bitwarden | Help Center Article

ADMIN CONSOLE > REPORTING

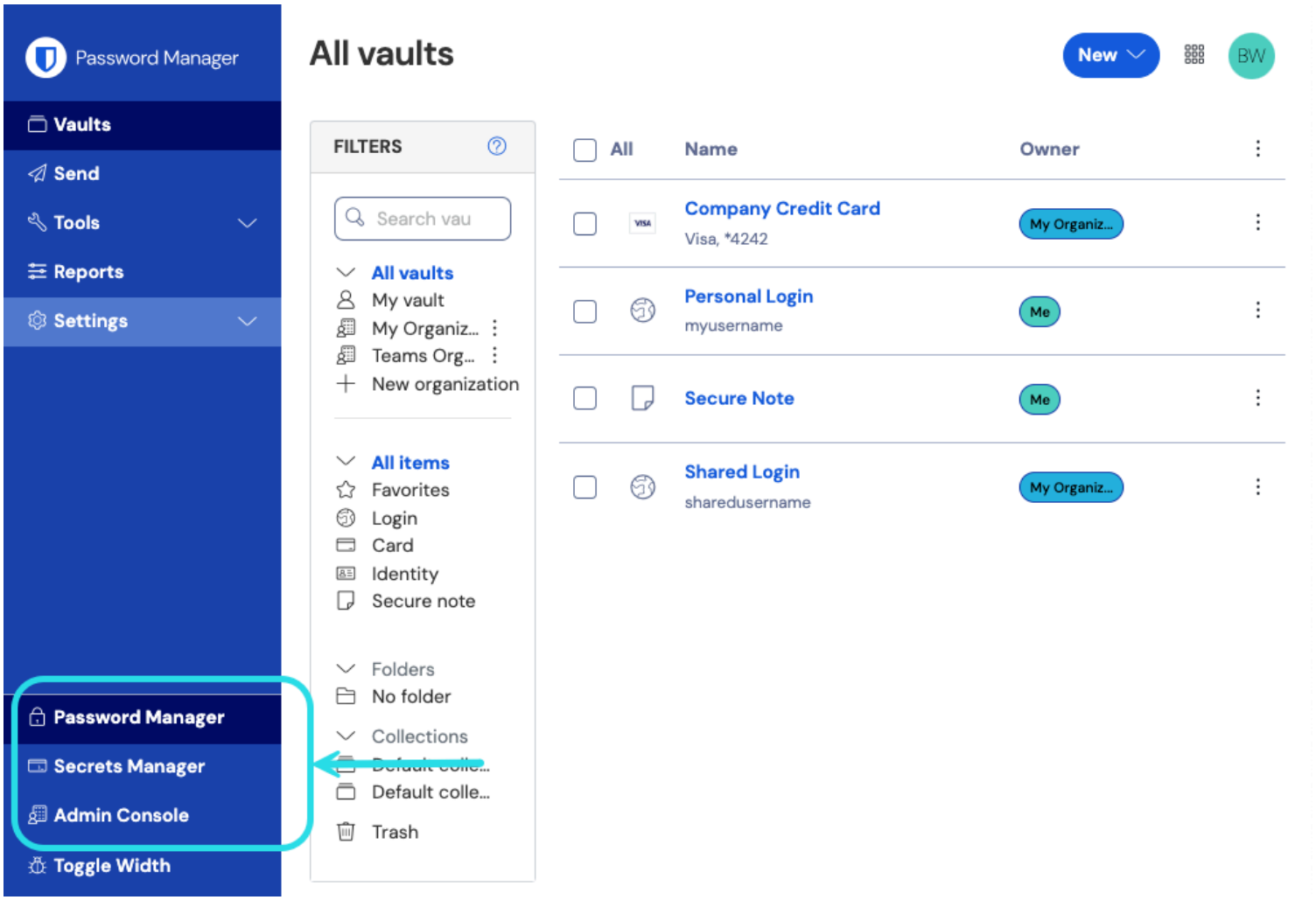
Event Logs

View in the help center:
https://bitwarden.com/help/event-logs/

Event Logs

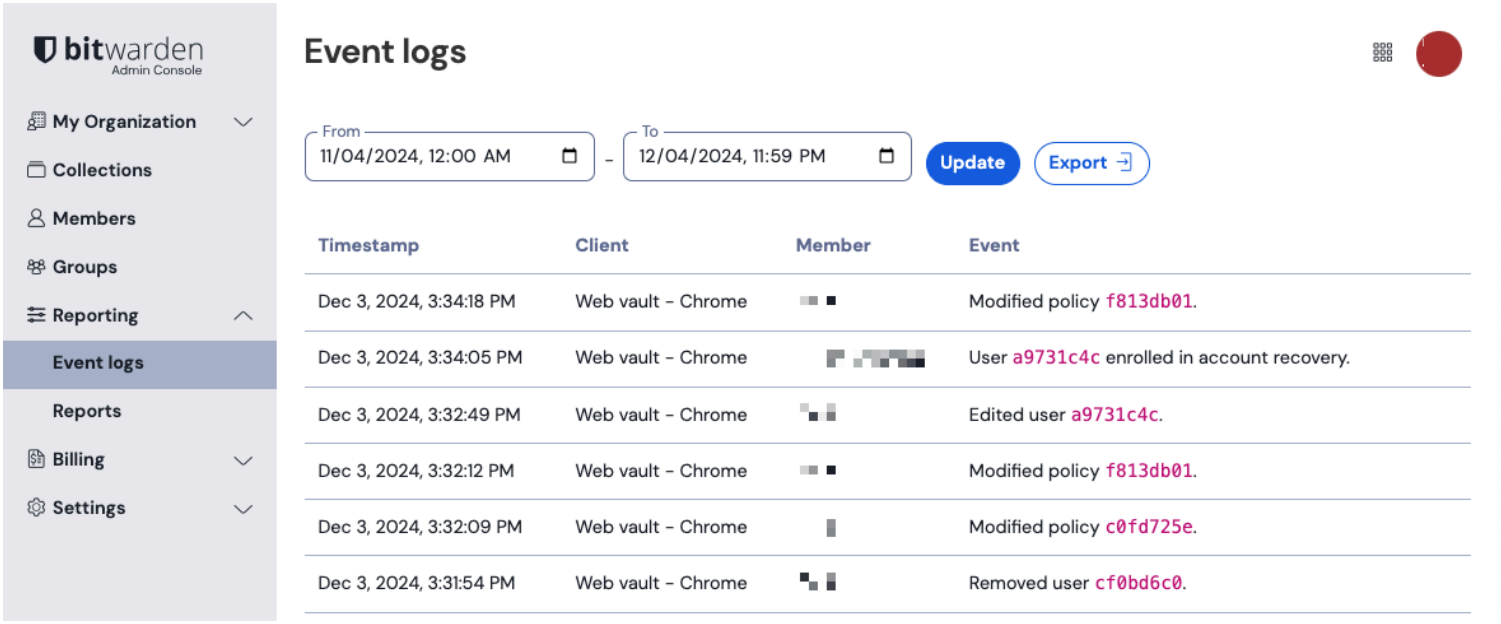
Event logs are timestamped records of events that occur within your Teams or Enterprise organization. To access event logs:

1. Log in to the Bitwarden web app and open the Admin Console using the product switcher:



Product switcher

2. Select **Reporting** → **Event logs** from the navigation:



Event logs

Events logs are exportable, accessible from the `/events` endpoint of the Bitwarden Public API, and are retained indefinitely, however only 367 days worth of data may be viewed at a time (as dictated by the range selectors).

Events are captured at both the Bitwarden client and server, with most events occurring at the client. While server event capture is instantaneous and quickly processed, clients push event data to the server every 60 seconds, so you may observe small delays in the reporting of recent events. Furthermore, client events data is communicated data an API call, and this is retried until success. As a result, if the client cannot communicate with the API or is somehow modified to not send events then they will not be received and therefore processed.

Inspect events

On the **Event logs** view in the web app, selecting a pink resource identifier (e.g. `1e685004`) will do two things:

1. Open a dialog box with a list of events associated with that resource. For example, selecting an item's identifier will open a list of times the item has been edited, viewed, etc., including which member took each action.

2. Navigate to a view where you access the resource. For example, selecting a member's identifier from **Event logs** will take you to the **Members** view and automatically filter the list down to that member.

Events list

Event logs record over 60 different types of events. The event logs screen captures a **Timestamp** for the event, client app information including application type and IP (accessed by hovering over the globe icon), the **User** connected to the event, and an **Event** description.

> **Note**
>
> Each **Event** is associated with a type code (`1000`, `1001`, etc.) that identifies the action captured by the event. Type codes are used by the Bitwarden Public API to identify the action documented by an event.

All Event types are listed below, with their corresponding type codes:

User events

- Logged In. (1000)
- Changed account password. (1001)
- Enabled/updated two-step login. (1002)
- Disabled two-step login. (1003)
- Recovered account from two-step login. (1004)
- Login attempted failed with incorrect password. (1005)
- Login attempt failed with incorrect two-step login. (1006)
- User exported their individual vault items. (1007)
- User updated a password issued through account recovery. (1008)
- User migrated their decryption key with Key Connector. (1009)
- User requested device approval. (1010)

Item events

- Created item item-identifier. (1100)
- Edited item item-identifier. (1101)
- Permanently Deleted item item-identifier. (1102)
- Created attachment for item item-identifier. (1103)
- Deleted attachment for item item-identifier. (1104)
- Moved item item-identifier to an organization. (1105)
- Edited collections for item item-identifier (1106)
- Viewed item item-identifier. (1107)
- Viewed password for item item-identifier. (1108)
- Viewed hidden field for item item-identifier. (1109)
- Viewed security code for item item-identifier. (1110)
- Copied password for item item-identifier. (1111)
- Copied hidden field for item item-identifier. (1112)
- Copied security code for item item-identifier. (1113)

- Autofilled item item-identifier. (1114)
- Sent item item-identifier to trash. (1115)
- Restored item item-identifier. (1116)
- Viewed Card Number for item item-identifier. (1117)

Collection events

- Created collection collection-identifier. (1300)
- Edited collection collection-identifier. (1301)
- Deleted collection collection-identifier. (1302)

Group events

- Created group group-identifier. (1400)
- Edited group group-identifier. (1401)
- Deleted group group-identifier. (1402)

Organization events

- Invited user user-identifier. (1500)
- Confirmed user user-identifier. (1501)
- Edited user user-identifier. (1502)
- Removed user user-identifier. (1503)
- Edited groups for user user-identifier. (1504)
- Unlinked SSO for user user-identifier. (1505)
- user-identifier enrolled in account recovery. (1506)
- user-identifier withdrew from account recovery. (1507)
- Master Password reset for user-identifier. (1508)
- Reset SSO link for user user-identifier. (1509)
- user-identifier logged in using SSO for the first time. (1510)
- Revoked organization access for user-identifier (1511)
- Restored organization access for user-identifier (1512)

- Approved device for user-identifier. (1513)
- Denied device for user-identifier. (1514)
- Deleted user user-identifier - an owner/admin deleted the user account. (1515)
- User user-identifier left organization. (1516)
- Edited organization settings. (1600)
- Purged organization vault. (1601)
- Exported organization vault. (1602)
- Organization Vault access by a managing Provider. (1603)
- Organization enabled SSO. (1604)
- Organization disabled SSO. (1605)
- Organization enabled Key Connector. (1606)
- Organization disabled Key Connector. (1607)
- Families Sponsorships synced. (1608)
- Modified collection management setting. (1609)
- Modified policy policy-identifier. (1700)
- Added domain domain-name. (2000)
- Removed domain domain-name. (2001)
- Domain-name verified. (2002)
- Domain-name not verified. (2003)

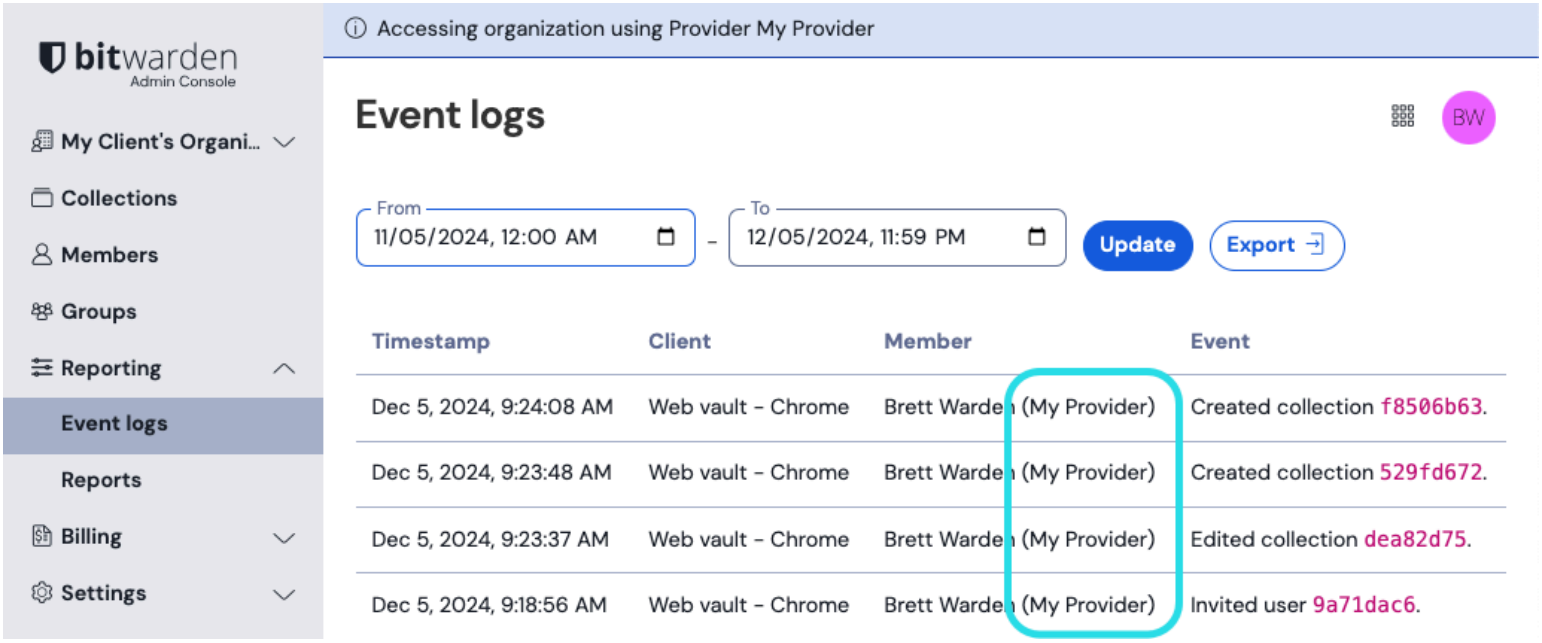
Secrets Manager events

Secrets Manager events are available both from the **Reporting** tab of your organization vault and from the service account Event logs page. The following Secrets Manager events are captured:

- Accessed secret secret-identifier. (2100)

Provider events

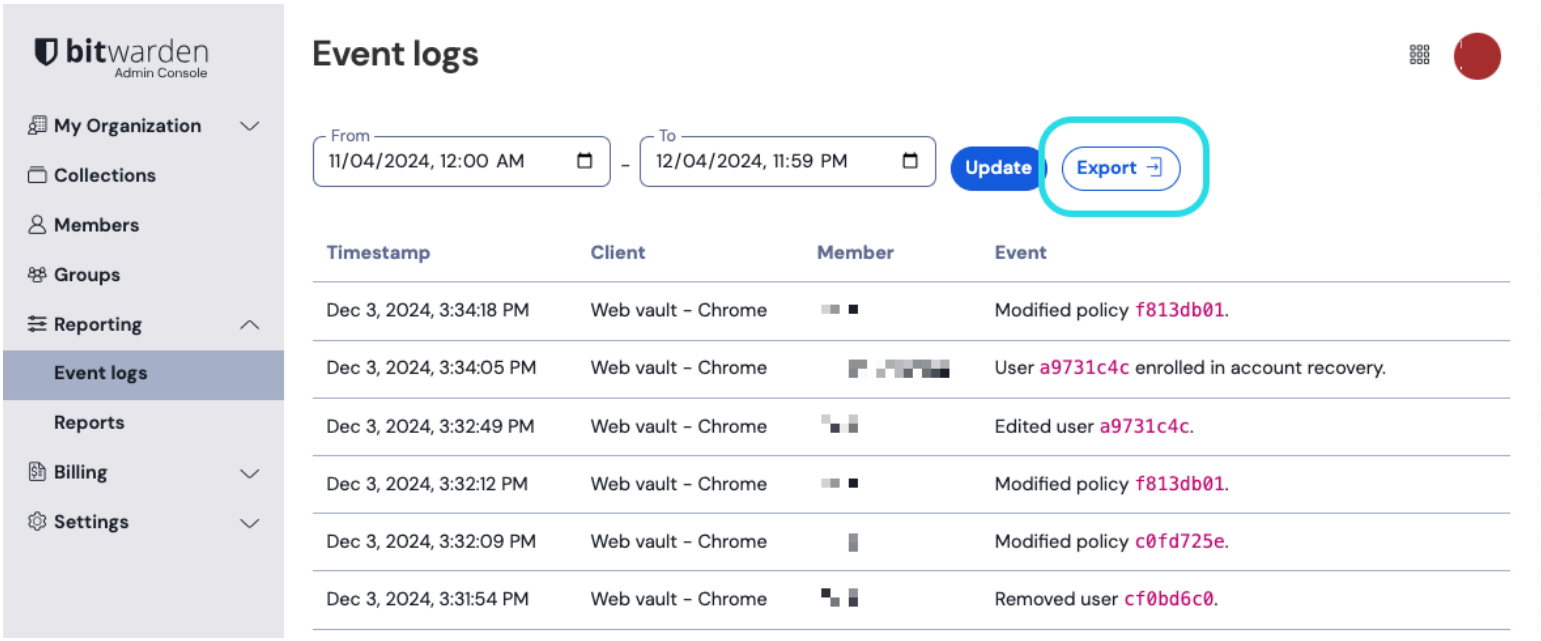
When any of the above events is executed by a member of an administering provider, the **User** column will record the name of the provider. Additionally, a provider-specific event will record whenever a member of an administering provider accesses your organization vault:



Provider accessing events

Export events

Exporting event logs will create a `.csv` of all events within the specified date range:



Export Event Logs

For example:

```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
```

API responses

Accessing event logs from the `/events` endpoint of the Bitwarden Public API will return a JSON response such as the following:

```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"
}
```

SIEM and external systems integrations

When exporting data from Bitwarden into other systems, a combination of data from the exports, API and CLI may be used to gather data. For example, using Bitwarden RESTful APIs to gather data around the structure of the organization:

- GET /public/members returns the members, ids, and assigned groupids
- GET /public/groups returns all the groups, ids, assigned collections, and their permissions
- GET /public/collections returns all collections, and their assigned groups

Once you have the unique id for each member, group, and collection, you can now use the CLI tool to gather information using the CLI command `bw-list` to retrieve the following items in JSON format:

- Org members
- Items
- Collections
- Groups

After gathering this data, you can join rows on their unique ids to build a reference to all parts of your Bitwarden organization. For more information on using the Bitwarden CLI, see the Bitwarden command-line tool (CLI).