

Oracle Banking Digital Experience

Social Payments - Twitter Setup Guide

Release 18.3.0.0.0

Part No. F12056-01

December 2018

ORACLE®

Socail Payments - Twitter Setup Guide

December 2018

Oracle Financial Services Software Limited

Oracle Park

Off Western Express Highway

Goregaon (East)

Mumbai, Maharashtra 400 063

India

Worldwide Inquiries:

Phone: +91 22 6718 3000

Fax: +91 22 6718 3001

www.oracle.com/financialservices/

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Table of Contents

1. Preface	4
1.1 Intended Audience	4
1.2 Documentation Accessibility	4
1.3 Access to Oracle Support	4
1.4 Structure	4
1.5 Related Information Sources	4
2. Social Payments - Twitter	5
3. Twitter Console Configurations	6
4. OBDX Configurations	13

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.

Introduction provides brief information on the overall functionality covered in the User Manual.

The subsequent chapters provide information on transactions covered in the User Manual.

Each transaction is explained in the following manner:

- Introduction to the transaction
- Screenshots of the transaction
- The images of screens used in this user manual are for illustrative purpose only, to provide improved understanding of the functionality; actual screens that appear in the application may vary based on selected browser, theme, and mobile devices.
- Procedure containing steps to complete the transaction- The mandatory and conditional fields of the transaction are explained in the procedure.

If a transaction contains multiple procedures, each procedure is explained. If some functionality is present in many transactions, this functionality is explained separately.

1.5 Related Information Sources

For more information on Oracle Banking Digital Experience Release 18.3.0.0.0, refer to the following documents:

- Oracle Banking Digital Experience Licensing Guide
- Oracle Banking Digital Experience Installation Manuals

2. Social Payments - Twitter

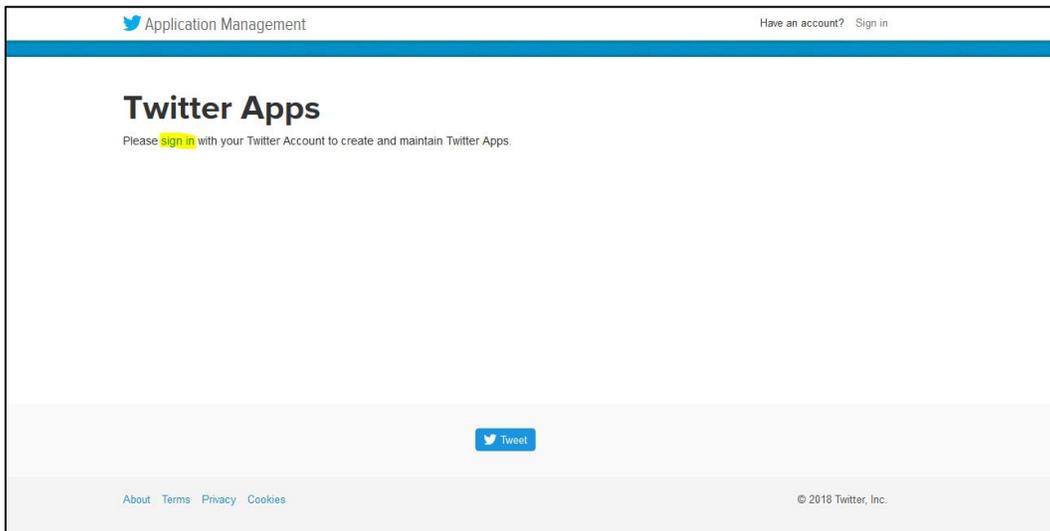
A Social Payment involves the transfer of money to an individual via social media. Social payments simplify digital payments by affording the initiator of the payment, the convenience of not having to know or remember the recipient's account information.

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.

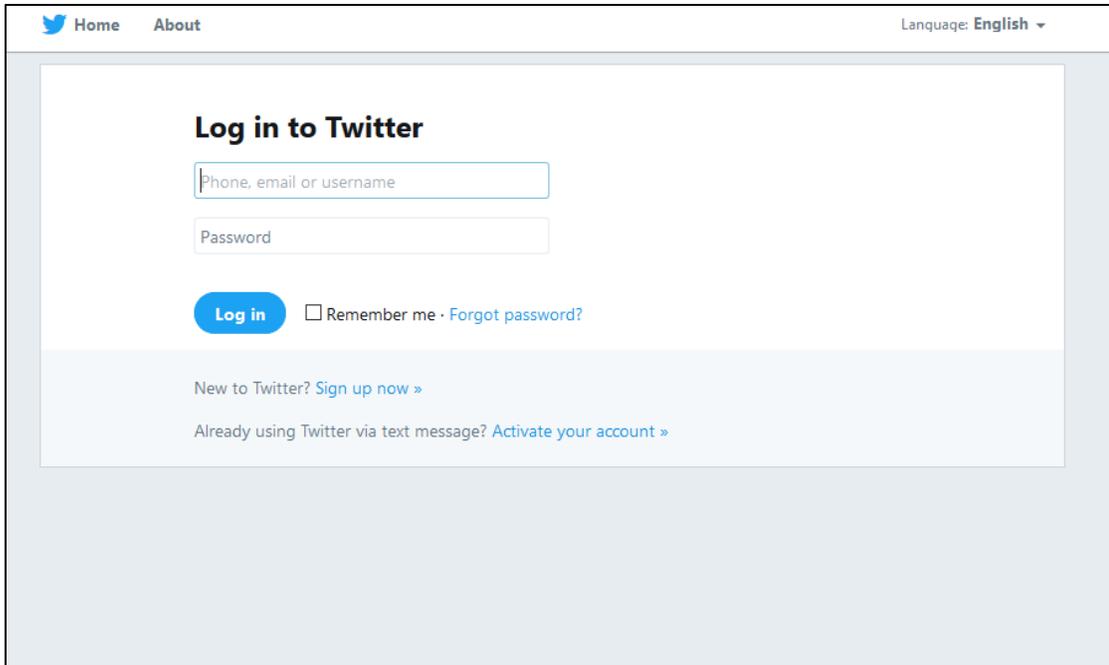
3. Twitter Console Configurations

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.

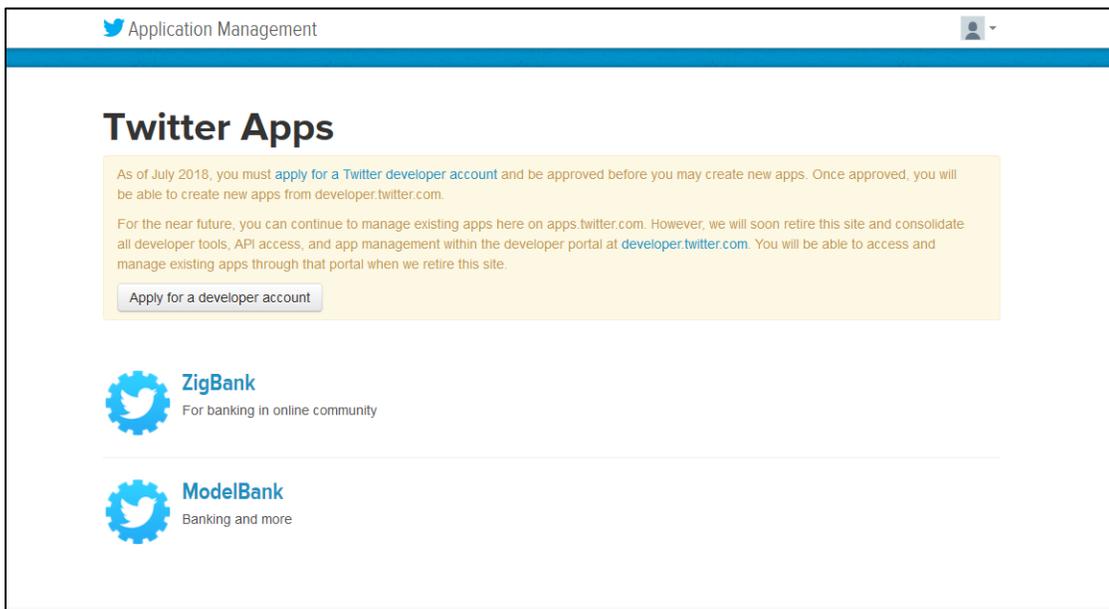


3. Login to the bank's Twitter account by entering user ID and password of the associated account in the provided fields. (The bank is required to have a twitter account.)



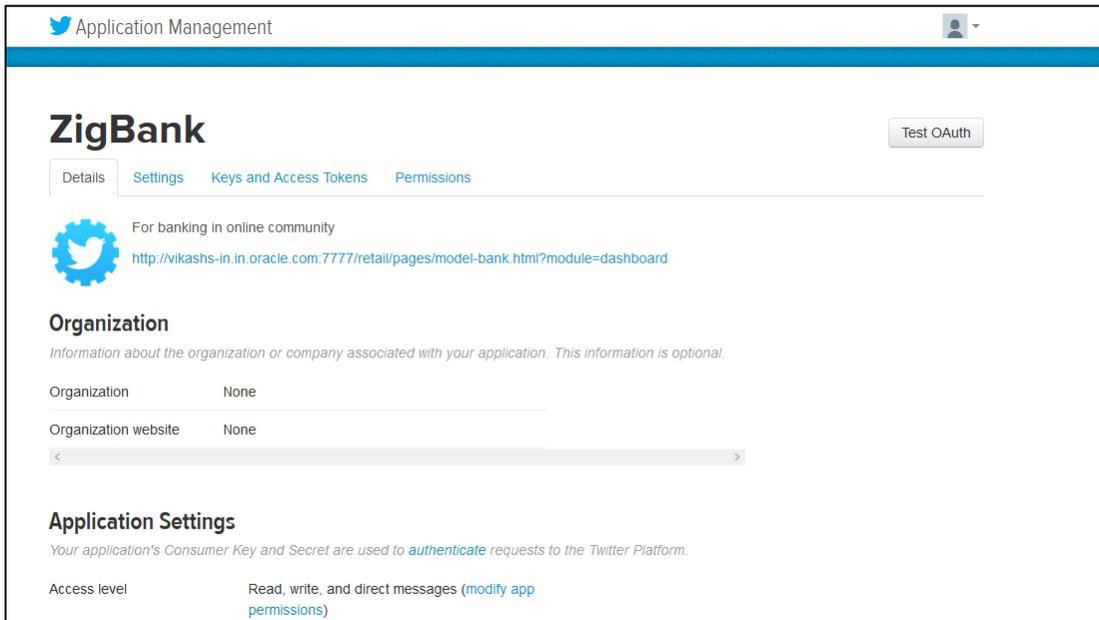
The screenshot shows the Twitter login interface. At the top, there are links for "Home" and "About", and a language selector set to "English". The main heading is "Log in to Twitter". Below this, there are two input fields: "Phone, email or username" and "Password". A blue "Log in" button is positioned to the left of a "Remember me" checkbox and a "Forgot password?" link. Below the login fields, there are two links: "New to Twitter? Sign up now »" and "Already using Twitter via text message? Activate your account »".

4. You will then be redirected to the Application Management page that lists the apps that have been made by the logged in user.



The screenshot shows the "Application Management" page. The header includes the Twitter logo, "Application Management", and a user profile icon. The main heading is "Twitter Apps". A yellow warning box contains the following text: "As of July 2018, you must [apply for a Twitter developer account](#) and be approved before you may create new apps. Once approved, you will be able to create new apps from [developer.twitter.com](#). For the near future, you can continue to manage existing apps here on [apps.twitter.com](#). However, we will soon retire this site and consolidate all developer tools, API access, and app management within the developer portal at [developer.twitter.com](#). You will be able to access and manage existing apps through that portal when we retire this site." Below the warning box is a button labeled "Apply for a developer account". The page lists two apps: "ZigBank" with the description "For banking in online community" and "ModelBank" with the description "Banking and more".

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.



The screenshot shows the Twitter Application Management interface for an application named "ZigBank". At the top, there is a navigation bar with the Twitter logo and the text "Application Management". Below this, the app name "ZigBank" is prominently displayed, along with a "Test OAuth" button. A menu bar contains tabs for "Details", "Settings", "Keys and Access Tokens", and "Permissions". The "Settings" tab is currently selected. Underneath, there is a section for the app's profile, including a Twitter icon, the text "For banking in online community", and a URL: "http://vikashs-in.in.oracle.com:7777/retail/pages/model-bank.html?module=dashboard". Below this is the "Organization" section, which includes fields for "Organization" (set to "None") and "Organization website" (set to "None"). The "Application Settings" section is partially visible, showing the "Access level" set to "Read, write, and direct messages (modify app permissions)".

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

The screenshot shows the 'Application Management' interface for an application named 'ZigBank'. The page has a blue header with the Twitter logo and 'Application Management' text. Below the header, the application name 'ZigBank' is displayed in large font, with a 'Test OAuth' button to its right. A navigation bar contains tabs for 'Details', 'Settings', 'Keys and Access Tokens', and 'Permissions'. The 'Details' tab is active, showing the 'Application Details' section. This section includes three main fields: 'Name', 'Description', and 'Website', each with a text input field and a small explanatory note below it. The 'Name' field contains 'ZigBank'. The 'Description' field contains 'For banking in online community'. The 'Website' field contains 'http://vikashs-in.in.oracle.com:7777/retail/pages/model-bank.html?module=dash'. Below these fields is a 'Callback URLs' section with a note and two input fields containing 'http://localhost:7779/digx-social/callback' and 'http://5e70788d.ngrok.io/digx-social/callback'. A 'Test OAuth' button is also visible in the top right corner of the application details area.

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.

Privacy Policy URL

The URL for your application or service's privacy policy. The URL will be shared with users authorizing this application.

Terms of Service URL

The URL for your application or service's terms of service. The URL will be shared with users authorizing this application.

Allow this application to be used to [Sign in with Twitter](#)

Application Icon
 **Change icon**
 No file selected.
Maximum size of 700k. JPG, GIF, PNG.

Organization
Organization name

The organization or company behind this application, if any.

Organization website

The organization or company behind this application's web page, if any.

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

Organization
Organization name

The organization or company behind this application, if any.

Organization website

The organization or company behind this application's web page, if any.

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.

The screenshot shows the Twitter Application Management interface for an application named 'ZigBank'. The 'Settings' tab is selected, displaying the following information:

- Consumer Key (API Key):** 2iTA9Gp52uW...ZEM10BfNY1!lc
- Consumer Secret (API Secret):** XRy5FuZigP...CCM19NGC...aU3Gr0dC0dLp...TTTTT...mU10r9vUf
- Access Level:** Read, write, and direct messages (modify app permissions)
- Owner:** zigbank
- Owner ID:** 884658235013189636

At the bottom, there are two buttons under 'Application Actions': 'Regenerate Consumer Key and Secret' and 'Change App Permissions'.

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

The screenshot shows the Twitter Application Management interface for 'ZigBank' with the 'Permissions' tab selected. The 'Access' section is visible, with the following options:

- What type of access does your application need?
 - Read only
 - Read and Write
 - Read, Write and Access direct messages

Note: Changes to the application permission model will only reflect in access tokens obtained after the permission model change is saved. You will need to re-negotiate existing access tokens to alter the permission level associated with each of your application's users.

The 'Additional Permissions' section is also visible, with the following option:

- Request email addresses from users

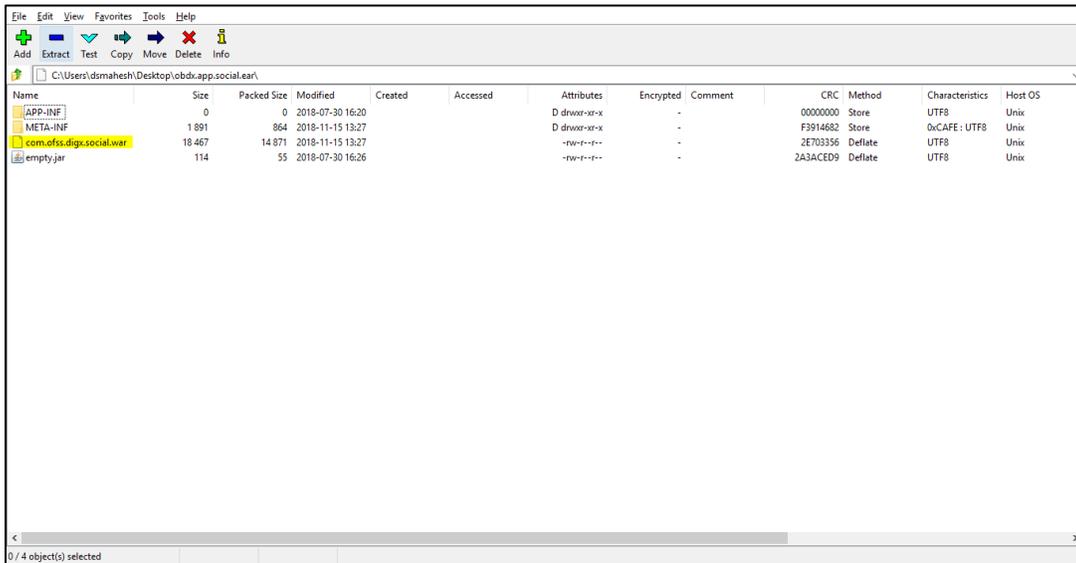
10. For a better understanding of the **Access** permission that suits the app, click on the **Application Permission Model** link. Check the **Additional Permissions** check box, if required.

Whenever the permission level is changed, the keys and tokens must be regenerated in order for the change to be visible.

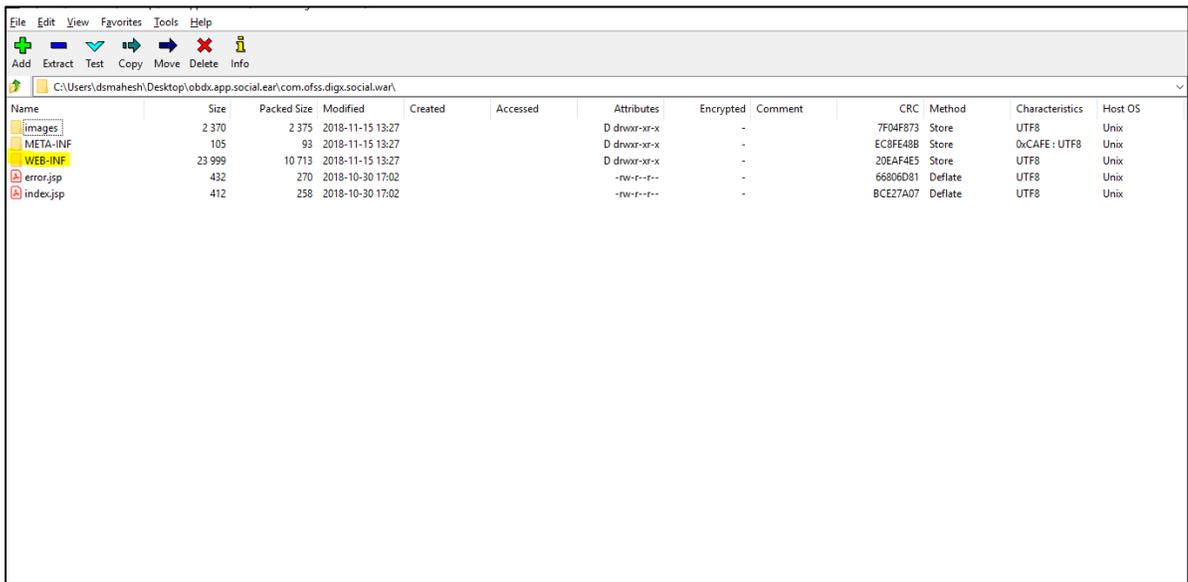
This implicitly means that the client must make its users reauthorize the app using the new keys and secret.

4. OBDX Configurations

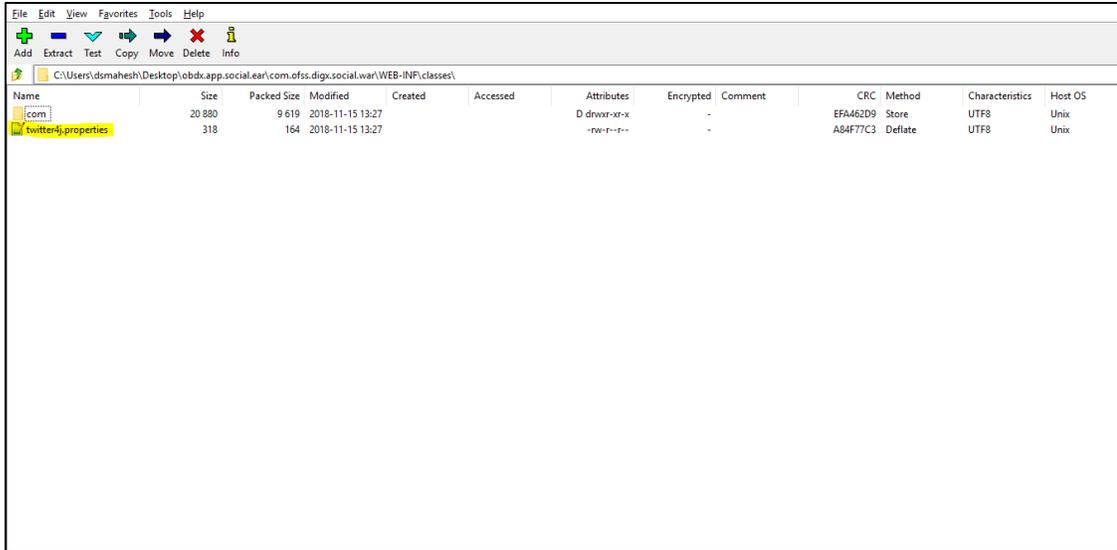
1. Open the EAR “obdx.app.social.ear” to configure the Consumer Keys and Secret.



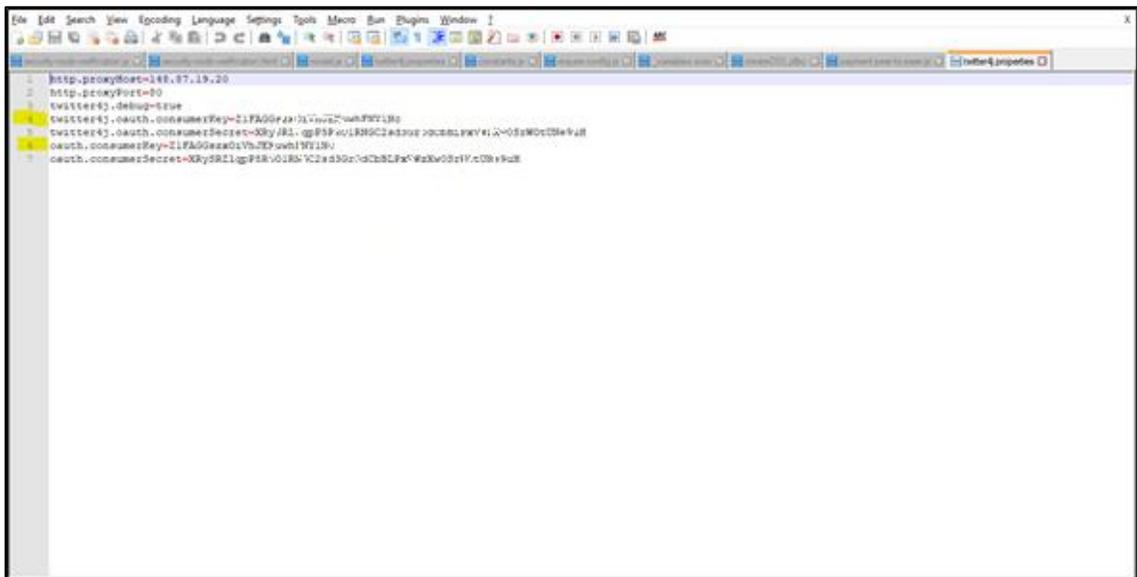
2. Open “obdx.app.social.war”



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



- 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:



- After configuring the “twitter4j.properties” file, save and close it. Re-deploy the EAR on to the server with the changes.