From: **David Zachrich - TCS** dave@tcssoftware.com
Subject: TCS OAuth2 provider access
Date: March 27, 2019 at 20:01
To: Lawrence McDaniel lpm0073@gmail.com, mbrody@tldsystems.com
Cc: Dan Kline dkline@nyspma.org, david@jaffemanagement.com, Tim Rorris tim@tcssoftware.com

Hi Lawrence and Michael,

We now have a working TCS OAuth2 provider service running in our staging environment for you to access and test your Single Sign-on solution.

Upon completion of your testing, we will deploy to production.

First, you will need to register your app using the endpoint, https://staging.associationdatabase.com/oauth/applications/new?org_id=NYSPMA.

The org_id parameter is important in that it identifies from which client organization, in this case NYSPMA, within the TCS WebSuite2® multi-tenant application, the app you are registering will be able to access information.

The org_id is shown on the new application registration form, but entry is disabled.

As an alternative to passing the org_id parameter, the admin user can login directly at our site using the url, https://staging.associationdatabase.com/aws/NYSPMA, after which you can navigate to the /oauth/applications/new endpoint without any additional parameter.

Each of the other fields on the new application form are standard for an OAuth2 application registration.

The first time you attempt to access this endpoint, you will be prompted to login, if you have not already done so.

I have added an admin account, 'nyspma_oauth_admin' for this purpose. The password for this account will follow in a separate email.

I have also created an additional 3 regular member test user accounts that the admin user can modify from our site as necessary.

The account names and passwords are as follows:

USER	PASSWORD
Testing1@test.com	Testing1
Testing2@test.com	Testing2
Testing3@test.com	Testing3

These accounts will be deleted after the test period is complete.

Upon registration of your application with our site, you'll be presented the application credentials: Application ID and Client Secret, which should be kept secure.

The app should then be authorized in order to obtain an authorization code via the callback method that you specify.

This code is then used to obtain an access_token and a refresh token. The authorization code expires in 10 minutes and the access token expires in 2 hours.

In order to obtain a new access token, send the refresh token to the /oauth/token endpoint with a grant_type=refresh_token.

While we will be evaluating and adding additional services as the need arises, the only currently available api service is the endpoint '/api/user', which returns the currently logged in user information.

We have a publicly available ruby gem, available at https://github.com/tcssoftware/omniauth-tcs, which was created to build a ruby client for testing the TCS OAuth2 provider service. You can access and use as needed.

Once you are satisfied that you can register your application, authenticate users and obtain the profile information you need, we will deploy the solution to our production environment.

All production environment endpoints are exactly these same as the staging endpoint with only the hostname changing from 'staging.associationdatabase.com' to 'associationdatabase.com', which chase the new app registration form url to https://associationdatabase.com/oauth/applications/new?org_id=NYSPMA.

I am available all day tomorrow and Friday to discuss.

Please call our office and ask for either Tim or myself.

Thanks.

Thanks,

Dave

David Zachrich
Consultant
TCS Software, Inc.
Dublin, Ohio
614.451.5010
dave@tcssoftware.com