

ADMIN CONSOLE

Bitwarden Public API

View in the help center:

<https://bitwarden.com/help/public-api/>

Bitwarden Public API

The Bitwarden Public API provides organizations a suite of tools for managing members, collections, groups, event logs, and policies.

Tip

This API does not allow for management of individual vault items. If this is what you need to accomplish, use the [Vault Management API](#) instead.

The Public API is a RESTful API with predictable resource-oriented URLs, accepts JSON-encoded request bodies, returns JSON-encoded responses, and uses standard HTTP response codes, authentication, and verbs.

The Public API is compatible with the OpenAPI Specification (OAS3) and publishes a compliant [swagger.json](#) definition file. Explore the OpenAPI Specification using the Swagger UI:

- For public cloud-hosted instances: <https://bitwarden.com/help/api/>
- For self-hosted instances: <https://your.domain.com/api/docs/>

Note

Access to the Bitwarden Public API is available customers on all Enterprise and Teams organizations. For more information, see [About Bitwarden Plans](#).

Endpoints

Base URL

For cloud-hosted, <https://api.bitwarden.com> or <https://api.bitwarden.eu>.

For self-hosted, <https://your.domain.com/api>.

Authentication endpoints

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

For self-hosted, <https://your.domain.com/identity/connect/token>.

Authentication

The API uses bearer access tokens to authenticate with protected API endpoints. Bitwarden uses an [OAuth2 Client Credentials](#) application request flow to grant bearer access tokens from the endpoint. Authentication requests take `client_id` and `client_secret` as required parameters.

Tip

The API key used to authenticate with the Public API is **not the same** as the [personal API Key](#). Organization API keys will have a `client_id` with format `"organization.ClientId"`, whereas personal API keys will have a `client_id` with format `"user.clientId"`.

The API Key `client_id` and `client_secret` can be obtained by an owner from the Admin Console vault by navigating to **Settings** → **Organization info** screen and scrolling down to the **API key** section:

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

[Get organization API key](#)

If, as an owner, you want to share the API key with an admin or other user, use a secure communication method like [Bitwarden Send](#).

Warning

Your organization API key enables full access to your organization. Keep your API key private. If you believe your API key has been compromised, select **Settings > Organization info > Rotate API key** button on this screen. Active implementations of your current API key will need to be reconfigured with the new key before use.

Bearer access tokens

To obtain a bearer access token, make a **POST** request with **Content-Type: application/x-www-form-urlencoded** with your **client_id** and **client_secret** to the **authentication endpoint**. When using the API for organization management, you will always use **grant_type=client_credentials** and **scope=api.organization**. For example:

```
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>'
```

This request will result in the following response:

Bash

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

In this response, **3600** represents the expiration value (in seconds), meaning this token is valid for 60 minutes after being issued. Making an API call with an expired token will return a **401 Unauthorized** response code.

Content types

The Bitwarden Public API communicates with `application/json` requests and responses, with one exception:

The `authentication endpoint` expects an `application/x-www-form-urlencoded` request, however will respond with `application/json`.

Sample request

Bash

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

Where `<TOKEN>` is the value for the `access_token:` key in the obtained `bearer access token`.

This request will result in a response:

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 has a public [status page](#), where you can find information about service health and incidents for all services including the Public API.

Response codes

The Bitwarden Public API uses conventional HTTP response codes to indicate the success or failure of an API request:

Status Code	Description
200 OK	Everything worked as expected.
400 Bad Request	The request was unacceptable, possibly due to missing or malformed parameter(s).

Status Code	Description
401 Unauthorized	The bearer access token was missing, invalid, or expired.
404 Not Found	The requested resource doesn't exist.
429 Too Many Requests	Too many requests hit the API too quickly. We recommend scaling back the number of requests.
500, 502, 503, 504 Server Error	Something went wrong on Bitwarden's end. These are rare, but contact us if they occur.

Further reading

For more information about using the Bitwarden Public API, see the following articles:

- [Bitwarden Public API OAS Specification](#)
- [Event logs](#)