

CONSOLA DE ADMINISTRADOR > MÁS

Guía de Migración de Equipos y Empresa

Ver en el centro de ayuda:

<https://bitwarden.com/help/teams-enterprise-migration-guide/>

Guía de Migración de Equipos y Empresa

La migración segura de su organización con Bitwarden es sencilla y segura. Simplemente siga los pasos en esta guía para migrar datos y usuarios desde su administrador de contraseñas existente:

1. [Exporta tus datos](#) .
2. [Crea y configura tu organización Bitwarden](#) .
3. [Importe sus datos a Bitwarden](#) .
4. [Incorpore a sus usuarios](#) .
5. [Configure el acceso a colecciones y elementos de la bóveda](#) .



Tip

If you need assistance during your migration, our [Customer Success team is here to help!](#)

Alcance

Este documento describe las mejores prácticas para migrar datos seguros desde su(s) administrador(es) de contraseñas actuales a una [organización Bitwarden Teams o Enterprise](#) , construyendo una infraestructura para la seguridad basada en métodos simples y escalables.

La gestión de contraseñas es crucial para la seguridad organizacional y la eficiencia operativa. Proporcionar información sobre los mejores métodos para realizar la migración y configuración está diseñado para minimizar el enfoque de prueba y error que a menudo se necesita al intercambiar herramientas de la empresa.

Los pasos en este documento **están listados en el orden recomendado** para facilitar su uso y una incorporación fluida para los usuarios.

Paso 1: Exporta tus datos

Exportar datos de otro administrador de contraseñas será diferente para cada solución, y en algunos casos puede ser un poco complicado. Utilice una de nuestras [Guías de Importar & Exportar](#) para obtener ayuda, por ejemplo con la exportación desde [Lastpass](#) o [1Password](#).

La recopilación de una exportación completa de sus datos puede requerir la asignación de carpetas compartidas o elementos a un solo usuario para exportar, o la realización de múltiples exportaciones entre usuarios con los permisos apropiados. Además, los datos exportados pueden incluir datos de propiedad individual junto con datos compartidos/organizacionales, así que asegúrese de eliminar los elementos individuales del archivo de exportación antes de [importar a Bitwarden](#).

Note

We recommend paying special attention to the location of the following types of data during export:

- Secure documents
- Secure file attachments
- Secure notes
- SSH / RSA key files
- Shared folders
- Nested shared items
- Any customized structures within your password management infrastructure

Paso 2: Configura tu organización

Las organizaciones de Bitwarden relacionan a los usuarios y los elementos de la caja fuerte para [compartir de forma segura](#) los inicios de sesión, notas, tarjetas e identidades.

Tip

It's important that you create your organization first and [import data to it directly](#), rather than importing the data to an individual account and then [moving items](#) to the organization secondarily.

1. **Crea tu organización** . Comienza creando tu organización. Para aprender cómo, consulta [este artículo](#).

Note

To self-host Bitwarden, create an organization on the Bitwarden cloud, generate a [license key](#), and use the key to [unlock organizations](#) on your server.

2. **Usuarios administrativos incorporados** . Con su organización creada, los procedimientos de configuración adicionales pueden facilitarse al incorporar algunos [usuarios administrativos](#). Es importante que **no comiences la incorporación del usuario final** en este punto, ya que quedan algunos pasos para preparar tu organización. Aprende cómo invitar a los administradores [aquí](#).
3. **Configurar servicios de identidad** . Las organizaciones de Empresa admiten [iniciar sesión con inicio de sesión único](#) (SSO) utilizando ya sea SAML 2.0 o OpenID Connect (OIDC). Para configurar SSO, abre la pantalla de **Ajustes** → **Single Sign-On** en la Consola de Administrador, accesible por [propietarios y administradores de la organización](#).
4. **Habilite las políticas empresariales** . Las [políticas de Empresa](#) permiten a las organizaciones implementar reglas para los usuarios, por ejemplo, requiriendo el uso de inicio de sesión en dos pasos. Se recomienda encarecidamente que configure las políticas antes de incorporar usuarios.

Paso 3: Importar a su organización

Para importar datos a su organización:

1. Inicia sesión en la aplicación web de Bitwarden y abre la Consola de Administrador utilizando el conmutador de producto (☰):

The screenshot displays the Bitwarden web interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, Password Manager (highlighted with a red circle), Secrets Manager (pointed to by a red arrow), Admin Console, and Toggle Width. The main content area is titled 'All vaults' and features a 'FILTERS' sidebar with a search bar and categories like 'All vaults', 'All items', 'Folders', and 'Collections'. The main list shows several vaults with columns for selection, name, owner, and actions.

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

Selector de producto

2. Navega a **Ajustes** → **Importar Datos**:

Import data

Destination

Collection
-- Select a collection --

Select this option if you want the imported file contents moved to a collection

Data

File format (required)
-- Select --

Select the import file

Choose File No file chosen

or copy/paste the import file contents

Import data

Consola de administrador importar

- Desde el menú desplegable de formato, elige un **Formato de archivo** (ver [Recomendaciones de importación](#) abajo).
- Seleccione el botón **Elegir archivo** y agregue el archivo para importar.

Warning

Import to Bitwarden can't check whether items in the file to import are duplicative of items in your vault. This means that **importing multiple files will create duplicative** vault items if an item is already in the vault and in the file to import.

- Seleccione el botón **Importar datos** para completar su importación.

Actualmente, los archivos adjuntos no están incluidos en las operaciones de importar de Bitwarden y deberán ser subidos a su caja fuerte manualmente. Para obtener más información, consulte [Archivos Adjuntos](#).

Tip

You should also recommend to employees that they export their individually-owned data from your existing password manager and prepare it for import into Bitwarden. Learn more [here](#).

Importar recomendaciones

Al importar datos a su organización, tiene dos opciones:

- Para importar el formato de archivo predeterminado de tu anterior administrador de contraseñas.

2. Para condicionar un **.CSV** específico de Bitwarden para importar.

Recomendamos formatear su archivo para importar como un Bitwarden **.CSV** para obtener los mejores resultados, o para usuarios avanzados, como un archivo Bitwarden **.JSON**. Para obtener instrucciones sobre cómo formar un archivo de importación específico de Bitwarden, consulte [esta guía de importación](#).

Paso 4: Incorporar usuarios

Bitwarden admite la incorporación manual a través de la caja fuerte web y la incorporación automatizada a través de integraciones SCIM o sincronización desde su servicio de directorio existente:

Manual de incorporación

Para garantizar la seguridad de su organización, Bitwarden aplica un proceso de 3 pasos para incorporar a un nuevo miembro, [invitar](#) → [aceptar](#) → [confirmar](#). Aprende cómo invitar a nuevos usuarios [aquí](#).

Incorporación automatizada

La incorporación automatizada de usuarios está disponible a través de las integraciones SCIM con [Azure AD](#), [Okta](#), [OneLogin](#) y [JumpCloud](#), o utilizando [Directory Connector](#), una aplicación independiente disponible en una [aplicación de escritorio](#) y una herramienta [ILC](#) que sincronizará usuarios y grupos de su servicio de directorio existente.

Cualquiera que uses, los usuarios son automáticamente invitados a unirse a la organización y pueden ser confirmados manualmente o automáticamente usando la [herramienta Bitwarden ILC](#).

Paso 5: Configurar el acceso a las colecciones y elementos

Comparta elementos de la caja fuerte con sus usuarios finales configurando el acceso a través de colecciones, grupos y permisos a nivel de grupo o usuario:

Colecciones

Bitwarden empodera a las organizaciones para compartir Datos sensibles de manera fácil, segura y escalable. Esto se logra segmentando secretos compartidos, elementos, inicios de sesión, etc. en **colecciones**.

Las colecciones pueden organizar elementos seguros de muchas maneras, incluyendo por función empresarial, asignación de grupo, niveles de acceso a aplicaciones, o incluso protocolos de seguridad. Las colecciones funcionan como carpetas compartidas, permitiendo un control de acceso consistente y compartiendo entre grupos de usuarios.

Las carpetas compartidas de otros administradores de contraseñas pueden importarse como colecciones en Bitwarden utilizando la plantilla de importación de la organización que se encuentra tipo: enlace de activo id: 4DdJLATEuhMYIE581pPErF y colocando el nombre de la carpeta compartida en la columna **Colección**, por ejemplo, transformando:

url	username	password	extra	name	grouping	fav
https://azure.microsoft.com/en-us/	AzureUser	5HDXWtuAAK3SX8		Azure Login	Shared-Systems	0
https://github.com/login	GitHubUser	P4JUghjRfhKrDJ		Github	Shared-Systems	0
https://adobe.com	AdobeUser	T6RYSbD5mn78ab		Adobe Login	Shared-Design	0
https://shutterstock.com	ShutterStock	749bs2saWb3bxH		Shutterstock	Shared-Design	0
https://usps.com	USPSUser	6UmtWLkGydBMaZ		USPS Shipping	Shared-Shipping	0
https://ups.com	UPSUser	YBD7ftBZbosS9u		UPS Login	Shared-Shipping	0
https://fedex.com	FedexUser	y44xgs5fiyYZNU		FedExUser	Shared-Shipping	0

Migration Export Example

en:

collections	type	name	notes	fields	login_uri	login_username	login_password	login_totp
Shared-Systems	login	Azure Login			https://azure.microsoft.com/en-us/	AzureUser	5HDXWtuAAK3SX8	
Shared-Systems	login	Github			https://github.com/login	GitHubUser	P4JUghjRfhKrDJ	
Shared-Design	login	Adobe Login			https://adobe.com	AdobeUser	T6RYSbD5mn78ab	
Shared-Design	login	Shutterstock			https://shutterstock.com	ShutterStock	749bs2saWb3bxH	
Shared-Shipping	login	USPS Shipping			https://usps.com	USPSUser	6UmtWLkGydBMaZ	
Shared-Shipping	login	UPS Login			https://ups.com	UPSUser	YBD7ftBZbosS9u	
Shared-Shipping	login	FedExUser			https://fedex.com	FedexUser	y44xgs5fiyYZNU	

Migration Import Example

Las colecciones pueden ser compartidas tanto con grupos como con usuarios individuales. Limitar el número de usuarios individuales que pueden acceder a una colección hará que la gestión sea más eficiente para los administradores. Aprende más [aquí](#).

Grupos

Usar grupos para compartir es la forma más efectiva de proporcionar acceso a credenciales y secretos. Los grupos, como los usuarios, pueden ser sincronizados a su organización utilizando SCIM o Directory Connector.

Permisos

Los permisos para las colecciones de Bitwarden pueden ser asignados a nivel de grupo o de usuario. Esto significa que cada grupo o usuario puede ser configurado con permisos para la misma colección. Los permisos de la colección incluyen opciones para **Sólo Lectura** y **Ocultar Contraseñas**.

Bitwarden utiliza una unión de permisos para determinar los permisos de acceso finales para un usuario y un elemento de colección ([aprende más](#)). Por ejemplo:

- El usuario A es parte del grupo de Soporte de Nivel 1, que tiene acceso a la colección de Soporte, con permiso de sólo lectura.
- El usuario A también es miembro del grupo de Gestión de Soporte, que tiene acceso a la colección de Soporte, con acceso de lectura y escritura.
- En este escenario, el Usuario A podrá leer–escribir en la Colección.

Apoyo a la migración

El equipo de Éxito del Cliente de Bitwarden está disponible 24/7 con soporte prioritario para su organización. Si necesita asistencia o tiene preguntas, no dude en [contactarnos](#).