

CRC FICO API

REPRESENTATIONAL STATE TRANSFER (ResT)

Version 1.0 | 12th September 2018

# End Point

## Payload

## Security

Generating Access Tokens

After registering on our site, go ahead and create a client copy the client is and the callback url which will be used to generate access token as shown below

Make a redirect request to 'http://your-app.com/oauth/authorize?’

Appending the credentials of the user at the end.

Route::get('/redirect', function () {

$query = http\_build\_query([

'client\_id' => 'client-id',

'redirect\_uri' => 'http://example.com/callback',

'response\_type' => 'code',

'scope' => '',

]);

return redirect('http://your-app.com/oauth/authorize?'.$query);

});

If the user approves the authorization request, they will be redirected back to the consuming application. The consumer should then issue a POST request to your application to request an access token. The request should include the authorization code that was issued by your application when the user approved the authorization request. In this example, we'll use the Guzzle HTTP library to make the POST request:

Route::get('/callback', function (Request $request) {

$http = new GuzzleHttp\Client;

$response = $http->post('http://your-app.com/oauth/token', [

'form\_params' => [

'grant\_type' => 'authorization\_code',

'client\_id' => 'client-id',

'client\_secret' => 'client-secret',

'redirect\_uri' => 'http://example.com/callback',

'code' => $request->code,

],

]);

return json\_decode((string) $response->getBody(), true);

});

Passing the token

### **Passing The Access Token**

When calling routes that are protected by Passport, your application's API consumers should specify their access token as a Bearer token in the Authorization header of their request. For example, when using the Guzzle HTTP library:

$response = $client->request('GET', '/api/user', [

'headers' => [

'Accept' => 'application/json',

'Authorization' => 'Bearer '.$accessToken,

],

]);