

AlarmBiller - Using POSTMAN with REST API

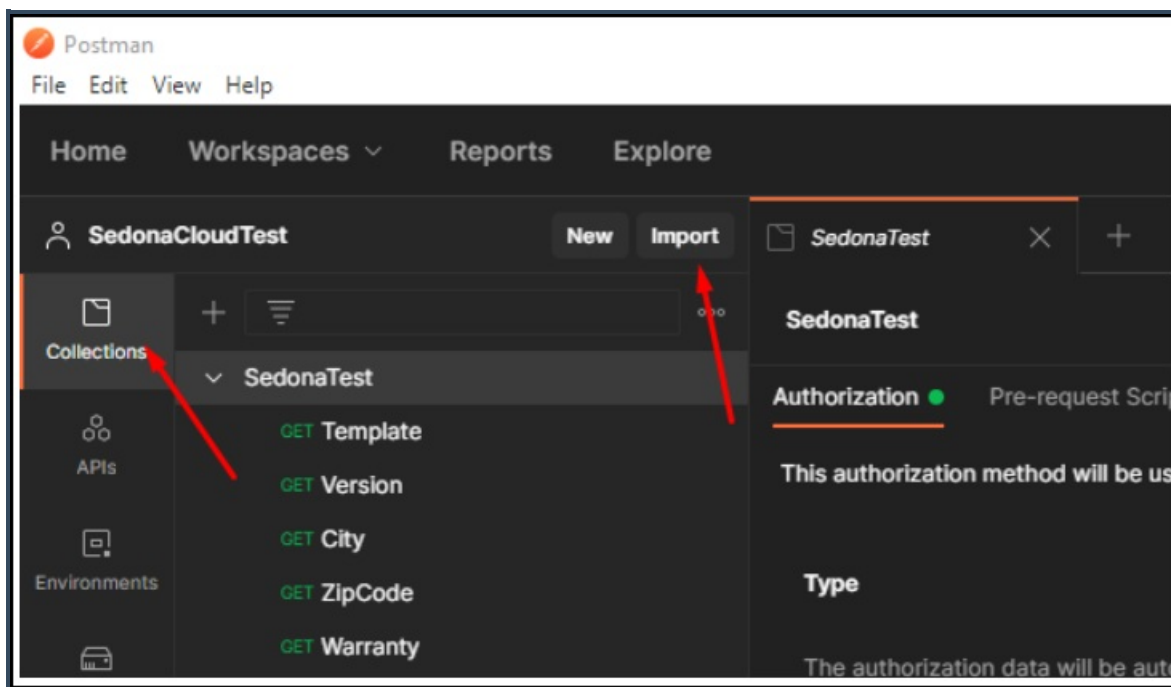
12/18/2023 5:05 pm EST

Overview

The AlarmBiller REST API is used for third-party access. This is also used by the Stages Integration. Because it uses HTTPS calls to an IIS server, it allows very quick testing through several tools. This document covers one called POSTMAN which is a free tool for testing REST APIs.

Importing Demo Collection

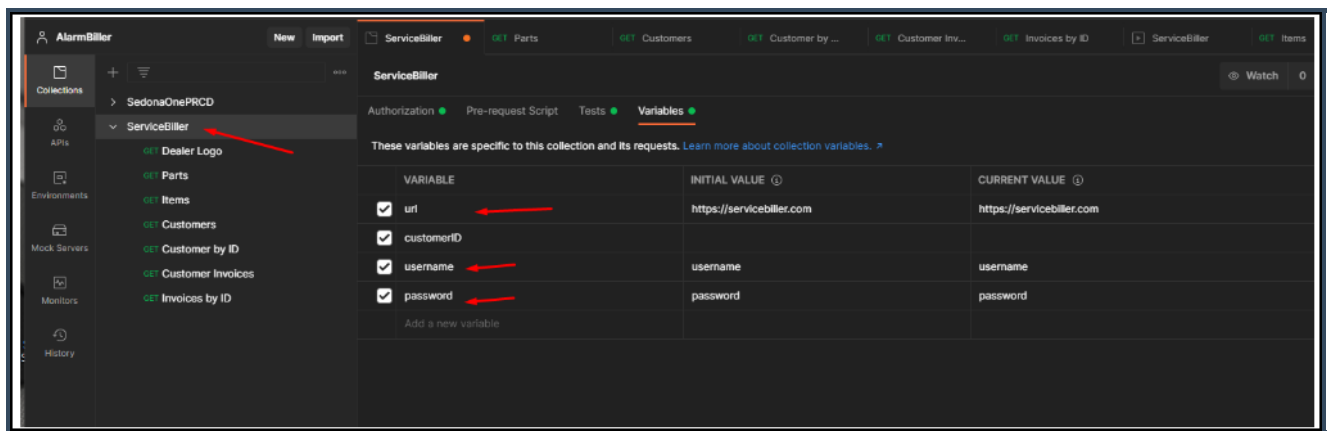
Click on the Import button on the top left part of the POSTMAN interface. Drag and drop the attached .JSON file for the demo collection.



Once this collection is imported, click on the ServiceBiller collection.

Change to the "Variables" tab.

Update the Variables settings for url, username, and password with your correct values for AlarmBiller and click the update button at the bottom of the form. You may need to hit the Reset All button if there are current values already in place.



You are now set up and ready to begin working with API calls. You can rename the collection to better describe the AlarmBiller system you are hitting.

Getting Authorized with OAUTH

The first thing that must happen before any API calls can be made is to get an OAUTH token for your user. We do this from the collection Authorization tab so that all subsequent calls can inherit this token. AlarmBiller uses OAuth 2.0 as the authorization token. This is added to the HTTP request as a Bearer token in the request header.

Now you can configure and get a new token. Make sure it is set for Password Credentials as the Grant Type.

▼ Configure New Token

Token Name

ServiceBiller

Grant Type

Password Credentials ▼

Access Token URL ⓘ

{{url}}/connect/token

Client ID ⓘ

sedonaonemobile ⚠

Client Secret ⓘ

FF91009A-7934-4B1C-A366-0D23 ⚠

Username

{{username}}

Password

..... 🔒

Scope ⓘ

sedonaoneapi sedonaonescope paym

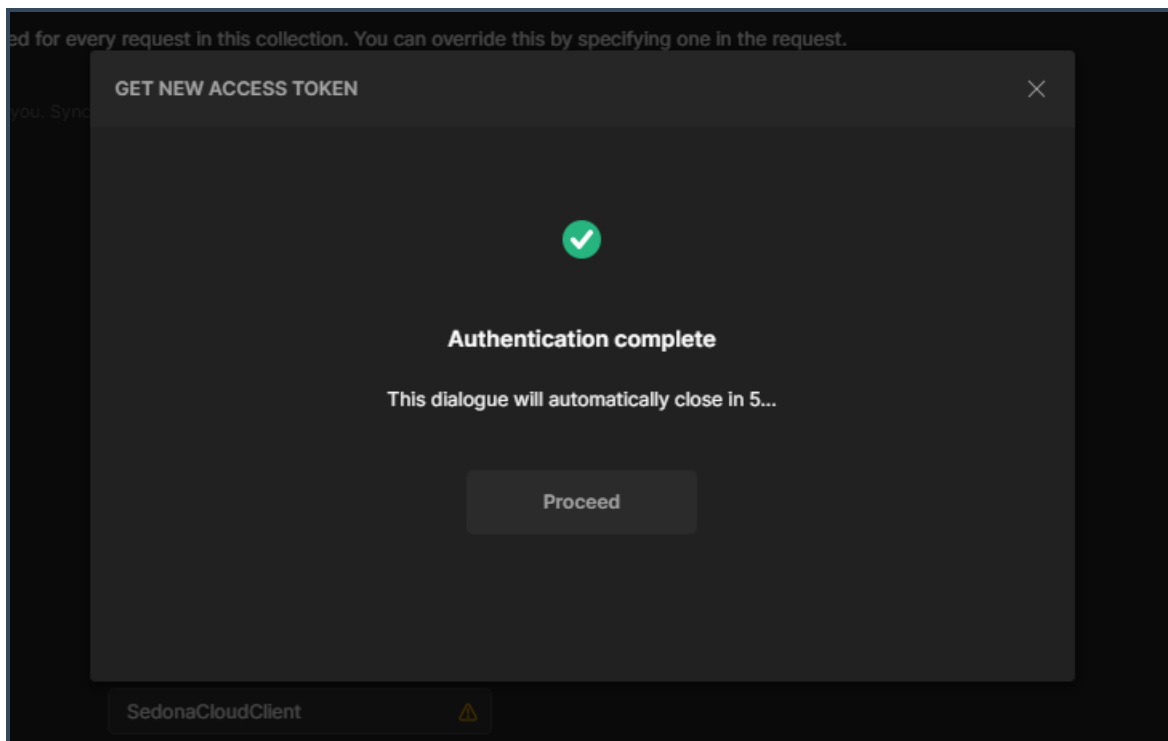
Client Authentication

Send as Basic Auth header ▼

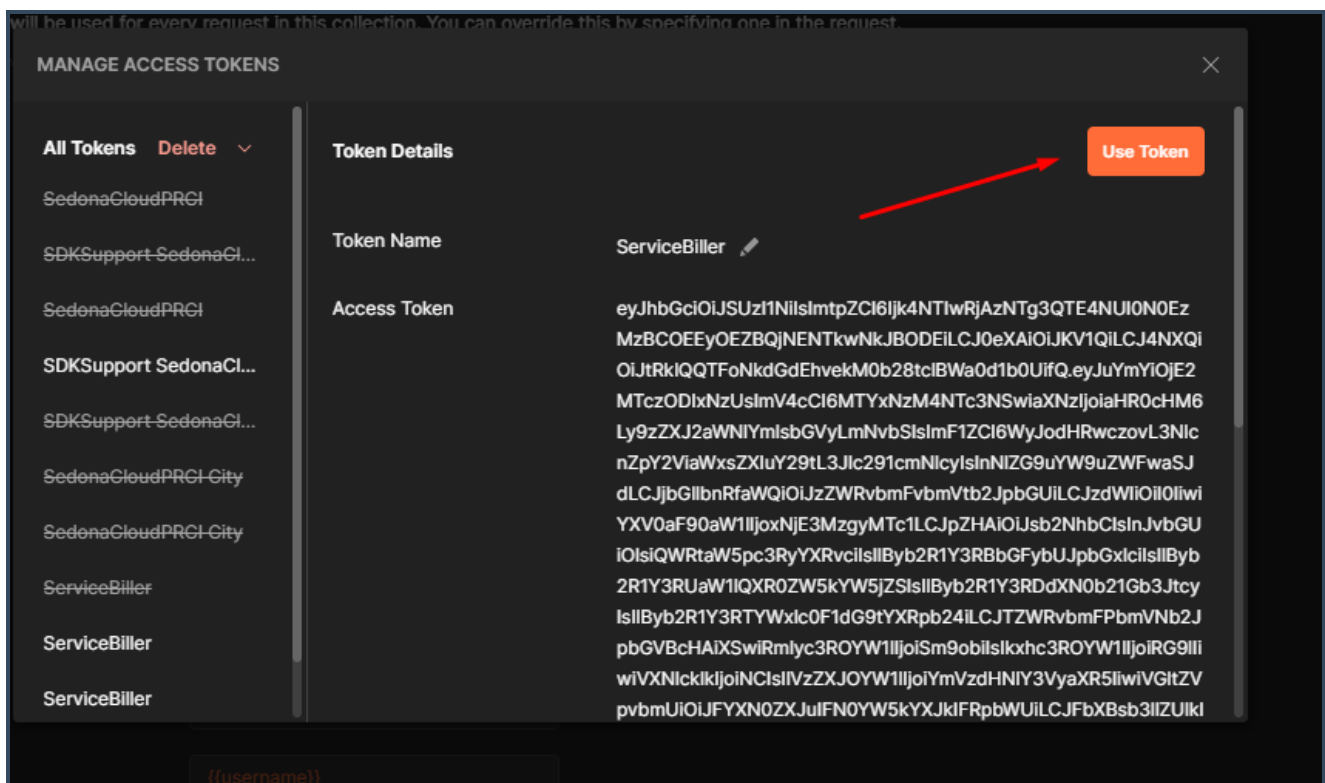
🗑 Clear cookies ⓘ

Get New Access Token

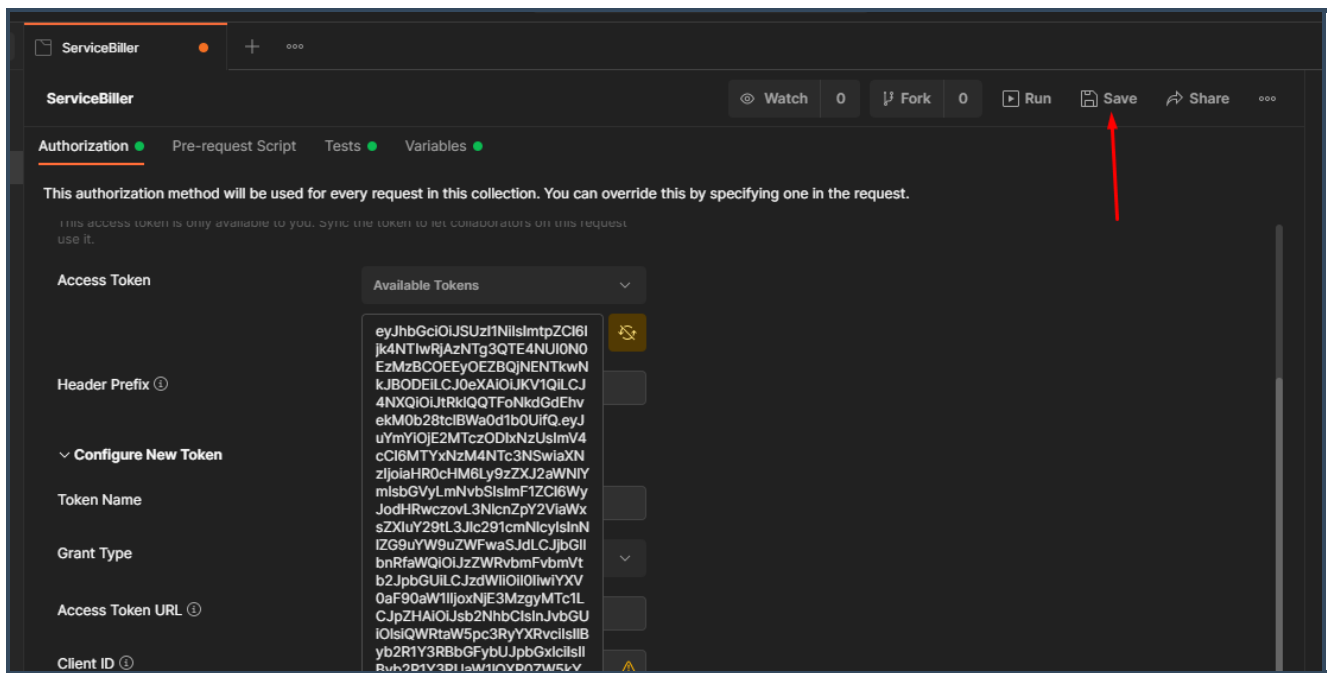
Hit the Get New Access Token button and you should get an OAUTH token back.



Click the Proceed button and then click the Use Token button.



Not you have an OAuth Token.



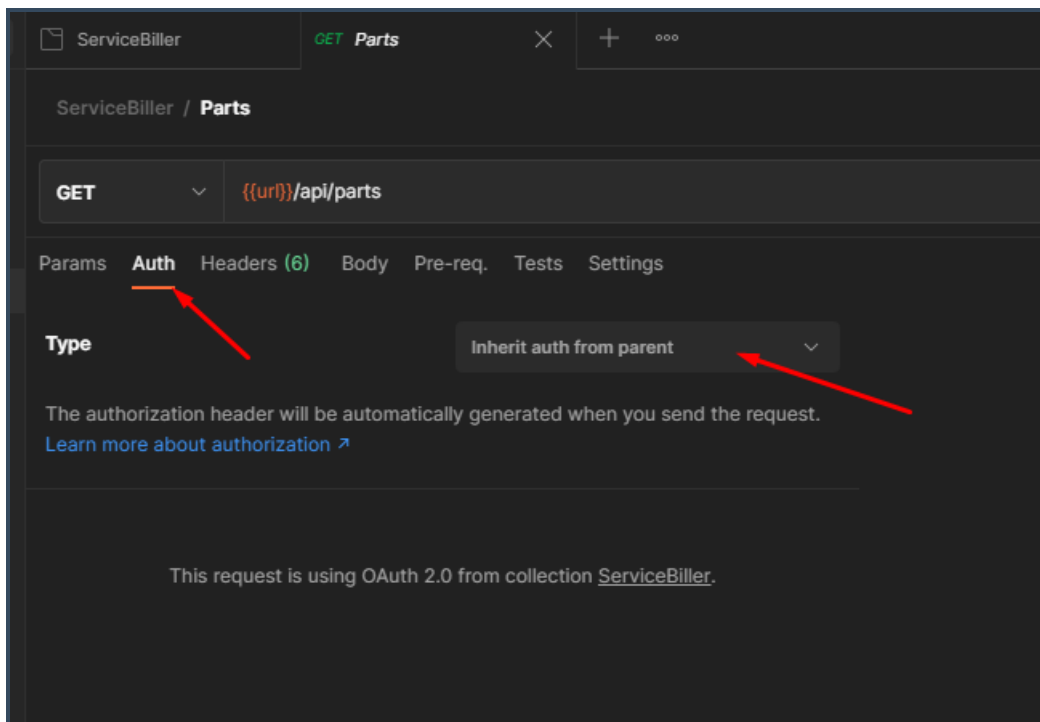
Important! Make sure to hit the Save button to store that token for the rest of your API calls.

Once you have this working you can move on to the next steps.

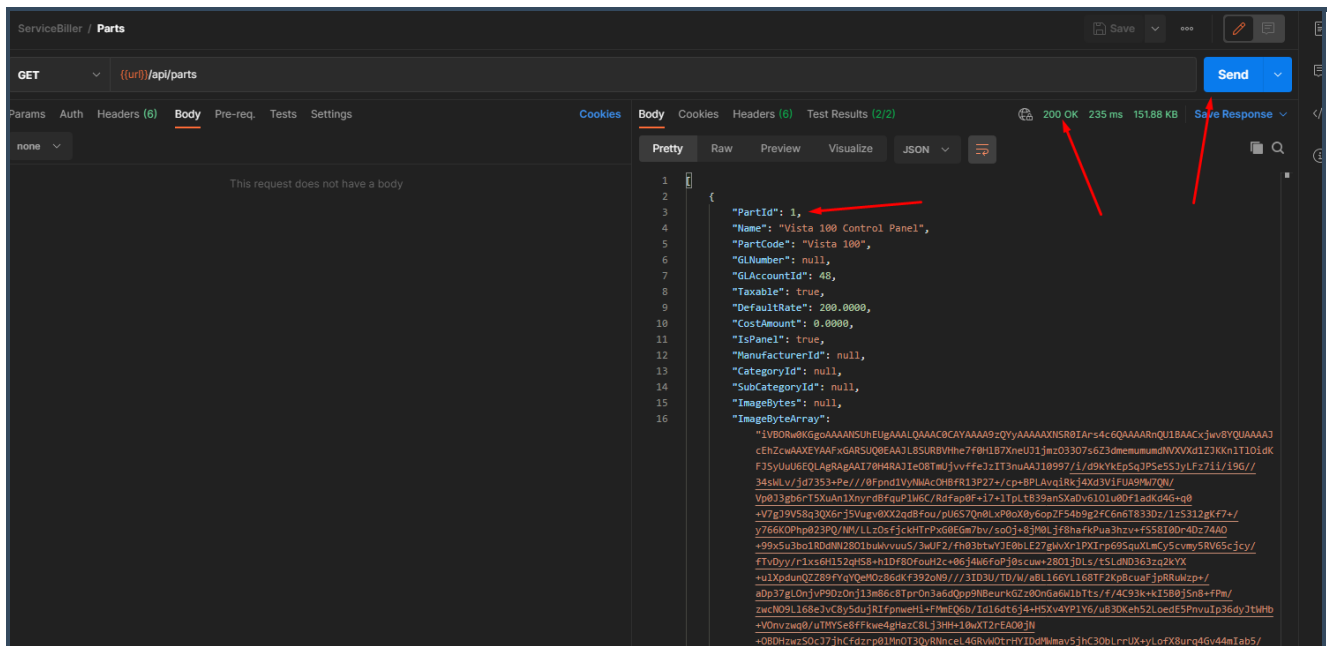
Making API Calls

Now that you have a valid OAUTH token, we can hit the various API endpoints and make requests. An easy one to start with is requesting the list of Parts in the SedonaOne database. You probably will not need to request this in practice, but I use it just to make sure the basic connection is working.

Open the Parts Request. This already has the parent Auth setup to be used under the Authorization tab.

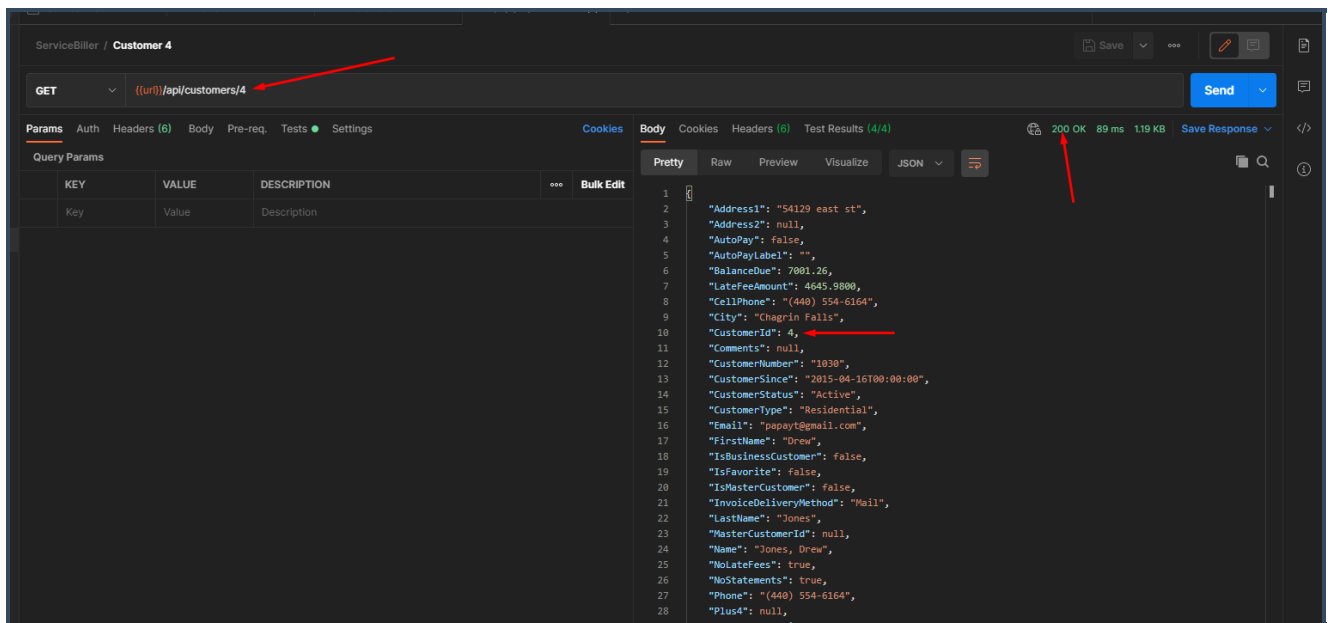


This request does not require a body message so you can just hit send. It should return a JSON array object showing that the connection is working to the API including sending in the OAUTH token.



You can now work through the other API calls.

Many of the API calls have variables in the URL Path as well as data that must be sent in the Body of the message. These vary by the endpoint so you must refer to the documentation on the structure. The demo collection has some of my values and must be updated accordingly. For example the Customer 4 is calling my customer. You will have to use your own value.



API Documentation

Our REST APIs use Swagger to self document the calls. This is hosted by the API and can be used to tell what the calls are for that version of the installed software. This means that one customer can be on a different version than another and have their own specific documentation. To view the documentation, simply replace the base URL in this example:

<https://bestsecurity.servicebiller.com/api/help/index.html>