DevResults API

Last Modified on 07/18/2025 11:36 am EDT

In this article:

- **Creating an API Token**
- **Using the API to access components of the DevResults app**
- **Using in-app API Keys**

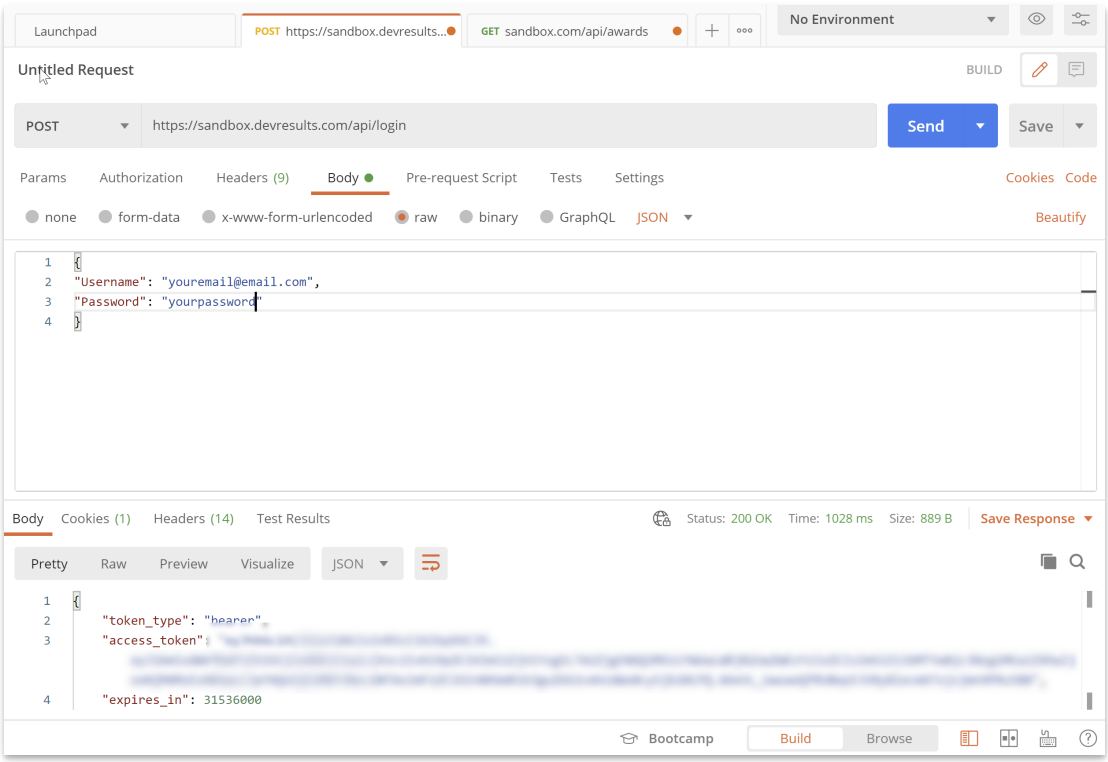
An API (Application Program Interface) lets you access components of one application for use in another. DevResults' API allows you to pull information from your DevResults site to use or display in another application or website. You can find a complete guide to our API documentation, either at **https://www.devresults.com/api-help**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

Creating an API Token

An API token is a unique string that verifies a user or application's identity and grants access to an API. 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), send a POST request to **create an API token**. Make sure you select the "raw" and "JSON" settings for the body of the request.

> **Note:** If you need an API Token for an API Key instead of for a user, pass the **API Key** as your **username** and pass the **API Secret** as the **password**.



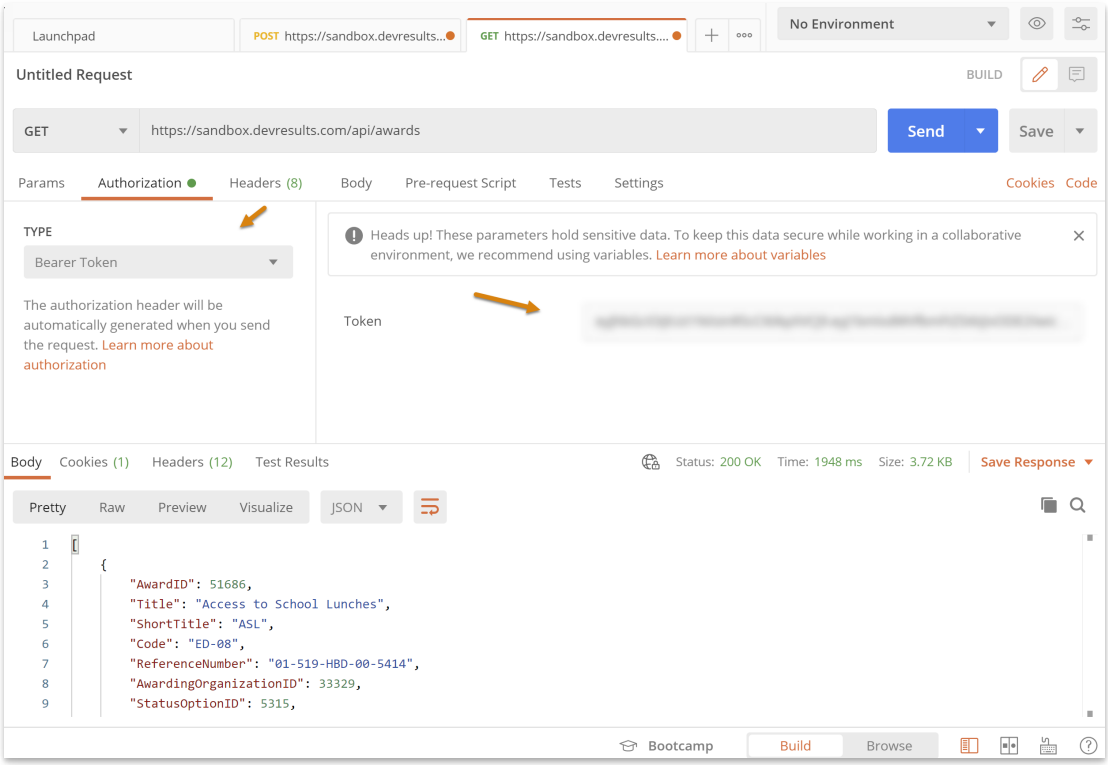
Once you hit the **Send** button, you will receive an API token (or "access token") which will be valid for one year.

Using the API

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 projects** 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 configure API keys in the DevResults app. API keys are special "users" who can only access the API and are useful in several situations:

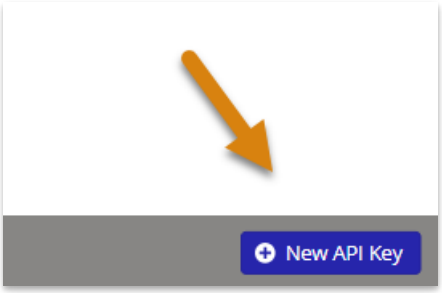
1. When a users with broad permissions would prefer to use an account with limited permissions to access the API
2. When users must authenticate using a Single Sign-On provider and are unable to use passwords

1. Configure API Access

To create an API Key, you'll need permission to create new users. In DevResults, navigate to **API Keys** in the **Administration** menu:

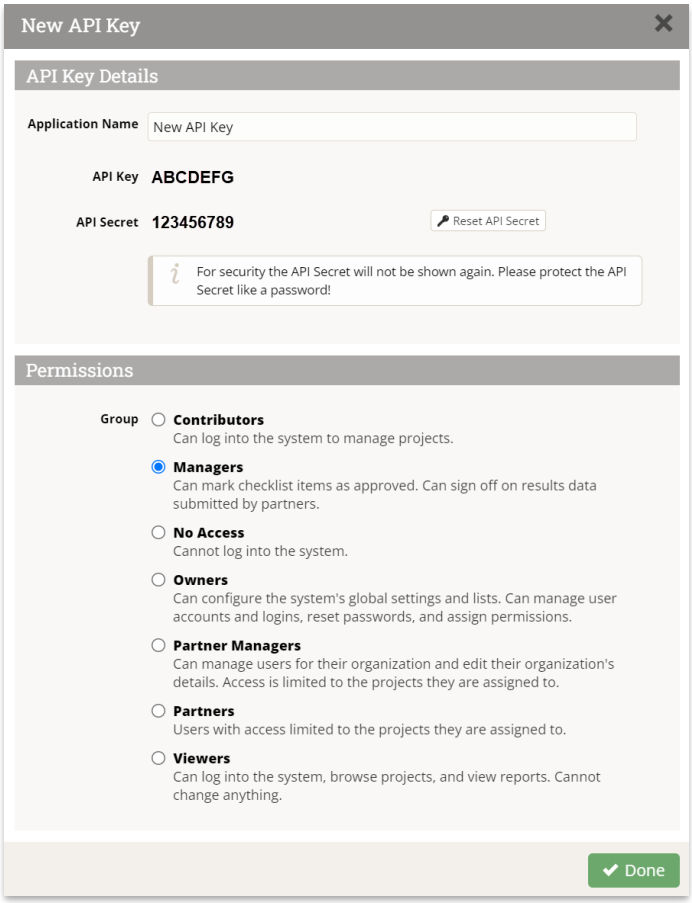
You will now be presented with a list of any previously configured applications. Do not re-use previously configured application keys; these keys are used to track which application made changes in DevResults. If a key is re-used, you will lose the ability to track the source of changes.

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



Enter application name that you'll use the API key for and click **+Add 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.



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**.

Related Articles