Using the Crowdicity API

Authorisation for API use

Before using the API, you must register to receive a client id and client secret, which you will then use to make requests.

API Client Account

Crowdicity API uses OAuth 2.0 protocol for authentication and authorization. To start using, you must have a full (validated) account in the Crowdicity platform. After login (desktop version) go to your profile (click the user icon in the top right -> “Go to profile”) and choose “API” from the profile menu bar. You will see a list of your existing API clients and API requests, both of which will be empty if this is your first API request. To apply for an API client account click “Apply for a new API client”. A form will appear. Fill it in to describe your project and reason for using the API and send it by clicking “Apply”.

As soon as the application is reviewed by the community administrator, your client will be created and access granted. Community administrators should click the “API” option in the grey “Crowd Management” menu to display a list of current requests.

You will see a new record on your API community client list. First column is a client id field (client_id) which will be used together with client secret to obtain an auth code. To finish the creation process, select “generate password” and optionally add an endpoint which will be used for every authorisation attempt. Click “save”. Your new password will be generated (client_secret), please note it in any secure way as it will not be shown again after refresh.

Auth code

Auth code is short lived token, used to create/exchange to an access token (access_token).

To obtain an auth code (auth_code) make a GET request to https://api.crowdicity.com/v2/auth/code?client_id={client_id}&client_secret={client_secret}

If you left the endpoint field empty in the access configuration, the auth_code will be returned as a result of the request, otherwise the system will make a call to the endpoint url and will pass the auth code as a url parameter.
Access token

To obtain an access token (`access_token`) and refresh token (`refresh_token`), make a POST request to

https://api.crowdicit.com/v2/auth

with parameters

auth_code={auth_code}
client_id={client_id}
client_secret={client_secret}

The response will be formatted as a JSON string and contain following data

```json
{
  "access_token": "{access_token}"
  "refresh_token": "{refresh_token}"
}
```

API calls

Every API call, which needs authorisation should contain following header:

Authorization: bearer `{access_token}`

Refreshing Access Token

In case of access token expiration, make a POST call to

https://api.crowdicit.com/v2/auth/refreshtoken

with parameter

refresh_token={refresh_token}

The response will contain a new access_token & refresh_token in JSON format (same as creating a new access token using access code)

Validating Access Token

When a token validation will be needed, make a POST call to

https://api.crowdicit.com/v2/auth/validatetoken

with parameter

access_token={access_token}
The response will be as following:

```json
{
    "valid": {true/false}
}
```

API Reference

The API reference is available here: https://api.crowdicity.com/doc