Social Payments - Twitter Setup Guide
Oracle Banking Digital Experience
Release 22.1.0.0.0

Part No. F56934-01

May 2022

ORACLE®

Social Payments - Twitter Setup Guide

May 2022

Table of Contents

1. Preface

1.1 Intended Audience

This document is intended for the following audience*:*

- Customers
- Partners

1.2 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

1.3 Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit

http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit

http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1.4 Structure

This manual is organized into the following categories:

Preface gives information on the intended audience. It also describes the overall structure of the User Manual.

The subsequent chapters describes following details:

- Introduction
- Preferences & Database
- Configuration / Installation.

1.5 Related Information Sources

For more information on Oracle Banking Digital Experience Release 22.1.0.0.0, refer to the following documents:

- Oracle Banking Digital Experience Installation Manuals

ORACLE®

2. Social Payments - Twitter

A Social Payment involves the transfer of money to an individual via social media. Social payments simplify digital payments by affording the initiator of the payment, the convenience of not having to know or remember the recipient's account information.

This document defines the means by which Twitter can be enabled as a mode under OBDX Peer to Peer Payments, by selecting which, retail users can initiate transfers towards Twitter Handles.

Home

ORACLE®

3. Twitter Console Configurations

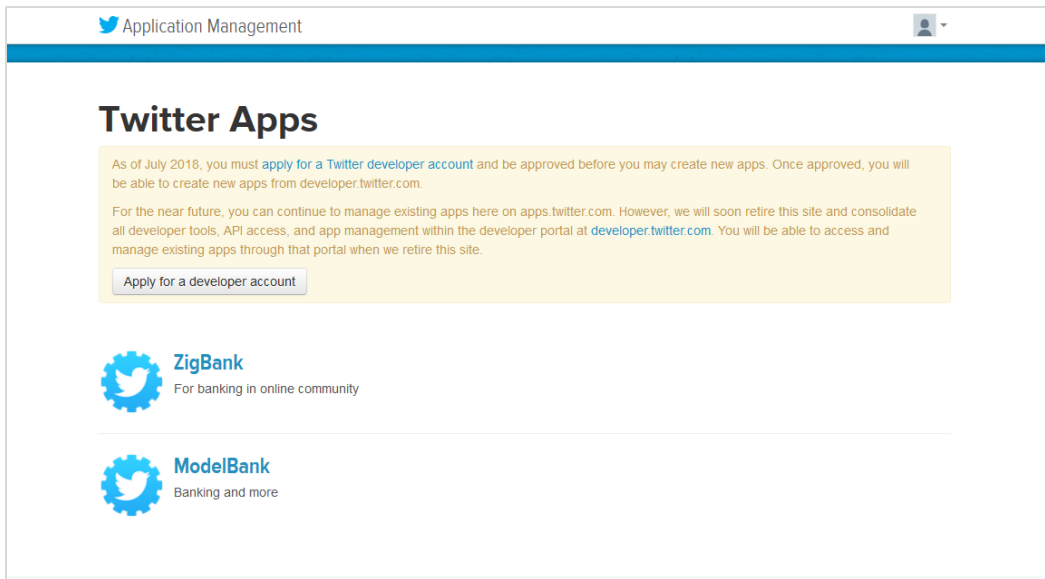This section documents the steps involved in enabling Twitter as a made for Peer to Peer payments in OBDX.

1. Navigate to the Twitter Application Management page - https://apps.twitter.com/
2. Click on the **sign in** link to login to the twitter account with which the app is associated.
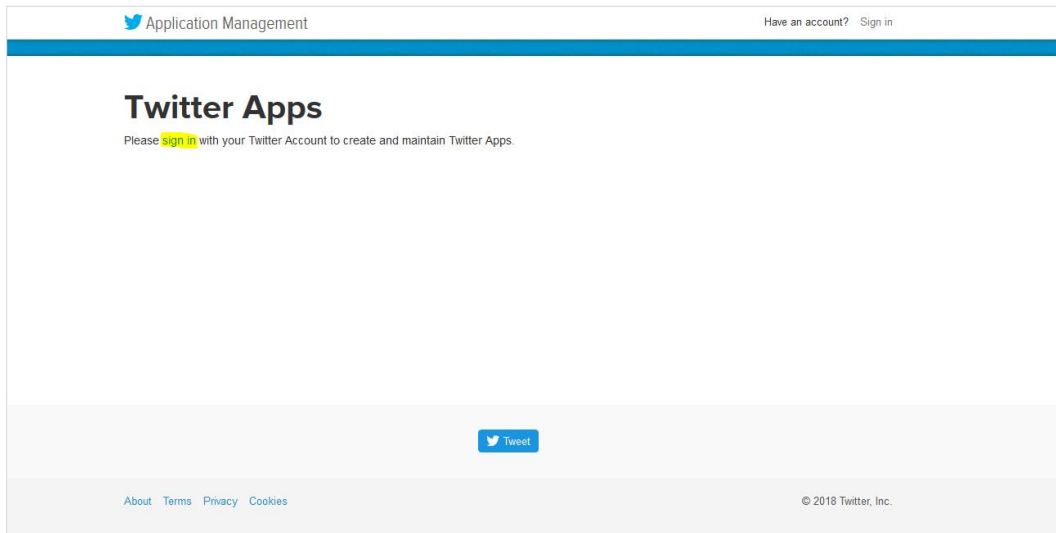
3. Login to the bank's Twitter account by entering user ID and password of the associated account in the provided fields. (The bank is required to have a twitter account.)
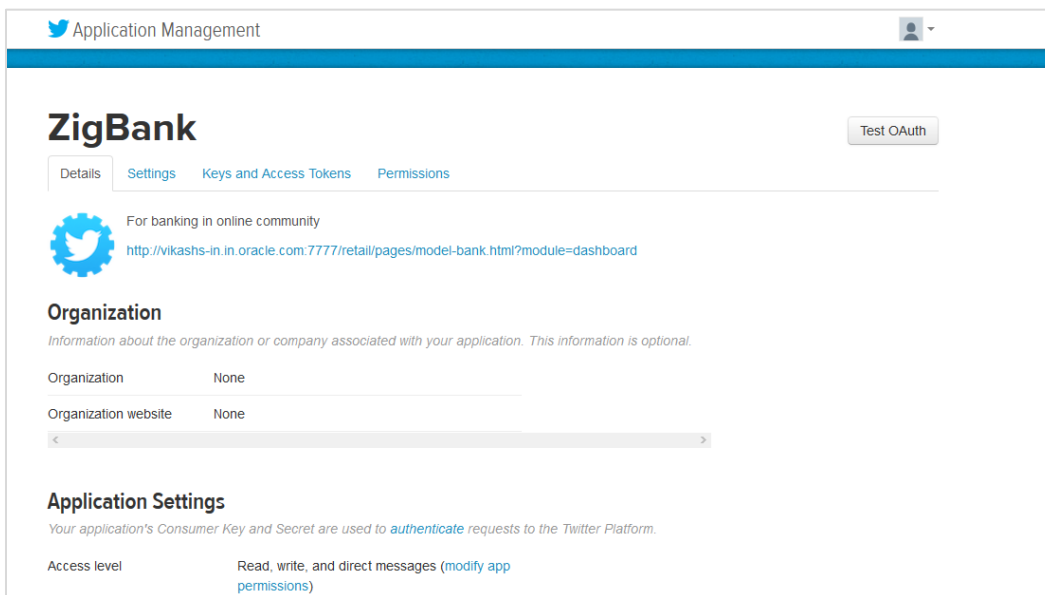
ORACLE®
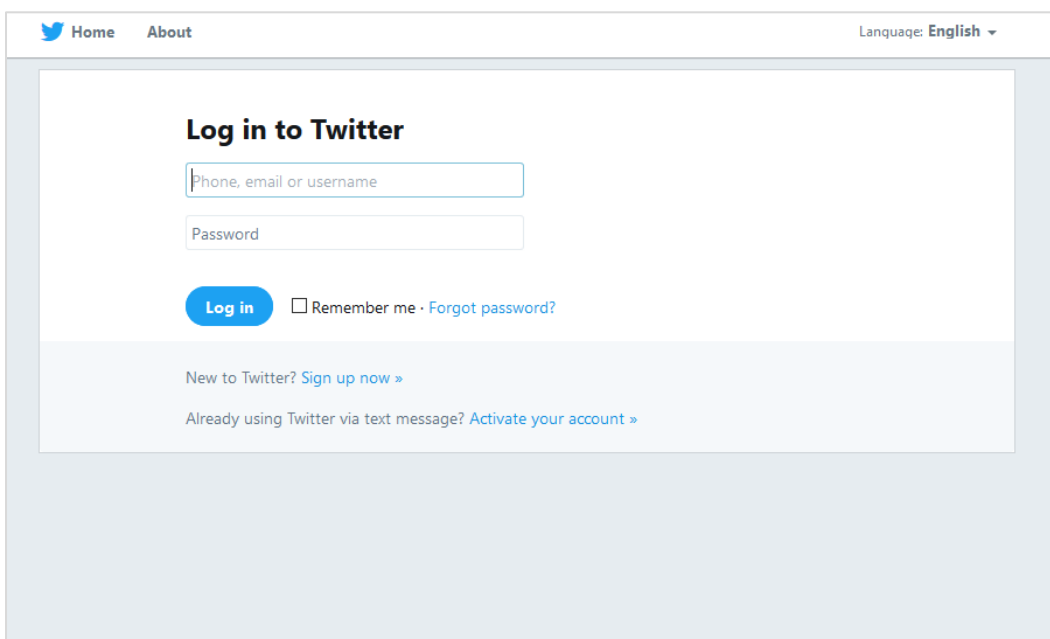
4. You will then be redirected to the Application Management page that lists the apps that have been made by the logged in user.

5. Select the app for which the setup needs to be configured. A new app will have to be created if this page is being accessed for the first time. After selecting an app, the menu page of that app will be displayed.

ORACLE®

6. Click on the **Settings** tab to define Callback URLs, the Client's App Website and other information.

Enter a name to be associated with the app in the **Name** field. Add a description of the app in the **Description** field. Enter the app's website and the callback URIs in the **Website** and **Callback URLs** fields respectively. All these parameters are mandatory for the client's app to authorize the user. The name, description and website as entered in these fields is displayed when the user is authorizing the app. Callback is required to redirect the user after signing in and authorizing the app.

Enter URL as -

https://<bankDomain>/digx-social/callback

Only one call back URL is sufficient. Multiple URLs (upto 10) can be added in case of production, UAT setup etc.

Additionally, if provided, add the links for Privacy Policy and Terms of Service by scrolling down. Also add the Application Icon that will be displayed to the user while authorizing the App. Add Client's name and the website to be displayed to the user at the time of authorization.

Additionally, the bank's icon can be uploaded against the **Application Icon** option, which will be displayed when user logs in to his/her twitter account.

ORACLE®

7. Update the settings by scrolling further down and clicking on the **Update Settings** button.

8. Click on the **Keys and Access Token** tab to access the app's consumer key/secret and access key/secret. The Consumer Key and Consumer Secret with owner name and owner ID are displayed. On scrolling down, you will be able to view the Access Token and Access Token Secret. Note and save this access token and secret. Never share the app's consumer secret and access secret.

ORACLE®

9. Click on the **Permissions** tab to set the permissions required by the app that is best suited for optimum functioning.

ORACLE®

10. For a better understanding of the **Access** permission that suits the app, click on the **Application Permission Model** link. Check the **Additional Permissions** check box, if required.
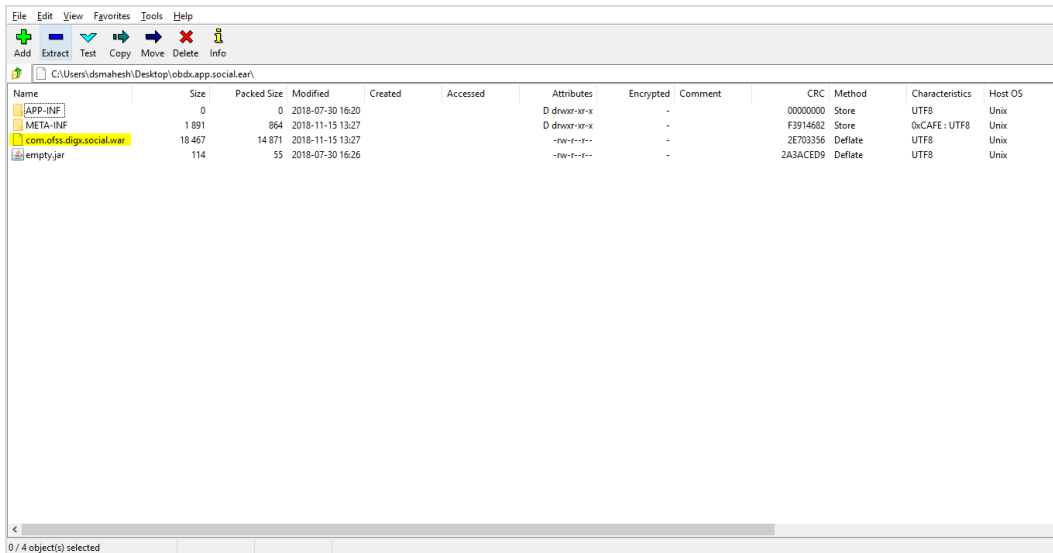
Whenever the permission level is changed, the keys and tokens must be regenerated in order for the change to be visible.

This implicitly means that the client must make its users reauthorize the app using the new keys and secret.
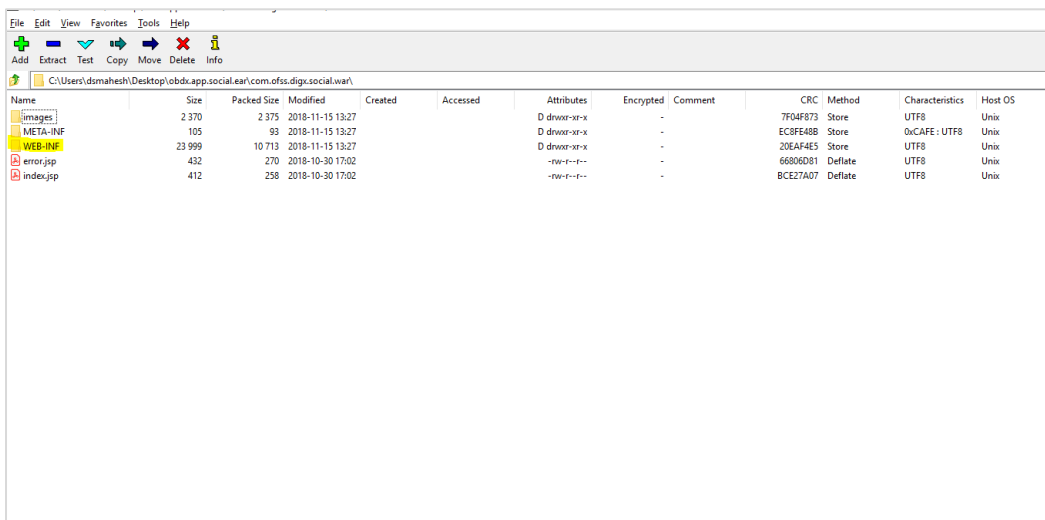
Home

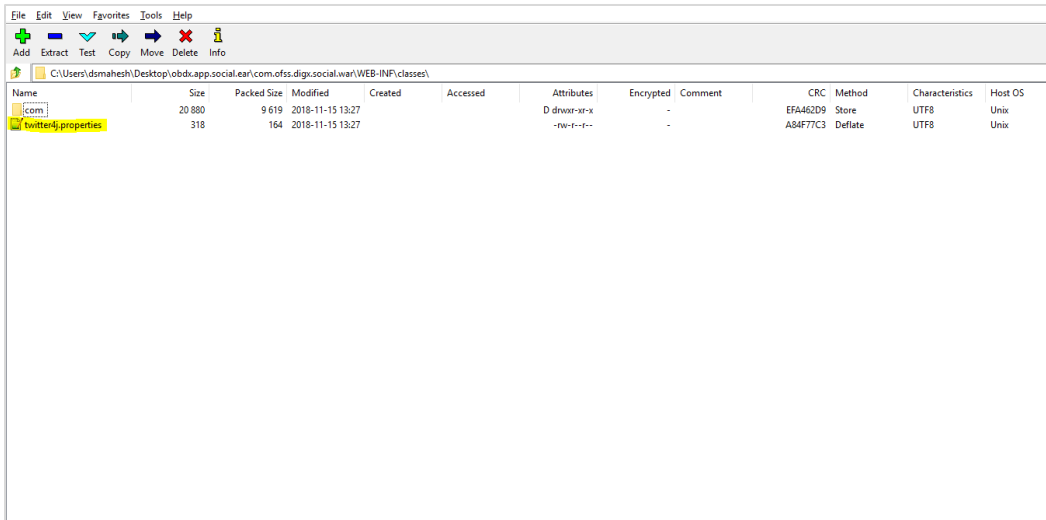ORACLE®

4. OBDX Configurations

1. Open the EAR "obdx.app.social.ear" to configure the Consumer Keys and Secret.

2. Open "obdx.app.social.war"

3. Open "WEB-INF" and open "classes". You will get "twitter4j.properties". Open the File.

ORACLE®

4. Put in the consumer key and secret generated in Section 3 at shown below. The OBDX server needs access to the twitter URL. If proxy is required, configure proxy settings as shown below:
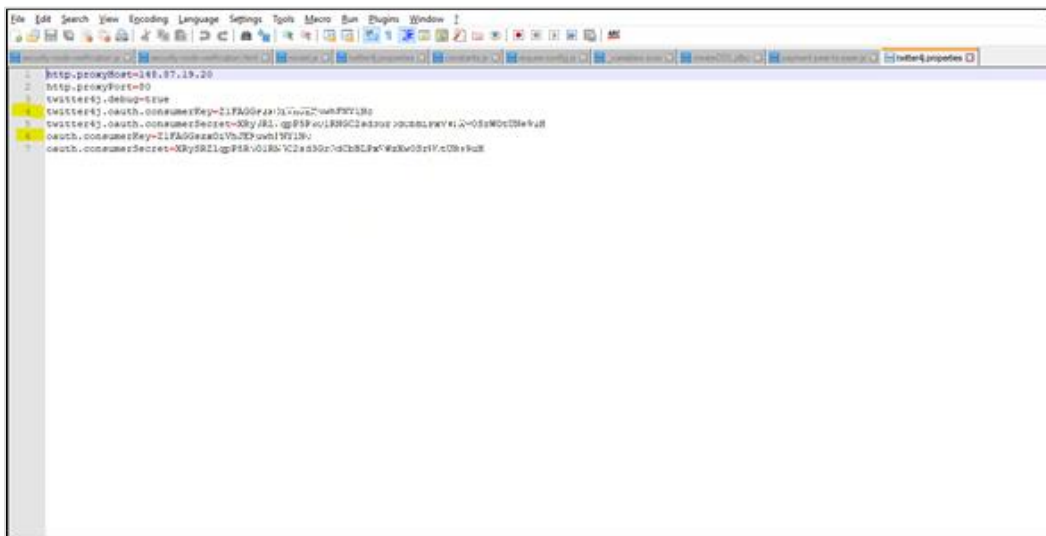
5. After configuring the "twitter4j.properties" file, save and close it. Re-deploy the EAR on to the server with the changes.

Home

ORACLE®