ADMINISTRADOR DE SECRETOS > COMIENZA

Gestiona tu Organización

Gestiona tu Organización

> **Note**
> Para obtener una visión general completa de la incorporación a Bitwarden, por favor revise esta guía para obtener más información.

Como organización que utiliza el Administrador de secretos, compartirás muchas de las herramientas originalmente utilizadas por el administrador de contraseñas. Este artículo cubre estas áreas comunes y proporciona enlaces para compartir documentación donde sea apropiado.

> **Note**
> Si eres completamente nuevo en las organizaciones de Bitwarden, te recomendamos que consultes nuestro artículo sobre cómo empezar como administrador de una organización.

Políticas empresariales

Las políticas permiten a las organizaciones de la Empresa imponer reglas de seguridad para sus miembros, por ejemplo, exigiendo el uso de inicio de sesión en dos pasos. Aunque algunas políticas se aplican principalmente al administrador de contraseñas, hay un puñado de políticas que son ampliamente aplicables a los usuarios del Administrador de secretos:

- Requiere inicio de sesión en dos pasos
- Requisitos de la contraseña maestra
- Reinicio de contraseña maestra
- Organización única
- Autenticación de inicio de sesión único
- Tiempo de espera de la caja fuerte excedido

> **Tip**
> Si eres nuevo en Bitwarden, recomendamos establecer políticas antes de incorporar a tus usuarios.

Gestión de usuarios

La gestión de usuarios para las organizaciones del Administrador de secretos es similar a las organizaciones que utilizan el administrador de contraseñas, sin embargo, algunos elementos específicos del Administrador de secretos incluyen otorgar acceso a los miembros de la organización al Administrador de secretos, diferencias de rol de miembro, y especificar asientos de usuario y cuentas de servicio.

Incorporación

Existen varios métodos diferentes para incorporar usuarios a su organización Bitwarden. Algunos de los métodos comúnmente utilizados se destacan aquí:

Manual

La caja fuerte web de Bitwarden proporciona una interfaz simple e intuitiva para invitar a nuevos usuarios a unirse a su organización. Este método es mejor para pequeñas organizaciones o aquellas que no están utilizando servicios de directorio como Azure AD o Okta. Aprende cómo empezar.

SCIM

Los servidores de Bitwarden proporcionan un punto final de SCIM que, con una clave API SCIM válida, aceptará solicitudes de su proveedor de identidad para la provisión y desprovisión de usuarios y grupos. Este método es mejor para organizaciones más grandes que utilizan un servicio de directorio habilitado para SCIM o un IdP. Aprende cómo empezar.

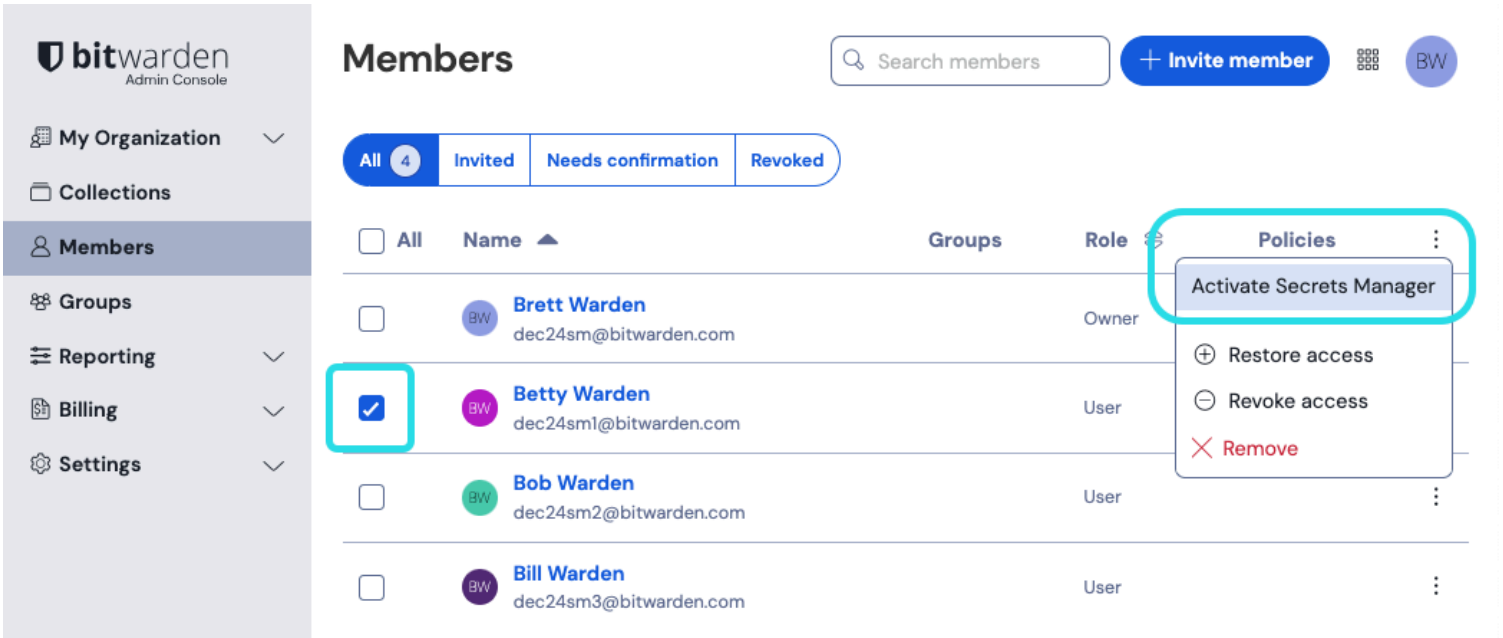
Conector de Directorio

Directory Connector provisiona automáticamente usuarios y grupos en su organización Bitwarden extrayendo de una selección de servicios de directorio fuente. Este método es mejor para organizaciones más grandes que utilizan servicios de directorio que no admiten SCIM. Aprende cómo empezar.

Acceso al Administrador de secretos

Una vez incorporados, otorgue a los miembros individuales de su organización acceso al Administrador de secretos:

1. Abra la vista de **Miembros** de su organización y seleccione los miembros a los que desea dar acceso al Administrador de secretos.
2. Usando el menú ⋮, selecciona **Activar Administrador de secretos** para conceder acceso a los miembros seleccionados:



Añadir usuarios al Administrador de secretos

Tip

Dar a los miembros acceso al Administrador de secretos no les dará automáticamente acceso a los proyectos almacenados o secretos. Necesitarás asignar acceso a las personas o grupos a los proyectos a continuación.

Roles de miembro

La siguiente tabla describe lo que cada rol de miembro puede hacer dentro del Administrador de secretos. Durante la beta, los usuarios tienen el mismo rol de miembro para el Administrador de secretos que se les asigna para el administrador de contraseñas:

Rol del miembro	Descripción
Usuario	Los usuarios pueden crear sus propios secretos, proyectos, cuentas de servicio y tokens de acceso. Pueden editar estos objetos una vez creados. Los usuarios deben ser asignados a proyectos o cuentas de servicio para interactuar con objetos existentes, y se les puede dar acceso de **Puede leer** o **Puede leer, escribir**.
Administrador	Los administradores tienen automáticamente acceso de **Pueden leer, escribir** a todos los secretos, proyectos, cuentas de servicio y tokens de acceso. Los administradores pueden asignarse a sí mismos acceso al Administrador de secretos y asignar acceso a otros miembros al Administrador de secretos.
Propietario	Los propietarios tienen automáticamente acceso a todos los secretos, proyectos, cuentas de servicio y tokens de acceso para **Pueden leer, escribir**. Los propietarios pueden asignarse a sí mismos acceso al Administrador de secretos y asignar acceso a otros miembros al Administrador de secretos.

Note

Los roles personalizados actualmente no están delimitados con opciones para el Administrador de secretos, sin embargo, aún pueden usarse para asignar capacidades específicas del administrador de contraseñas o capacidades más amplias de la organización.

Grupos

Los grupos relacionan entre sí a los miembros individuales y proporcionan una forma escalable de acceder a proyectos específicos y obtener permisos para ellos. Al agregar nuevos miembros, añádelos a un grupo para que hereden automáticamente los permisos configurados de ese grupo. Más información.

Una vez que se crean los grupos en la consola de administrador, asígnales a los proyectos desde la aplicación web del Administrador de secretos.

Inicio de sesión único

Iniciar sesión con SSO es la solución de Bitwarden para el inicio de sesión único. Usando el inicio de sesión con SSO, las organizaciones de Empresa pueden aprovechar su Proveedor de Identidad existente para autenticar a los usuarios con Bitwarden utilizando los protocolos SAML 2.0 o Open ID Connect (OIDC). Aprende cómo empezar.

Administración de recuperación de cuenta

La recuperación de cuentas permite a los administradores designados recuperar cuentas de usuario de la organización de la Empresa y restaurar el acceso en el caso de que un empleado olvide su contraseña maestra. La recuperación de cuenta puede ser activada para una organización habilitando la política de administración de recuperación de cuenta. Aprende cómo empezar.

Registro de Eventos

Los registros de eventos son registros con marca de tiempo de los eventos que ocurren dentro de su organización de Equipos o Empresa. Los eventos del Administrador de secretos están disponibles tanto desde el **Informe → Registros de eventos** de la caja fuerte de su organización como desde la página de registros de eventos de la cuenta de servicio.

Los registros de eventos se pueden exportar y se conservan indefinidamente. Mientras que muchos eventos son aplicables a todos los productos de Bitwarden y algunos son específicos para el Administrador de Contraseñas, el Administrador de Secretos registrará específicamente lo siguiente:

- Secreto accedido por una cuenta de servicio

Autoalojamiento

Las organizaciones de Empresa pueden autoalojar el Administrador de secretos de Bitwarden usando Docker en máquinas Linux y Windows. Si no has autoalojado Bitwarden antes, usa esta guía para ponerte en el camino correcto.

Si ya está autoalojando una organización de Bitwarden Empresa y desea obtener acceso al Administrador de secretos en ese servidor:

1. Regístrese para una suscripción de Administrador de secretos en su organización de Bitwarden alojada en la nube.
2. Actualiza tu servidor autoalojado a, como mínimo, 2023.10.0.
3. Recupere un nuevo archivo de licencia de su organización alojada en la nube y cárguelo en su servidor autohospedado .

> **Note**
>
> El Administrador de secretos autoalojado no es compatible con la opción de despliegue unificado autoalojado de Bitwarden. Las organizaciones de Equipos y Empresa deben usar una instalación estándar de Linux o Windows.