

BEHEERCONSOLE

Openbare API van Bitwarden

Openbare API van Bitwarden

De Bitwarden Public API biedt organisaties een reeks tools voor het beheren van leden, collecties, groepen, gebeurtenislogboeken en beleidsregels.

💡 Tip

Met deze API is het niet mogelijk om individuele kluisitems te beheren. Als je dit wilt bereiken, gebruik dan de [Vault Management API](#).

De Public API is een RESTful API met voorspelbare resource-georiënteerde URL's, accepteert JSON-gecodeerde request bodies, retourneert JSON-gecodeerde responses en gebruikt standaard HTTP response codes, authenticatie en verbs.

De openbare API is compatibel met de OpenAPI Specification (OAS3) en publiceert een compatibele [swagger.json](#) definitiebestand. Verken de OpenAPI-specificatie met de Swagger UI:

- Voor publieke cloud-gehoste instanties: <https://bitwarden.com/help/api/>
- Voor zelf gehoste instanties: <https://your.domain.com/api/docs/>

📘 Note

Toegang tot de Bitwarden Public API is beschikbaar voor klanten van alle Enterprise- en Teams-organisaties. Voor meer informatie, zie [Over Bitwarden Plannen](#).

Eindpunten

Basis URL

Voor cloud-hosted, <https://api.bitwarden.com> of <https://api.bitwarden.eu>.

Voor zelf gehost, <https://your.domain.com/api>.

Eindpunten voor verificatie

Voor cloud-hosted, <https://identity.bitwarden.com/connect/token> of <https://identity.bitwarden.eu/connect/token>.

Voor zelf gehost, <https://your.domain.com/identity/connect/token>.

Authenticatie

De API maakt gebruik van tokens om zich te authenticeren bij beschermde API-eindpunten. Bitwarden gebruikt een [OAuth2 Client Credentials](#) aanvraagstroom om tokens toe te kennen vanaf het eindpunt. Authenticatieverzoeken hebben `client_id` en `client_secret` als vereiste parameters.

💡 Tip

De API-sleutel die wordt gebruikt voor verificatie met de Openbare API is **niet dezelfde** als de [persoonlijke API-sleutel](#). API-sleutels voor organisaties hebben een `client_id` met het formaat "`organization.ClientId`", terwijl persoonlijke API-sleutels een `client_id` hebben met het formaat "`user.clientId`".

De API Key `client_id` en `client_secret` kunnen door een eigenaar worden verkregen via de Admin Console vault door te navigeren naar **Instellingen** → **Organisatie info** scherm en naar beneden te scrollen naar de **API key** sectie:

Organization info

Organization name (required)

Billing email (required)

Business name

[Save](#)

API Key

Your API key can be used to authenticate to the Bitwarden public API. [Learn more](#)

[View API key](#) [Rotate API key](#)

Collection management

Verkrijg een organisatie API sleutel

Als u als eigenaar de API-sleutel wilt delen met een beheerder of andere gebruiker, gebruik dan een veilige communicatiemethode zoals [Bitwarden Send](#).

Warning

De API-sleutel van je organisatie geeft volledige toegang tot je organisatie. Houd je API-sleutel privé. Als u denkt dat uw API-sleutel gecompromitteerd is, selecteer dan **Instellingen > Organisatie info > Draai API-sleutel** knop op dit scherm. Actieve implementaties van uw huidige API-sleutel moeten voor gebruik opnieuw worden geconfigureerd met de nieuwe sleutel.

Toegangstokens aan toonder

Om een token voor toegang tot de drager te verkrijgen, doe je een **POST-verzoek** met **Content-Type: application/x-www-form-urlencoded** met je **client_id** en **client_secret** naar het **authenticatie-eindpunt**. Als je de API gebruikt voor organisatiebeheer, gebruik je altijd **grant_type=client_credentials** en **scope=api.organization**. Bijvoorbeeld:

Bash

```
curl -X POST \
  https://identity.bitwarden.com/connect/token \
  -H 'Content-Type: application/x-www-form-urlencoded' \
  -d 'grant_type=client_credentials&scope=api.organization&client_id=<ID>&client_secret=<SECRET>'
```

Dit verzoek resulteert in het volgende antwoord:

Bash

```
{
  "access_token": "<TOKEN>",
  "expires_in": 3600,
  "token_type": "Bearer"
}
```

In dit antwoord vertegenwoordigt **3600** de vervalwaarde (in seconden), wat betekent dat dit token 60 minuten geldig is nadat het is uitgegeven. Als u een API-aanroep doet met een verlopen token, krijgt u een **401 onbevoegd** responscode.

Typen inhoud

De Bitwarden Public API communiceert met `application/json` requests en responses, met één uitzondering:

Het authenticatie-eindpunt verwacht een `application/x-www-form-urlencoded` verzoek, maar zal antwoorden met `application/json`.

Monsteraanvraag

Bash

```
curl -X GET \
  https://api.bitwarden.com/public/collections \
  -H 'Authorization: Bearer <TOKEN>'
```

Waarbij is de waarde voor de `access_token`: sleutel in het verkregen toegangsbewijs voor de drager.

Dit verzoek zal resulteren in een antwoord:

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"
}
```

Status

Bitwarden heeft een openbare [statuspagina](#), waar je informatie kunt vinden over de gezondheid van diensten en incidenten voor alle diensten, inclusief de Openbare API.

Antwoordcodes

De Bitwarden Public API gebruikt conventionele HTTP responscodes om het succes of falen van een API verzoek aan te geven:

Statuscode	Beschrijving
200 OK	Alles werkte zoals verwacht.
400 Slecht Verzoek	Het verzoek was onacceptabel, mogelijk door ontbrekende of misvormde parameter(s).

Statuscode	Beschrijving
401 Niet toegestaan	Het token voor toegang tot de drager ontbrak, was ongeldig of verlopen.
404 niet gevonden	De gevraagde bron bestaat niet.
429 Te veel verzoeken	Te veel verzoeken raken de API te snel. We raden aan om het aantal verzoeken terug te brengen.
500, 502, 503, 504 Serverfout	Er ging iets mis bij Bitwarden. Dit komt zelden voor, maar neem contact met ons op als dit gebeurt.

Verder lezen

Voor meer informatie over het gebruik van de Bitwarden Public API, zie de volgende artikelen:

- [Bitwarden Openbare API OAS Specificatie](#)
- [Gebeurtenislogboeken](#)