IT Collect OAuth

Access & Refresh Token Rules

August 2021

General Services Administration

Office of Government-wide Policy

Document Change Record

Version Number	Date	Description
1.0	August 2021	Created IT Collect document formalizing access and refresh token rules

IT Collect OAuth Overview

The IT Collect API uses an OAuth2 authorization framework to grant agency CPIC data management tools access to submit and update submissions on IT Collect. With the OAuth implementation, you can securely connect your vendor tool via an IT Collect provided Client ID and Secret. With the new implementation of this framework, authorization flow happens seamlessly in an automated manner based on your tool configuration. The IT Collect OAuth server generates access tokens for API authorization in JSON Web Token format. Each access token carries scopes related to your agency.

OAuth2 has several authorization workflows. IT Collect only supports Authorization Code and Refresh Token grant types.

Please reach out to our support team (itdb-support@gsa.gov) to get your individual Client ID and Secret. IT Collect requires your application's redirect URL to register the Client ID, unless you are using the default Postman redirect/callback URL (https://oauth.pstmn.io/v1/callback) for testing purposes. IT Collect requires Secrets to use Refresh tokens. However, IT Collect does not mandate the use of Secrets for standard Access Tokens.

Authorization endpoints:

{{baseUrl}}/oauth/authorize	Used to authorize your application and get authorization code
{{baseUrl}}/oauth/token	Used to get access and refresh tokens

Session Timeouts and Token Expiration Rules

Item	Limit
Login.Gov	Your login.gov session with IT Collect OAuth service is limited to **15 mins**
Authorization Code	Your authorization code is limited to **120 seconds** and can be used only once
Access Token	Your token is valid for **30 mins.**

Refresh Token	Your refresh token is valid for **3 hours**. Refresh tokens cannot be used in place of access tokens. Because of the longer life of refresh tokens, vendors should securely store tokens and associated secrets.

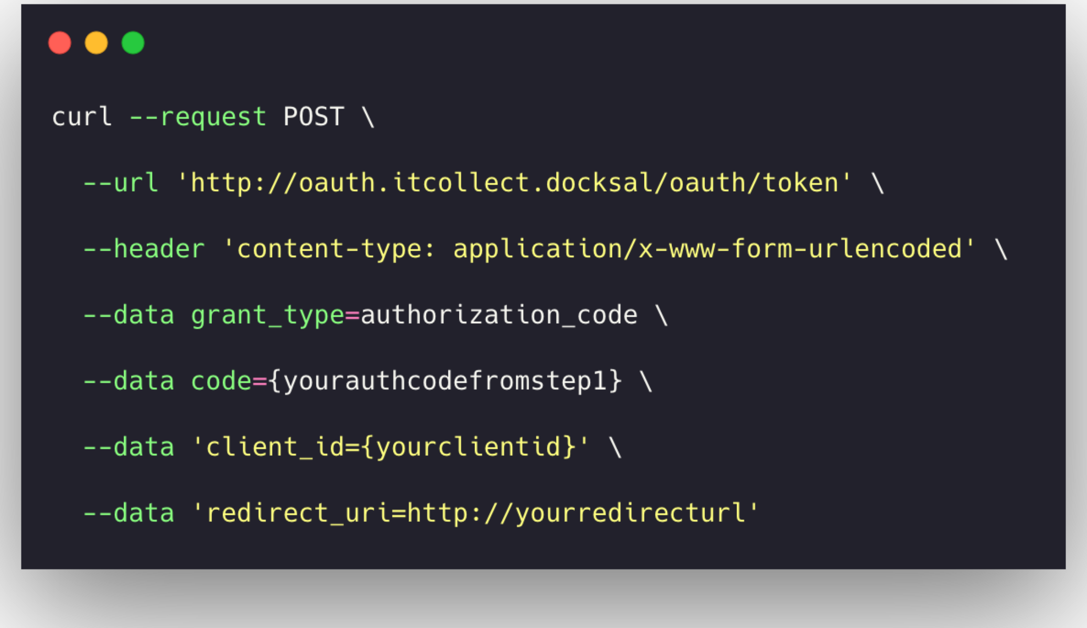
Authorization Flow

To get the authorization code, first direct your application to the production URL:

https://itcollect.itdashboard.gov/oauth/authorize?response_type=code&client_id={yourclientid}&redirect_uri=http://agencytool.gov/redirecturl

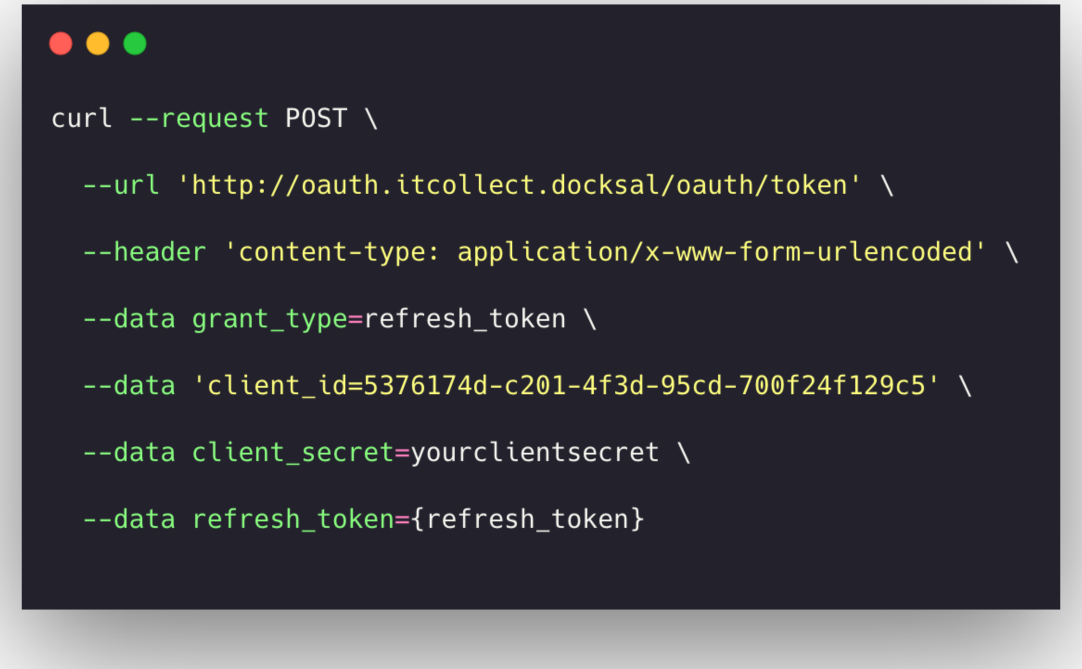
Upon successful authentication and authorization, you will be redirected to your application's redirect URL with the authorization code appended to your URL:

To obtain token:



```
curl --request POST \
  --url 'http://oauth.itcollect.docksal/oauth/token' \
  --header 'content-type: application/x-www-form-urlencoded' \
  --data grant_type=authorization_code \
  --data code={yourauthcodefromstep1} \
  --data 'client_id={yourclientid}' \
  --data 'redirect_uri=http://yourredirecturl'
```

To obtain a new access token using refresh token:



```
curl --request POST \
  --url 'http://oauth.itcollect.docksal/oauth/token' \
  --header 'content-type: application/x-www-form-urlencoded' \
  --data grant_type=refresh_token \
  --data 'client_id=5376174d-c201-4f3d-95cd-700f24f129c5' \
  --data client_secret=yourclientsecret \
  --data refresh_token={refresh_token}
```