bitwarden | Artículo del Centro de Ayuda

CONSOLA DE ADMINISTRADOR > INFORMANDO

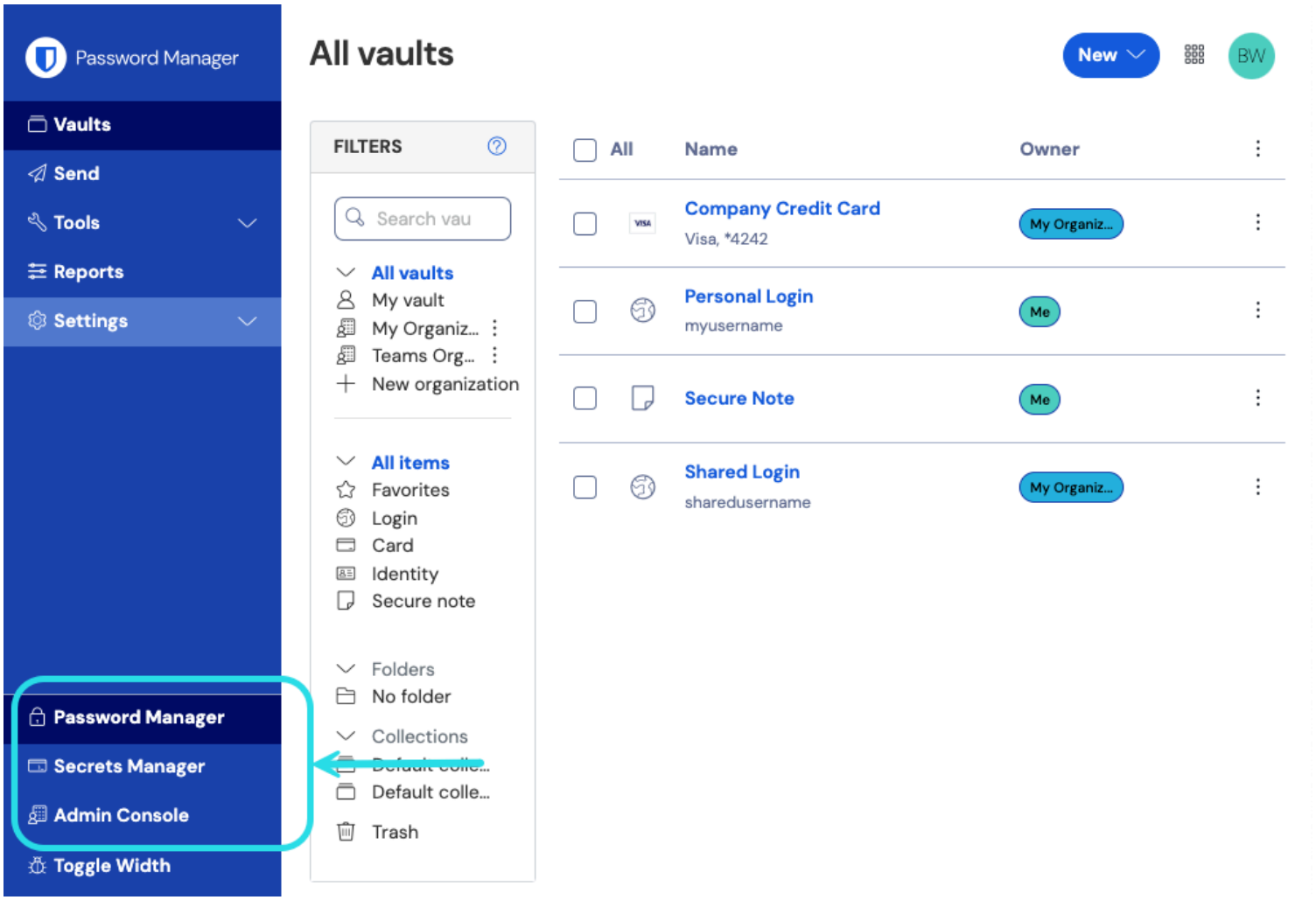
Registros de Eventos

Ver en el centro de ayuda:
https://bitwarden.com/help/event-logs/

Registros de Eventos

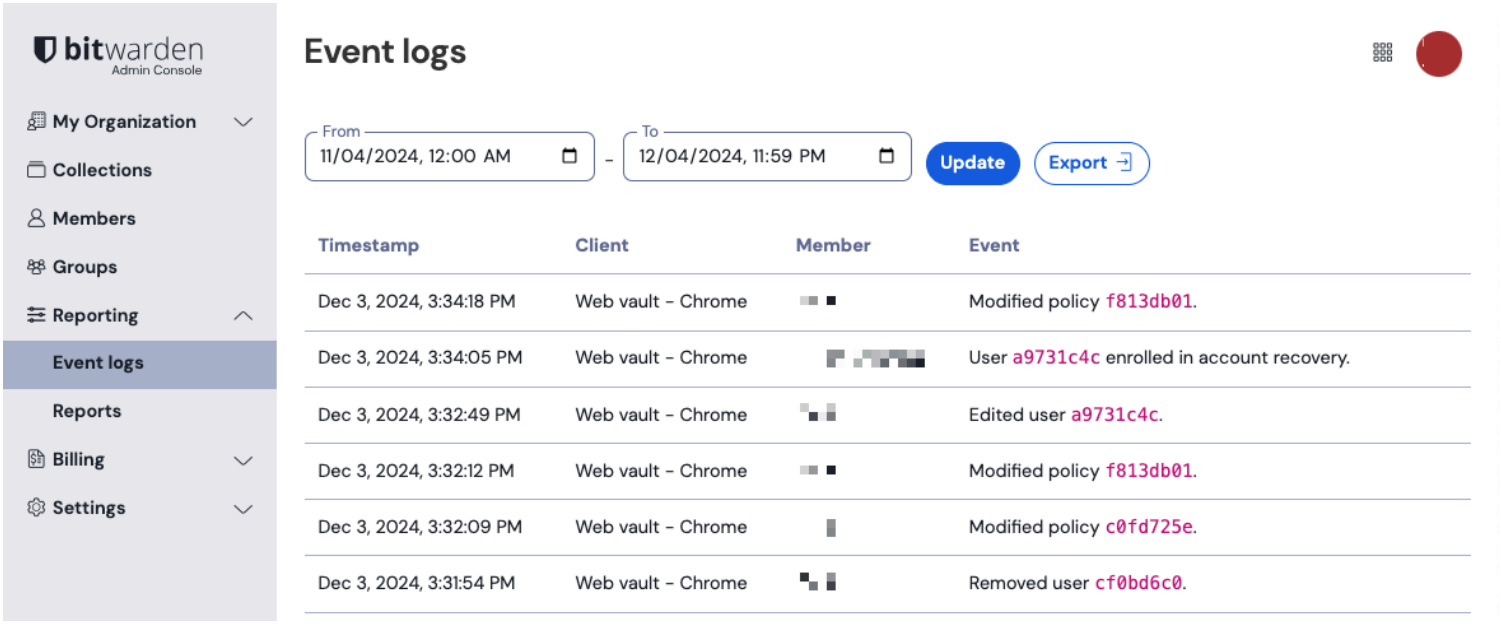
Los registros de eventos son registros con marca de tiempo de los eventos que ocurren dentro de su organización de Equipos o Empresa. Para acceder a los registros de eventos:

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



Selector de producto

2. Seleccione **Informe** → **Registros de eventos** desde la navegación:



Registro de Eventos

Los registros de eventos se pueden exportar, son accesibles desde el punto final `/events` de la API pública de Bitwarden, y se conservan indefinidamente, sin embargo, solo se pueden ver 367 días de datos a la vez (según lo dictado por los selectores de rango).

La mayoría de los eventos capturan acciones realizadas en varios clientes de Bitwarden, que envían datos de eventos al servidor cada 60 segundos, por lo que puede observar pequeños retrasos en el informe de eventos recientes.

Inspeccionar eventos

En la vista de **Registros de eventos** en la aplicación web, seleccionar un identificador de recurso rosa (por ejemplo, `1e685004`) hará dos cosas:

1. Abra un cuadro de diálogo con una lista de eventos asociados con ese recurso. Por ejemplo, seleccionar el identificador de un elemento abrirá una lista de las veces que el elemento ha sido editado, visto, etc., incluyendo qué miembro realizó cada acción.

2. Navega a una vista donde puedes acceder al recurso. Por ejemplo, seleccionar el identificador de un miembro de **Registros de eventos** te llevará a la vista de **Miembros** y filtrará automáticamente la lista hasta ese miembro.

Lista de eventos

Los registros de eventos registran más de 50 tipos diferentes de eventos. La pantalla de registros de eventos captura una **Marca de tiempo** para el evento, información de la aplicación del cliente incluyendo el tipo de aplicación y la IP (accesible al pasar el cursor sobre el icono del globo), el **Usuario** conectado al evento, y una descripción del **Evento**.

> **Note**
>
> Cada **Evento** está asociado con un código de tipo (`1000`, `1001`, etc.) que identifica la acción capturada por el evento. Los códigos de tipo son utilizados por la API pública de Bitwarden para identificar la acción documentada por un evento.

Todos los tipos de eventos están listados a continuación, con sus correspondientes códigos de tipo:

Eventos de usuario

- Iniciado sesión. (`1000`)

- Cambiada contraseña de la cuenta. (1001)
- Habilitado/actualizado inicio de sesión de dos pasos. (1002)
- Inicio de sesión de dos pasos desactivado. (1003)
- Cuenta recuperada de inicio de sesión de dos pasos. (1004)
- Intento de inicio de sesión fallido con contraseña incorrecta. (1005)
- El intento de inicio de sesión falló con un inicio de sesión de dos pasos incorrecto. (1006)
- El usuario exportó los elementos individuales de su caja fuerte. (1007)
- El usuario actualizó una contraseña emitida a través de la recuperación de cuenta. (1008)
- El usuario migró su clave de descifrado con Conector de clave. (1009)
- El usuario solicitó aprobación del dispositivo. (1010)

Eventos de elemento

- Elemento creado item-identifier. (1100)
- Elemento editado item-identifier. (1101)
- Elemento eliminado permanentemente item-identifier. (1102)
- Creado adjunto para el elemento identificador-de-elemento. (1103)
- Adjunto eliminado para el elemento identificador-de-elemento. (1104)
- Movió el elemento identificador de elemento a una organización. (1105)
- Colecciones editadas para el elemento item-identifier (1106)
- Elemento visto item-identifier. (1107)
- Contraseña vista para el elemento item-identifier. (1108)
- Visto campo oculto para el elemento identificador-de-elemento. (1109)
- Visto el código de seguridad para el elemento item-identifier. (1110)
- Contraseña copiada para el elemento item-identifier. (1111)
- Campo oculto copiado para el elemento identificador-de-elemento. (1112)
- Código de seguridad copiado para el elemento item-identifier. (1113)
- Elemento autocompletado identificador-de-elemento. (1114)
- Elemento enviado item-identifier a la basura. (1115)

- Elemento restaurado item-identifier. (1116)
- Número de tarjeta visto para el elemento item-identifier. (1117)

Eventos de colección

- Colección creada identificador-de-colección. (1300)
- Colección editada identificador-de-colección. (1301)
- Colección eliminada identificador-de-colección. (1302)

Eventos de grupo

- Grupo creado identificador-de-grupo. (1400)
- Grupo editado group-identifier. (1401)
- Grupo eliminado group-identifier. (1402)

Eventos de la organización

- Usuario invitado identificador de usuario. (1500)
- Usuario confirmado identificador-de-usuario. (1501)
- Usuario editado identificador-de-usuario. (1502)
- Usuario eliminado identificador-de-usuario. (1503)
- Grupos editados para el usuario user-identifier. (1504)
- SSO no vinculado para el usuario identificador-de-usuario. (1505)
- identificador-de-usuario se inscribió en la recuperación de cuenta. (1506)
- identificador-de-usuario se retiró de la recuperación de cuenta. (1507)
- Reinicio de la contraseña maestra para identificador-de-usuario. (1508)
- Restablecer enlace SSO para el usuario identificador-de-usuario. (1509)
- El identificador de usuario inició sesión usando SSO por primera vez. (1510)
- Acceso revocado a la organización para identificador de usuario (1511)
- Restaura el acceso a la organización para identificador de usuario (1512)
- Dispositivo aprobado para identificador de usuario. (1513)
- Dispositivo denegado para identificador-de-usuario. (1514)
- Ajustes de organización editados. (1600)

- Organización de caja fuerte purgada. (1601)
- Caja fuerte de organización exportada. (1602)
- Acceso a la caja fuerte de la organización por un Proveedor que gestiona. (1603)
- La organización habilitó SSO. (1604)
- La organización desactivó SSO. (1605)
- La organización habilitó el Conector de clave. (1606)
- La organización desactivó el Conector de clave. (1607)
- Patrocinios de Familias sincronizados. (1608)
- Política modificada identificador-de-política. (1700)
- Dominio añadido nombre-de-dominio. (2000)
- Dominio eliminado nombre-de-dominio. (2001)
- Nombre de dominio verificado. (2002)
- Nombre de dominio no verificado. (2003)

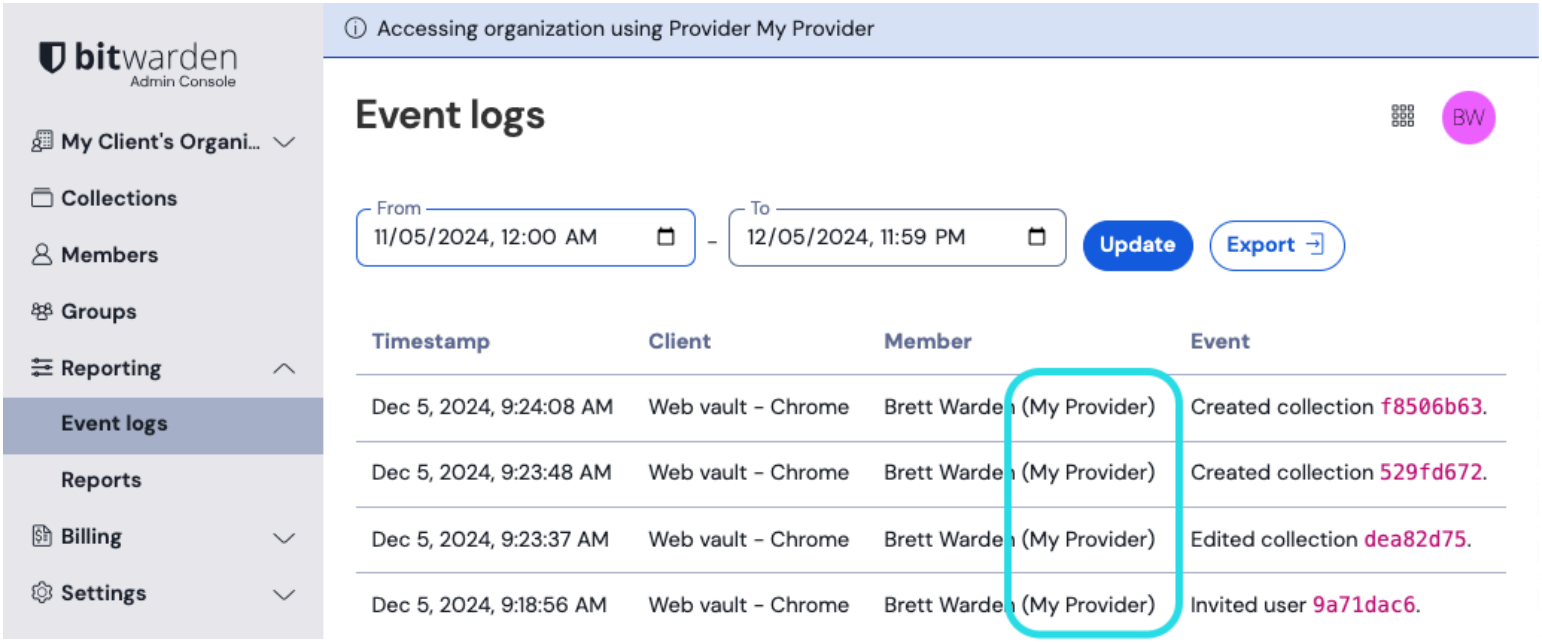
Eventos de Administrador de secretos

Los eventos del Administrador de secretos están disponibles tanto desde la pestaña de **Informe** de la caja fuerte de su organización como desde la página de registros de eventos de la cuenta de servicio. Los siguientes eventos del Administrador de secretos son capturados:

- Accedido secreto identificador-secreto. (2100)

Eventos de proveedores

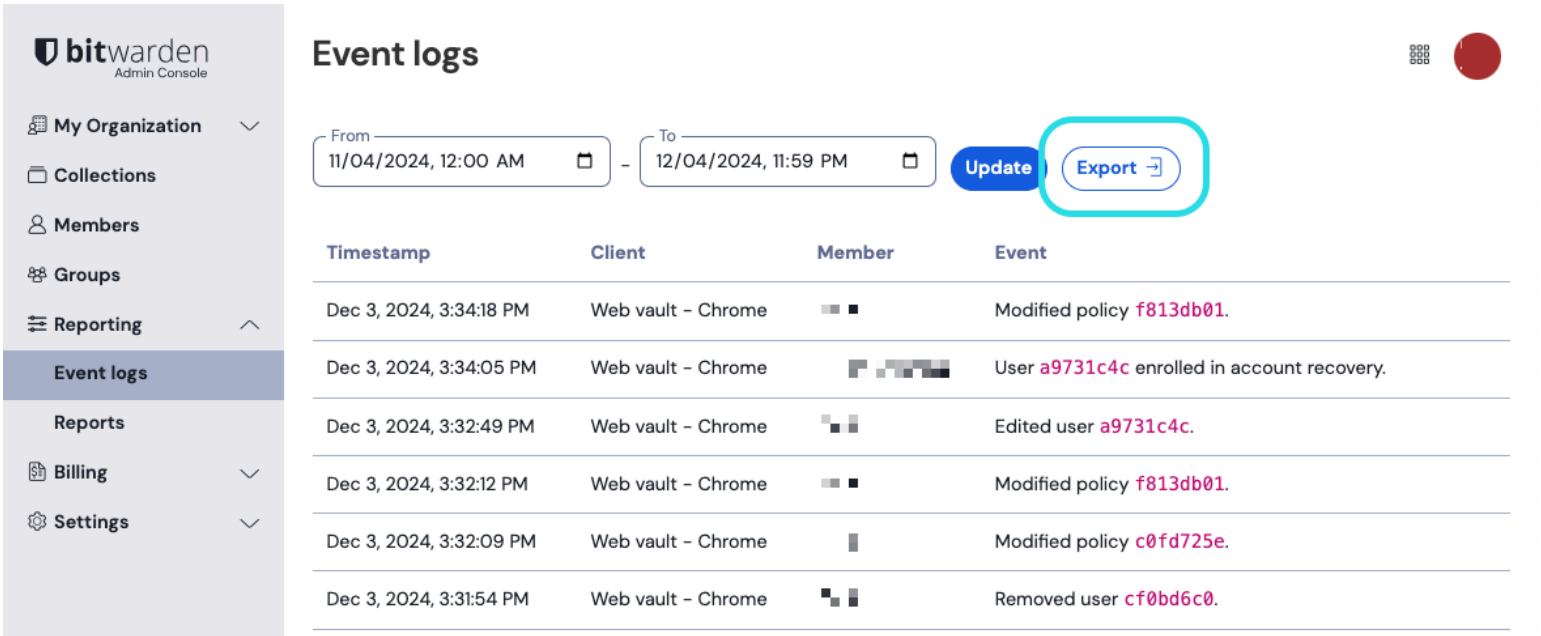
Cuando cualquiera de los eventos anteriores es ejecutado por un miembro de un proveedor administrador, la columna de **Usuario** registrará el nombre del proveedor. Además, un evento específico del proveedor registrará cada vez que un miembro de un proveedor administrador acceda a la caja fuerte de su organización:



Proveedor accediendo a eventos

Exportar eventos

Exportar registros de eventos creará un `.csv` de todos los eventos dentro del rango de fechas especificado:



Exportar Registros de Eventos

Por ejemplo:

```Bash
message,appIcon,appName,userId,userName,userEmail,date,ip,type
Logged in.,fa-globe,Web Vault - Chrome,1234abcd-56de-78ef-91gh-abcdef123456,Alice,alice@bitwarden.com,2021-06-14T14:22:23.331751Z,111.11.111.111,User_LoggedIn
Invited user zyxw9876.,fa-globe,Unknown,1234abcd-56de-78ef-91gh-abcdef123456,Alice,alice@bitwarden.com,2021-06-14T14:14:44.7566667Z,111.11.111.111,OrganizationUser_Invited
Edited organization settings.,fa-globe,Web Vault - Chrome,9876dcba-65ed-87fe-19hg-654321fedcba,Bob,bob@bitwarden.com,2021-06-07T17:57:08.1866667Z,222.22.222.222,Organization_Updated
```

Respuestas de API

Acceder a los registros de eventos desde el punto final `/events` de la API pública de Bitwarden devolverá una respuesta JSON como la siguiente:

```Bash
{
  "object": "list",
  "data": [
    {
      "object": "event",
      "type": 1000,
      "itemId": "string",
      "collectionId": "string",
      "groupId": "string",
      "policyId": "string",
      "memberId": "string",
      "actingUserId": "string",
      "date": "2020-11-04T15:01:21.698Z",
      "device": 0,
      "ipAddress": "xxx.xx.xxx.x"
    }
  ],
  "continuationToken": "string"
}
```

Integraciones de SIEM y sistemas externos

Al exportar datos de Bitwarden a otros sistemas, se puede utilizar una combinación de datos de las exportaciones, API e ILC para recopilar datos. Por ejemplo, utilizando las APIs RESTful de Bitwarden para recopilar datos sobre la estructura de la organización:

- GET /public/members devuelve los miembros, ids y groupids asignados
- GET /public/groups devuelve todos los grupos, ids, colecciones asignadas y sus permisos.
- GET /public/collections devuelve todas las colecciones, y sus grupos asignados.

Una vez que tienes el id único para cada miembro, grupo y colección, ahora puedes usar la herramienta ILC para recopilar información usando el comando ILC `bw-list` para recuperar los siguientes elementos en formato JSON:

- Miembros de la org
- Elementos
- Colecciones
- Grupos

Después de recopilar estos datos, puedes unir filas en sus identificadores únicos para construir una referencia a todas las partes de tu organización Bitwarden. Para obtener más información sobre cómo usar el Bitwarden ILC, consulte la herramienta de línea de comandos de Bitwarden (ILC).