Climb API Documentation

Contents

[Overview 1](#_Toc78963348)

[API Authorization 1](#_Toc78963349)

[Retrieving an Access Token 1](#_Toc78963350)

[Using the Access Token 2](#_Toc78963351)

[Swagger 2](#_Toc78963352)

[Postman 3](#_Toc78963353)

[Command Prompt 3](#_Toc78963354)

[Switching Workgroups 3](#_Toc78963355)

# Overview

The Climb API can be used to retrieve, create, and update data stored in the Climb database. All data changes made via the API will be reflected in the UI, and all changes made in the UI will be reflected in the API responses.

# API Authorization

The Climb API uses the Oauth 2.0 bearer token authorization type. An access token must be retrieved from the token endpoint and sent as a Bearer token in an authorization header with every API request.

## Retrieving an Access Token

The token endpoint is <http://climb-admin.azurewebsites.net/api/token> and is protected by Basic authentication. You can supply your Climb username and password as a base64 encoded authorization header in the GET request to retrieve an access token. If you don’t have a Climb username and password, then you must first register for a Climb account at climb.bio. The image below shows how Postman can be used to retrieve an access token for the Climb API. This will add an authorization header with the value **“Basic encodedString”** to the GET request, where **encodedString = “climbUsername:climbPassword”** base64 encoded.

Graphical user interface, text, application

Description automatically generated

A successful token response looks like the following. The **access\_token** attribute is the part that is required to access the Climb API. The token is valid for 3600 seconds (60 minutes) as indicated in the response.

Text

Description automatically generated

## Using the Access Token

The access token retrieved from the token endpoint (process described above) must be sent as an Authorization header with the “Bearer” prefix in every API request.

### Swagger

To apply the access token to API requests made via Swagger, click the green Authorize button at the top of the page:

Graphical user interface

Description automatically generated with medium confidence

In the modal that appears, paste your access token in the “Value” input field, then click “authorize”

Graphical user interface, text, application

Description automatically generated

You can now use any of the endpoints in Swagger to send API requests to the Climb API.

### Postman

The image below shows how to input the access token to access the Climb API via Postman. For Authorization Type, be sure to select the “OAuth 2.0” option.Graphical user interface, text, application, email

Description automatically generated

### Command Prompt

The following is an example of using the access token to send an API request to GET the animals in your current Climb workgroup.

**curl -X GET "https://api.climb.bio/api/animals" -H "accept: \*/\*" -H "Authorization: Bearer paste\_access\_token\_here"**

## Switching Workgroups

The access token can only be used to access data for one Climb workgroup. If you have access to multiple Climb workgroups, then you must change your current workgroup and retrieve a new access token to retrieve data for the other workgroup via the API.

The **GET /api/workgroups** endpoint can be used to retrieve a list of all the workgroups to which you have access. To update your current workgroup, use the PUT /api/workgroups/{workgroupKey} endpoint where the **{workgroupKey}** is the key for the workgroup to which you would like to switch.

Graphical user interface, application

Description automatically generated

After you have switched workgroups, your access token will no longer work, and you will need to retrieve a new one using the token endpoint described above.