

# DevResults API

Last Modified on 09/01/2023 1:22 pm EDT

In this article:

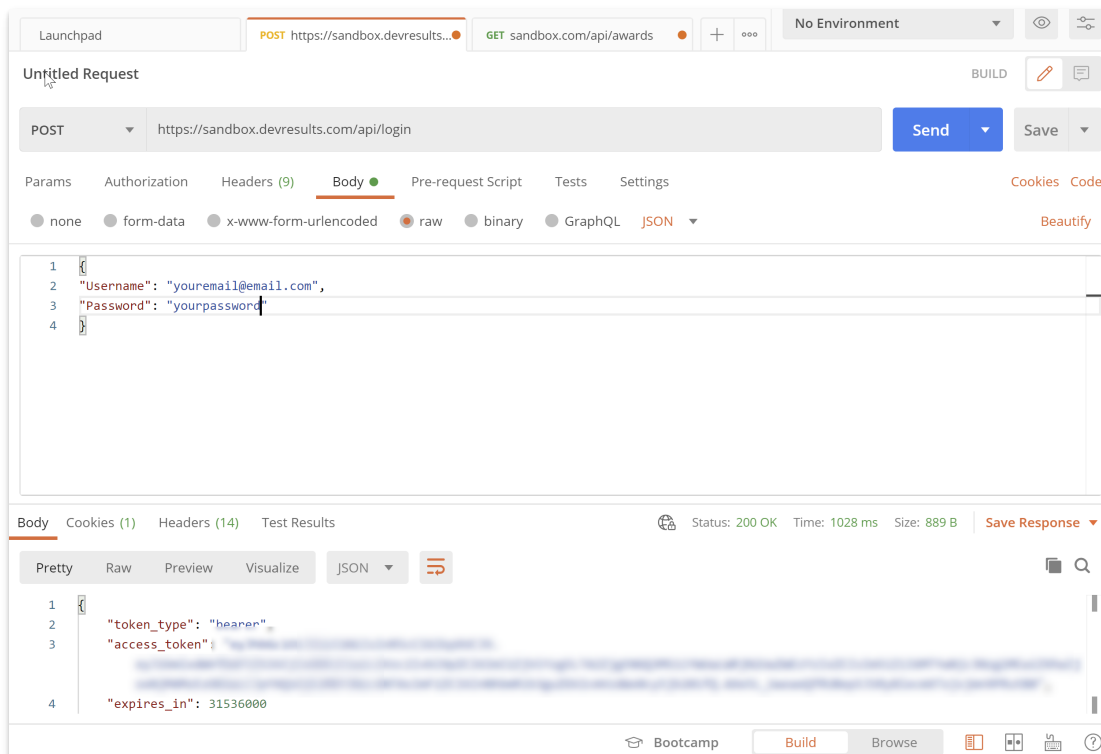
- **Using an external API tool to access components of the DevResults app**
- **Using in-app API Keys**

An API (Application Program Interface) lets you access components of one application for use in another. DevResults' API allows you to pull information from your DevResults site to use or display in another application or website. You can find a complete guide to our API documentation, either at <https://www.devresults.com/api-help> or at [\[your\\_site\].devresults.com/api-help](https://[your_site].devresults.com/api-help)

## External API Tool

The easiest way to use the API is to download a tool like **Postman** (make sure you have downloaded the desktop app) that allows you to make API requests.

Once you've logged into Postman (or a similar app), create a new request. Your first request will be an POST request to **create an API token**.

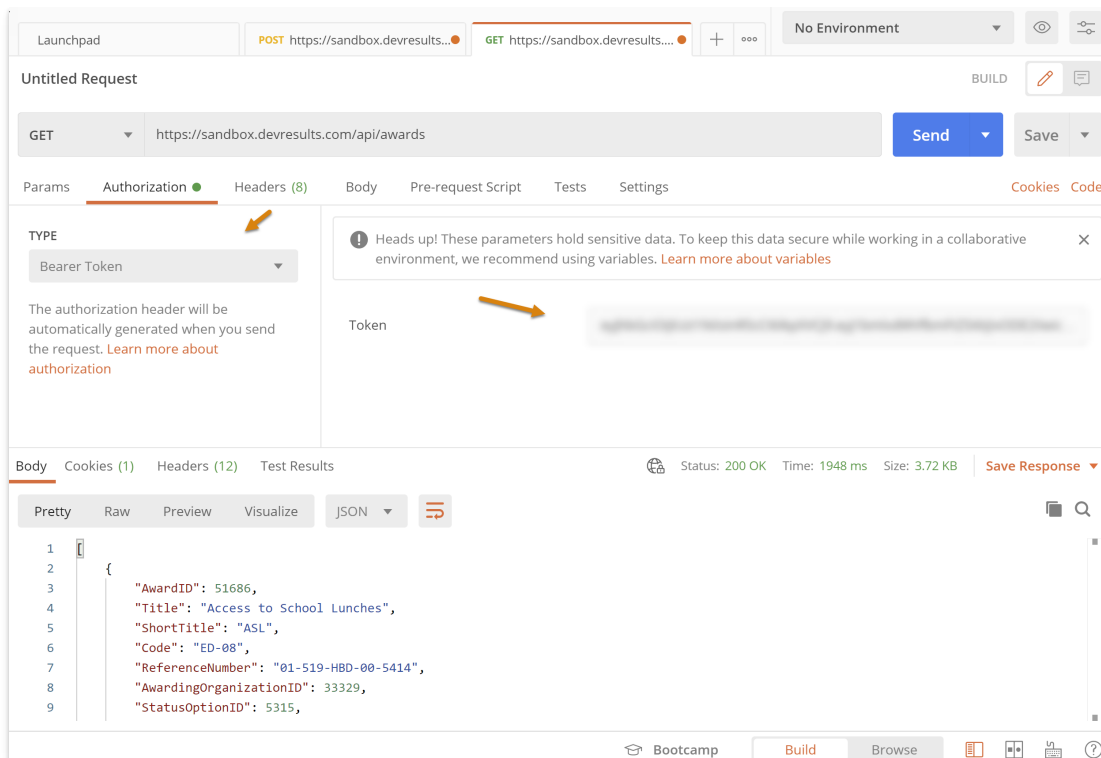


**NOTE:** Make sure you select "Raw" and "JSON" when entering your username and password.

Once you hit the **Send** button, you will receive an API token (or "access token") which will be valid for one year. You can now use the access token as a bearer token to make GET, POST, PUT, and DELETE requests with the API.

As an example, here is how you would set up a GET request to **list all activities** in your site.

Select "Bearer Token" under **Type** of Authorization and enter in your access token. Then click **Send**.



## In-app API Keys:

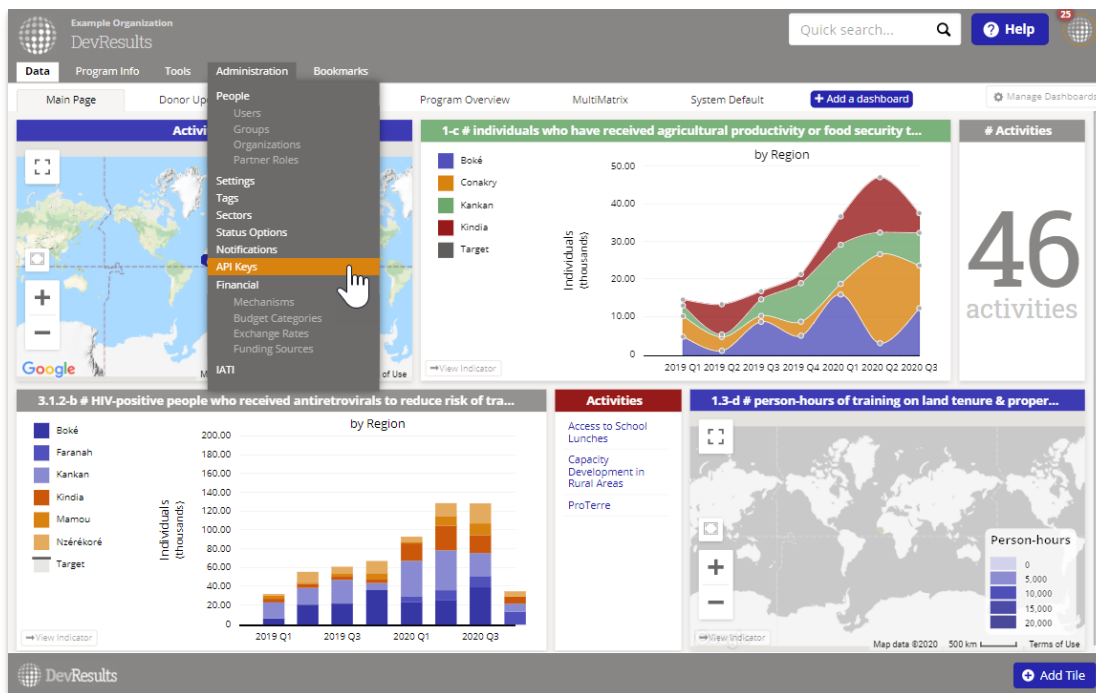
You can also manually configure API keys in-app. API keys are special "users" who can only access the API and are useful in several situations:

1. When a users with broad permissions would prefer to use an account with limited permissions to access the API
2. When users must authenticate using a Single Sign-On provider and are unable to use passwords

### 1. Configure API Access

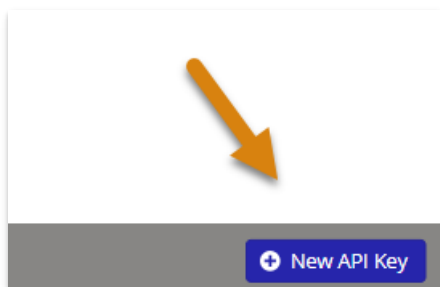
This step is completed inside the DevResults application. You'll need to have high enough access to be able to create new users before proceeding.

Once you have access and are logged in to the application, navigate to API Keys in the **Administration** menu:



You will now be presented with a list of any previously configured applications. DO NOT re-use previously configured application keys. These keys are used to track which application made changes in DevResults. If a key is re-used, you will lose the ability to track the source of changes.

Next, you'll want to create a new API Key for your application. To do so, click the **New API Key** button:



You will be presented with a dialog and prompted to input the application name:

The 'Create New API Key' dialog box is shown. It has a title bar with a close button. Below the title, there is a text input field labeled 'Application Name' containing the text 'New API Key'. At the bottom left is a 'Cancel' button, and at the bottom right is a green 'Add API Key' button with a white plus icon.

Choose an application name and click the **Add API Key** button to finalize the creation of the new API Key. Once the key is created, you will be taken to the API Key Details page where you will be able to modify the name of your application, see both the API Key and API Secret, select the user group and associated permissions for the new API key, as well as reset the API Secret if needed.

### New API Key

#### API Key Details

Application Name

API Key **ABCDEFGG**

API Secret **123456789** [Reset API Secret](#)

*For security the API Secret will not be shown again. Please protect the API Secret like a password!*

#### Permissions

Group  **Contributors**  
Can log into the system to manage projects.

**Managers**  
Can mark checklist items as approved. Can sign off on results data submitted by partners.

**No Access**  
Cannot log into the system.

**Owners**  
Can configure the system's global settings and lists. Can manage user accounts and logins, reset passwords, and assign permissions.

**Partner Managers**  
Can manage users for their organization and edit their organization's details. Access is limited to the projects they are assigned to.

**Partners**  
Users with access limited to the projects they are assigned to.

**Viewers**  
Can log into the system, browse projects, and view reports. Cannot change anything.

[Done](#)

**Note:** While you will always be able to edit the name and user group/permissions of an existing API key, you will not be able to see or recover an existing API Secret. The secret is only displayed once and then it is hidden, even from DevResults staff. Treat it like a password (that's why it's called a *secret*) and be prepared to reset the secret if you lose it.

## 2. Accessing the API

API Keys can be used to **create an API token** the same way as individual user accounts. Pass the API Key as your username and pass the API Secret as the password when generating a token, and follow the **same steps as above**.

Didn't answer your question? Please email us at [help@devresults.com](mailto:help@devresults.com).

---

## Related Articles

---