

ADMINISTRATOR KONSOLE > BERICHTE

Ereignisprotokolle

Ansicht im Hilfezentrum:

<https://bitwarden.com/help/event-logs/>

Ereignisprotokolle

Ereignisprotokolle sind zeitgestempelte Aufzeichnungen von Ereignissen, die innerhalb Ihrer Teams oder Enterprise Organisation auftreten. Um auf Ereignisprotokolle zuzugreifen:

1. Melden Sie sich bei der Bitwarden-Web-App an und öffnen Sie die Administrator-Konsole mit dem Produktschalter (☰):

The screenshot displays the Bitwarden web application interface. On the left, a dark blue sidebar contains navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, Password Manager, Secrets Manager, Admin Console, and Toggle Width. The main content area is titled 'All vaults' and features a 'FILTERS' panel on the left and a list of vaults on the right. The 'FILTERS' panel includes a search bar and a list of categories: All vaults, All items, Folders, Collections, and Trash. The 'All items' category is expanded, showing options like Favorites, Login, Card, Identity, Secure note, No folder, and Default colle... (highlighted with a red arrow). The vaults list has columns for Name and Owner, with entries like 'Company Credit Card', 'Personal Login', 'Secure Note', and 'Shared Login'. A red circle highlights the 'Admin Console' option in the sidebar.

Produktwechsler

2. Wählen Sie **Berichterstattung** → **Ereignisprotokolle** aus der Navigation:

- My Organization
- Collections
- Members
- Groups
- Reporting
- Event logs
- Reports
- Billing
- Settings

Event logs

From - To
Update
Export

Timestamp	Client	Member	Event
Dec 3, 2024, 3:34:18 PM	Web vault - Chrome	■ ■	Modified policy f813db01 .
Dec 3, 2024, 3:34:05 PM	Web vault - Chrome	■ ■ ■ ■ ■ ■ ■ ■	User a9731c4c enrolled in account recovery.
Dec 3, 2024, 3:32:49 PM	Web vault - Chrome	■ ■ ■	Edited user a9731c4c .
Dec 3, 2024, 3:32:12 PM	Web vault - Chrome	■ ■	Modified policy f813db01 .
Dec 3, 2024, 3:32:09 PM	Web vault - Chrome	■	Modified policy c0fd725e .
Dec 3, 2024, 3:31:54 PM	Web vault - Chrome	■ ■ ■	Removed user cf0bd6c0 .

Ereignisprotokolle

Ereignisprotokolle sind exportierbar, zugänglich vom `/events` Endpunkt der [Bitwarden Öffentliche API](#), und werden unbegrenzt aufbewahrt, jedoch können nur Daten für 367 Tage auf einmal angesehen werden (wie von den Bereichsauswählern vorgegeben).

Die meisten Ereignisse erfassen Aktionen, die in verschiedenen Bitwarden-Clients durchgeführt werden, welche Ereignisdaten alle 60 Sekunden an den Server senden, daher können Sie kleine Verzögerungen bei der Berichterstattung über kürzlich aufgetretene Ereignisse feststellen.

Ereignisse überprüfen

Auf der **Ereignisprotokolle** Ansicht in der Web-App führt die Auswahl einer rosa Ressourcenkennung (z.B. **1e685004**) zu zwei Dingen:

- Öffnen Sie ein Dialogfeld mit einer Liste von Ereignissen, die mit dieser Ressource verbunden sind. Zum Beispiel öffnet die Auswahl der Kennung eines Eintrags eine Liste der Zeiten, zu denen der Eintrag bearbeitet, angesehen usw. wurde, einschließlich welches Mitglied jede Aktion durchgeführt hat.
- Navigieren Sie zu einer Ansicht, in der Sie auf die Ressource zugreifen können. Zum Beispiel führt die Auswahl der Kennung eines Mitglieds aus den **Ereignisprotokollen** Sie zur **Mitglieder** Ansicht und filtert die Liste automatisch auf dieses Mitglied herunter.

Liste der Veranstaltungen

Ereignisprotokolle zeichnen über 50 verschiedene Typen von Ereignissen auf. Der Bildschirm für Ereignisprotokolle erfasst einen **Zeitstempel** für das Ereignis, Client-App-Informationen einschließlich Anwendungstyp und IP (zugänglich durch Überfahren des Globus-Symbols), den mit dem Ereignis verbundenen **Benutzer** und eine **Ereignis** Beschreibung.

Note

Jedes **Ereignis** ist mit einem Typ-Code (**1000**, **1001**, usw.) verbunden, der die durch das Ereignis erfasste Aktion identifiziert. Typcodes werden von der [Bitwarden Öffentlichen API](#) verwendet, um die Aktion zu identifizieren, die von einem Ereignis dokumentiert wird.

Alle Veranstaltungstypen sind unten aufgeführt, zusammen mit ihren entsprechenden Typ-Codes:

Benutzereignisse

- Angemeldet. (1000)
- Geändertes Konto Passwort. (1001)
- Aktivierte/Aktualisierte zweistufige Zugangsdaten. (1002)
- Zweistufige Zugangsdaten deaktiviert. (1003)
- Konto durch Zwei-Schritt-Zugangsdaten wiederhergestellt. (1004)
- Anmeldeversuch mit falschem Passwort fehlgeschlagen. (1005)
- Der Versuch, sich mit den falschen zweistufigen Zugangsdaten anzumelden, ist fehlgeschlagen. (1006)
- Der Benutzer hat seine einzelnen Tresor-Einträge exportiert. (1007)
- Benutzer hat ein durch [Kontowiederherstellung](#) ausgegebenes Passwort aktualisiert. (1008)
- Der Benutzer hat seinen Entschlüsselungsschlüssel mit [Key Connector](#) migriert. (1009)
- Benutzer hat um [Gerätefreigabe](#) gebeten. (1010)

Eintrag Ereignisse

- Erstellter Eintrag *item-identifizier*. (1100)
- Bearbeiteter Eintrag *item-identifizier*. (1101)
- Dauerhaft gelöschter Eintrag *item-identifizier*. (1102)
- Anhang für Eintrag *item-identifizier* erstellt. (1103)
- Gelöschter Anhang für Eintrag *item-identifizier*. (1104)
- Verschobener Eintrag *item-identifizier* zu einer Organisation. (1105)
- Bearbeitete Sammlungen für den Eintrag *item-identifizier* (1106)
- Betrachteter Eintrag *item-identifizier*. (1107)
- Angesehenes Passwort für den Eintrag *item-identifizier*. (1108)
- Angesehenes verstecktes Feld für den Eintrag *item-identifizier*. (1109)
- Angesehener Sicherheitscode für den Eintrag *item-identifizier*. (1110)
- Kopiertes Passwort für den Eintrag *item-identifizier*. (1111)
- Kopiertes verstecktes Feld für den Eintrag *item-identifizier*. (1112)
- Kopierter Sicherheitscode für den Eintrag *item-identifizier*. (1113)

- Auto-Ausfüllen Eintrag *item-identifier*. (1114)
- Gesendeter Eintrag *item-identifier* in den Papierkorb verschoben. (1115)
- Wiederhergestellter Eintrag *item-identifier*. (1116)
- Angesehene Kartenummer für den Eintrag *item-identifier*. (1117)

Sammlungsveranstaltungen

- Erstellte Sammlung *collection-identifier*. (1300)
- Bearbeitete Sammlung *Sammlungs-Kennung*. (1301)
- Gelöschte Sammlung *collection-identifier*. (1302)

Gruppenveranstaltungen

- Erstellte Gruppe *group-identifier*. (1400)
- Bearbeitete Gruppe *group-identifier*. (1401)
- Gelöschte Gruppe *group-identifier*. (1402)

Veranstaltungen der Organisation

- Eingeladener Benutzer *Benutzerkennung*. (1500)
- Bestätigter Benutzer *Benutzerkennung*. (1501)
- Bearbeiteter Benutzer *user-identifier*. (1502)
- Entfernter Benutzer *Benutzer-Identifikator*. (1503)
- Bearbeitete Gruppen für Benutzer *user-identifier*. (1504)
- Nicht verknüpftes SSO für Benutzer *user-identifier*. (1505)
- *Benutzerkennung*, die bei der Kontowiederherstellung registriert ist. (1506)
- *Benutzer-Identifikator* hat sich von der Konto-Wiederherstellung zurückgezogen. (1507)
- Master-Passwort zurücksetzen für *Benutzerkennung*. (1508)
- SSO-Link für den Benutzer *user-identifier* zurücksetzen. (1509)
- *Benutzerkennung* hat sich zum ersten Mal mit SSO angemeldet. (1510)
- Zugriff auf die Organisation für *Benutzerkennung* (1511) widerrufen
- Stellt den Zugang zur Organisation für *Benutzerkennung* (1512) wieder her
- Genehmigtes Gerät für *Benutzerkennung*. (1513)

- Gerät für *Benutzererkennung* verweigert. (1514)
- Bearbeitete Organisationseinstellungen. (1600)
- Gelöschter Tresor der Organisation. (1601)
- Exportierter Organisationstresor. (1602)
- Zugriff auf den Organisationstresor durch einen verwaltenden [Anbieter](#). (1603)
- Organisation hat SSO aktiviert. (1604)
- Organisation hat SSO deaktiviert. (1605)
- Organisation ermöglichte Key Connector. (1606)
- Organisation hat Key Connector deaktiviert. (1607)
- Families Sponsorings synchronisiert. (1608)
- Geänderte Richtlinie *Richtlinien-Kennung*. (1700)
- Hinzugefügte Domain *domain-name*. (2000)
- Entfernte Domain *domain-name*. (2001)
- *Domain-Name* verifiziert. (2002)
- *Domain-Name* nicht verifiziert. (2003)

Secrets Manager Ereignisse

Secrets Manager Ereignisse sind sowohl über den **Bericht** Tab Ihres Organisationstresors als auch über die [Ereignisprotokollseite des Dienstkonto](#) verfügbar. Die folgenden Secrets Manager Ereignisse werden erfasst:

- Zugriff auf geheimes *Geheimnis-Kennung*. (2100)

Anbieterveranstaltungen

Wenn eines der oben genannten Ereignisse von einem Mitglied eines [verwaltenden Anbieters](#) ausgeführt wird, wird in der **Benutzer**-Spalte der Name des Anbieters aufgezeichnet. Zusätzlich wird ein anbieterspezifisches Ereignis aufgezeichnet, wann immer ein Mitglied eines verwaltenden Anbieters auf Ihren Organisationstresor zugreift:

① Accessing organization using Provider My Provider

Event logs

From 11/05/2024, 12:00 AM - To 12/05/2024, 11:59 PM **Update** **Export**

Timestamp	Client	Member	Event
Dec 5, 2024, 9:24:08 AM	Web vault - Chrome	Brett Warden (My Provider)	Created collection f8506b63 .
Dec 5, 2024, 9:23:48 AM	Web vault - Chrome	Brett Warden (My Provider)	Created collection 529fd672 .
Dec 5, 2024, 9:23:37 AM	Web vault - Chrome	Brett Warden (My Provider)	Edited collection dea82d75 .
Dec 5, 2024, 9:18:56 AM	Web vault - Chrome	Brett Warden (My Provider)	Invited user 9a71dac6 .

Anbieter greift auf Ereignisse zu

Exportveranstaltungen

Das Exportieren von Ereignisprotokollen erstellt eine **.CSV** aller Ereignisse innerhalb des angegebenen Datumsbereichs:

Event logs

From 11/04/2024, 12:00 AM - To 12/04/2024, 11:59 PM **Update** **Export**

Timestamp	Client	Member	Event
Dec 3, 2024, 3:34:18 PM	Web vault - Chrome	■ ■	Modified policy f813db01 .
Dec 3, 2024, 3:34:05 PM	Web vault - Chrome	■ ■ ■ ■ ■ ■	User a9731c4c enrolled in account recovery.
Dec 3, 2024, 3:32:49 PM	Web vault - Chrome	■ ■	Edited user a9731c4c .
Dec 3, 2024, 3:32:12 PM	Web vault - Chrome	■ ■	Modified policy f813db01 .
Dec 3, 2024, 3:32:09 PM	Web vault - Chrome	■	Modified policy c0fd725e .
Dec 3, 2024, 3:31:54 PM	Web vault - Chrome	■ ■	Removed user cf0bd6c0 .

Export von Ereignisprotokollen

Zum Beispiel:

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.c
om,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-Antworten

Der Zugriff auf Ereignisprotokolle vom `/events` Endpunkt der Bitwarden Öffentliche API liefert eine JSON-Antwort wie die folgende:

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 und Integrationen externer Systeme

Beim Export von Daten aus Bitwarden in andere Systeme kann eine Kombination von Daten aus dem Export, API und CLI verwendet werden, um Daten zu sammeln. Zum Beispiel, die Verwendung von Bitwarden RESTful APIs, um Daten über die Struktur der Organisation zu

sammeln:

- GET /public/members gibt die Mitglieder, IDs und zugewiesenen Gruppen-IDs zurück
- GET /public/groups gibt alle Gruppen, IDs, zugewiesene Sammlungen und deren Berechtigungen zurück.
- GET /public/collections gibt alle Sammlungen und ihre zugeordneten Gruppen zurück.

Sobald Sie die eindeutige ID für jedes Mitglied, jede Gruppe und jede Sammlung haben, können Sie nun das CLI-Tool verwenden, um Informationen mit dem CLI-Befehl `bw-list` zu sammeln und die folgenden Einträge im JSON-Format abzurufen:

- Org Mitglieder
- Einträge
- Sammlungen
- Gruppen

Nachdem Sie diese Daten gesammelt haben, können Sie Zeilen anhand ihrer eindeutigen IDs verbinden, um eine Referenz zu allen Teilen Ihrer Bitwarden-Organisation zu erstellen. Für weitere Informationen zur Verwendung des Bitwarden CLI, siehe [das Bitwarden-Befehlszeilentool \(CLI\)](#).