionar muchos aspectos de esa colección.
Elementos compartidos	Creó y compartió varios elementos de la caja fuerte que son propiedad de la organización y residen en la colección de su Equipo.

Una vez que Alice sea eliminada de su organización:

Área de producto	Descripción
Aplicaciones de cliente	Puede continuar utilizando cualquier aplicación de Bitwarden para acceder a su caja fuerte individual, sin embargo, **todos perderán inmediatamente el acceso** a la caja fuerte de la organización, todas las colecciones y todos los elementos compartidos.
Correo electrónico y contraseña maestra	Puede continuar iniciando sesión usando `alice@company.com` y `p@ssw0rD`, sin embargo, dado que ella no tendrá acceso a su bandeja de entrada `@company.com` , se le debe aconsejar que cambie el correo electrónico asociado con su cuenta de Bitwarden.

Área de producto	Descripción
Elementos individuales	Todavía podrá usar su caja fuerte individual y acceder a los elementos almacenados en ella.
Permisos en la organización	Perderá **inmediatamente todos los permisos y acceso a** cualquier cosa relacionada con la organización.
Autenticación en dos pasos	No podrá usar Duo 2FA de la organización para acceder a su caja fuerte, pero puede configurar una de nuestras opciones de inicio de sesión en dos pasos gratis o mejorar a Premium para más.
Colecciones creadas	La "colección del Equipo de Marketing" de Alice será retenida por los propietarios y administradores de la organización, quienes pueden asignar un nuevo usuario con permiso para gestionar.
Elementos compartidos	La propiedad de las colecciones y elementos compartidos **pertenece a la organización**, por lo que Alice perderá el acceso a todos estos elementos a pesar de haberlos creado.

Tip

Los dispositivos fuera de línea almacenan en caché una copia de sólo lectura de los datos de la caja fuerte, incluyendo los datos de la caja fuerte organizacional. Si anticipas la explotación maliciosa de esto, las credenciales a las que el miembro tenía acceso deben ser actualizadas cuando lo elimines de la organización.

Desaprovisionamiento avanzado

Warning

Para aquellas cuentas que no tienen una contraseña maestra como resultado de SSO con dispositivos de confianza, eliminarlos de su organización o revocar su acceso cortará todo acceso a su cuenta de Bitwarden a menos que:

1. Les asignas una contraseña maestra usando recuperación de cuenta de antemano.
2. El usuario inicia sesión al menos una vez después de la recuperación de la cuenta para completar completamente el flujo de trabajo de recuperación de la cuenta.

Toma de control administrativo

Usando la política de restablecimiento de la contraseña maestra, los propietarios y administradores en su organización pueden restablecer la contraseña maestra de un usuario durante la sucesión.

Restablecer la contraseña maestra de un usuario cierra la sesión de todas las sesiones activas de Bitwarden del usuario y restablece sus credenciales de inicio de sesión a las especificadas por el administrador, lo que significa que ese administrador (y solo ese administrador) tendrá las llaves de los datos de la caja fuerte del usuario, incluyendo los elementos en la caja fuerte individual. Esta táctica de toma de control de la caja fuerte es comúnmente utilizada por las organizaciones para asegurar que los empleados no retengan acceso a

elementos individuales de la caja fuerte que pueden estar relacionados con el trabajo y pueden ser utilizados para facilitar auditorías de todas las credenciales que un empleado puede haber estado utilizando.

> **Note**
>
> **Admin password reset does not bypass two-step login**. In many cases, we recommend using SSO as some IdPs will allow you to configure 2FA and 2FA bypass policies for your users.

Eliminando la caja fuerte individual

Si su organización requiere control en tiempo real de todos los elementos de la caja fuerte, puede usar la Política de eliminación individual de la caja fuerte para requerir que los usuarios guarden todos los elementos de la caja fuerte en la organización. Esto evitará la necesidad de tomar el control y auditar la cuenta de un usuario durante la sucesión, ya que estará completamente vacía de datos una vez que se retire de la organización.

Eliminación de cuenta sin inicio de sesión

Como se mencionó anteriormente, eliminar un usuario de su organización no elimina automáticamente su cuenta de Bitwarden. En el flujo de trabajo de sucesión básico, cuando se elimina a un usuario, ya no puede acceder a la organización ni a ningún elemento o colección compartidos, sin embargo, aún podrá iniciar sesión en Bitwarden usando su contraseña maestra existente y acceder a cualquier elemento individual de la caja fuerte.

Las organizaciones que deseen eliminar completamente la cuenta, incluyendo todos los elementos individuales de la caja fuerte, pueden ser capaces de usar uno de los siguientes métodos para hacerlo durante la sucesión:

1. Si estás autoalojando Bitwarden, un administrador autorizado puede eliminar la cuenta desde el Portal del Administrador del Sistema.

2. Si la cuenta tiene una dirección de correo electrónico @yourcompany.com que tu empresa controla, puedes usar el flujo de trabajo de eliminar sin iniciar sesión y confirmar la eliminación dentro de la bandeja de entrada @yourcompany.com.

Diseñando su organización para su negocio

En Bitwarden, a menudo decimos que la gestión de contraseñas es la gestión de personas, y podemos adaptar los flujos de trabajo adecuados para su organización. Al ofrecer una amplia gama de opciones, compartidas a través de nuestro enfoque de código abierto, los clientes pueden estar seguros de que pueden satisfacer sus propias necesidades individuales.

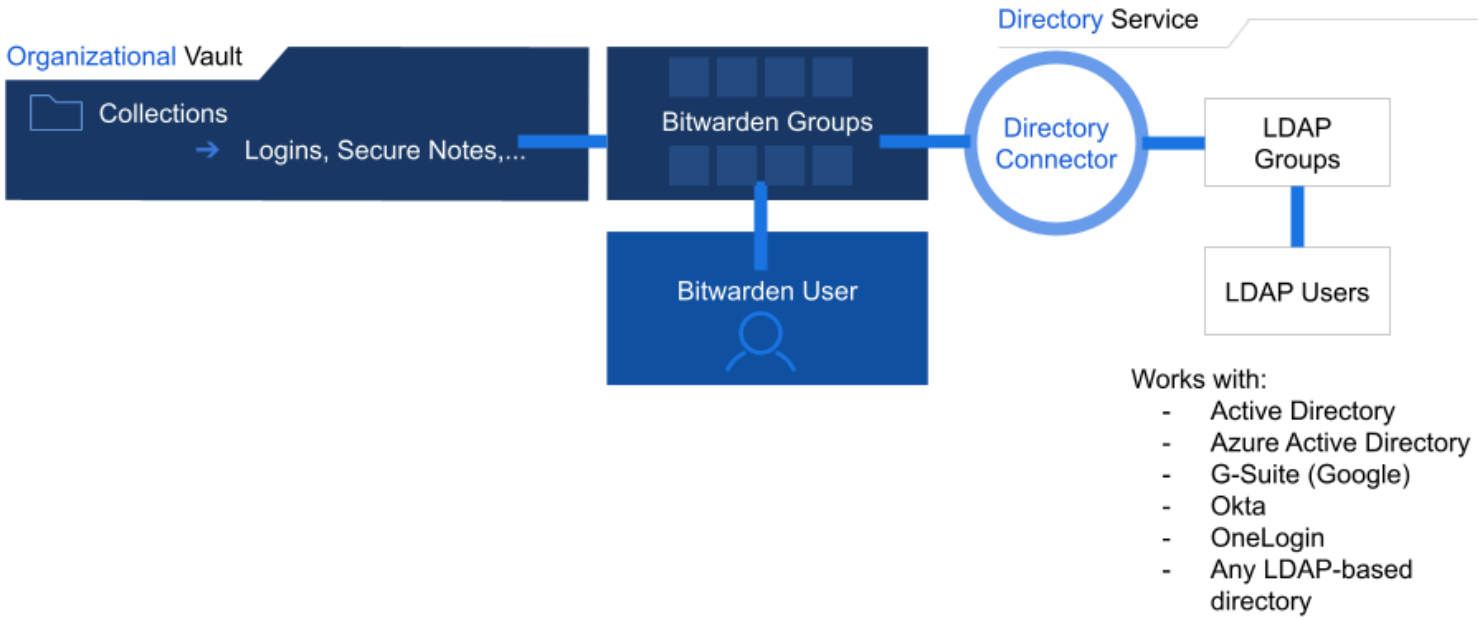
Comience hoy con una prueba gratuita de Enterprise o Teams.

SCIM

Para organizaciones de Empresa con grandes bases de usuarios que operan utilizando una identidad compatible (actualmente, Azure AD, Okta, OneLogin y JumpCloud), las integraciones SCIM se pueden utilizar para aprovisionar automáticamente miembros y grupos en su organización Bitwarden. Más información.

Conector de Directorio

Para empresas con grandes bases de usuarios que operan utilizando servicios de directorio (LDAP, AD, Okta y otros), Directory Connector puede sincronizar usuarios y grupos desde el directorio a la organización Bitwarden. Directory Connector es una aplicación independiente que se puede ejecutar en cualquier lugar con acceso a sus directorios y a Bitwarden.



Directory Connector

Muchas organizaciones de Equipos y Empresa de Bitwarden centran sus esfuerzos de incorporación en el Conector de Directorio y utilizan las áreas de administración de la caja fuerte de la organización para gestionar las relaciones entre grupos y colecciones.

El Conector de Directorio hará:

- Sincroniza los grupos de directorio basados en LDAP con los grupos de Bitwarden
- Sincroniza usuarios dentro de cada grupo
- Invita a nuevos usuarios a unirse a la organización.
- Eliminar usuarios eliminados de la organización

Inicia sesión con SSO

Las organizaciones de Bitwarden Empresa pueden integrarse con su proveedor de identidad existente (IdP) utilizando SAML 2.0 u OIDC para permitir a los miembros de su organización iniciar sesión en Bitwarden utilizando SSO. El inicio de sesión con SSO separa la autenticación de usuario de la descifrado de la caja fuerte:

La **autenticación** se completa a través de su IdP elegido y mantiene cualquier proceso de autenticación de dos factores conectado a ese IdP. La **descifrado** de los datos de la caja fuerte requiere la clave individual del usuario, que se deriva en parte de la contraseña maestra. Hay dos opciones de descifrado, ambas requerirán que los usuarios se autentiquen utilizando sus credenciales regulares de SSO.

- **Contraseña maestra** : una vez autenticados, los miembros de la organización descifrarán los datos de la bóveda utilizando sus contraseñas maestras .
- **Cifrado gestionado por el cliente**: Conecta el inicio de sesión con SSO a tu servidor de claves de descifrado autoalojado. Al usar esta opción, los miembros de la organización no necesitarán usar su contraseña maestra para descifrar los datos de la caja fuerte. En cambio, Conector de clave recuperará una clave de descifrado almacenada de manera segura en una base de datos de su propiedad y gestionada por usted.

- Aproveche su proveedor de identidad existente.
- Protege la encriptación de extremo a extremo de tus datos.
- Proporcionar usuarios automáticamente.
- Configura el acceso con o sin SSO.
- Descifra los datos de la caja fuerte de acuerdo a las necesidades de seguridad de tu empresa.

Políticas empresariales

Las organizaciones de la Empresa pueden implementar una variedad de políticas diseñadas para establecer una base segura para cualquier negocio. Las políticas incluyen:

- **Requiere inicio de sesión en dos pasos:** Requiere que los usuarios configuren el inicio de sesión en dos pasos en sus cuentas personales.
- **Requisitos de contraseña maestra:** establezca requisitos mínimos para la seguridad de la contraseña maestra.
- **Generador de contraseñas:** establezca requisitos mínimos para la configuración del generador de contraseñas.
- **Organización única:** impide que los usuarios se unan a otras organizaciones.
- **Eliminar bóveda individual:** solicite a los usuarios que guarden elementos de la bóveda en una organización eliminando la opción de propiedad personal.

> **Tip**
>
> The **Remove individual vault** policy, for example, fits into earlier discussion regarding the interplay between individual vaults and organization vaults. Some companies may desire the assurance of have all credentials retained in the organization vault. A possible implementation could involve allowing each individual user to have their own collection, which unlike individual vaults could be overseen by organization owners and admins.

Registro de Eventos

Las organizaciones de Bitwarden incluyen acceso a registros de eventos, que se pueden ver directamente desde la caja fuerte web o exportar para ser analizados dentro de los sistemas de gestión de información y eventos de seguridad (SIEM) como Splunk. Los registros de eventos incluyen información sobre:

- Interacciones usuario-elemento
- Cambios realizados en los elementos de la caja fuerte
- Eventos de incorporación
- Cambios en la configuración de la organización
- Mucho, mucho más

> **Tip**
> In addition to these benefits, customers appreciate the ability to tightly integrate Bitwarden into their existing systems. Bitwarden offers a robust public API and a fully-featured command line interface (CLI) for further integration into existing organization workflows.

Autoalojamiento

Siguiendo el enfoque de Bitwarden de ofrecer la gestión de contraseñas en cualquier lugar y en todas partes, Bitwarden proporciona una opción de autoalojamiento para abordar una gama aún más amplia de casos de uso para las Empresas. Hay muchas razones por las que una empresa puede elegir autoalojarse. Específicamente en lo que respecta a la incorporación, sucesión y funcionalidades mejoradas, aquí hay algunas de las razones por las que las empresas eligen hacerlo:

- **Eliminación inmediata de cuentas de usuario:** debido a que usted controla el servidor, los usuarios se pueden eliminar por completo (incluida su bóveda individual).
- **Control de acceso a la red** : los propietarios de la organización pueden determinar qué acceso a la red deben utilizar los empleados para acceder a su servidor Bitwarden.
- **Ajustes avanzados de proxy:** Los administradores pueden elegir habilitar o deshabilitar ciertos tipos de dispositivos para acceder al servidor de Bitwarden.
- **Usar un clúster de base de datos existente:** Conéctate a una base de datos existente de Microsoft SQL Server. Se admitirán bases de datos adicionales en el futuro.
- **Aumentar el almacenamiento para archivos adjuntos y Bitwarden Enviar:** Los archivos adjuntos para elementos de Bitwarden o Bitwarden Enviar se conservan en el almacenamiento proporcionado por el usuario.

Junta las piezas

El Conector de Directorio, inicio de sesión con SSO, políticas de Empresa y su caja fuerte funcionan bien individualmente o en armonía para optimizar su experiencia de incorporación, sucesión y gestión de la organización. La siguiente tabla detalla cómo podría verse al unir estas piezas en un proceso suave:

Paso	Descripción
Sincronizar	Utilice Directory Connector para la sincronización de grupos y usuarios a Bitwarden desde su servicio de directorio existente.
Invitar	El Conector de Directorio emitirá automáticamente invitaciones a los usuarios en sincronización.
Autenticar	Empareje su inicio de sesión con la implementación de SSO con la política de SSO para requerir que los usuarios se registren con SSO cuando acepten sus invitaciones.

Paso	Descripción
Administrar	Utilice la caja fuerte web para promover a algunos usuarios a diferentes roles y para asegurar que las relaciones de grupo-colección estén configuradas para otorgar el acceso correcto a los usuarios correctos.
Re-sincronizar	Vuelva a ejecutar periódicamente el Conector de Directorio para eliminar usuarios de Bitwarden que ya no están activos en su servicio de directorio y para comenzar la incorporación de nuevos empleados.

Preguntas Frecuentes

P: Si un empleado ya tiene una cuenta de Bitwarden, ¿podemos adjuntarla a la organización para que no necesiten otra cuenta de Bitwarden?

R: ¡ Sí! Puedes. Algunos clientes recomiendan que antes de agregar usuarios a la organización, esos usuarios tengan una caja fuerte de Bitwarden adjunta a su correo electrónico de la empresa. Esta elección es específica de la empresa y ambos enfoques funcionan.

P: ¿Cuando un empleado se va, podemos desvincular su cuenta de la organización para que ya no tengan acceso a las credenciales de la empresa y no pierdan sus credenciales de propiedad individual?

R: ¡ Sí! Eso es exactamente lo que implica la desaprovisionamiento.

P: ¿Podemos evitar que los empleados dupliquen las credenciales de la organización de la empresa en su caja fuerte individual?

R: ¡ Sí! Usando nuestra completa suite de controles de acceso basados en roles puedes hacer que las credenciales sean de **sólo lectura** para prevenir la duplicación.