bitwarden | Artikel Helpcentrum

BEHEERCONSOLE > RAPPORTAGE

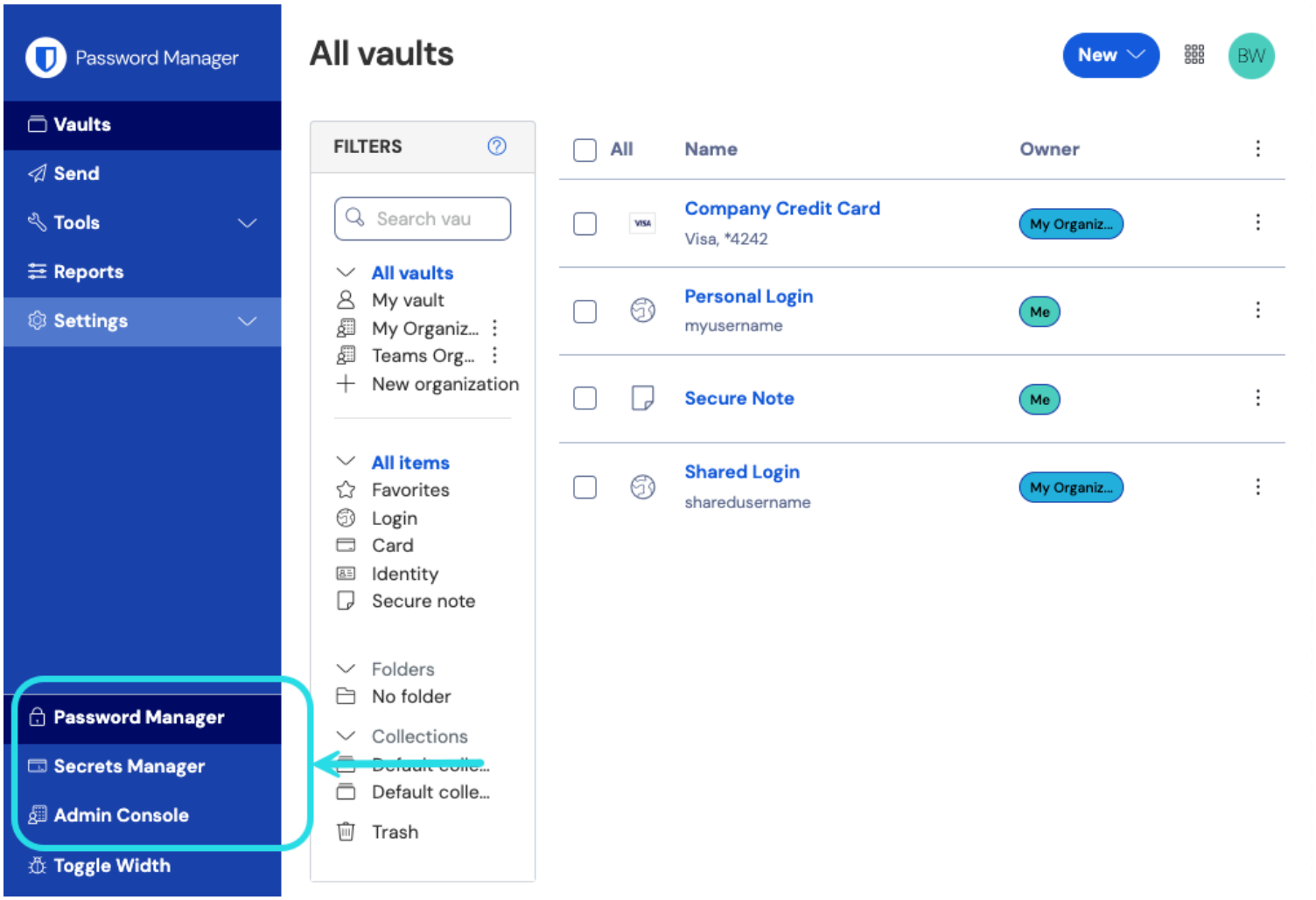
Gebeurtenislogboeken

Weergeven in het Helpcentrum:
https://bitwarden.com/help/event-logs/

Gebeurtenislogboeken

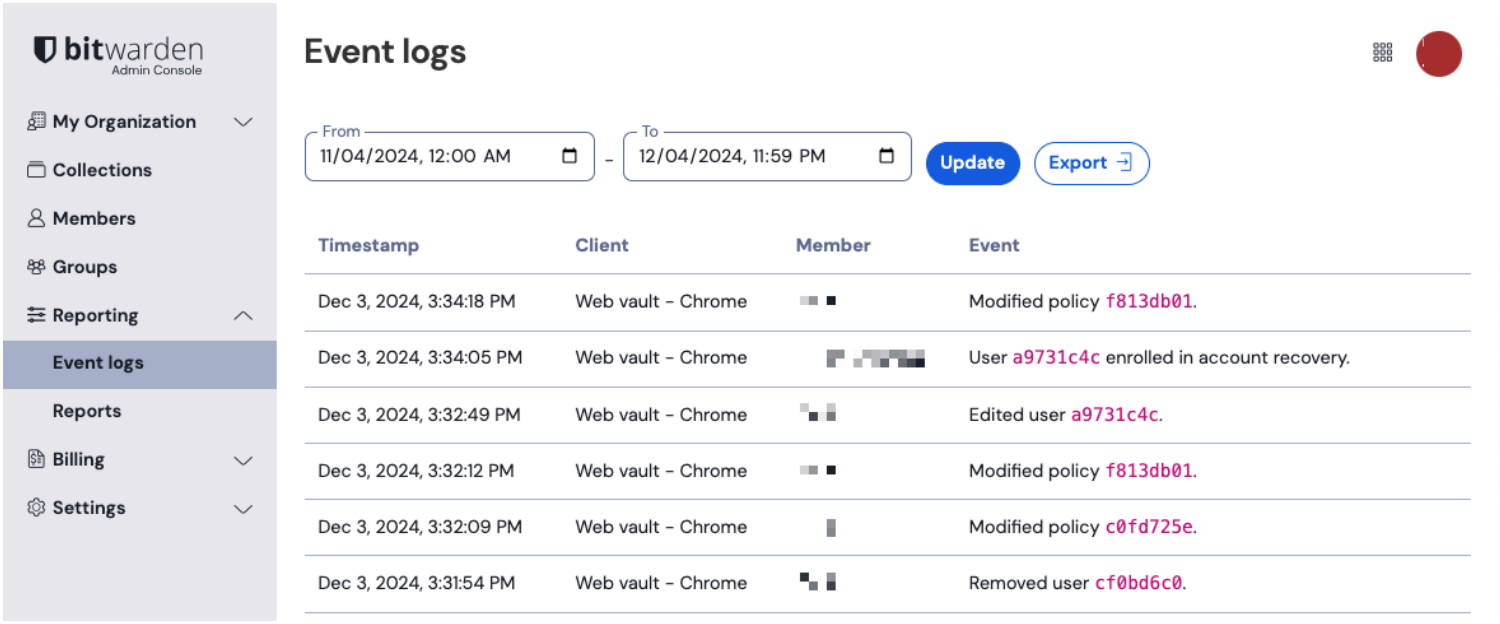
Gebeurtenislogs zijn tijdstempels van gebeurtenissen die plaatsvinden binnen je Teams of Enterprise-organisatie. Gebeurtenislogboeken openen:

1. Log in op de Bitwarden web app en open de Admin Console met behulp van de product switcher (⊞):



Product switcher

2. Selecteer **Rapportage** → **Gebeurtenislogboeken** in de navigatie:



Gebeurtenislogboeken

Gebeurtenissenlogboeken kunnen worden geëxporteerd en zijn toegankelijk via het `/events` eindpunt van de Bitwarden Openbare API. Ze worden voor onbepaalde tijd bewaard, maar er kunnen slechts gegevens van 367 dagen per keer worden bekeken (zoals bepaald door de bereikselectors).

De meeste gebeurtenissen leggen acties vast die zijn uitgevoerd in verschillende Bitwarden-clients, die elke 60 seconden gebeurtenisgegevens naar de server sturen, dus u kunt kleine vertragingen waarnemen in de rapportage van recente gebeurtenissen.

Gebeurtenissen inspecteren

In de weergave **Gebeurtenislogboeken** in de web-app doet het selecteren van een roze resource-identifier (bijv. `1e685004`) twee dingen:

1. Open een dialoogvenster met een lijst van gebeurtenissen die bij die bron horen. Als je bijvoorbeeld de identifier van een item selecteert, krijg je een lijst te zien met de keren dat het item bewerkt, bekeken, etc. is, inclusief welk lid elke actie ondernam.

2. Navigeer naar een weergave waar je de bron opent. Als je bijvoorbeeld de identificatie van een lid selecteert in **Gebeurtenislogboeken**, ga je naar de weergave **Leden** en wordt de lijst automatisch gefilterd tot dat lid.

Evenementenlijst

Gebeurtenislogboeken registreren meer dan 50 verschillende soorten gebeurtenissen. Het logboekscherm van de gebeurtenis bevat een **tijdstempel** voor de gebeurtenis, informatie over de client-app inclusief applicatietype en IP (toegankelijk door met de muis over het pictogram wereldbol te gaan), de **gebruiker** die met de gebeurtenis verbonden was en een beschrijving van **de gebeurtenis**.

> **Note**
>
> Elke **gebeurtenis** is geassocieerd met een typecode (`1000`, `1001`, enz.) die de actie identificeert die door de gebeurtenis wordt vastgelegd. Typecodes worden door de Bitwarden Public API gebruikt om de actie te identificeren die door een gebeurtenis wordt gedocumenteerd.

Alle gebeurtenistypen staan hieronder vermeld, met de bijbehorende typecodes:

Gebeurtenissen voor gebruikers

- Aangemeld. (1000)
- Wachtwoord van account gewijzigd. (1001)
- Inloggen in twee stappen ingeschakeld/geactualiseerd. (1002)
- Inloggen in twee stappen uitgeschakeld. (1003)
- Account hersteld van inloggen in twee stappen. (1004)
- Inlogpoging mislukt met onjuist wachtwoord. (1005)
- Aanmeldingspoging mislukt met onjuiste tweestapsaanmelding. (1006)
- Gebruiker heeft zijn individuele kluisitems geëxporteerd. (1007)
- Gebruiker heeft een wachtwoord bijgewerkt dat is uitgegeven via accountherstel. (1008)
- Gebruiker heeft zijn ontcijferingssleutel gemigreerd met Key Connector. (1009)
- Door gebruiker aangevraagde goedkeuring voor apparaat. (1010)

Item gebeurtenissen

- Aangemaakt item *item-identifier*. (1100)
- Bewerkt item *item-identifier*. (1101)
- Permanent verwijderd item *item-identifier*. (1102)
- Bijlage aangemaakt voor item *item-identifier*. (1103)
- Bijlage voor *item-identificatie* verwijderd. (1104)
- *Item-identifier* verplaatst naar een organisatie. (1105)
- Bewerkte collecties voor item *item-identifier* (1106)
- Bekeken item *item-identifier*. (1107)
- Wachtwoord bekeken voor item *item-identifier*. (1108)
- Verborgen veld voor item *item-identifier* bekeken. (1109)
- Beveiligingscode voor item *item-identifier* bekeken. (1110)
- Wachtwoord gekopieerd voor item *item-identifier*. (1111)
- Verborgen veld voor item *item-identifier* gekopieerd. (1112)
- Gekopieerde beveiligingscode voor item *item-identifier*. (1113)

- Automatisch ingevuld item *item-identifier*.(1114)
- Item *item-identifier* naar prullenbak gestuurd.(1115)
- Hersteld item *item-identifier*.(1116)
- Bekeken kaartnummer voor item *item-identifier*.(1117)

Gebeurtenissen

- Collectie *collectie-identifier* aangemaakt.(1300)
- Bewerkte collectie *collectie-identificatiecode*.(1301)
- Verwijderde collectie *collectie-identifier*.(1302)

Groepsevenementen

- Groep *groepsidentificatie* aangemaakt.(1400)
- Bewerkte groep *Groepsidentificatie*.(1401)
- Verwijderde groep *groep-identifier*.(1402)

Organisatie evenementen

- Uitgenodigde gebruiker *gebruikersidentificatie*.(1500)
- Bevestigde gebruiker *gebruikersidentificatie*.(1501)
- Bewerkte gebruiker *gebruikersidentificatie*.(1502)
- *Gebruiker-identificatie* verwijderd.(1503)
- Bewerkte groepen voor gebruiker *user-identifier*.(1504)
- Niet gekoppelde SSO voor *gebruiker-identificatie*.(1505)
- *user-identifier* geregistreerd voor accountherstel.(1506)
- *user-identifier* teruggetrokken uit accountherstel.(1507)
- Hoofdwachtwoord opnieuw ingesteld voor *gebruiker-identificatie*.(1508)
- SSO-koppeling opnieuw instellen voor *gebruiker-identificatie*.(1509)
- *user-identifier* heeft zich voor het eerst aangemeld met SSO.(1510)
- Toegang organisatie ingetrokken voor *gebruiker-ID* (1511)
- Herstelt toegang tot organisatie voor *gebruiker-ID* (1512)
- Goedgekeurd apparaat voor *gebruikersidentificatie*.(1513)

- Geweigerd apparaat voor *gebruikersidentificatie*. (1514)
- Bewerkte organisatie-instellingen. (1600)
- Gezuiverde organisatiekluis. (1601)
- Geëxporteerde organisatie kluis. (1602)
- Organisatie Kluis toegang door een beherende Aanbieder. (1603)
- Organisatie ingeschakeld SSO. (1604)
- Organisatie uitgeschakeld SSO. (1605)
- Organisatie ingeschakeld Key Connector. (1606)
- Organisatie uitgeschakeld Key Connector. (1607)
- Gezinnen Sponsoring gesynchroniseerd. (1608)
- Gewijzigd beleid *policy-identifier*. (1700)
- Domein *domeinnaam* toegevoegd. (2000)
- Domein *domeinnaam* verwijderd. (2001)
- *Domeinnaam* geverifieerd. (2002)
- *Domeinnaam* niet geverifieerd. (2003)

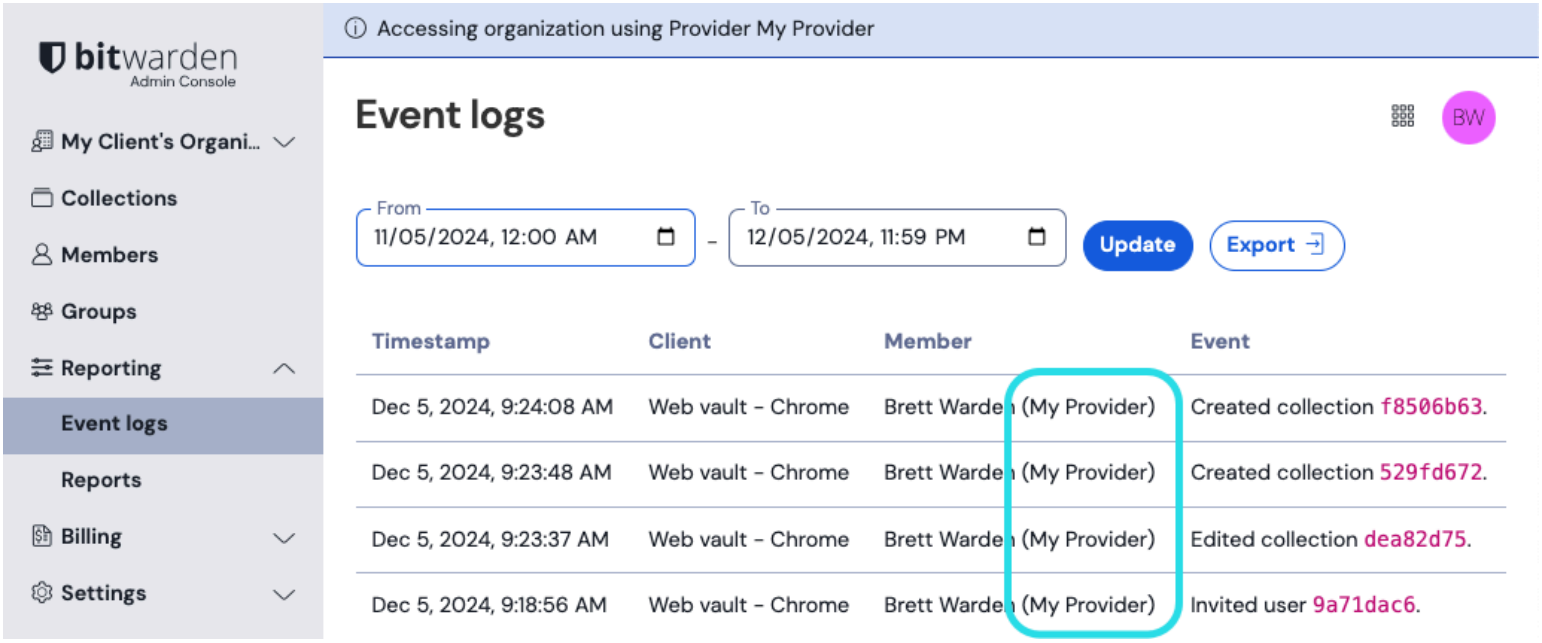
Geheimen Manager-gebeurtenissen

Gebeurtenissen van Secrets Manager zijn zowel beschikbaar op het tabblad **Rapportage** van je organisatiekluis als op de pagina Gebeurtenissenlogboeken van de serviceaccount. De volgende gebeurtenissen van Secrets Manager worden vastgelegd:

- Toegang *geheim-identificatiecode*. (2100)

Evenementen voor aanbieders

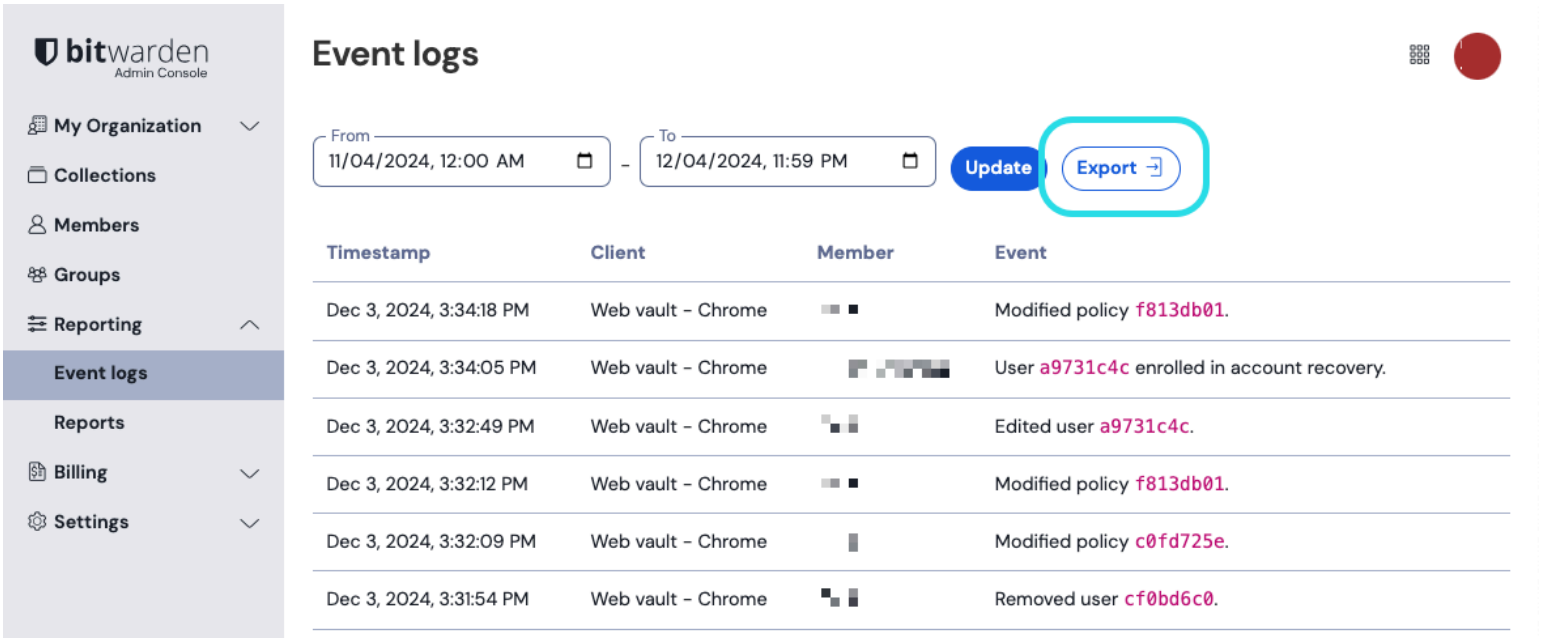
Wanneer een van de bovenstaande gebeurtenissen wordt uitgevoerd door een lid van een administrator provider, zal de kolom **User** de naam van de provider weergeven. Daarnaast zal een provider-specifieke gebeurtenis registreren wanneer een lid van een administrerende provider toegang krijgt tot de kluis van je organisatie:



Provider toegang tot gebeurtenissen

Gebeurtenissen exporteren

Gebeurtenislogboeken exporteren maakt een `.csv` van alle gebeurtenissen binnen het opgegeven datumbereik:



Gebeurtenislogboeken exporteren

Bijvoorbeeld:

```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-reacties

Toegang tot gebeurtenislogboeken via het `/events` eindpunt van de Bitwarden Publieke API levert een JSON antwoord op zoals het volgende:

```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 en integraties met externe systemen

Bij het exporteren van gegevens van Bitwarden naar andere systemen kan een combinatie van gegevens uit de export, API en CLI worden gebruikt om gegevens te verzamelen. Bijvoorbeeld door gebruik te maken van Bitwarden RESTful API's om gegevens te verzamelen over de structuur van de organisatie:

- GET /public/members retourneert de leden, id's en toegewezen groepids
- GET /public/groups retourneert alle groepen, id's, toegewezen verzamelingen en hun rechten
- GET /public/collections retourneert alle collecties en hun toegewezen groepen

Zodra je de unieke id hebt voor elk lid, groep en collectie, kun je nu de CLI tool gebruiken om informatie te verzamelen met het CLI commando `bw-list` om de volgende items op te halen in JSON formaat:

- Org-leden
- Items
- Collecties
- Groepen

Nadat u deze gegevens hebt verzameld, kunt u rijen samenvoegen op basis van hun unieke id's om een referentie te maken naar alle onderdelen van uw Bitwarden-organisatie. Voor meer informatie over het gebruik van de Bitwarden CLI, zie de Bitwarden command-line tool (CLI).