Mobile Application Builder-Android Guide
Oracle Banking Digital Experience
Patchset Release 22.2.4.0.0

Part No. F72987-01

June 2024

Mobile Application Builder-Android Guide

June 2024

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/

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 Patchset Release 22.2.4.0.0, refer to the following documents:

- Oracle Banking Digital Experience Installation Manuals

2. OBDX Servicing Application

2.1 Prerequisites

OBDX Android App is supported only on versions n (current) and n-1 release.

a. Download and Install node Js (will be downloaded to default path)

b. Install node js from https://nodejs.org

c. DOWNLOAD AND INSTALL ANDROID STUDIO

d. Download and install Android Studio from https://developer.android.com/studio/index.html

e. Download and Install Android platforms

f. Update Android SDK to latest API Level.

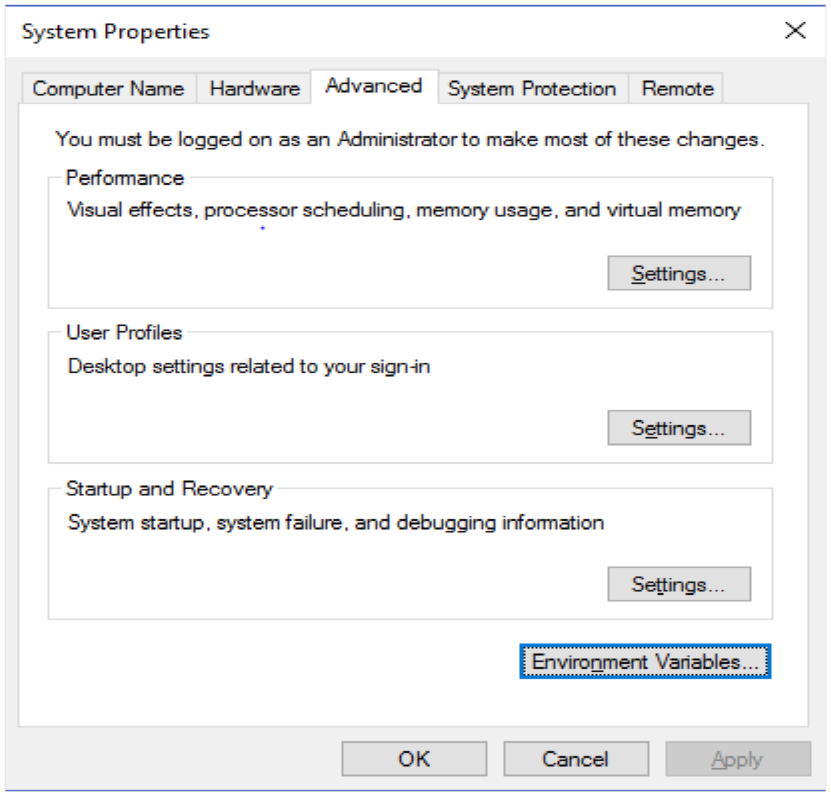
g. Gradle Version: gradle-4.6

h. Android Gradle Plugin Version (3.4.0): 'com.android.tools.build:gradle:3.4.0' or above

i. Set Environment variables

j. Set following system variables:

1. Click on Windows key and type Environment Variables.
2. A dialog box will appear. Click on the Environment Variables button as shown below



You must be logged on as an Administrator to make most of these changes.

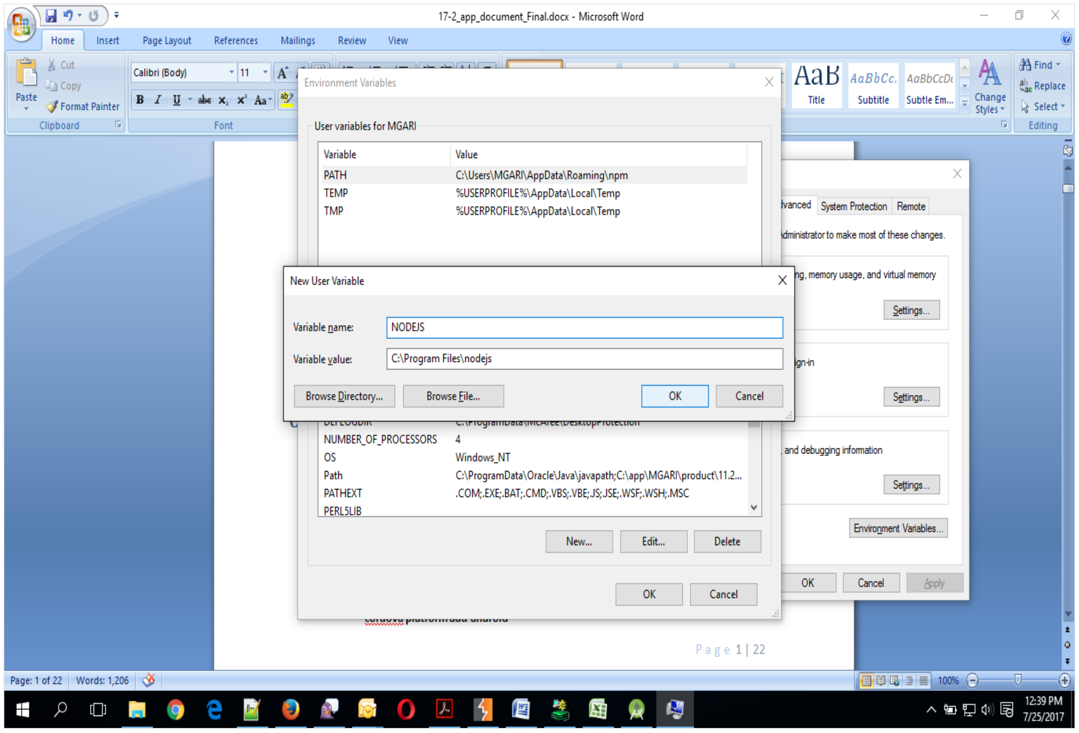
Visual effects, processor scheduling, memory usage, and virtual memory

Desktop settings related to your sign-in

System startup, system failure, and debugging information

3. NODEJS <nodejs_path> Example: *"C:\Program Files\nodejs\".*

k. Add the above variables in “*PATH*” system variable.



Environment Variables

User variables for MGARI

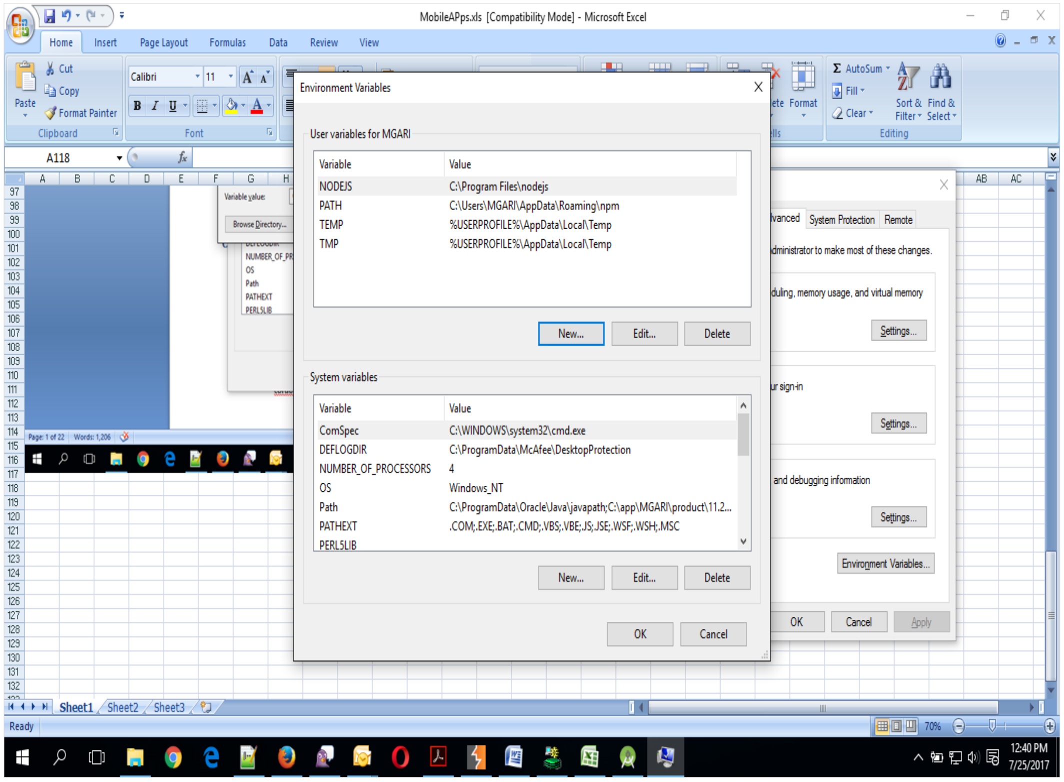
Variable	Value
PATH	C:\Users\MGARI\AppData\Roaming\npm
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

New User Variable

Variable name: NODEJS

Variable value: C:\Program Files\nodejs

Variable	Value
NUMBER_OF_PROCESSORS	4
OS	Windows_NT
Path	C:\ProgramData\Oracle\Java\javapath;C:\app\MGARI\product\11.2...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PERL5LIB	



Environment Variables

User variables for MGARI

Variable	Value
NODEJS	C:\Program Files\nodejs
PATH	C:\Users\MGARI\AppData\Roaming\npm
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
ComSpec	C:\WINDOWS\system32\cmd.exe
DEFLOGDIR	C:\ProgramData\McAfee\DesktopProtection
NUMBER_OF_PROCESSORS	4
OS	Windows_NT
Path	C:\ProgramData\Oracle\Java\javapath;C:\app\MGARI\product\11.2...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PERL5LIB	

In 20.1, you can create app in two ways-using local UI or using remote UI (if want to create using remote go to section **Create project using Remote UI2.2** else directly to section **Local UI**)

2.2 Create project using Remote UI

a. Index.html changes(use Android Studio or any other editor)

- Update the server URL in app.properties against KEY_SERVER_URL key. This is the URL where the UI is also hosted.

  After this proceed to **2.4 Importing in Android Studio** directly.

2.3 Local UI by running on local machine or local server.

2.3.1 Adding UI to workspace

Use any 1 option below of a/b

a) Building un-built UI (required in case of customizations)

1. For this version, since the UI is built with webpack, the built UI cannot be modified from with the mobile workspace as it is minified code. Hence, either bank can hoist the UI is two ways:
   - Use local machine as local server and host the UI on local development machine and connect the application using localhost.
   - OR host the UI on local development server and point the application to that server URL
1. UI is same for internet and mobile, same build process of internet to be followed.

   Bank can follow the UI build steps from “Oracle Banking Digital Experience User Interface Guide”.

2. For building UI for mobile, Open scripts->webpack->webpack.dev.js and add below line in devServer object:

   as below:

```
headers: {
        "Access-Control-Allow-Origin": "*"
},
```

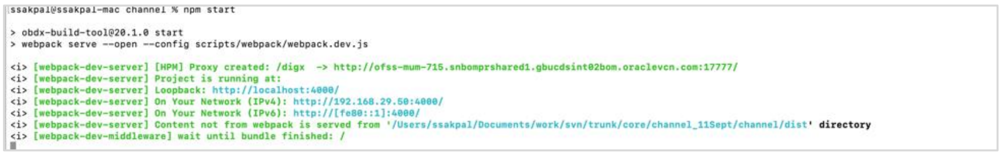
   SAMPLE:

```
devServer: {
  static: path.join(__dirname,
                    "../../dist"),
  compress: true,
port: 4000,
hot: false,
client: false,
headers: {
        "Access-Control-Allow-Origin": "*"
},
```

3. Also, in webpack.dev.js comment out below lines inside “entry” key.

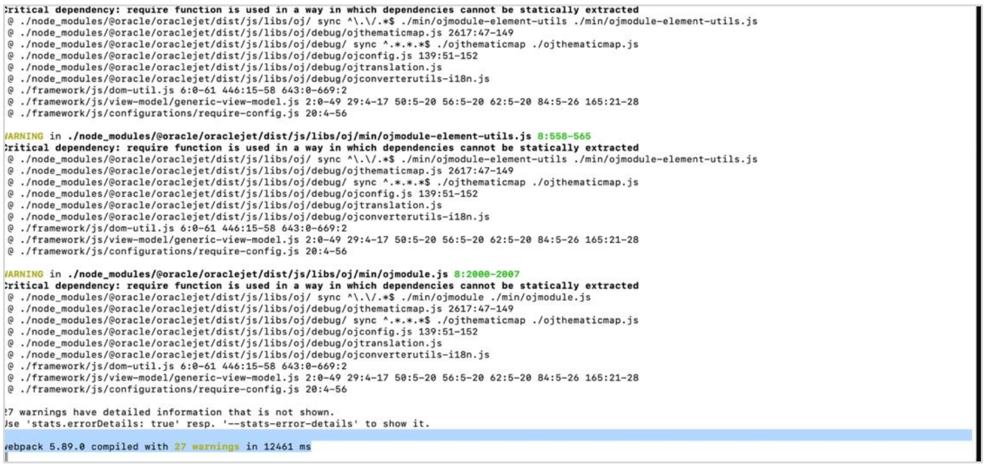
```
entry: {
    //  main: "framework/js/configurations/require-config.js",
     // Runtime code for hot module replacement
     //hot: 'webpack/hot/dev-server.js',
     // Dev server client for web socket transport, hot and live reload logic
//client: 'webpack-dev-server/client/index.js?hot=true&live-//reload=true',
   },
```

4. Once the UI is built, run below command to start a local server on the development machine using below command:
   - npm run start



```
ssakpal@ssakpal-mac channel % npm start

> obdx-build-tool@20.1.0 start
> webpack serve --open --config scripts/webpack/webpack.dev.js

<i> [webpack-dev-server] [HPM] Proxy created: /digx  -> http://ofss-mum-715.snbomprshared1.gbucdsint02bom.oraclevcn.com:17777/
<i> [webpack-dev-server] Project is running at:
<i> [webpack-dev-server] Loopback: http://localhost:4000/
<i> [webpack-dev-server] On Your Network (IPv4): http://192.168.29.50:4000/
<i> [webpack-dev-server] On Your Network (IPv6): http://[fe80::1]:4000/
<i> [webpack-dev-server] Content not from webpack is served from '/Users/ssakpal/Documents/work/svn/trunk/core/channel_11Sept/channel/dist' directory
<i> [webpack-dev-middleware] wait until bundle finished: /
```

   - Once this server starts, below is the window which appears. This indicates local server is started.



```
:ritical dependency: require function is used in a way in which dependencies cannot be statically extracted
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/ sync ^\.\/.*$ ./min/ojmodule-element-utils ./min/ojmodule-element-utils.js
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ojthematicmap.js 2617:47-149
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ sync ^.*.*.*$ ./ojthematicmap ./ojthematicmap.js
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ojconfig.js 139:51-152
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ojtranslation.js
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ojconverterutils-i18n.js
 @ ./framework/js/dom-util.js 6:0-61 446:15-58 643:0-669:2
 @ ./framework/js/view-model/generic-view-model.js 2:0-49 29:4-17 50:5-20 56:5-20 62:5-20 84:5-26 165:21-28
 @ ./framework/js/configurations/require-config.js 20:4-56

/ARNING in ./node_modules/@oracle/oraclejet/dist/js/libs/oj/min/ojmodule-element-utils.js 8:558-565
:ritical dependency: require function is used in a way in which dependencies cannot be statically extracted
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/ sync ^\.\/.*$ ./min/ojmodule-element-utils ./min/ojmodule-element-utils.js
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ojthematicmap.js 2617:47-149
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ sync ^.*.*.*$ ./ojthematicmap ./ojthematicmap.js
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ojconfig.js 139:51-152
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ojtranslation.js
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ojconverterutils-i18n.js
 @ ./framework/js/dom-util.js 6:0-61 446:15-58 643:0-669:2
 @ ./framework/js/view-model/generic-view-model.js 2:0-49 29:4-17 50:5-20 56:5-20 62:5-20 84:5-26 165:21-28
 @ ./framework/js/configurations/require-config.js 20:4-56

/ARNING in ./node_modules/@oracle/oraclejet/dist/js/libs/oj/min/ojmodule.js 8:2000-2007
:ritical dependency: require function is used in a way in which dependencies cannot be statically extracted
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/ sync ^\.\/.*$ ./min/ojmodule ./min/ojmodule.js
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ojthematicmap.js 2617:47-149
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ sync ^.*.*.*$ ./ojthematicmap ./ojthematicmap.js
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ojconfig.js 139:51-152
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ojtranslation.js
 @ ./node_modules/@oracle/oraclejet/dist/js/libs/oj/debug/ojconverterutils-i18n.js
 @ ./framework/js/dom-util.js 6:0-61 446:15-58 643:0-669:2
 @ ./framework/js/view-model/generic-view-model.js 2:0-49 29:4-17 50:5-20 56:5-20 62:5-20 84:5-26 165:21-28
 @ ./framework/js/configurations/require-config.js 20:4-56

:7 warnings have detailed information that is not shown.
Jse 'stats.errorDetails: true' resp. '--stats-error-details' to show it.

vebpack 5.89.0 compiled with 27 warnings in 12461 ms
```

   - Point the “key_server_url” to http://localhost:4000 and run the application on simulator. To run on device, the internet proxy should allow localhost domain to accept incoming requests.

If it is blocked, UI should be built and "npm start" command should be executed on a development server machine which is accessible in the network. They "key_server_url" will then point to that local server URL instead of localhost

b) Using built UI (out of box shipped with installer)

Available at --

OBDX_Installer/installables/ui/deploy (Main release, OBDX installer), OBDX_Patch_Installer/installables/ui/deploy (Patchsets)

- There will be production enabled dist generated in the built UI.
- Bank can either directly deploy this dist to their server and point the application to that server as mentioned in point a above OR
- Bank can copy the dist folder in their workspace and follow steps from point 3in section 2.5.
- If bank wants to do any changes, point a) steps needs to be followed.

NOTE: If banks want to debug UI in production builds, then dist should be created with below configuration enabled in webpack.prod.js

devtool: 'eval',

- This will however increase the files deployed on server and reduce the proformance on production. Refer Webpack documentation https://webpack.js.org/configuration/devtool/ for more details.

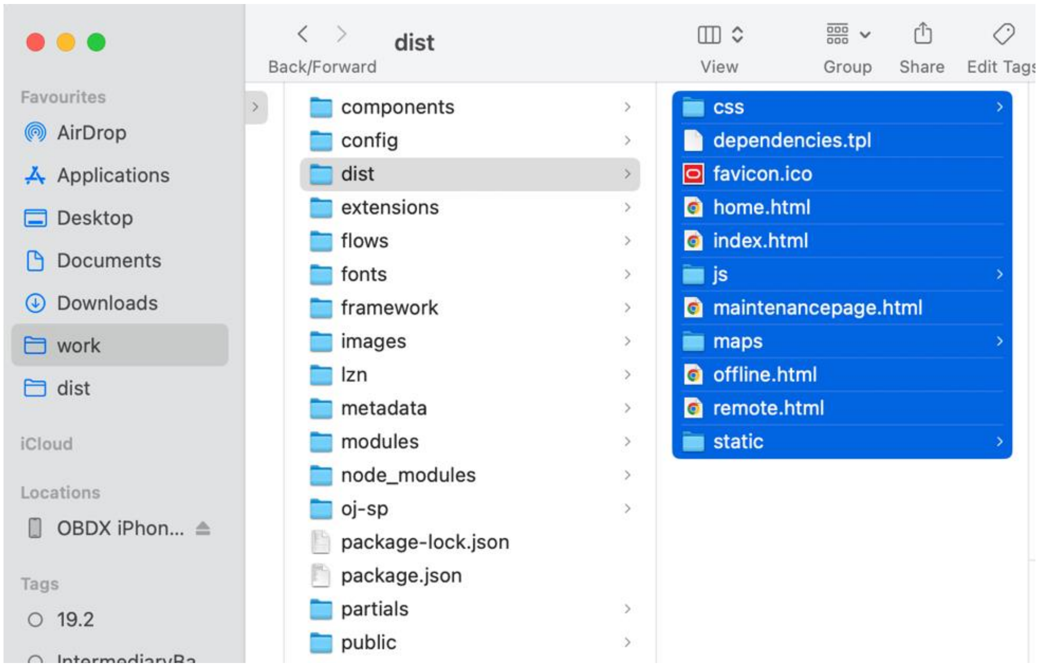
2.3.2 Create Project Using local UI within the workspace

1. Extract the unbuilt UI and follow steps up to 5 in the above section 2.4.
2. After step 4, run below command to generate dist folder.

   npm run webpack-dev – this will generate development enabled dist

   npm run webpack-build- this will generate production enabled dist
3. Once the dist folder is created, copy all files inside dist folder and save it in the

   workspace_installer/zigbank/platforms/android/app/src/main/assets/www/.



4. Open Index.html and home.html and add below line inside head section below meta tag

   <script src="cordova.js" type=”text/javascript”></script>

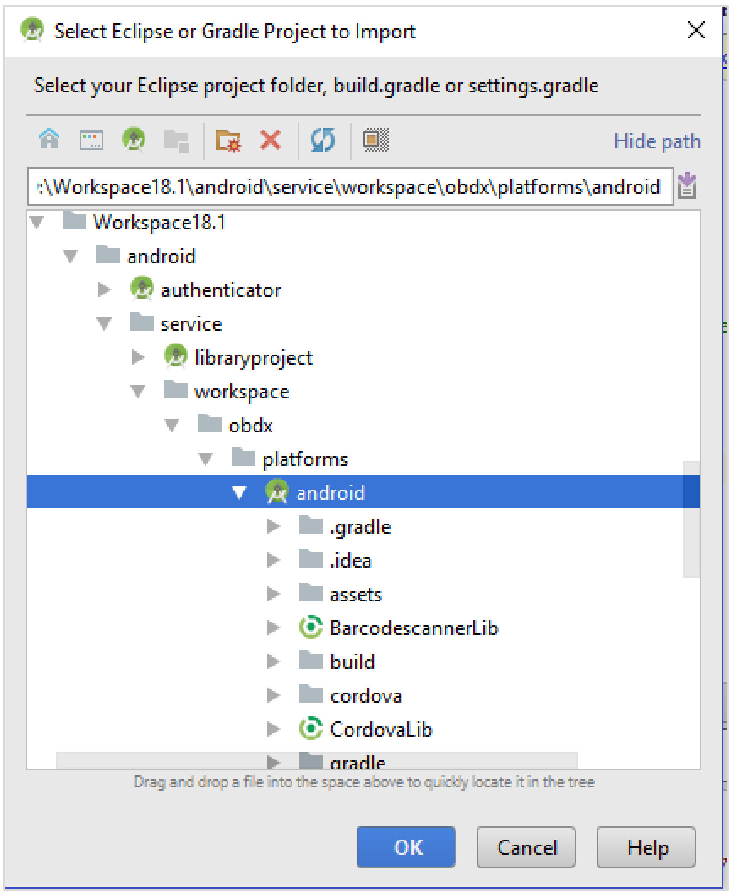
5. Set the server URL in app.properties against key_server_url. This is the URL where backend services are hosted.

6. With this setup, since the files generated in dist folder are minified format we cannot change the code. If any change needs to be done in any UI file, then the changes must be done in the UI folder, built it again to generate dist and copy the files to workspace again. Since this is tedious process, we recommend to setup local server and host UI there for development.

2.4 Importing in Android Studio

Open Android Studio

1. Import zigbank**/**platforms**/**android in android studio by clicking on Open an Existing Project.


Select Eclipse or Gradle Project to Import

Select your Eclipse project folder, build.gradle or settings.gradle

:\Workspace18.1\android\service\workspace\obdx\platforms\android

```
▼ Workspace18.1
  ▼ android
    ▶ authenticator
    ▼ service
      ▶ libraryproject
      ▼ workspace
        ▼ obdx
          ▼ platforms
            ▼ android
              ▶ .gradle
              ▶ .idea
              ▶ assets
              ▶ BarcodescannerLib
              ▶ build
              ▶ cordova
              ▶ CordovaLib
              ▶ gradle
```

Drag and drop a file into the space above to quickly locate it in the tree

2.5 Widget Functionality

Widgets are Android native feature. Below widgets are available in the application

1. All Accounts Widgets – Widget, showing all accounts balances & account numbers.

2. Account Details Widget - Widget, showing account balance of default account and last 5 transactions of the same account, can be added to the phone home screen. If default account is not set, then the details of the account fetched first is shown.

3. Multi-Functional Widget – Widget showing default account balance. If default account is not present, it shows details of account fetched first. Additionally, it has option to scan to pay feature

4. Scan to Pay Widget – Widget which allows to scan to pay.

Prerequisite:

Quick Snapshot feature needs to be enabled in the app application from the login screen. (Refer function doc - User Manual Oracle Banking Digital Experience Quick Snapshot.docx)

Please enable below property in app.properties file

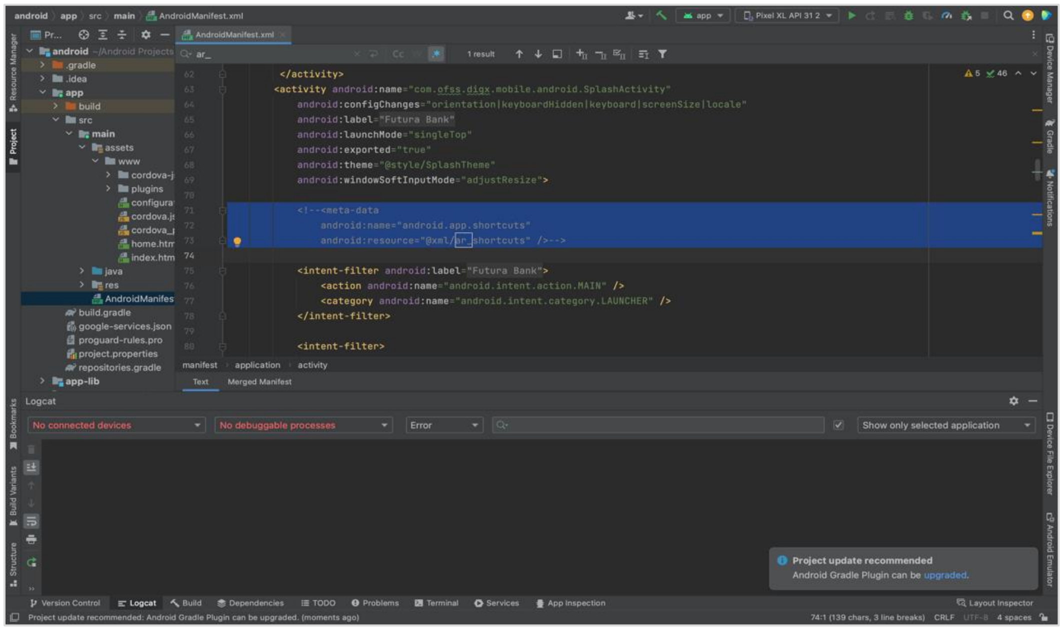
```
<bool name="ENABLE_WIDGET">true</bool>
```

If bank does not want this feature, then they can disable this by making above flag to false.

2.6 Scan to Pay from Application Icon –

Users can long press on bank's application icon on home screen and click on scan-to-pay option to scan QR and make payments.

To enable this feature uncomment below from app's AndroidManifest.xml



```
        </activity>
       <activity android:name="com.ofss.digx.mobile.android.SplashActivity"
           android:configChanges="orientation|keyboardHidden|keyboard|screenSize|locale"
           android:label="Futura Bank"
           android:launchMode="singleTop"
           android:exported="true"
           android:theme="@style/SplashTheme"
           android:windowSoftInputMode="adjustResize">

           <!--<meta-data
               android:name="android.app.shortcuts"
               android:resource="@xml/ar_shortcuts" />-->

           <intent-filter android:label="Futura Bank">
               <action android:name="android.intent.action.MAIN" />
               <category android:name="android.intent.category.LAUNCHER" />
           </intent-filter>

           <intent-filter>
```

2.7 Scan Card using Augmented Reality

Users can scan card and view account details and transactions of the account associated with the card.

To enable this feature, do the same step which is mentioned on 2.6 section.

2.8 Passkey (Passwordless login)

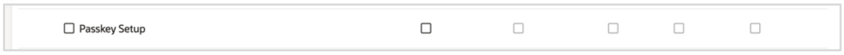
Passkeys are a safer and easier replacement for passwords. With passkeys, users can sign in to apps and websites using a biometric sensor (such as a fingerprint or facial recognition), PIN, or pattern. This provides a seamless sign-in experience, freeing your users from having to remember usernames or passwords.

Passkeys are supported only on devices that run Android 9 (API level 28) or higher

TO DISBALE THIS OPTION:

By doing this, passkey option will not be available to users withing the application. User will not be able to register for passkey and also will not be able to login using passkey. Follow below steps

a. Remove RTM access from Client Servicing -> Authentication - > Passkey Setup for Mobile Application/Mobile (Responsive) and Internet touch points

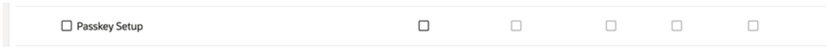


b. Set this flag in channel-framework-js-configurations-config..js to false

thirdPartyAPIs -> passkey -> required -> false

TO ENABLE THIS OPTION:

1. Add RTM access from Client Servicing -> Authentication - > Passkey Setup for Mobile Application,Mobile (Responsive) and Internet touch points



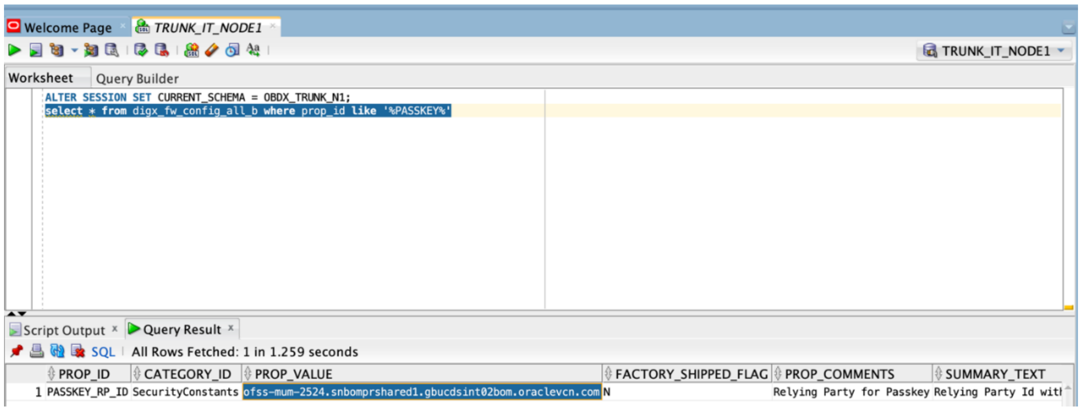
2. Set this flag in channel-framework-js-configurations-config.js to true

   thirdPartyAPIs -> passkey -> required -> true

3. Along with above, we need below server side and application side settup

Server-Side Setup:

1. Update the relying party in below property select prop_value from digx_fw_config_all_b where prop_id='PASSKEY_RP_ID'



```
ALTER SESSION SET CURRENT_SCHEMA = OBDX_TRUNK_N1;
select * from digx_fw_config_all_b where prop_id like '%PASSKEY%'
```

All Rows Fetched: 1 in 1.259 seconds

	PROP_ID	CATEGORY_ID	PROP_VALUE	FACTORY_SHIPPED_FLAG	PROP_COMMENTS	SUMMARY_TEXT
1	PASSKEY_RP_ID	SecurityConstants	ofss-mum-2524.snbomprshared1.gbucdsint02bom.oraclevcn.com	N	Relying Party for Passkey	Relying Party Id witl

2. Note – Relying partId is the domain name if the website to which credentials will be associated. (Eg google.com, example.com etc)

   Relying party origin is the relying party of website prefixed with protocol without the port.

(E,g, https://google.com, https://example.com)

a. Create assetlinks file (assetlinks.json) -

   A Digital Asset Links JSON file must be published on your website to indicate the Android apps that are associated with the website and verify the app's URL intents.

The following example assetlinks.json file grants link-opening rights to a com.example Android app:

```
[{

        "relation": ["delegate_permission/common.handle_all_urls"],

        "target": {

           "namespace": "android_app",

                 "package_name": "com.example",


"sha256_cert_fingerprints":["14:6D:E9:83:C5:73:06:50:D8:EE:B9:95:2F:34:FC:64:16:A0:
83:42:E6:1D:BE:A8:8A:04:96:B2:3F:CF:44:E5"]

        }

}]
```

The JSON file uses the following fields to identify associated apps:

package_name: The application ID declared in the app's build.gradle file.

sha256_cert_fingerprints: The SHA256 fingerprints of your app’s signing certificate. You can use the following command to generate the fingerprint via the Java keytool:

```
keytool -list -v -keystore my-release-key.keystore
```

b. Publish assestlinks.json file-

This file needs to be on https server with valid SSL certificate

You must publish your JSON verification file at the following location:

https://domain.name/.well-known/assetlinks.json

For example, if your sign-in domain is signin.example.com, host the JSON file at https://signin.example.com/.well-known/assetlinks.json.

Verify your assetlink json on below statement list tester-

https://developers.google.com/digital-asset-links/tools/generator

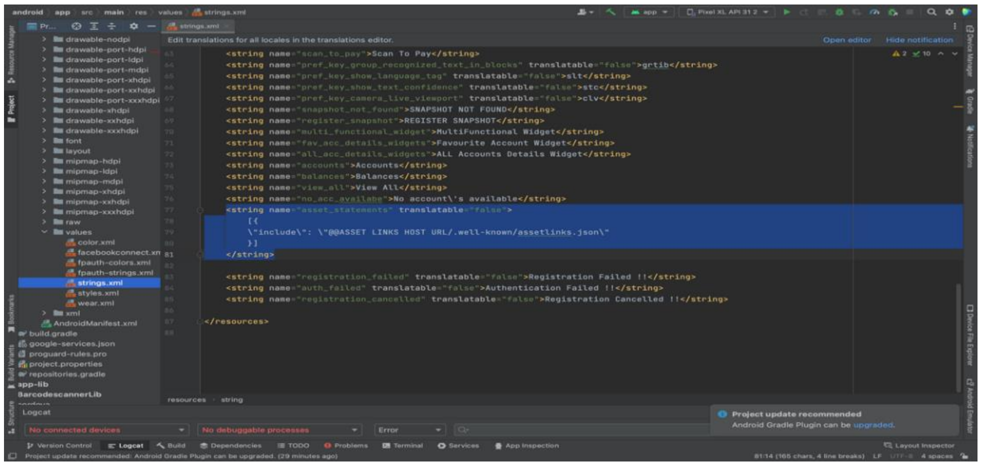
The MIME type for the Digital Assets Link file needs to be JSON. Make sure the server sends a Content-Type: application/json header in the response.

Need to change host and port in Obdx.conf as, ProxyPass "/.well-known" "http://100.76.157.55:7003/digx-admin/sms/v1/.well-known"

ProxyPassReverse "/.well-known" "http://100.76.157.55:7003/digx-admin/sms/v1/.well-known"

After the setup is done, this file must be accessible on mobile browser with this url. There should not by any redirects for accessing this file.

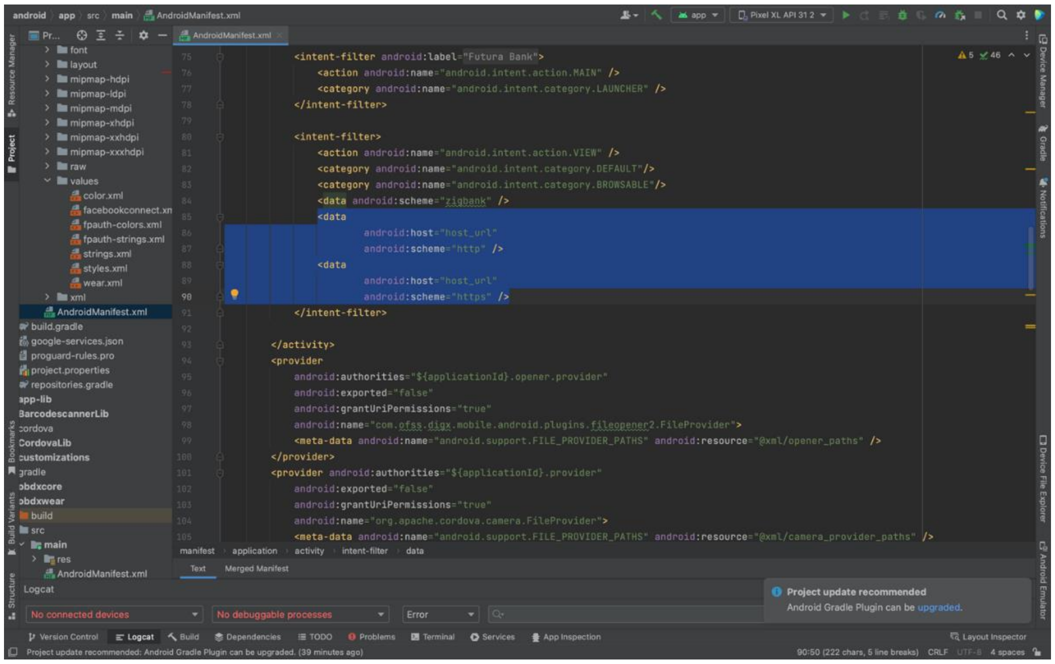
c. Add assetlinks.json file host in app's strings.xml file.



```
    <string name="scan_to_pay">Scan To Pay</string>
    <string name="pref_key_group_recognized_text_in_blocks" translatable="false">grtib</string>
    <string name="pref_key_show_language_tag" translatable="false">slt</string>
    <string name="pref_key_show_text_confidence" translatable="false">stc</string>
    <string name="pref_key_camera_live_viewport" translatable="false">clv</string>
    <string name="snapshot_not_found">SNAPSHOT NOT FOUND</string>
    <string name="register_snapshot">REGISTER SNAPSHOT</string>
    <string name="multi_functional_widget">MultiFunctional Widget</string>
    <string name="fav_acc_details_widgets">Favourite Account Widget</string>
    <string name="all_acc_details_widgets">ALL Accounts Details Widget</string>
    <string name="accounts">Accounts</string>
    <string name="balances">Balances</string>
    <string name="view_all">View All</string>
    <string name="no_acc_availabe">No account\'s available</string>
    <string name="asset_statements" translatable="false">
        [{
        \"include\": \"@@ASSET LINKS HOST URL/.well-known/assetlinks.json\"
        }]
    </string>

    <string name="registration_failed" translatable="false">Registration Failed !!</string>
    <string name="auth_failed" translatable="false">Authentication Failed !!</string>
    <string name="registration_cancelled" translatable="false">Registration Cancelled !!</string>

</resources>
```

2.9 Deeplinking - To open reset password, claim money links with the application

Please add host url under data tag in app’s AndroidManifest.xml as,

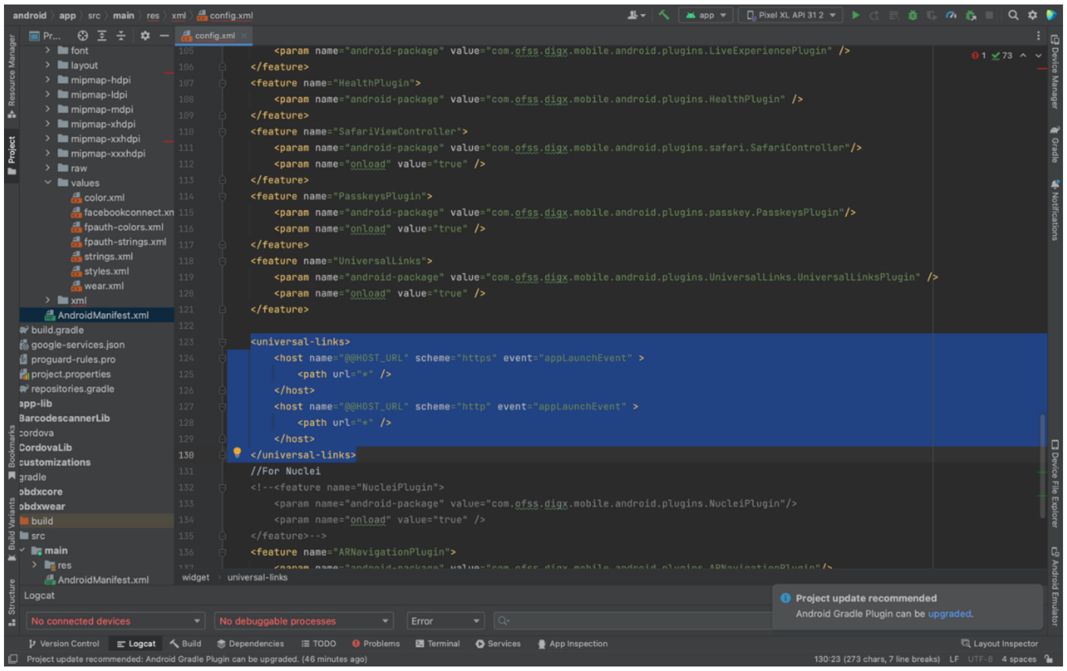


```
        <intent-filter android:label="Futura Bank">
            <action android:name="android.intent.action.MAIN" />
            <category android:name="android.intent.category.LAUNCHER" />
        </intent-filter>

        <intent-filter>
            <action android:name="android.intent.action.VIEW" />
            <category android:name="android.intent.category.DEFAULT"/>
            <category android:name="android.intent.category.BROWSABLE"/>
            <data android:scheme="zigbank" />
            <data
                    android:host="host_url"
                    android:scheme="http" />
            <data
                    android:host="host_url"
                    android:scheme="https" />
        </intent-filter>

    </activity>
    <provider
        android:authorities="${applicationId}.opener.provider"
        android:exported="false"
        android:grantUriPermissions="true"
        android:name="com.ofss.digx.mobile.android.plugins.fileopener2.FileProvider">
        <meta-data android:name="android.support.FILE_PROVIDER_PATHS" android:resource="@xml/opener_paths" />
    </provider>
    <provider android:authorities="${applicationId}.provider"
        android:exported="false"
        android:grantUriPermissions="true"
        android:name="org.apache.cordova.camera.FileProvider">
        <meta-data android:name="android.support.FILE_PROVIDER_PATHS" android:resource="@xml/camera_provider_paths" />
```

Note – Please add host url without https or http.

For e.g. If your deeplink url is https://exmple.com/test then you can add only example.com in the data tag

Similary you can add the same host url in app’s config.xml under universal-links tag as,



```
        <param name="android-package" value="com.ofss.digx.mobile.android.plugins.LiveExperiencePlugin" />
    </feature>
    <feature name="HealthPlugin">
        <param name="android-package" value="com.ofss.digx.mobile.android.plugins.HealthPlugin" />
    </feature>
    <feature name="SafariViewController">
        <param name="android-package" value="com.ofss.digx.mobile.android.plugins.safari.SafariController"/>
        <param name="onload" value="true" />
    </feature>
    <feature name="PasskeysPlugin">
        <param name="android-package" value="com.ofss.digx.mobile.android.plugins.passkey.PasskeysPlugin"/>
        <param name="onload" value="true" />
    </feature>
    <feature name="UniversalLinks">
        <param name="android-package" value="com.ofss.digx.mobile.android.plugins.UniversalLinks.UniversalLinksPlugin" />
        <param name="onload" value="true" />
    </feature>

    <universal-links>
        <host name="@@HOST_URL" scheme="https" event="appLaunchEvent" >
            <path url="*" />
        </host>
        <host name="@@HOST_URL" scheme="http" event="appLaunchEvent" >
            <path url="*" />
        </host>
    </universal-links>
    //For Nuclei
    <!--<feature name="NucleiPlugin">
        <param name="android-package" value="com.ofss.digx.mobile.android.plugins.NucleiPlugin"/>
        <param name="onload" value="true" />
    </feature>-->
    <feature name="ARNavigationPlugin">
```

Project update recommended
Android Gradle Plugin can be upgraded.

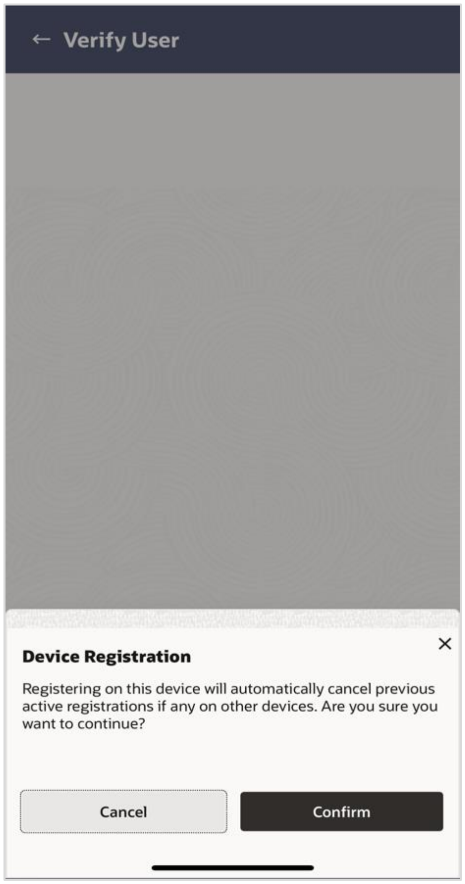
Project update recommended: Android Gradle Plugin can be upgraded. (46 minutes ago)

2.10 Device Registration and Push Registration Functionality

In this version, only one device is allowed to be registered for alternate login for the same username. If user tries to register another device with same username for alternate login, then the previous registration on other devices will be removed. User will get an error message if he/she tries to use PIN/PATTERN/BIOMETRIC on the de-registered devices.

While user registers his second device or same device again (by re-installing the application), a popup will appear to notify the same.

If user confirms, then the current device will be registered, and all previous registrations will be removed.



Device Registration

Registering on this device will automatically cancel previous active registrations if any on other devices. Are you sure you want to continue?

If user cancel, the process is exited.

Also, in this version, only one device is allowed to be registered for push.

Bank can allow multiple devices to be registered for same username in their setup by setting below two configurations:

ALLOWED_DEVICE_COUNT to any value between than 1 and 100.

- 1 will allow on one device registration.
- 100 will allow more than one device registration

ALLOWED_PUSH_DEVICE_COUNT any value between 1 and -1

- 1 will only one one device to be registered for push.
- -1 will only multiple devices to be registered for push

2.11 Location Tracking Metrics

This is optional. Bank needs to do if they need location tracking metrics for monitoring location-based data.
ALLOW_LOCATION_SHARE
By default, the value is false. If set to true, user will get location permission prompt to allow location tracking. It can be enabled if user's location needs to be tracked.

2.12 Displaying Rate Option to Redirect to Playstore Page

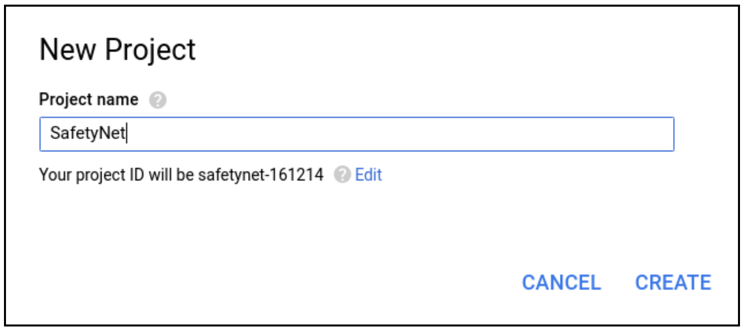
This is optional. User can have an option ("Rate Us") in settings to display Play Store rating for the application. This option can be enabled/disabled from UI.

Note: App should be listed on playstore before adding this functionality.

3. Google Play Integrity

a. Go to URL https://console.developers.google.com/

b. Create a new Project and set name of you project



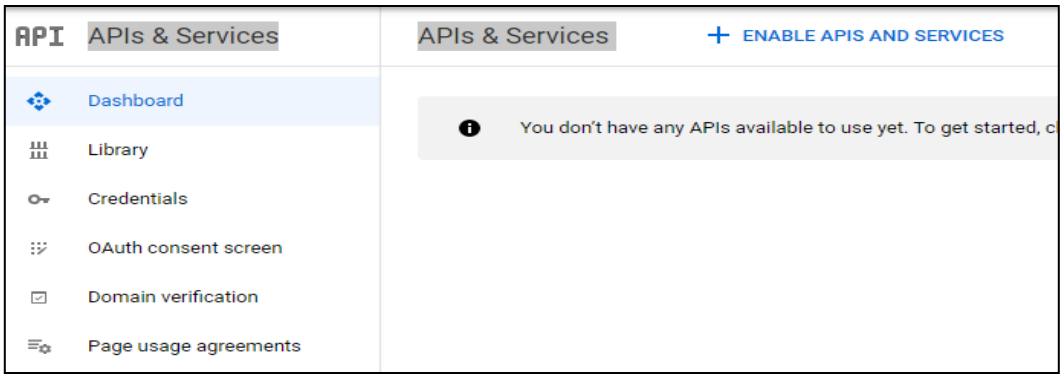
New Project

Project name: SafetyNet

Your project ID will be safetynet-161214 Edit

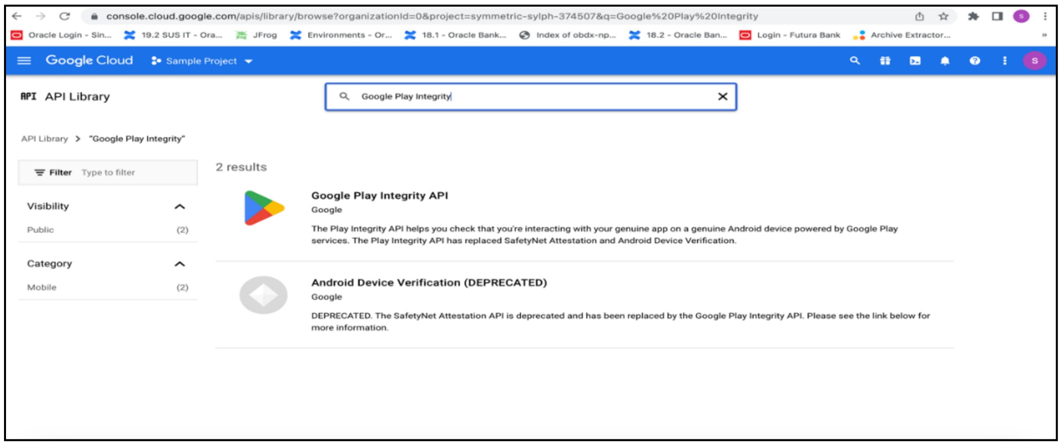
c. Choose **'API's & Services'** option from side bar.

d. In API's & Services > Dashboard > Choose **'Enable APIS AND SERVICES'**.



You don't have any APIs available to use yet. To get started, c

e. This will redirect to **'Library'** where we need to search **'Google Play Integrity API'.**



console.cloud.google.com/apis/library/browse?organizationId=0&project=symmetric-sylph-374507&q=Google%20Play%20Integrity

Google Play Integrity

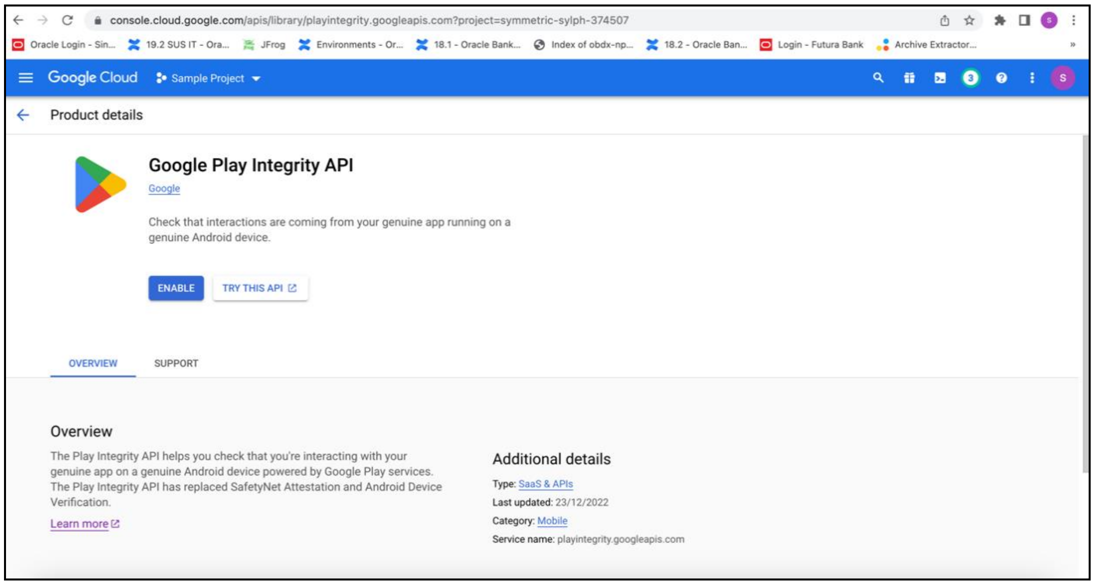
API Library > "Google Play Integrity"

2 results

Google Play Integrity API
Google
The Play Integrity API helps you check that you're interacting with your genuine app on a genuine Android device powered by Google Play services. The Play Integrity API has replaced SafetyNet Attestation and Android Device Verification.

Android Device Verification (DEPRECATED)
Google
DEPRECATED. The SafetyNet Attestation API is deprecated and has been replaced by the Google Play Integrity API. Please see the link below for more information.

f. Click on Google Play Integrity API and enable it



console.cloud.google.com/apis/library/playintegrity.googleapis.com?project=symmetric-sylph-374507

Product details

Google Play Integrity API

Google

Check that interactions are coming from your genuine app running on a genuine Android device.

Overview

The Play Integrity API helps you check that you're interacting with your genuine app on a genuine Android device powered by Google Play services. The Play Integrity API has replaced SafetyNet Attestation and Android Device Verification.

Learn more

Additional details

Type: SaaS & APIs

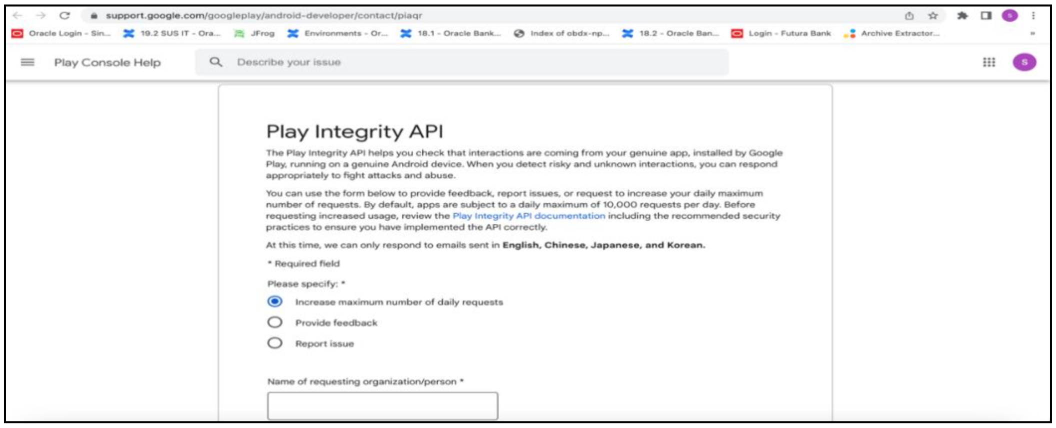
Last updated: 23/12/2022

Category: Mobile

Service name: playintegrity.googleapis.com

g. If the application usage is high, the quota request form needs to be submitted. Please fill quota request form from below site. Also select below options.

https://support.google.com/googleplay/android-developer/contact/piaqr



support.google.com/googleplay/android-developer/contact/piaqr

Play Console Help

Play Integrity API

The Play Integrity API helps you check that interactions are coming from your genuine app, installed by Google Play, running on a genuine Android device. When you detect risky and unknown interactions, you can respond appropriately to fight attacks and abuse.

You can use the form below to provide feedback, report issues, or request to increase your daily maximum number of requests. By default, apps are subject to a daily maximum of 10,000 requests per day. Before requesting increased usage, review the Play Integrity API documentation including the recommended security practices to ensure you have implemented the API correctly.

At this time, we can only respond to emails sent in **English, Chinese, Japanese, and Korean.**

* Required field

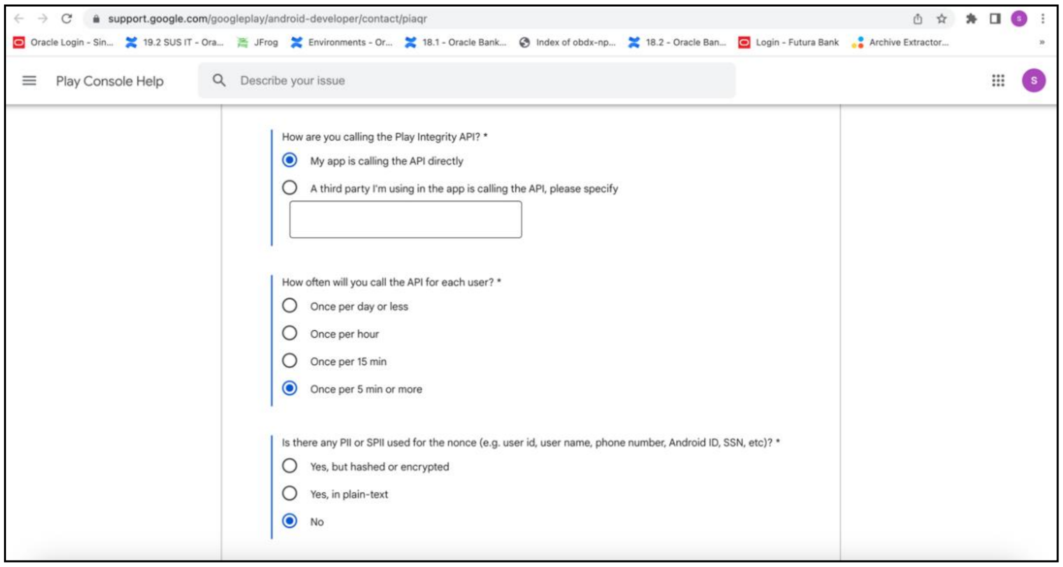
Please specify: *

[✓ Increase maximum number of daily requests]

Provide feedback

Report issue

Name of requesting organization/person *



How are you calling the Play Integrity API? *

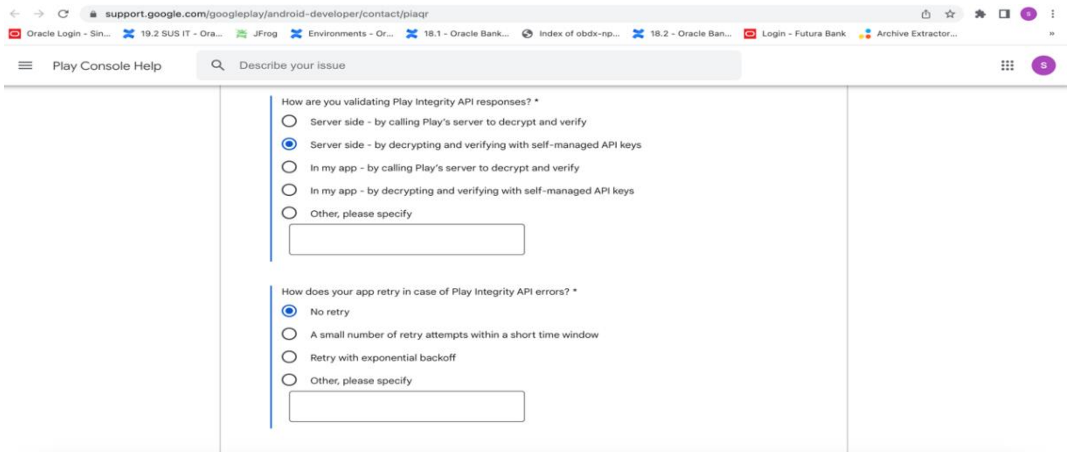
- [✓ My app is calling the API directly]
- A third party I'm using in the app is calling the API, please specify

How often will you call the API for each user? *

- Once per day or less
- Once per hour
- Once per 15 min
- [✓ Once per 5 min or more]

Is there any PII or SPII used for the nonce (e.g. user id, user name, phone number, Android ID, SSN, etc)? *

- Yes, but hashed or encrypted
- Yes, in plain-text
- [✓ No]

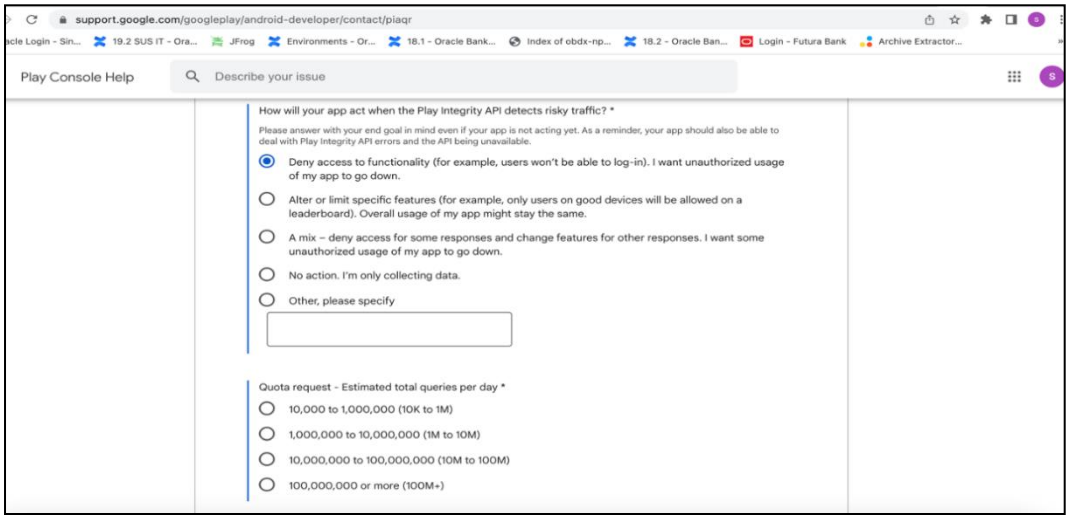


How are you validating Play Integrity API responses? *

- Server side - by calling Play's server to decrypt and verify
- [✓ Server side - by decrypting and verifying with self-managed API keys]
- In my app - by calling Play's server to decrypt and verify
- In my app - by decrypting and verifying with self-managed API keys
- Other, please specify

How does your app retry in case of Play Integrity API errors? *

- [✓ No retry]
- A small number of retry attempts within a short time window
- Retry with exponential backoff
- Other, please specify



How will your app act when the Play Integrity API detects risky traffic? *

Please answer with your end goal in mind even if your app is not acting yet. As a reminder, your app should also be able to deal with Play Integrity API errors and the API being unavailable.

- [✓ Deny access to functionality (for example, users won't be able to log-in). I want unauthorized usage of my app to go down.]
- Alter or limit specific features (for example, only users on good devices will be allowed on a leaderboard). Overall usage of my app might stay the same.
- A mix – deny access for some responses and change features for other responses. I want some unauthorized usage of my app to go down.
- No action. I'm only collecting data.
- Other, please specify

Quota request - Estimated total queries per day *

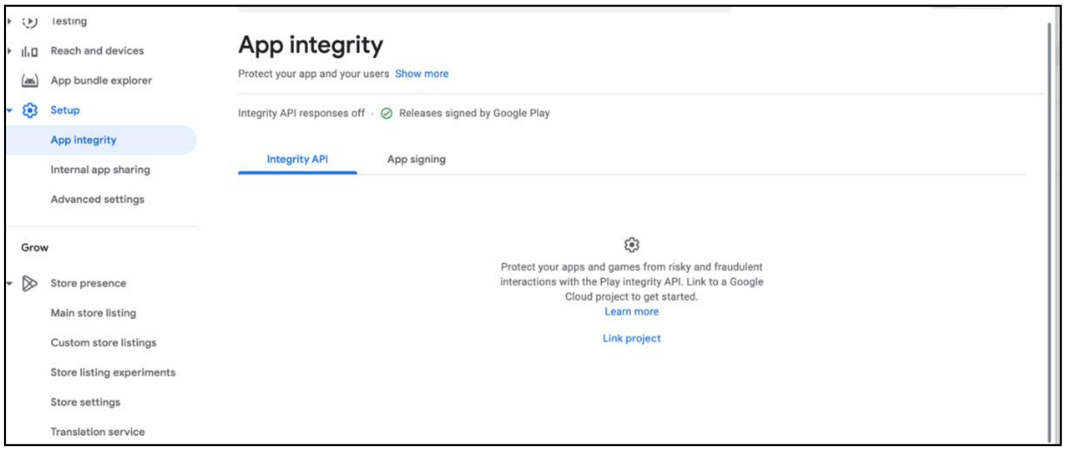
- 10,000 to 1,000,000 (10K to 1M)
- 1,000,000 to 10,000,000 (1M to 10M)
- 10,000,000 to 100,000,000 (10M to 100M)
- 100,000,000 or more (100M+)

Quota request - Estimated total queries per day * → The approximate load, Play Integrity API is called once each time the app in opened

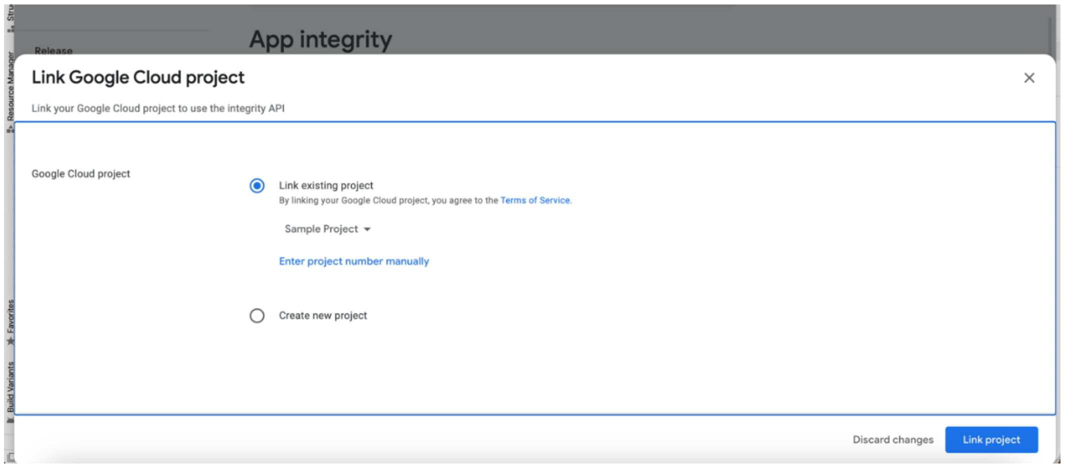
Quota request - Estimated peak queries per second → Leave blank

h. To enable Play Integrity responses please follow below steps-

Go to Google Play Console->Side Menu->Setup->App Integrity


Testing
Reach and devices
App bundle explorer
Setup
App integrity
Internal app sharing
Advanced settings
Grow
Store presence
Main store listing
Custom store listings
Store listing experiments
Store settings
Translation service
App integrity
Protect your app and your users Show more
Integrity API responses off
Releases signed by Google Play
Integrity API
App signing
Protect your apps and games from risky and fraudulent interactions with the Play integrity API. Link to a Google Cloud project to get started.
Learn more
Link project

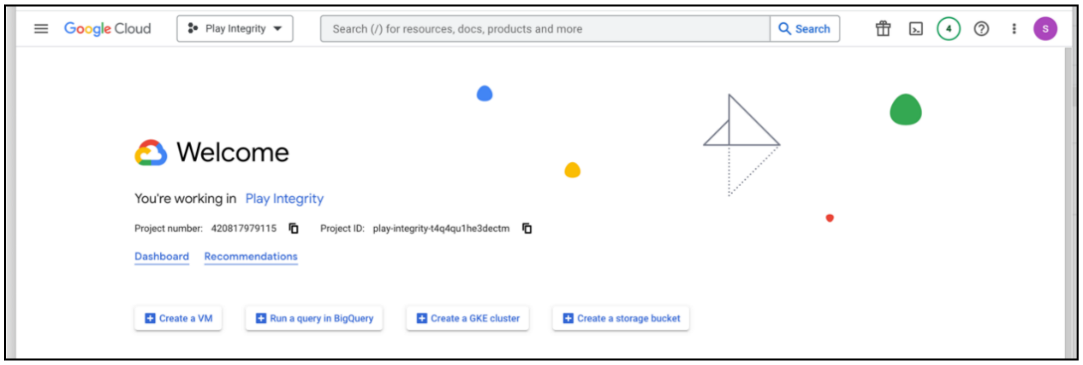
Click on **Link project** and then link your existing google cloud project. If it is not created then create new and link the same.


App integrity
Link Google Cloud project
Link your Google Cloud project to use the integrity API
Google Cloud project
Link existing project
By linking your Google Cloud project, you agree to the Terms of Service.
Sample Project
Enter project number manually
Create new project
Discard changes
Link project

i. Add project number in below property of app.properties

```
<string name="GOOGLE_CLOUD_PROJECT_NO">@@GOOGLE_CLOUD_PROJECT NO</string>
```

You will get the project number on google cloud console project



You're working in Play Integrity

Project number: 420817979115 Project ID: play-integrity-t4q4qu1he3dectm

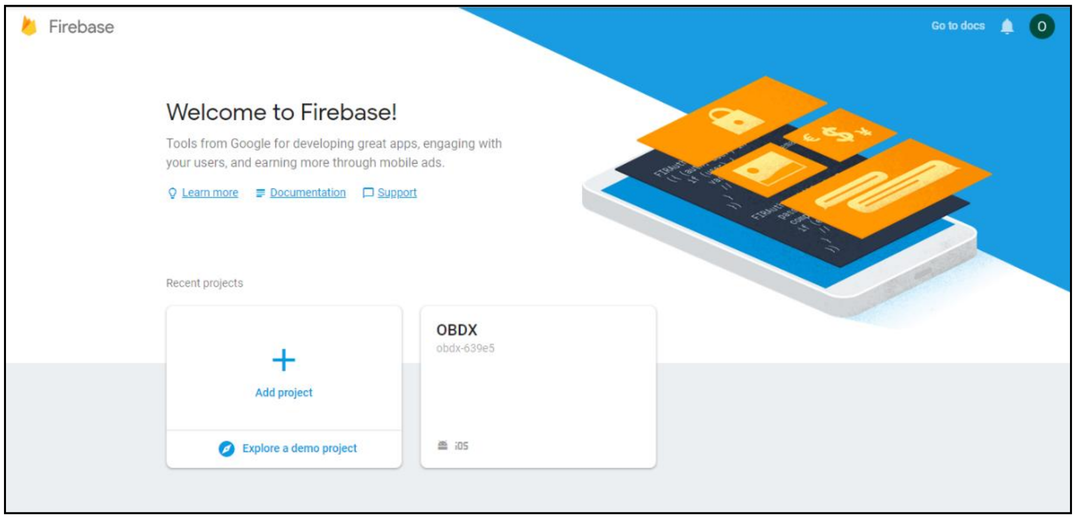
j. Mention the time in seconds to which app can hit the play integrity api. By default it is 300seconds but you can configure as per the requirement. Please use below property in RootCheckFlags.java(workspace_installer/zigbank/platforms/android/app/src/main/java/com/ofss/digx/mobile/android/)

long playIntegrityAPICallTime = your_time_in_seconds;

4. FCM Push Notifications

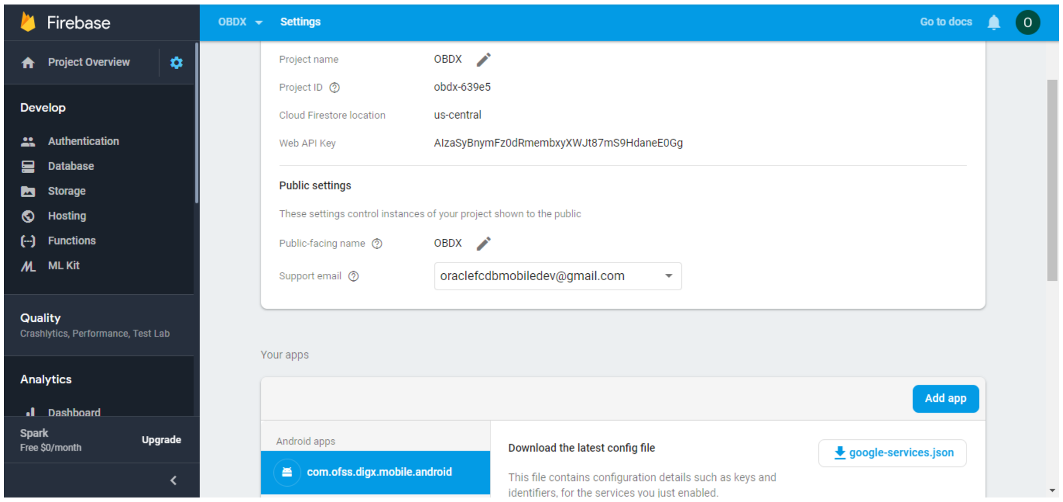
a. Go to URL https://firebase.google.com/

b. Traverse to console and create a project



c. Download google-services.json from below page and save to (zigbank\platforms\android\app) directory.

d. Remember to keep the projects package name and firebase package name same.



Project name	OBDX
Project ID	obdx-639e5
Cloud Firestore location	us-central
Web API Key	AIzaSyBnymFz0dRmembxyXWJt87mS9HdaneE0Gg

Public settings

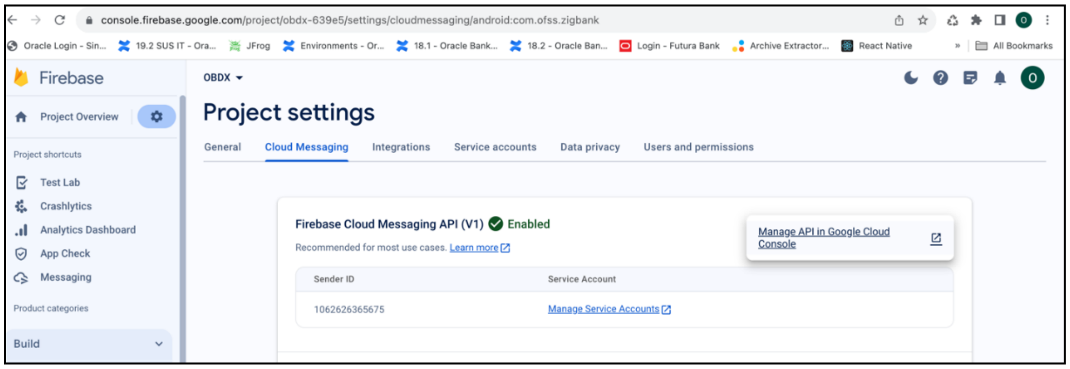
These settings control instances of your project shown to the public

Public-facing name	OBDX
Support email	oraclefcdbmobiledev@gmail.com

Download the latest config file

This file contains configuration details such as keys and identifiers, for the services you just enabled.

e. Traverse to cloud messaging tab Enable Firebase Cloud Messaging API(V1) by clicking on Manage API in Google Cloud Console.



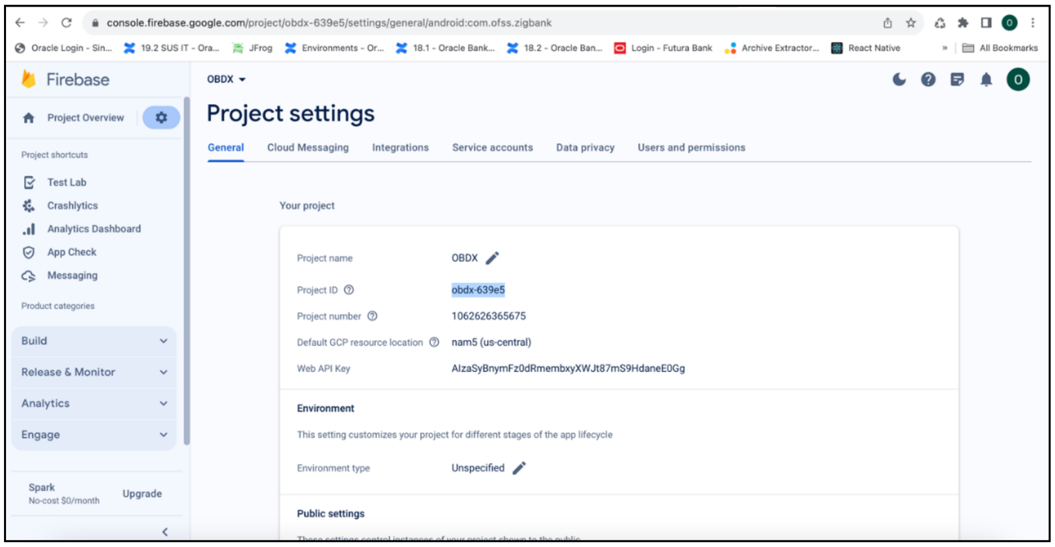
Project settings

Firebase Cloud Messaging API (V1) Enabled

Recommended for most use cases. Learn more

Sender ID	Service Account
1062626365675	Manage Service Accounts

f. Get the Project ID from Project Setting in Firebase console



Project settings

Your project

Project name	OBDX
Project ID	obdx-639e5
Project number	1062626365675
Default GCP resource location	nam5 (us-central)
Web API Key	AIzaSyBnymFz0dRmembxyXWJt87mS9HdaneE0Gg

Environment

This setting customizes your project for different stages of the app lifecycle

Environment type: Unspecified

Public settings

g. Update FCM URL in below table as-

update DIGX_FW_CONFIG_ALL_B set prop_value = 'https://fcm.googleapis.com/v1/projects/YOUR_PROJECT_ID/messages:send' where prop_id = 'FCM_URL';

Add YOUR_PROJECT_ID in url which is captured on above step

h. If proxy address is to be used, provide the same in database as mentioned in point 3.

i. Generate private key for your service account by using below steps-

- In the Firebase console, open **Settings >** Service Accounts

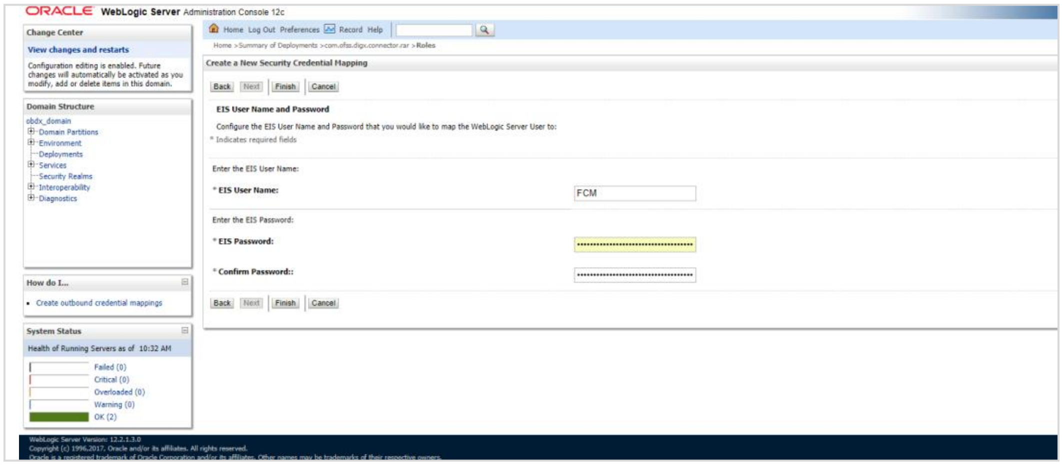
- Click **Generate New Private Key**, then confirm by clicking **Generate Key**

You can also follow below google doc -

https://firebase.google.com/docs/cloud-messaging/auth-server#provide-credentials-manually

Sr. No.	Table	PROP_ID	CATEGORY_ID	PROP_VALUE	Purpose
1	DIGX_FW_CONFIG_VAR_B	FCM	DispatchDetails	<Server_Key>	Service account json file content captured in above step
2	DIGX_FW_CONFIG_ALL_B	FCMKeyStore	DispatchDetails	DATABASE or CONNECTOR	Specifies whether to pick server key from database or from connector. Default DB (No change)
3	DIGX_FW_CONFIG_ALL_B	Proxy	DispatchDetails	<protocol,proxy_address>	Provides proxy address, if any, to be provided while connecting to APNS server. Delete row if proxy not required. Example: HTTP,148.50.60.8

If CONNECTOR is selected in Step 2 update password as below


ORACLE WebLogic Server Administration Console 12c
Home Log Out Preferences Record Help
Back Next Finish Cancel

Change Center

View changes and restarts

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Domain Structure

obdx_domain
- Domain Partitions
- Environment
- Deployments
- Services
- Security Realms
- Interoperability
- Diagnostics

How do I...

- Create outbound credential mappings

System Status

Health of Running Servers as of 10:32 AM

- Failed (0)
- Critical (0)
- Overloaded (0)
- Warning (0)
- OK (2)

Home >Summary of Deployments >com.ofss.digx.connector.rar >Roles

Create a New Security Credential Mapping

EIS User Name and Password

Configure the EIS User Name and Password that you would like to map the WebLogic Server User to:

* Indicates required fields

Enter the EIS User Name:

* EIS User Name: FCM

Enter the EIS Password:

* EIS Password: ••••••••••••••••••••••••••••••••••••

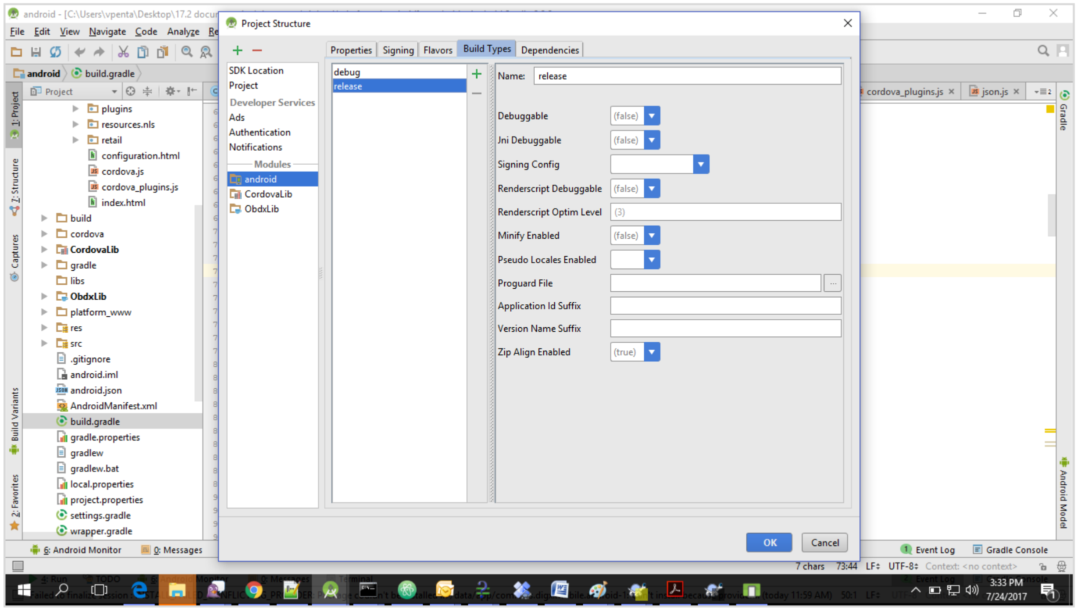
* Confirm Password:: ••••••••••••••••••••••••••••••••••••

WebLogic Server Version: 12.2.1.3.0
Copyright (c) 1996,2017, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Home

5. Build Release Artifacts

1. Clean and Rebuild your project in Android Studio.
2. In Android Studio, on the menu bar Click on **Build -> Edit Build Types ->** select **release**



Project Structure

Properties | Signing | Flavors | Build Types | Dependencies

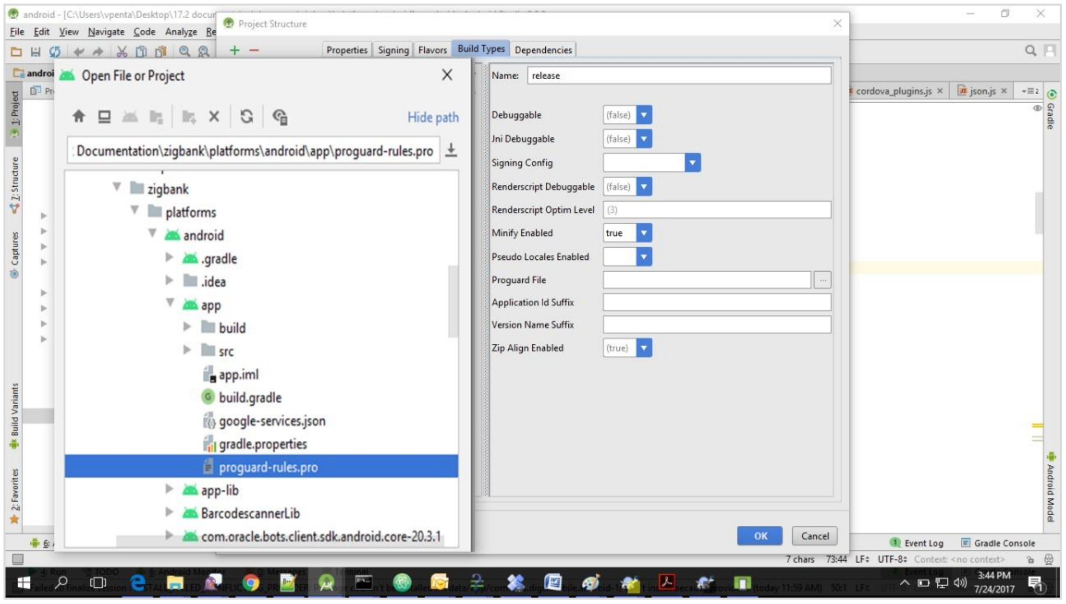
SDK Location
Project
Developer Services
Ads
Authentication
Notifications
Modules
android
CordovaLib
ObdxLib

debug
release

Name:	release
Debuggable	(false)
Jni Debuggable	(false)
Signing Config	
Renderscript Debuggable	(false)
Renderscript Optim Level	(3)
Minify Enabled	(false)
Pseudo Locales Enabled	
Proguard File	
Application Id Suffix	
Version Name Suffix	
Zip Align Enabled	(true)

OK Cancel

3. Set Minify Enabled -> True & click on Proguard File selection -> Navigate to proguard-rules.pro (zigbank\platforms\android\app)



Open File or Project

Hide path

Documentation\zigbank\platforms\android\app\proguard-rules.pro

```
zigbank
  platforms
    android
      .gradle
      .idea
      app
        build
        src
        app.iml
        build.gradle
        google-services.json
        gradle.properties
        proguard-rules.pro
      app-lib
      BarcodescannerLib
      com.oracle.bots.client.sdk.android.core-20.3.1
```

Name:	release
Debuggable	(false)
Jni Debuggable	(false)
Signing Config	
Renderscript Debuggable	(false)
Renderscript Optim Level	(3)
Minify Enabled	true
Pseudo Locales Enabled	
Proguard File	
Application Id Suffix	
Version Name Suffix	
Zip Align Enabled	(true)

OK Cancel

4. Click on OK -> again click on OK.
5. Adding URLs to app.properties.xml (customizations/src/main/res/values/)
   a. NONOAM (DB Authenticator setup)

SERVER_TYPE	**NONOAM**
KEY_SERVER_URL	Eg. https://mumaa012.in.oracle.com:18443
WEB_URL	Eg. https://mumaa012.in.oracle.com:18443
SERVER_CERTIFICATE_KEY	Refer point 6.7

   b. OBDXTOKEN (Token based mechanism)

SERVER_TYPE	**OBDXTOKEN**
KEY_SERVER_URL	Eg. https://mumaa012.in.oracle.com:18443
WEB_URL	Eg. https://mumaa012.in.oracle.com:18443
SERVER_CERTIFICATE_KEY	Refer point 6.7

   c. OAM Setup (Refer to installer pre requisite documents for OAuth configurations)

SERVER_TYPE	**OAM**
KEY_SERVER_URL	Eg. https://mumaa012.in.oracle.com:18443 (This URL must be of OHS without webgate)
WEB_URL	Eg. https://mumaa012.in.oracle.com:18443
KEY_OAUTH_PROVIDER_URL	http://mum00aon.in.oracle.com:14100/oauth2/rest/token
APP_CLIENT_ID	<Base64 of clientid:secret> of Mobile App client
APP_DOMAIN	OBDXMobileAppDomain
WATCH_CLIENT_ID	<Base64 of clientid:secret> of wearables
WATCH_DOMAIN	OBDXWearDomain
SNAPSHOT_CLIENT_ID	<Base64 of clientid:secret> of snapshot
SNAPSHOT_DOMAIN	OBDXSnapshotDomain
LOGIN_SCOPE	OBDXMobileAppResServer.OBDXLoginScope
SERVER_CERTIFICATE_KEY	Refer point 6.7

d. IDCS Setup

SERVER_TYPE	**IDCS**
KEY_SERVER_URL	Eg. https://mumaa012.in.oracle.com:18443 (This URL must be of OHS without webgate)
WEB_URL	Eg. https://mumaa012.in.oracle.com:18443
KEY_OAUTH_PROVIDER_URL	http://obdx-tenant01.identity.c9dev0.oc9qadev.com/oauth2/v1/token
APP_CLIENT_ID	<Base64 of clientid:secret> of Mobile App client
WATCH_CLIENT_ID	<Base64 of clientid:secret> of wearables
SNAPSHOT_CLIENT_ID	<Base64 of clientid:secret> of snapshot
LOGIN_SCOPE	obdxLoginScope
OFFLINE_SCOPE	urn:opc:idm:__myscopes__ offline_access
SERVER_CERTIFICATE_KEY	Refer point 6.7

6. Domain Based Setup (This is same for OBDX servicing App and Authenticator App)

   To use domain based setup please enable below flag in app.properties file -

   <string name="DOMAIN_BASED_CATEGORIZATION">true</string>

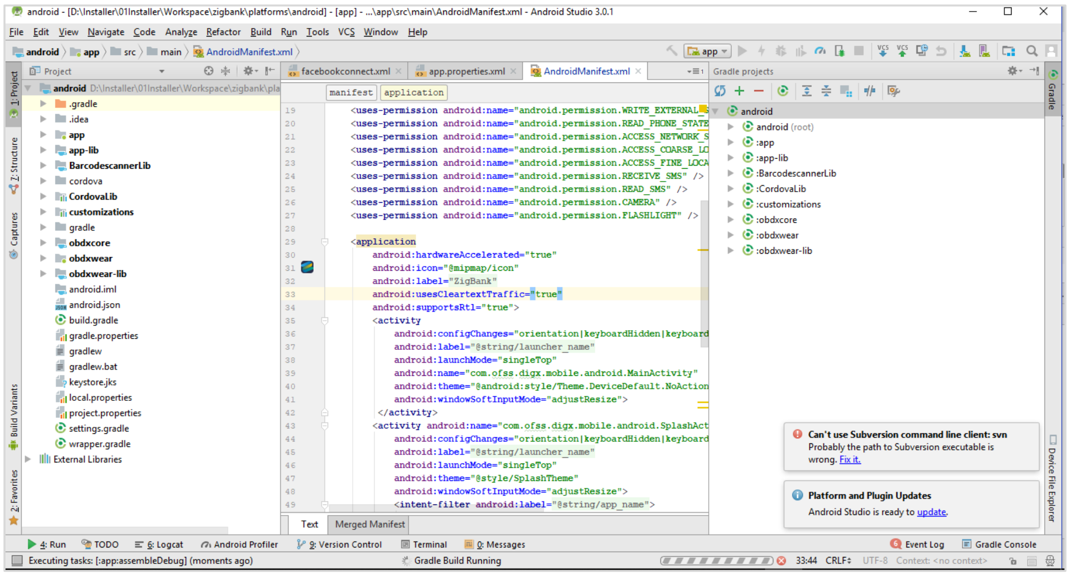
   If you are using local UI then enable below flag in config.js(platforms/android/app/src/main/assets/www/framework/js/configurations/config.js) file -

   ```
   domainDeployment: {
     enabled: true
   }
   ```

7. Adding chatbot support to mobile application (Optional)

CHATBOT_ID	The tenant ID
CHATBOT_URL	The URL for the ChatApp application in ODA

8. If using http protocol for development add (android:usesCleartextTraffic="true") to application tag of AndroidManifest.xml (on app & obdxwear target)



android - [D:\Installer\01Installer\Workspace\zigbank\platforms\android] - [app] - ...\app\src\main\AndroidManifest.xml - Android Studio 3.0.1

```
<uses-permission android:name="android.permission.WRITE_EXTERNAL_
<uses-permission android:name="android.permission.READ_PHONE_STATE
<uses-permission android:name="android.permission.ACCESS_NETWORK_S
<uses-permission android:name="android.permission.ACCESS_COARSE_LO
<uses-permission android:name="android.permission.ACCESS_FINE_LOCA
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.CAMERA" />
<uses-permission android:name="android.permission.FLASHLIGHT" />

<application
    android:hardwareAccelerated="true"
    android:icon="@mipmap/icon"
    android:label="ZigBank"
    android:usesCleartextTraffic="true"
    android:supportsRtl="true">
    <activity
        android:configChanges="orientation|keyboardHidden|keyboard
        android:label="@string/launcher_name"
        android:launchMode="singleTop"
        android:name="com.ofss.digx.mobile.android.MainActivity"
        android:theme="@android:style/Theme.DeviceDefault.NoAction
        android:windowSoftInputMode="adjustResize">
     </activity>
    <activity android:name="com.ofss.digx.mobile.android.SplashAct
        android:configChanges="orientation|keyboardHidden|keyboard
        android:label="@string/launcher_name"
        android:launchMode="singleTop"
        android:theme="@style/SplashTheme"
        android:windowSoftInputMode="adjustResize">
        <intent-filter android:label="@string/app_name">
```

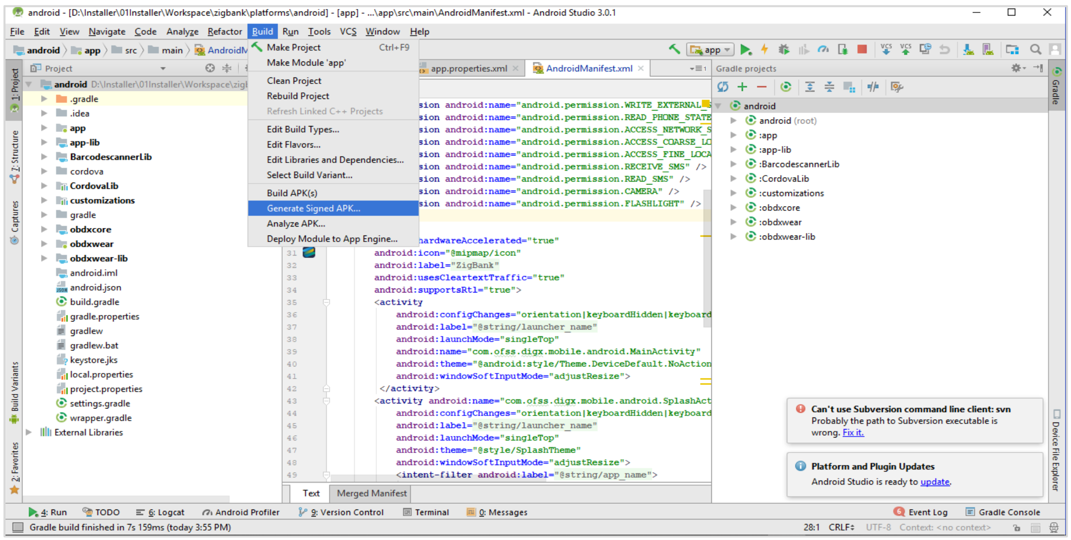
Can't use Subversion command line client: svn
Probably the path to Subversion executable is wrong. Fix it.

Platform and Plugin Updates
Android Studio is ready to update.

Executing tasks: [:app:assembleDebug] (moments ago)   Gradle Build Running

9. **For Generating Signed Apk:** To Generate release-signed apk as follows:

On menu bar click on Build -> Generate Signed Apk



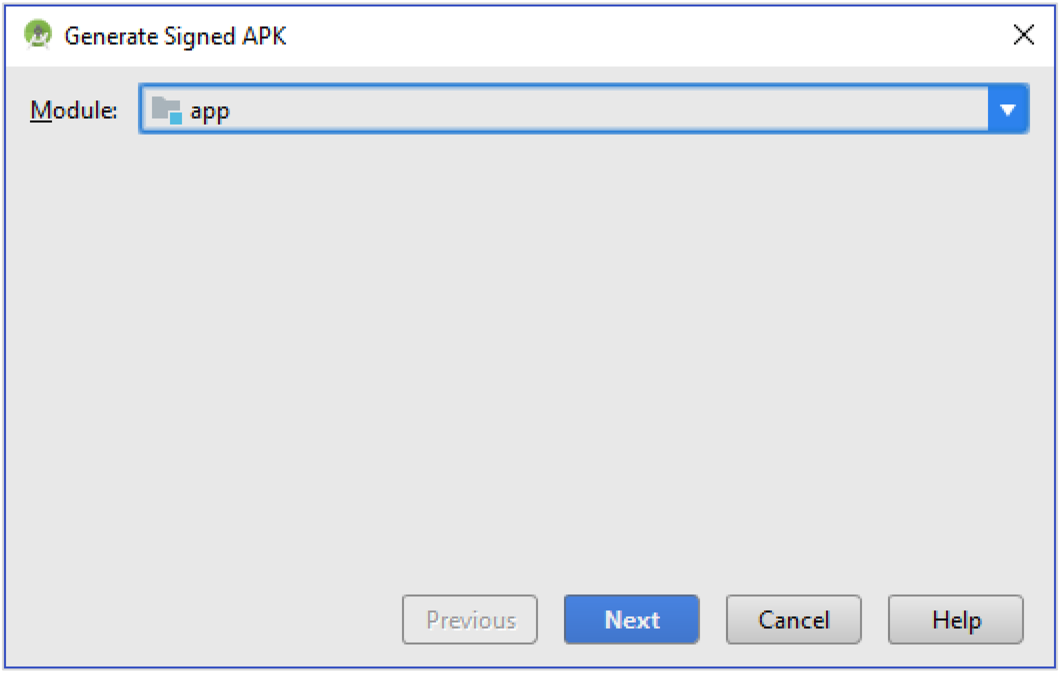
android - [D:\Installer\01Installer\Workspace\zigbank\platforms\android] - [app] - ...\app\src\main\AndroidManifest.xml - Android Studio 3.0.1

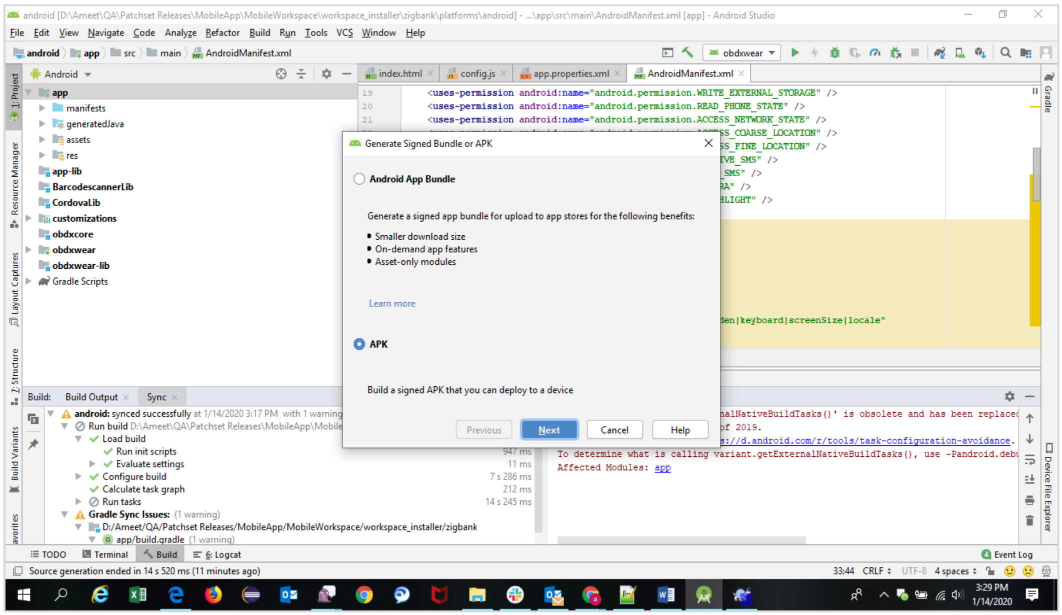
```
sion android:name="android.permission.WRITE_EXTERNAL_
sion android:name="android.permission.READ_PHONE_STATE
sion android:name="android.permission.ACCESS_NETWORK_S
sion android:name="android.permission.ACCESS_COARSE_LO
sion android:name="android.permission.ACCESS_FINE_LOCA
sion android:name="android.permission.RECEIVE_SMS" />
sion android:name="android.permission.READ_SMS" />
sion android:name="android.permission.CAMERA" />
sion android:name="android.permission.FLASHLIGHT" />

hardwareAccelerated="true"
    android:icon="@mipmap/icon"
    android:label="ZigBank"
    android:usesCleartextTraffic="true"
    android:supportsRtl="true">
    <activity
        android:configChanges="orientation|keyboardHidden|keyboard
        android:label="@string/launcher_name"
        android:launchMode="singleTop"
        android:name="com.ofss.digx.mobile.android.MainActivity"
        android:theme="@android:style/Theme.DeviceDefault.NoAction
        android:windowSoftInputMode="adjustResize">
     </activity>
    <activity android:name="com.ofss.digx.mobile.android.SplashAct
        android:configChanges="orientation|keyboardHidden|keyboard
        android:label="@string/launcher_name"
        android:launchMode="singleTop"
        android:theme="@style/SplashTheme"
        android:windowSoftInputMode="adjustResize">
        <intent-filter android:label="@string/app_name">
```

Can't use Subversion command line client: svn
Probably the path to Subversion executable is wrong. Fix it.

Platform and Plugin Updates
Android Studio is ready to update.

Gradle build finished in 7s 159ms (today 3:55 PM)





Android App Bundle

Generate a signed app bundle for upload to app stores for the following benefits:

- Smaller download size
- On-demand app features
- Asset-only modules

Learn more

[✓ APK]

Build a signed APK that you can deploy to a device

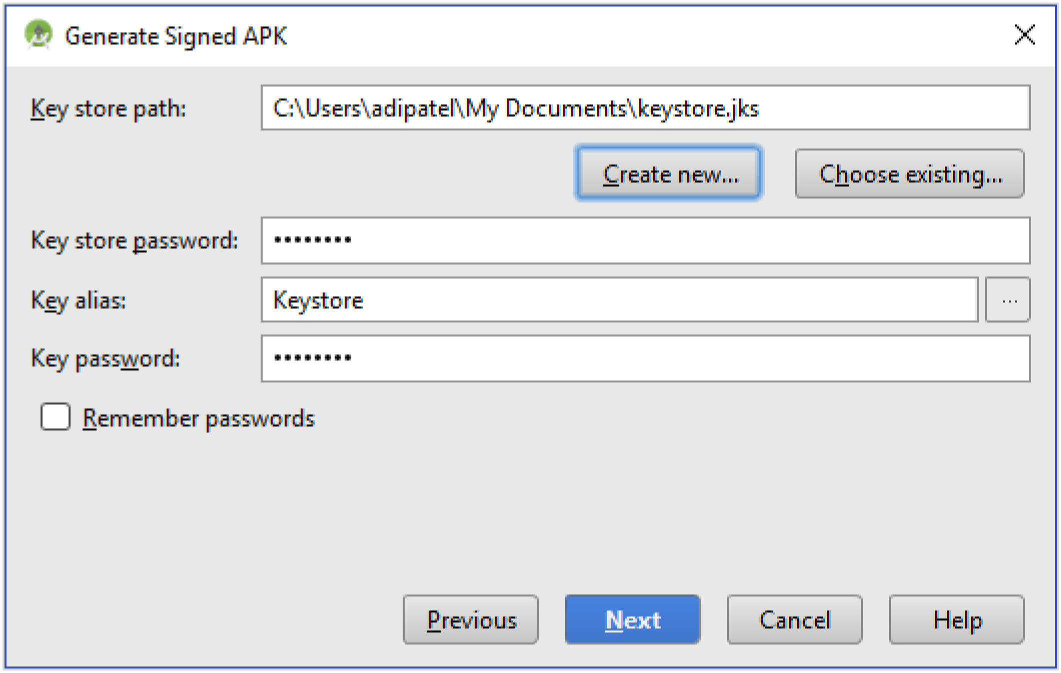
```
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
```

```
android: synced successfully at 1/14/2020 3:17 PM with 1 warning
  Run build D:\Ameet\QA\Patchset Releases\MobileApp\Mobile
    Load build
      Run init scripts                                    947 ms
      Evaluate settings                                    11 ms
    Configure build                                  7 s 286 ms
    Calculate task graph                                  212 ms
    Run tasks                                       14 s 245 ms
  Gradle Sync Issues: (1 warning)
    D:/Ameet/QA/Patchset Releases/MobileApp/MobileWorkspace/workspace_installer/zigbank
      app/build.gradle (1 warning)
```

```
To determine what is calling variant.getExternalNativeBuildTasks(), use -Pandroid.debu
Affected Modules: app
```

Source generation ended in 14 s 520 ms (11 minutes ago)

10. If you have an existing keystore.jks file then select choose Existing else click on Create New



Generate Signed APK

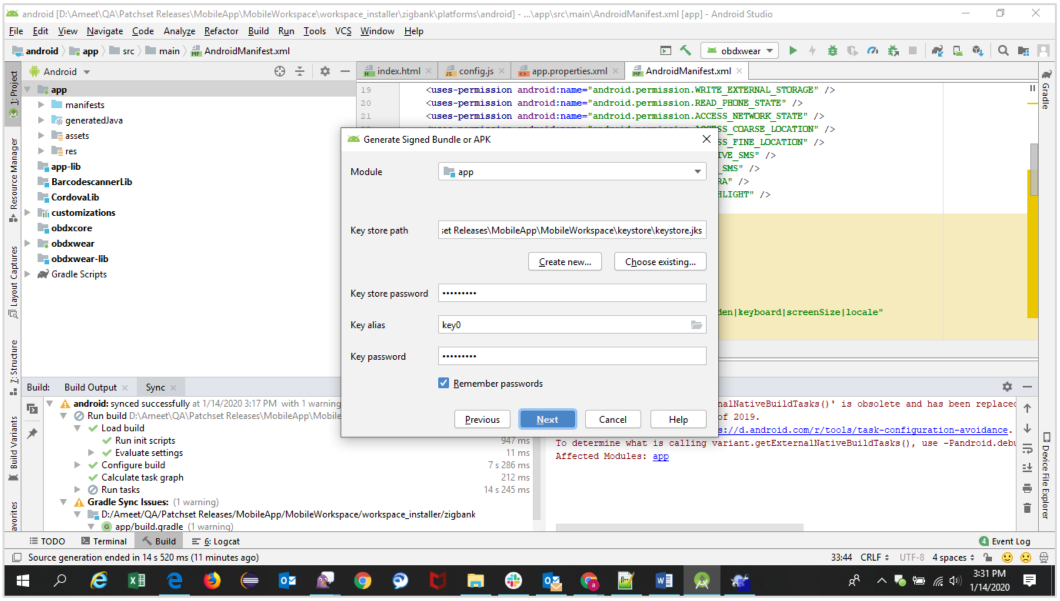
Key store path: C:\Users\adipatel\My Documents\keystore.jks

Key store password: ••••••••

Key alias: Keystore

Key password: ••••••••

[ ] Remember passwords



android [D:\Ameet\QA\Patchset Releases\MobileApp\MobileWorkspace\workspace_installer\zigbank\platforms\android] - ...\app\src\main\AndroidManifest.xml [app] - Android Studio

```
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
```

Generate Signed Bundle or APK

Module: app

Key store path: ;et Releases\MobileApp\MobileWorkspace\keystore\keystore.jks

Key store password: •••••••••

Key alias: key0

Key password: •••••••••

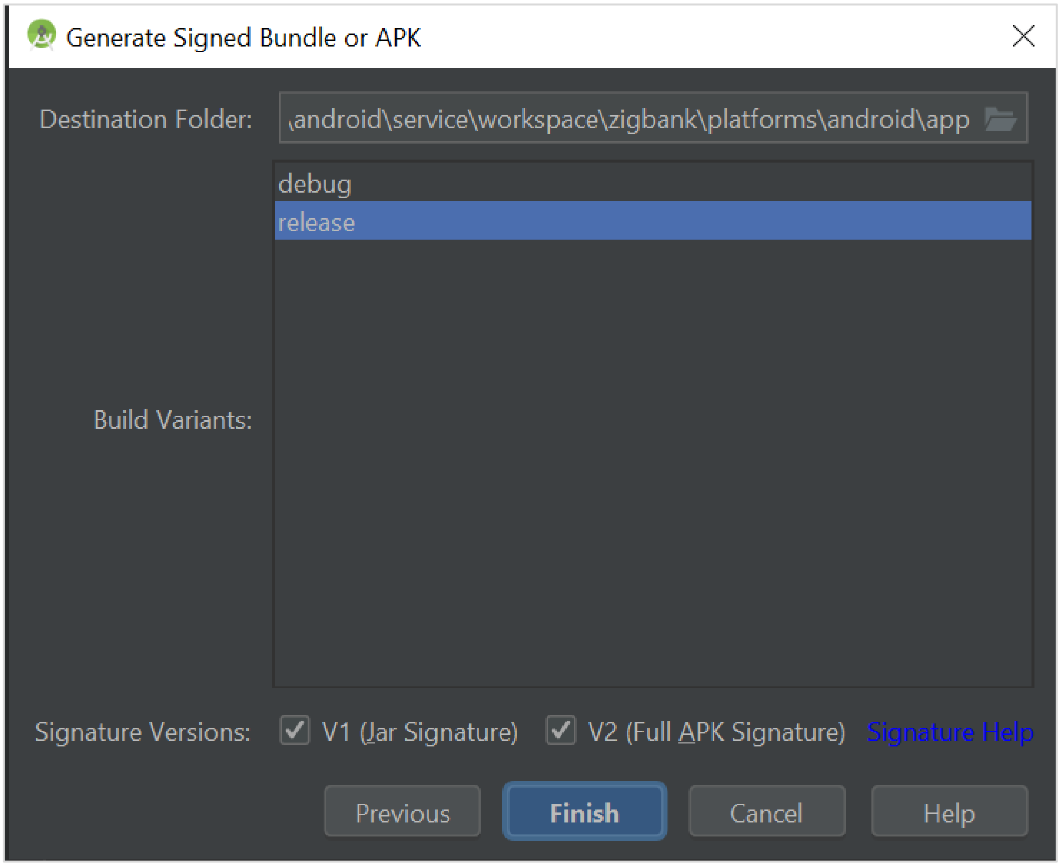
[✓] Remember passwords

```
android: synced successfully at 1/14/2020 3:17 PM with 1 warning
  Run build D:\Ameet\QA\Patchset Releases\MobileApp\Mobile
    Load build
      Run init scripts                         947 ms
      Evaluate settings                         11 ms
    Configure build                        7 s 286 ms
    Calculate task graph                       212 ms
    Run tasks                             14 s 245 ms
  Gradle Sync Issues: (1 warning)
    D:/Ameet/QA/Patchset Releases/MobileApp/MobileWorkspace/workspace_installer/zigbank
      app/build.gradle (1 warning)
```

```
nalNativeBuildTasks()' is obsolete and has been replaced
of 2019.
s://d.android.com/r/tools/task-configuration-avoidance.
To determine what is calling variant.getExternalNativeBuildTasks(), use -Pandroid.debu
Affected Modules: app
```

Source generation ended in 14 s 520 ms (11 minutes ago)

11. Select **Build Type** as **Release**, **Signature Version as V1(JAR Signature) and V2(Full APK Signature)** and Change APK Destination folder if you want and click on Finish



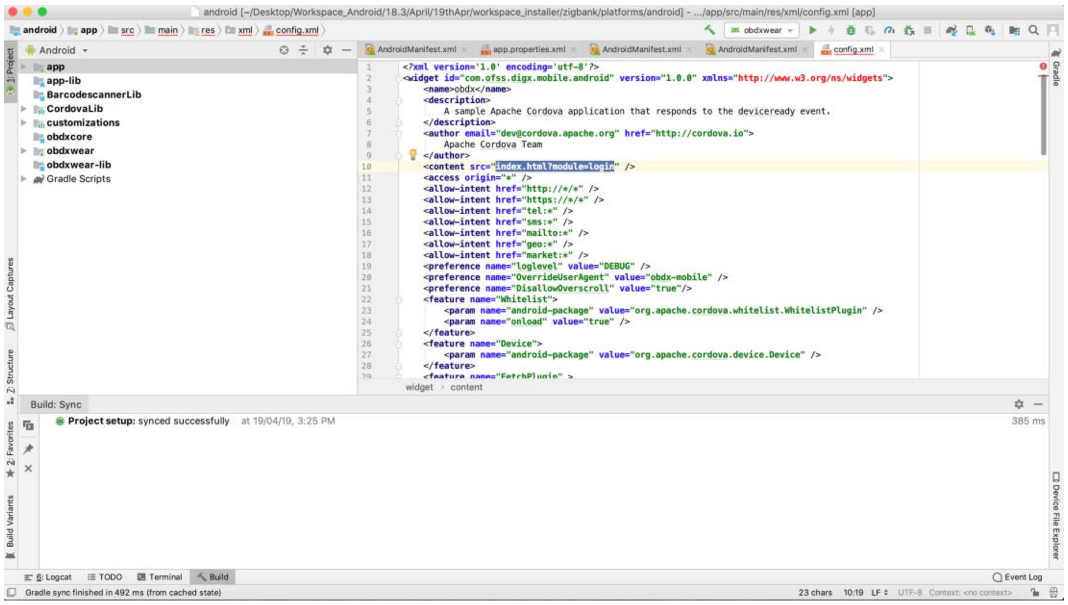
Destination Folder: \android\service\workspace\zigbank\platforms\android\app

Build Variants: debug, release (selected)

Signature Versions: ✓ V1 (Jar Signature) ✓ V2 (Full APK Signature)

12. This will generate APK by the given name and destination folder. Default APK Destination folder is **zigbank\platforms\android\app\release**
13. Run the App and select Device or Simulator.
14. **Repeat same steps (From step 8 and obdxwear as module) for OBDX Wear App for Release Signing.** Use proguard-rules.pro from **workspace_installer\zigbank\platforms\android\obdxwear** using explorer. The select obdxwear as the module and follow same signing steps with same keystore.
15. The application has a config page at launch to enter the URL of the server (for development only). To remove this page, update the config.xml as shown below

The application has config page to add URL. This is for development purpose only and can be removed using below step. (Update content src tag)



```
<?xml version='1.0' encoding='utf-8'?>
<widget id="com.ofss.digx.mobile.android" version="1.0.0" xmlns="http://www.w3.org/ns/widgets">
    <name>obdx</name>
    <description>
        A sample Apache Cordova application that responds to the deviceready event.
    </description>
    <author email="dev@cordova.apache.org" href="http://cordova.io">
        Apache Cordova Team
    </author>
    <content src="index.html?module=login" />
    <access origin="*" />
    <allow-intent href="http://*/*" />
    <allow-intent href="https://*/*" />
    <allow-intent href="tel:*" />
    <allow-intent href="sms:*" />
    <allow-intent href="mailto:*" />
    <allow-intent href="geo:*" />
    <allow-intent href="market:*" />
    <preference name="loglevel" value="DEBUG" />
    <preference name="OverrideUserAgent" value="obdx-mobile" />
    <preference name="DisallowOverscroll" value="true"/>
    <feature name="Whitelist">
        <param name="android-package" value="org.apache.cordova.whitelist.WhitelistPlugin" />
        <param name="onload" value="true" />
    </feature>
    <feature name="Device">
        <param name="android-package" value="org.apache.cordova.device.Device" />
    </feature>
```

Project setup: synced successfully at 19/04/19, 3:25 PM 385 ms

Gradle sync finished in 492 ms (from cached state)

16. Application will work on https only. If you want to run application on http then set targetSdkVersion, compileSdkVersion to 30 and buildToolsVersion to 30.0.3 in app's build.gradle(zigbank\platforms\android\app\) and remove remove below code from obdx.conf(config/obdx.conf).

```
<IfModule mod_headers.c>

    <If "%{HTTP_USER_AGENT} =~ /obdx-mobile-android/">

        Header edit Set-Cookie ^(.*)$ $1;SameSite=None;Secure

    </If>

    <If "%{HTTP_USER_AGENT} =~ /obdx-softtoken/">

        Header edit Set-Cookie ^(.*)$ $1;SameSite=None;Secure

    </If>

</IfModule>
```

17. To enable App Widget, please enable below flag in app.properties file:

```
<bool name="ENABLE_WIDGET">true</bool>
```

18. Disable below flag to reset the Biometric Alternate login on Add/Remove Fingerprint from mobile.

```
<bool name="ALLOW_FACE_BIOMETRIC">false</bool>
```

Note – This reset feature will support only if above flag is false.

19. Maintenance page configs-

Enable below flag to show maintenance page when server is under maintenance

```
<string name="SHOW_MAINTENANCE_PAGE">true</string>
```

Also add the status code returned when server is under main in below property-

```
<string-array name="MAINTENANCE_PAGE_STATUS_CODE">
  <item>Your Status Code</item>
</string-array>
```

Note- You can add multiple status code

20. To disable caching in app, make below flag to flase

```
<bool name="ENABLE_CACHING">true</bool>
```

6. OBDX Authenticator Application

1. This is an Authenticator Application which is used when bank has enabled Soft Token Authentication as Authentication mechanism for any transaction. This application basically supports one of below authentication:
   - HOTP: Random based Soft Token
   - TOTP: Time based Soft Token

2. Users should have this application installed and logged in and PIN is set before initiating any transaction which needs this token.
3. Based on the configuration set, user can any time log in with PIN and check the token and use that token for completing any transaction based on “Soft Token Authentication”

6.1 Authenticator UI (Follow any one step below)

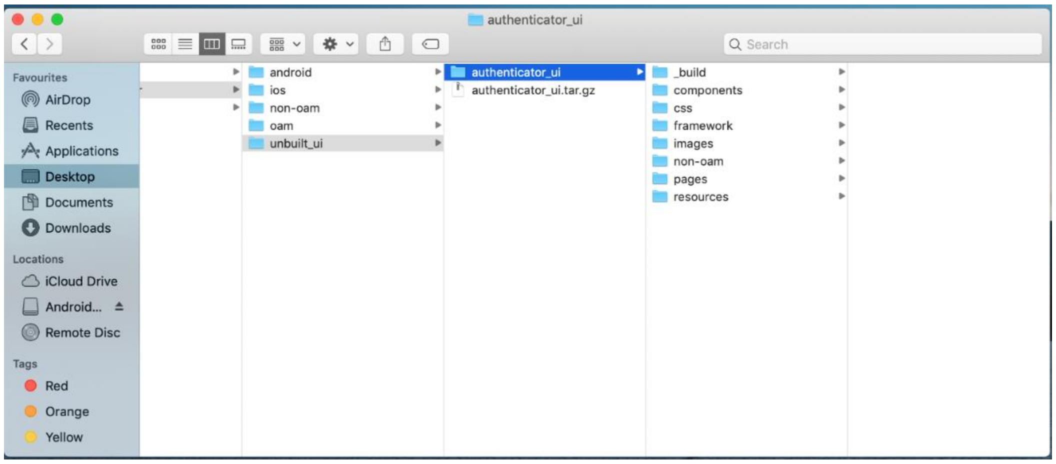
6.1.1 Using built UI

For TOKEN-BASED - Unzip dist.tar.gz directory fromOBDX_Patch_Mobile\authenticator\TOKEN-BASED

6.1.2 Building UI manually

Extract authenticator_ui.tar.gz from OBDX_Patch_Mobile\authenticator\unbuilt_ui.

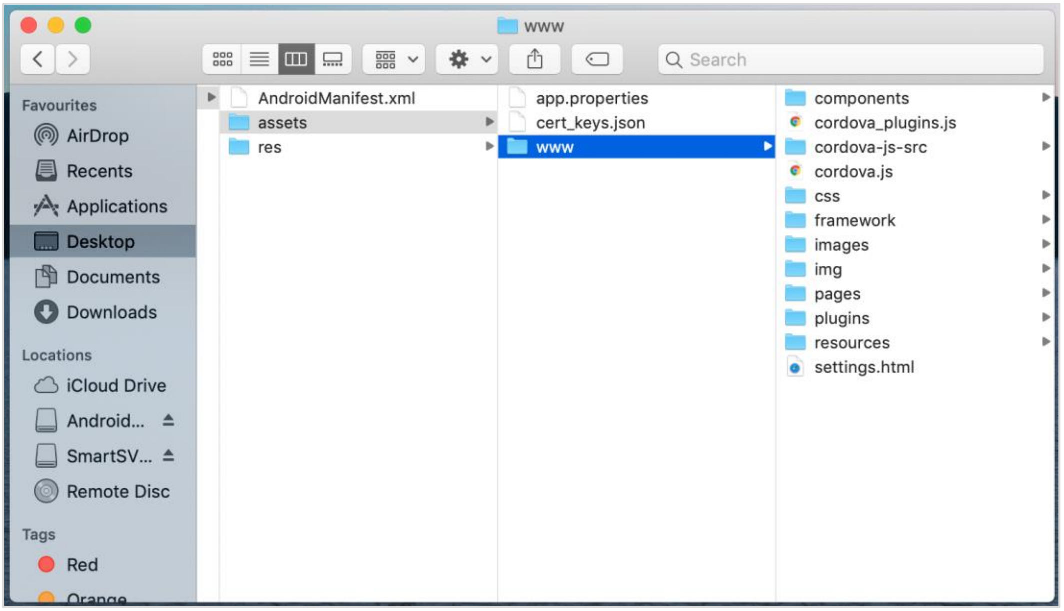
The folder structure is as shown:



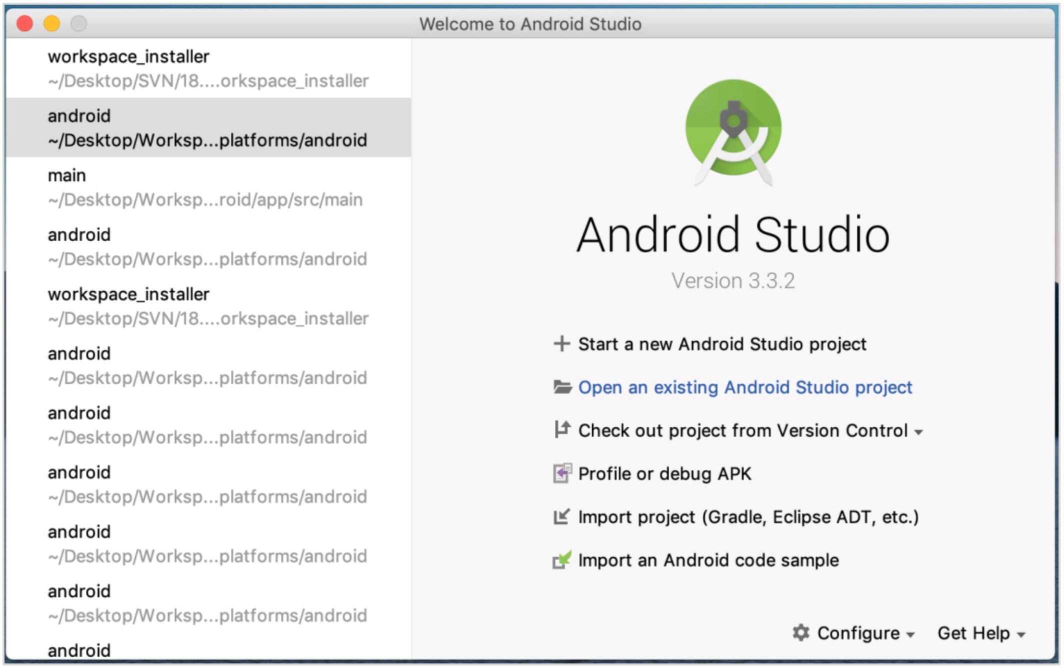
6.2 Authenticator Application Workspace Setup

1. Copy UI (Directories – components, css, framework, images, pages, resources)from /dist directory to workspace/installer/app/src/main/assets/www/

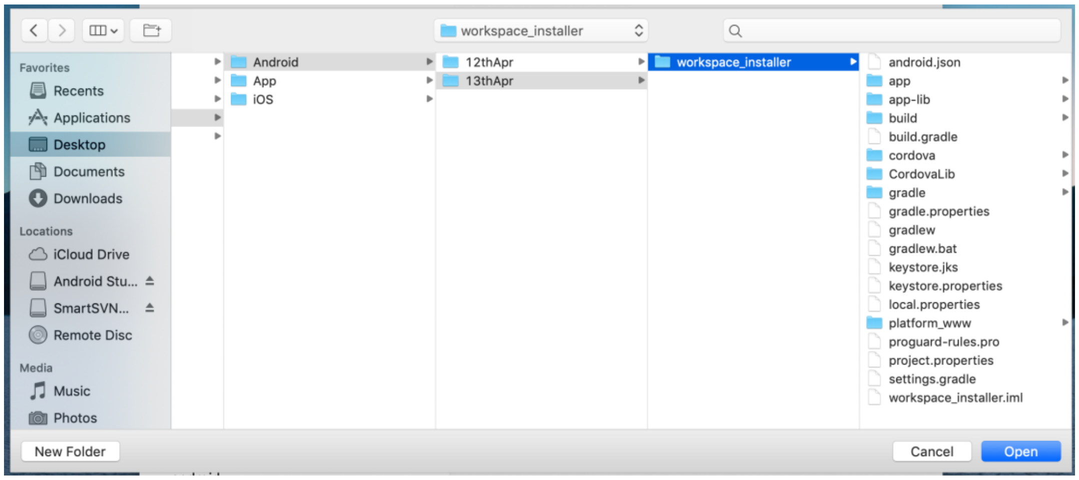
   In case any popup appears, click replace



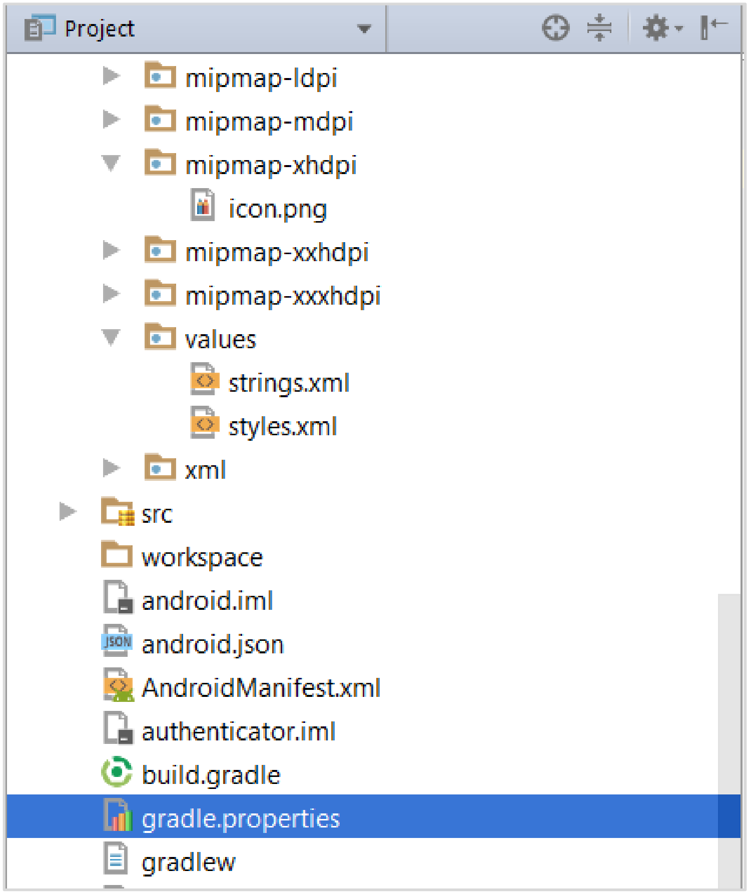
2. Launch Android Studio and open existing project


Welcome to Android Studio
workspace_installer
~/Desktop/SVN/18....orkspace_installer
android
~/Desktop/Worksp...platforms/android
main
~/Desktop/Worksp...roid/app/src/main
android
~/Desktop/Worksp...platforms/android
workspace_installer
~/Desktop/SVN/18....orkspace_installer
android
~/Desktop/Worksp...platforms/android
android
~/Desktop/Worksp...platforms/android
android
~/Desktop/Worksp...platforms/android
android
~/Desktop/Worksp...platforms/android
android
~/Desktop/Worksp...platforms/android
android
Android Studio
Version 3.3.2
Start a new Android Studio project
Open an existing Android Studio project
Check out project from Version Control
Profile or debug APK
Import project (Gradle, Eclipse ADT, etc.)
Import an Android code sample
Configure
Get Help

3. Open OBDX_Installer/workspace_installer folder in Android Studio.

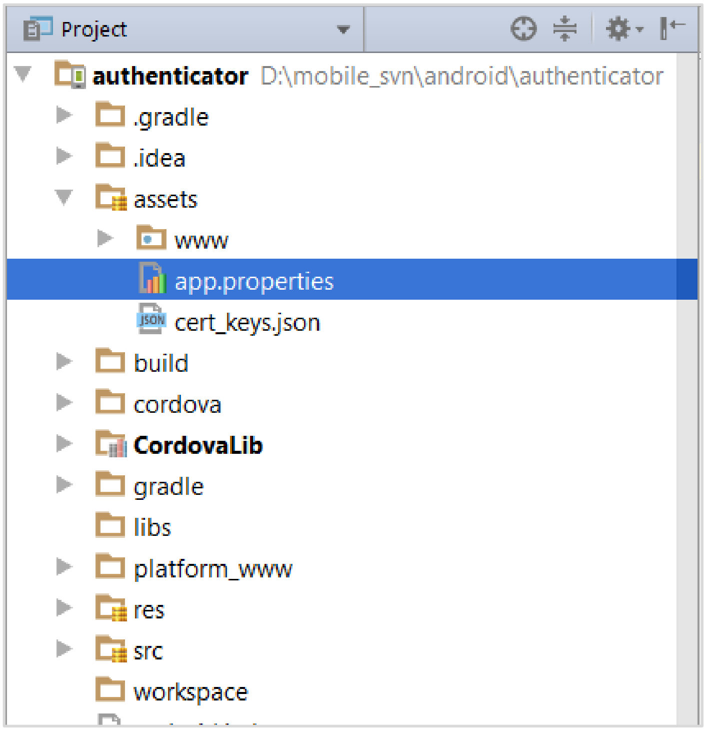


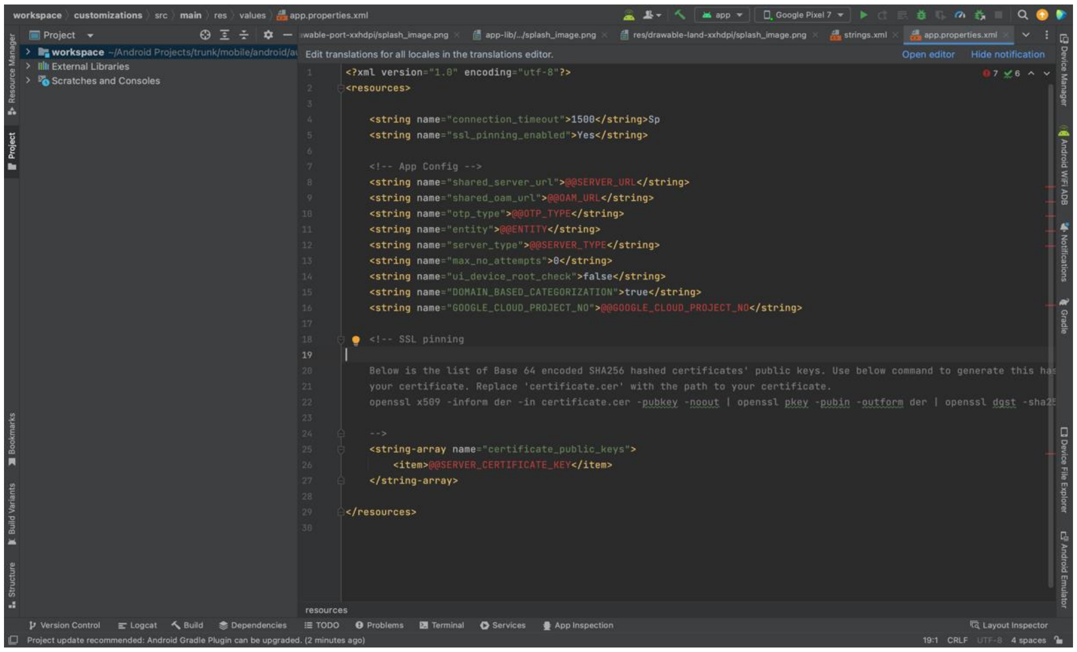
4. Open gradle.properties file and update following properties with relevant proxy address if required



```
systemProp.http.proxyHost = <proxy_address>

systemProp.https.proxyPort = <port_number>
```

5. Open "*assets\app.properties*" file and update following properties as per requirement





```xml
<?xml version="1.0" encoding="utf-8"?>
<resources>

    <string name="connection_timeout">1500</string>Sp
    <string name="ssl_pinning_enabled">Yes</string>

    <!-- App Config -->
    <string name="shared_server_url">@@SERVER_URL</string>
    <string name="shared_oam_url">@@OAM_URL</string>
    <string name="otp_type">@@OTP_TYPE</string>
    <string name="entity">@@ENTITY</string>
    <string name="server_type">@@SERVER_TYPE</string>
    <string name="max_no_attempts">0</string>
    <string name="ui_device_root_check">false</string>
    <string name="DOMAIN_BASED_CATEGORIZATION">true</string>
    <string name="GOOGLE_CLOUD_PROJECT_NO">@@GOOGLE_CLOUD_PROJECT_NO</string>

    <!-- SSL pinning

    Below is the list of Base 64 encoded SHA256 hashed certificates' public keys. Use below command to generate this has
    your certificate. Replace 'certificate.cer' with the path to your certificate.
    openssl x509 -inform der -in certificate.cer -pubkey -noout | openssl pkey -pubin -outform der | openssl dgst -sha25

    -->
    <string-array name="certificate_public_keys">
        <item>@@SERVER_CERTIFICATE_KEY</item>
    </string-array>

</resources>
```

resources

Project update recommended: Android Gradle Plugin can be upgraded. (2 minutes ago)

Set OTP type to HOTP/TOTP as per requirement.

Set Server Type to OBDXTOKEN

Set MAX No Attempts greater than 0

Set UI Device root check to true if you want to add check on login button.

Note: If selected authentication mechanism is not OAM based then remove "*shared_oam_url*" property.

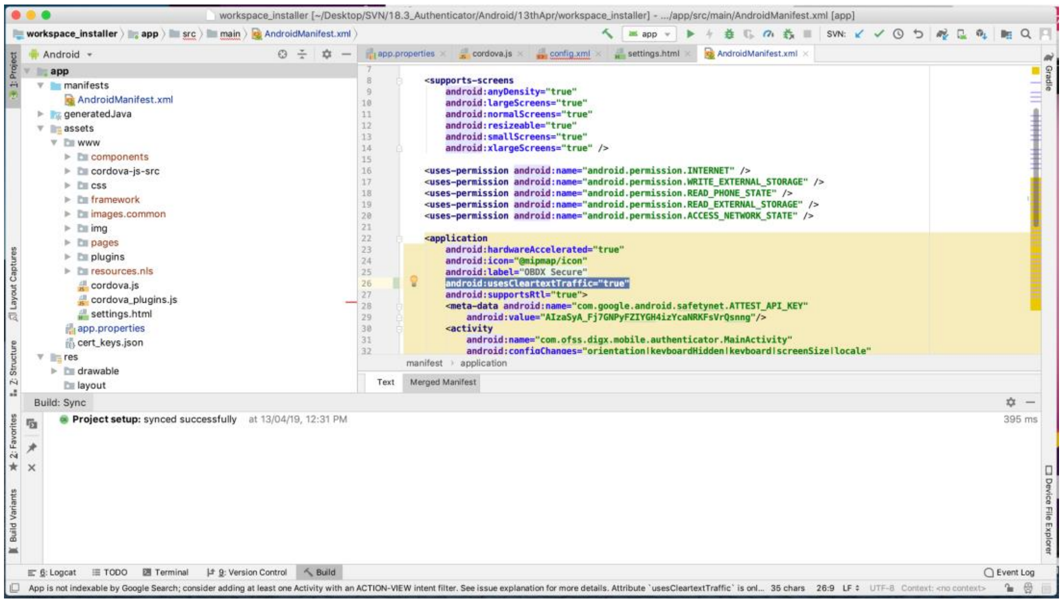
---

6. Click Build → Clean & Build → Rebuild project in Android Studio.
7. Click on Build → Edit Build Type → app → release

   Enable minify → true

   Add progurard file from workspace_installer/proguard-rules.pro

   Click OK
8. If using http protocol for development add (android:usesCleartextTraffic="true") to application tag of AndroidManifest.xml

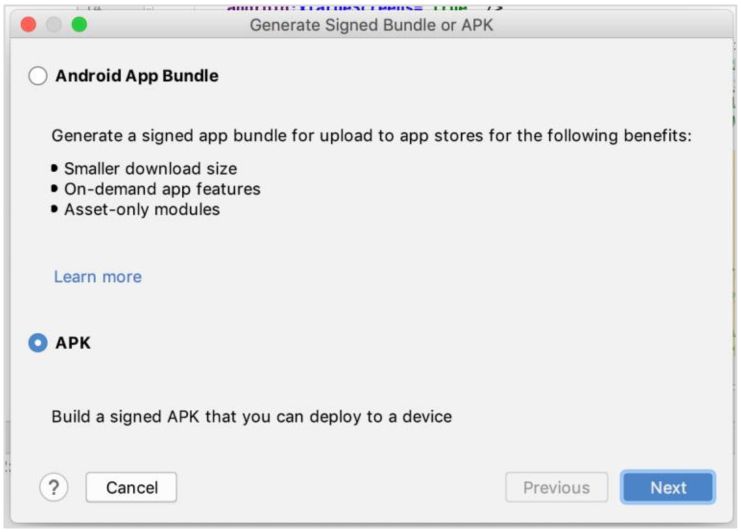


```
    <supports-screens
        android:anyDensity="true"
        android:largeScreens="true"
        android:normalScreens="true"
        android:resizeable="true"
        android:smallScreens="true"
        android:xlargeScreens="true" />

    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />

    <application
        android:hardwareAccelerated="true"
        android:icon="@mipmap/icon"
        android:label="OBDX Secure"
        android:usesCleartextTraffic="true"
        android:supportsRtl="true">
        <meta-data android:name="com.google.android.safetynet.ATTEST_API_KEY"
            android:value="AIzaSyA_Fj7GNPyFZIYGH4izYcaNRKFsVrQsnng"/>
        <activity
            android:name="com.ofss.digx.mobile.authenticator.MainActivity"
            android:configChanges="orientation|keyboardHidden|keyboard|screenSize|locale"
```

```
Project setup: synced successfully    at 13/04/19, 12:31 PM    395 ms
```

```
App is not indexable by Google Search; consider adding at least one Activity with an ACTION-VIEW intent filter. See issue explanation for more details. Attribute `usesCleartextTraffic` is onl...   35 chars   26:9   LF ÷   UTF-8   Context: <no context>
```

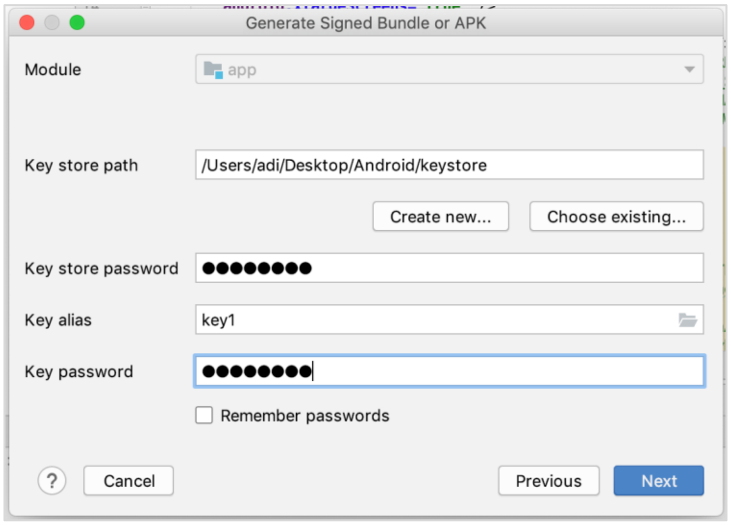
9. **For Generating Signed Apk:** To Generate release-signed apk as follows:
10. On menu bar click on Build -> Generate Signed Apk



Generate a signed app bundle for upload to app stores for the following benefits:

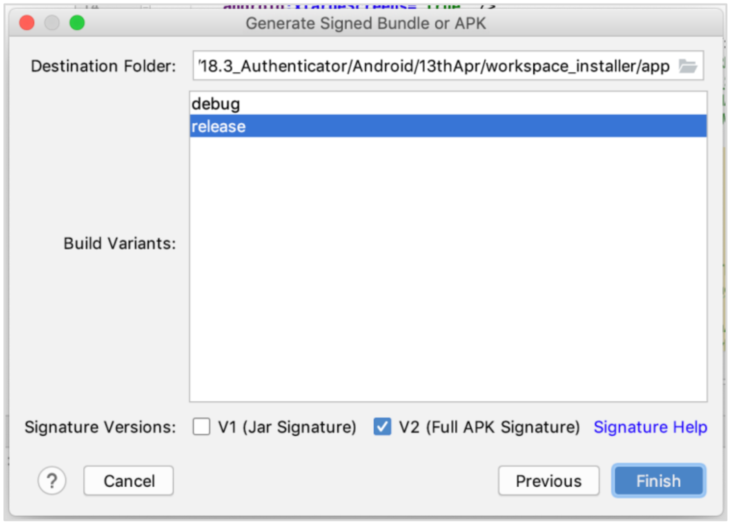
- Smaller download size
- On-demand app features
- Asset-only modules

Build a signed APK that you can deploy to a device



Module	app
Key store path	/Users/adi/Desktop/Android/keystore
Key store password	●●●●●●●●
Key alias	key1
Key password	●●●●●●●●

☐ Remember passwords



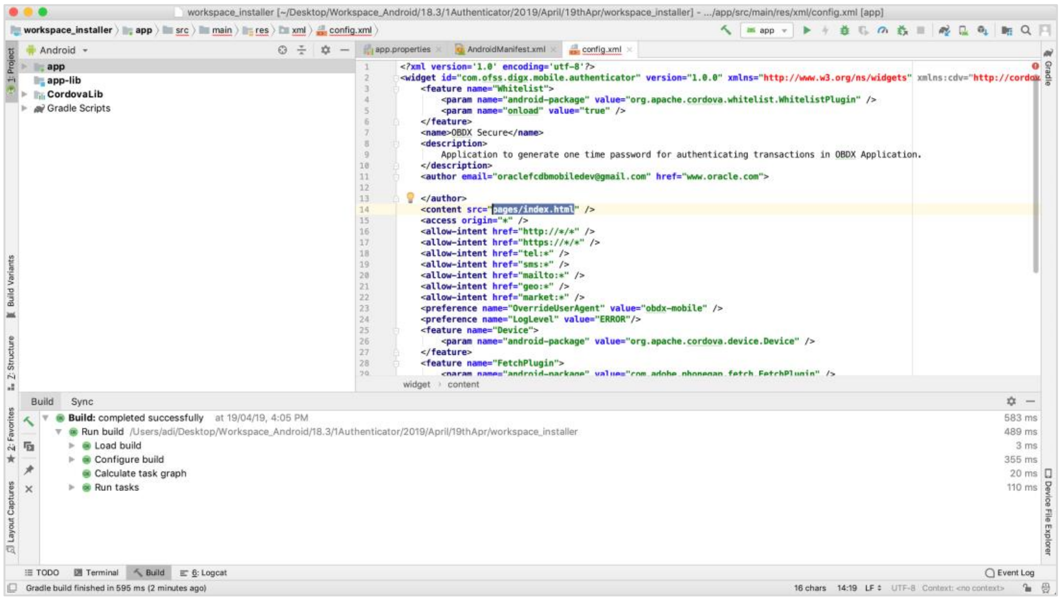
Destination Folder: '18.3_Authenticator/Android/13thApr/workspace_installer/app

Build Variants: debug, release (selected)

Signature Versions: ☐ V1 (Jar Signature) ☑ V2 (Full APK Signature)

Click Finish to generate .apk

The application has config page to add URL. This is for development purpose only and can be removed using below step. (Update content src tag)



workspace_installer [~/Desktop/Workspace_Android/18.3/1Authenticator/2019/April/19thApr/workspace_installer] - .../app/src/main/res/xml/config.xml [app]

```xml
<?xml version='1.0' encoding='utf-8'?>
<widget id="com.ofss.digx.mobile.authenticator" version="1.0.0" xmlns="http://www.w3.org/ns/widgets" xmlns:cdv="http://cordo
    <feature name="Whitelist">
        <param name="android-package" value="org.apache.cordova.whitelist.WhitelistPlugin" />
        <param name="onload" value="true" />
    </feature>
    <name>OBDX Secure</name>
    <description>
        Application to generate one time password for authenticating transactions in OBDX Application.
    </description>
    <author email="oraclefcdbmobiledev@gmail.com" href="www.oracle.com">

    </author>
    <content src="pages/index.html" />
    <access origin="*" />
    <allow-intent href="http://*/*" />
    <allow-intent href="https://*/*" />
    <allow-intent href="tel:*" />
    <allow-intent href="sms:*" />
    <allow-intent href="mailto:*" />
    <allow-intent href="geo:*" />
    <allow-intent href="market:*" />
    <preference name="OverrideUserAgent" value="obdx-mobile" />
    <preference name="LogLevel" value="ERROR"/>
    <feature name="Device">
        <param name="android-package" value="org.apache.cordova.device.Device" />
    </feature>
    <feature name="FetchPlugin">
        <param name="android-package" value="com.adobe.phonegap.fetch.FetchPlugin" />
```

```
Build: completed successfully   at 19/04/19, 4:05 PM                                              583 ms
  Run build /Users/adi/Desktop/Workspace_Android/18.3/1Authenticator/2019/April/19thApr/workspace_installer   489 ms
    Load build                                                                                      3 ms
    Configure build                                                                               355 ms
    Calculate task graph                                                                           20 ms
    Run tasks                                                                                     110 ms
```

Gradle build finished in 595 ms (2 minutes ago)

[Home](#)

7. Application Security Configuration

Root Check → Ensure Step 3.1 is completed

1. Open google developer console. Select your app then navigate to

   Setup-> App Integrity-> change option of Response Encryption

   In the window that appears, click Manage and download my response encryption keys and follow below steps to generate response encryption keys-

   a. Create a new private-public key pair. RSA key size must be 2048 bits using below command-

   openssl genrsa -aes128 -out your_path/private.pem 2048

   Then use your password phrase for creating private.pem and also use the same password for verifying the private.pem. Then hit the below command.

   openssl rsa -in your_path/private.pem -pubout -out your_path/public.pem

   Enter the same password which you have used while creating private.pem. These two files will now appear on your mentioned path. Then upload the public.pem file on the window which was appeared after clicking on Manage and download my response encryption keys option.Once you upload the public.pem file it will automatically download your_app_pkg_name.enc file. Then hit below command as,

   openssl rsautl -decrypt -oaep -inkey your_path/private.pem -in your_app_pkg_name.enc -out your_path/api_keys.txt

   Enter the password for private.pem. It will create api_keys.tx file on your path. It must be consist of VERIFICATION_KEY and DECRYPTION_KEY.

2. Maintain this VERIFICATION_KEY and DECRYPTION_KEY in **DIGX_FW_CONFIG_ALL_B** table corresponding to the following keys respectivel:

   PLAY_INTEGRITY_ENCRYPTION_KEY and **PLAY_INTEGRITY_DECRYPTION_KEY**

   An example query will be:

   update DIGX_FW_CONFIG_ALL_B set prop_value = 'YOUR_DECRYPTION_KEY' where prop_id = 'PLAY_INTEGRITY_DECRYPTION_KEY';

   update DIGX_FW_CONFIG_ALL_B set prop_value = 'YOUR_ENCRYPTION_KEY' where prop_id = 'PLAY_INTEGRITY_ENCRYPTION_KEY';

3. Similarly, Obtain the same keys for authenticator app by using above step 1 and then maintain those in **DIGX_FW_CONFIG_ALL_B** table corresponding to the following keys respectivel:

   PLAY_INTEGRITY_ENCRYPTION_KEY_AUTHENTICATOR and **PLAY_INTEGRITY_DECRYPTION_KEY_AUTHENTICATOR**

An example query will be:

update DIGX_FW_CONFIG_ALL_B set prop_value = 'YOUR_DECRYPTION_KEY' where prop_id = 'PLAY_INTEGRITY_DECRYPTION_KEY_AUTHENTICATOR';

update DIGX_FW_CONFIG_ALL_B set prop_value = 'YOUR_ENCRYPTION_KEY' where prop_id = 'PLAY_INTEGRITY_ENCRYPTION_KEY_AUTHENTICATOR';

4. Similarly, we also have to maintain package names of Servicing and Authenticator app in the same table, i.e. **DIGX_FW_CONFIG_ALL_B** corresponding to the following keys respectively:

   ANDROID_SERVICING_PACKAGE and ANDROID_AUTHENTICATOR_PACKAGE

   An example query will be:

   insert into digx_fw_config_all_b (PROP_ID, CATEGORY_ID, PROP_VALUE, FACTORY_SHIPPED_FLAG, PROP_COMMENTS, SUMMARY_TEXT, CREATED_BY, CREATION_DATE, LAST_UPDATED_BY, LAST_UPDATED_DATE, OBJECT_STATUS, OBJECT_VERSION_NUMBER) values ('ANDROID_SERVICING_PACKAGE', 'mobileconfig', 'com.ofss.zigbank', 'N', '', 'Stores device id in OUD', 'ofssuser', sysdate, 'ofssuser', sysdate, 'Y', 1,);

SSL Pinning

5. Get the list of Base 64 encoded SHA256 hashed certificates' public keys of server's valid certificates. Use below command to generate this hash for your certificate. Replace '<certificate.der>' with the path to your certificate.

   openssl x509 -inform der -in <certificate.der> -pubkey -noout | openssl pkey -pubin -outform der | openssl dgst -sha256 -binary | openssl enc -base64

6. Add the hashed keys generated in point 6 to **zigbank\platforms\android\customizations\src\main\res\values\app.properties.xml file** in 'certificate_public_keys' array. Append this key to 'sha256/' in an <item> tag as shown below. Multiple certificate keys can be added to 'certificate_public_keys' array by adding them in <item> tags.

   Eg.:

```
<string-array name="certificate_public_keys">

    <item>sha256/5kJvNEMw0KjrCAu7eXY5HZdvyCS13BbA0VJG1RSP91w=</item>

</string-array>
```

   Eg. for multiple certificates (In case OAM/IDCS is used):

```
<string-array name="certificate_public_keys">

    <item>sha256/5kJvNEMw0KjrCAu7eXY5HZdvyCS13BbA0VJG1RSP91w=</item>

     <item>sha256/3rgsgghoqrDegekpkkgk92Fgw1w7exyYCS1okef9Oo1w=</item>
```

```
</string-array>
```

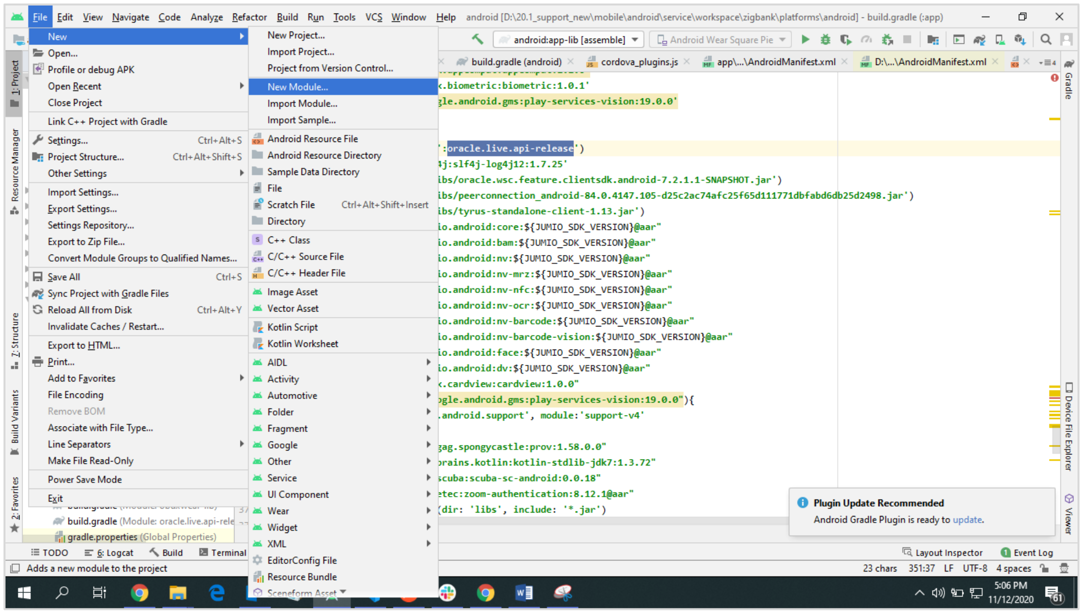
Home

8. Live Experience With Jumio Integration

1. Download live experience android sdk from below download link.

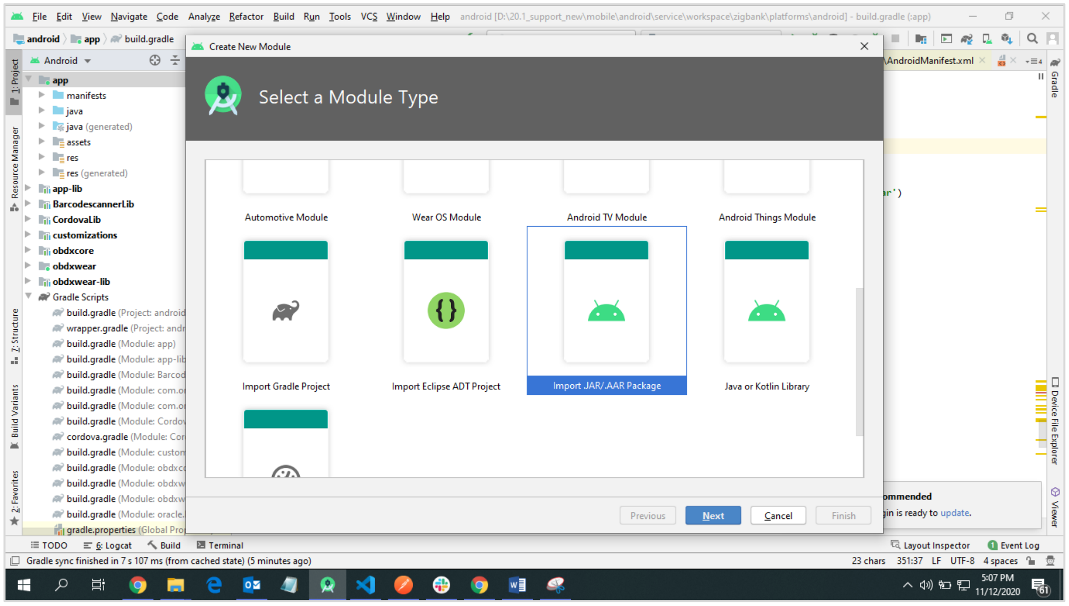
   https://www.oracle.com/downloads/cloud/oracle-live-experience-downloads.html

2. Import 'oracle.live.api-release' file as a New Module.



```
k.biometric:biometric:1.0.1'
gle.android.gms:play-services-vision:19.0.0'


':oracle.live.api-release')
4j:slf4j-log4j12:1.7.25'
ibs/oracle.wsc.feature.clientsdk.android-7.2.1.1-SNAPSHOT.jar')
ibs/peerconnection_android-84.0.4147.105-d25c2ac74afc25f65d111771dbfabd6db25d2498.jar')
ibs/tyrus-standalone-client-1.13.jar')
io.android:core:${JUMIO_SDK_VERSION}@aar"
io.android:bam:${JUMIO_SDK_VERSION}@aar"
io.android:nv:${JUMIO_SDK_VERSION}@aar"
io.android:nv-mrz:${JUMIO_SDK_VERSION}@aar"
io.android:nv-nfc:${JUMIO_SDK_VERSION}@aar"
io.android:nv-ocr:${JUMIO_SDK_VERSION}@aar"
io.android:nv-barcode:${JUMIO_SDK_VERSION}@aar"
io.android:nv-barcode-vision:${JUMIO_SDK_VERSION}@aar"
io.android:face:${JUMIO_SDK_VERSION}@aar"
io.android:dv:${JUMIO_SDK_VERSION}@aar"
k.cardview:cardview:1.0.0"
ogle.android.gms:play-services-vision:19.0.0"){
.android.support', module:'support-v4'

gag.spongycastle:prov:1.58.0.0"
brains.kotlin:kotlin-stdlib-jdk7:1.3.72"
scuba:scuba-sc-android:0.0.18"
etec:zoom-authentication:8.12.1@aar"
(dir: 'libs', include: '*.jar')
```

Plugin Update Recommended
Android Gradle Plugin is ready to update.


File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help
android [D:\20.1_support_new\mobile\android\service\workspace\zigbank\platforms\android] - build.gradle (:app)
android
app
build.gradle
Android
app
manifests
java
java (generated)
assets
res
res (generated)
app-lib
BarcodescannerLib
CordovaLib
customizations
obdxcore
obdxwear
obdxwear-lib
Gradle Scripts
build.gradle (Project: android)
wrapper.gradle (Project: andr
build.gradle (Module: app)
build.gradle (Module: app-lib
build.gradle (Module: Barcod
build.gradle (Module: com.o
build.gradle (Module: com.o
build.gradle (Module: Cordov
cordova.gradle (Module: Cor
build.gradle (Module: custom
build.gradle (Module: obdxc
build.gradle (Module: obdxw
build.gradle (Module: obdxw
build.gradle (Module: oracle.
gradle.properties (Global Pro
Create New Module
Select a Module Type
Automotive Module
Wear OS Module
Android TV Module
Android Things Module
Import Gradle Project
Import Eclipse ADT Project
Import JAR/.AAR Package
Java or Kotlin Library
Previous
Next
Cancel
Finish
AndroidManifest.xml
TODO
6: Logcat
Build
Terminal
Layout Inspector
Event Log
Gradle sync finished in 7 s 107 ms (from cached state) (5 minutes ago)
23 chars 351:37 LF UTF-8 4 spaces
5:07 PM
11/12/2020

3. Add Live Experience Client ID and Cloud Address in below two properties under app.properties.xml(zigbank\platforms\android\customizations\src\main\res\values)

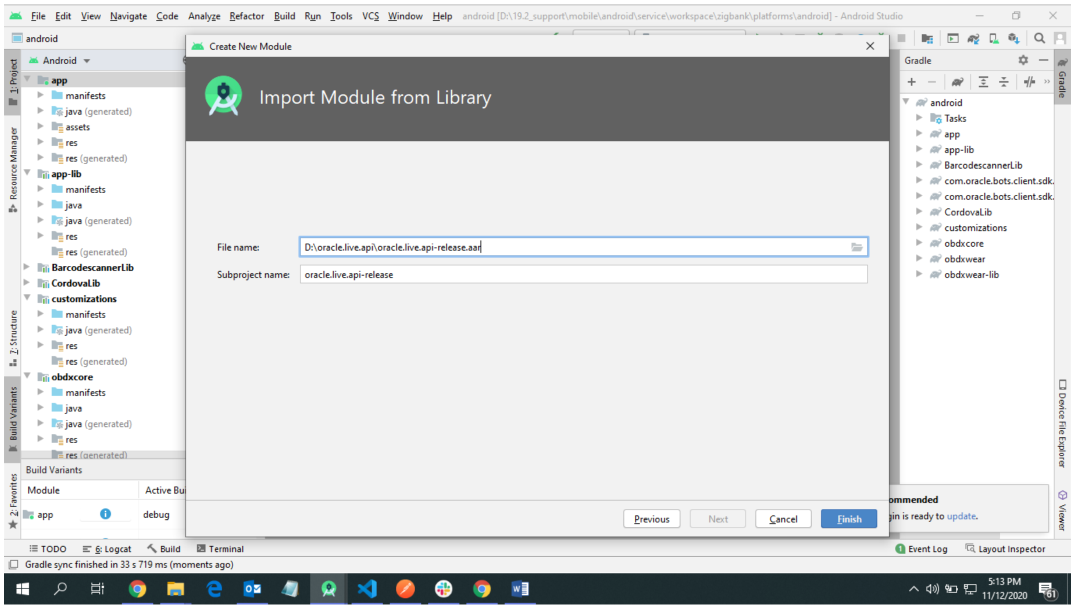
   <string name="LX_CLIENT_ID">@@CLIENT_ID</string>

   <string name="LX_ADDRESS">@@ADDRESS</string>

Note: Add LX_ADDRESS without https://

For example. If the LX_ADDRESS is https://live.oraclecloud.com then add only live.oraclecloud.com.

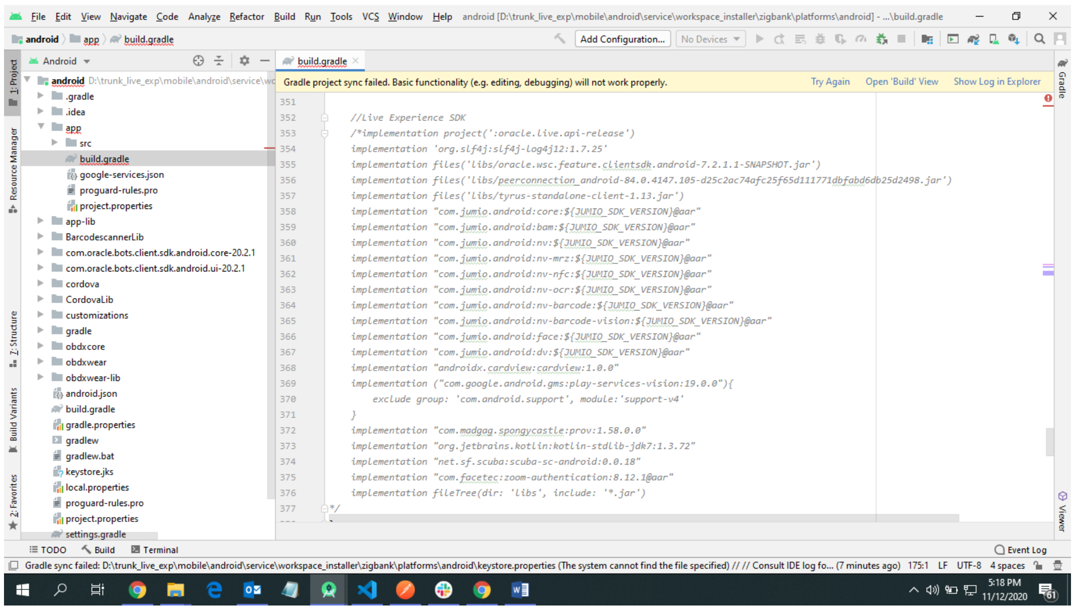
4. Click Next and navigate to oracle.live.api-release aar file location and click Finish.



File name: D:\oracle.live.api\oracle.live.api-release.aar

Subproject name: oracle.live.api-release

5. Un-comment the Live Experience SDK's from zigbank\platforms\android\app\build.gradle.

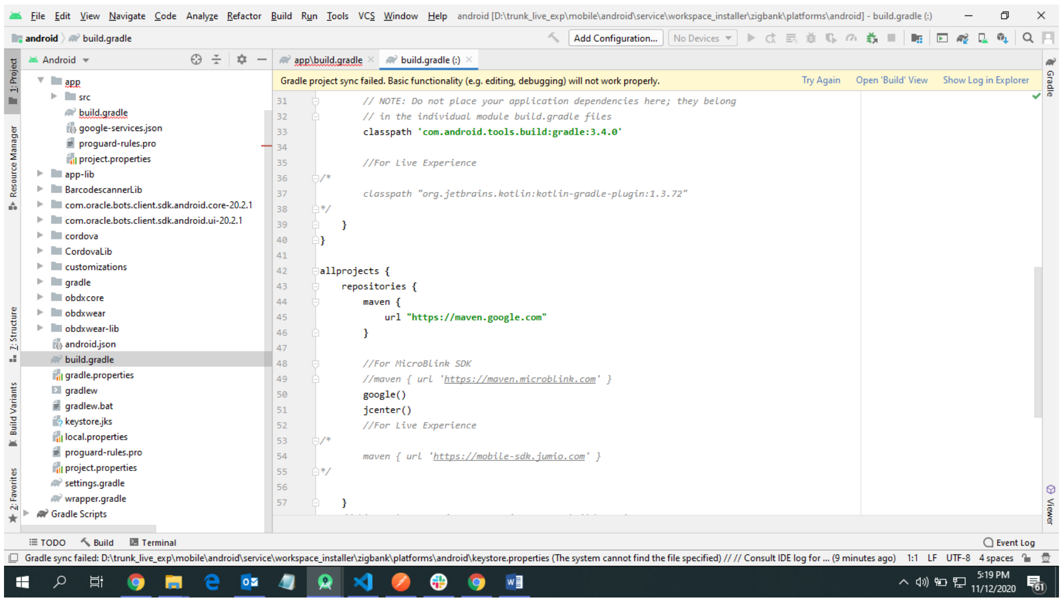


Gradle project sync failed. Basic functionality (e.g. editing, debugging) will not work properly.

```
    //Live Experience SDK
    /*implementation project(':oracle.live.api-release')
    implementation 'org.slf4j:slf4j-log4j12:1.7.25'
    implementation files('libs/oracle.wsc.feature.clientsdk.android-7.2.1.1-SNAPSHOT.jar')
    implementation files('libs/peerconnection_android-84.0.4147.105-d25c2ac74afc25f65d111771dbfabd6db25d2498.jar')
    implementation files('libs/tyrus-standalone-client-1.13.jar')
    implementation "com.jumio.android:core:${JUMIO_SDK_VERSION}@aar"
    implementation "com.jumio.android:bam:${JUMIO_SDK_VERSION}@aar"
    implementation "com.jumio.android:nv:${JUMIO_SDK_VERSION}@aar"
    implementation "com.jumio.android:nv-mrz:${JUMIO_SDK_VERSION}@aar"
    implementation "com.jumio.android:nv-nfc:${JUMIO_SDK_VERSION}@aar"
    implementation "com.jumio.android:nv-ocr:${JUMIO_SDK_VERSION}@aar"
    implementation "com.jumio.android:nv-barcode:${JUMIO_SDK_VERSION}@aar"
    implementation "com.jumio.android:nv-barcode-vision:${JUMIO_SDK_VERSION}@aar"
    implementation "com.jumio.android:face:${JUMIO_SDK_VERSION}@aar"
    implementation "com.jumio.android:dv:${JUMIO_SDK_VERSION}@aar"
    implementation "androidx.cardview:cardview:1.0.0"
    implementation ("com.google.android.gms:play-services-vision:19.0.0"){
        exclude group: 'com.android.support', module:'support-v4'
    }
    implementation "com.madgag.spongycastle:prov:1.58.0.0"
    implementation "org.jetbrains.kotlin:kotlin-stdlib-jdk7:1.3.72"
    implementation "net.sf.scuba:scuba-sc-android:0.0.18"
    implementation "com.facetec:zoom-authentication:8.12.1@aar"
    implementation fileTree(dir: 'libs', include: '*.jar')
*/
```

Gradle sync failed: D:\trunk_live_exp\mobile\android\service\workspace_installer\zigbank\platforms\android\keystore.properties (The system cannot find the file specified) // // Consult IDE log fo... (7 minutes ago)

6. Un-comment the gradle maven files for Live Experience from zigbank\platforms\android\build.gradle

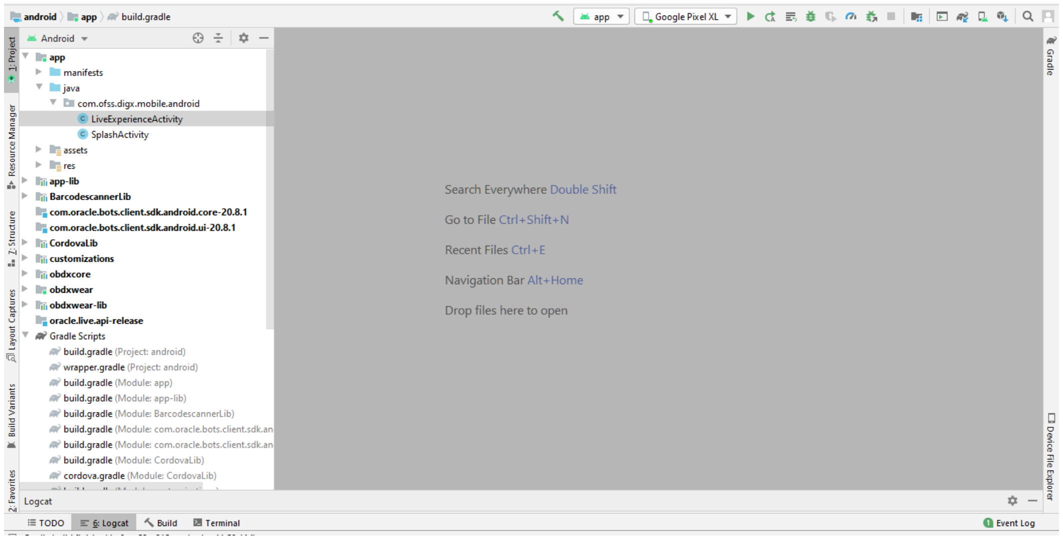


Gradle project sync failed. Basic functionality (e.g. editing, debugging) will not work properly.

```
        // NOTE: Do not place your application dependencies here; they belong
        // in the individual module build.gradle files
        classpath 'com.android.tools.build:gradle:3.4.0'

        //For Live Experience
/*
        classpath "org.jetbrains.kotlin:kotlin-gradle-plugin:1.3.72"
*/
    }
}

allprojects {
    repositories {
        maven {
            url "https://maven.google.com"
        }

        //For MicroBlink SDK
        //maven { url 'https://maven.microblink.com' }
        google()
        jcenter()
        //For Live Experience
/*
        maven { url 'https://mobile-sdk.jumio.com' }
*/

    }
```

Gradle sync failed: D:\trunk_live_exp\mobile\android\service\workspace_installer\zigbank\platforms\android\keystore.properties (The system cannot find the file specified) // // Consult IDE log for ... (9 minutes ago)

7. Add LiveExperienceActivtiy.java folder from AppExtensions\live experience\ at zigbank\platforms\android\app\src\main\java\com\ofss\digx\mobile\android

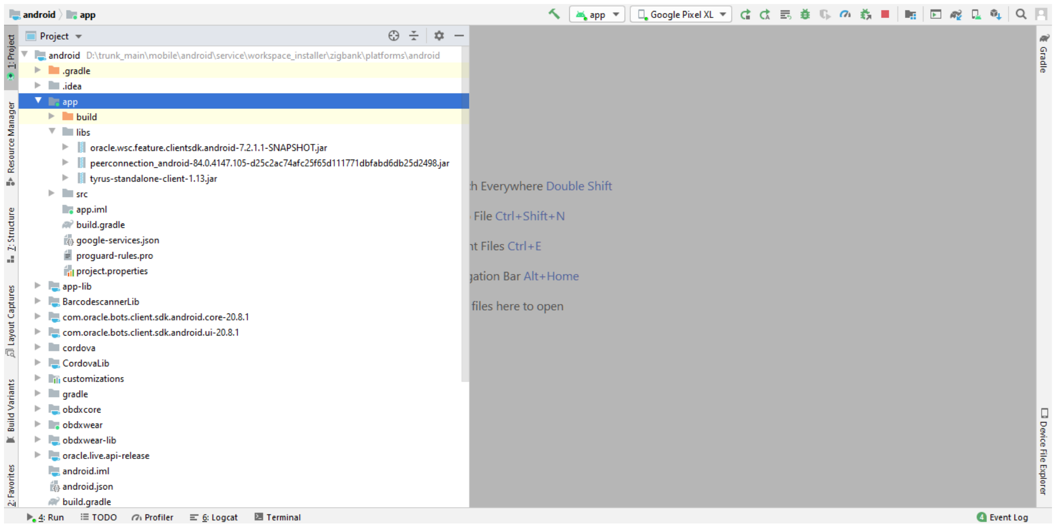

android
app
build.gradle
Android
app
manifests
java
com.ofss.digx.mobile.android
LiveExperienceActivity
SplashActivity
assets
res
app-lib
BarcodescannerLib
com.oracle.bots.client.sdk.android.core-20.8.1
com.oracle.bots.client.sdk.android.ui-20.8.1
CordovaLib
customizations
obdxcore
obdxwear
obdxwear-lib
oracle.live.api-release
Gradle Scripts
build.gradle (Project: android)
wrapper.gradle (Project: android)
build.gradle (Module: app)
build.gradle (Module: app-lib)
build.gradle (Module: BarcodescannerLib)
build.gradle (Module: com.oracle.bots.client.sdk.an
build.gradle (Module: com.oracle.bots.client.sdk.an
build.gradle (Module: CordovaLib)
cordova.gradle (Module: CordovaLib)
Search Everywhere Double Shift
Go to File Ctrl+Shift+N
Recent Files Ctrl+E
Navigation Bar Alt+Home
Drop files here to open
Logcat
TODO
6: Logcat
Build
Terminal
Event Log

8. Add libs folder at zigbank\platforms\android\app and copy below jars from downloaded sdk folder in it.

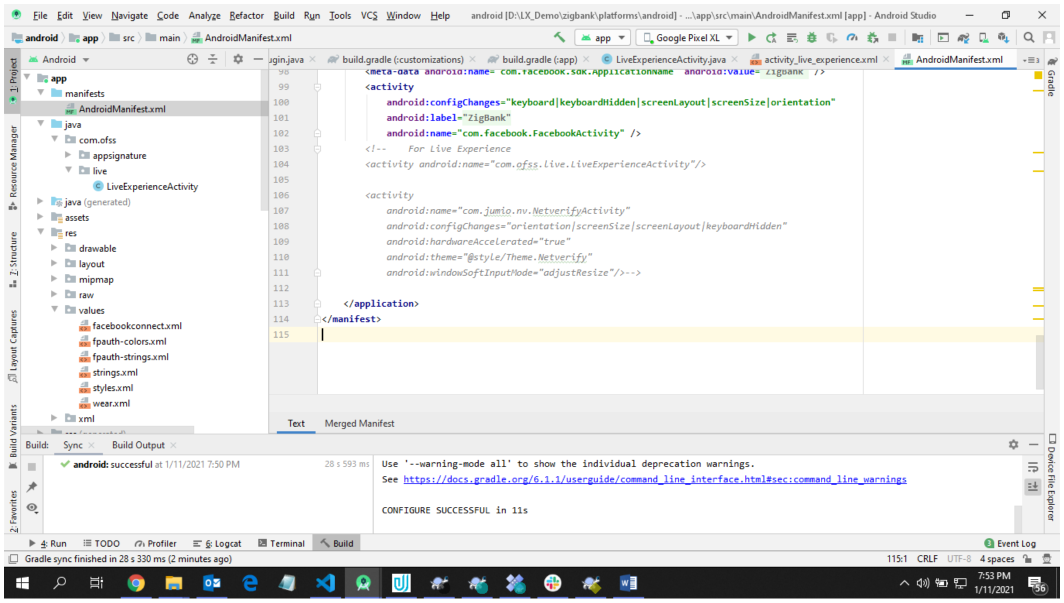
   i) oracle.wsc.feature.clientsdk.android-7.2.1.1-SNAPSHOT.jar

   ii) peerconnection_android-84.0.4147.105-25c2ac74afc25f65d111771dbfabd6db25d2498.jar

   iii) tyrus-standalone-client-1.13.jar


android
app
Project
android D:\trunk_main\mobile\android\service\workspace_installer\zigbank\platforms\android
.gradle
.idea
app
build
libs
oracle.wsc.feature.clientsdk.android-7.2.1.1-SNAPSHOT.jar
peerconnection_android-84.0.4147.105-d25c2ac74afc25f65d111771dbfabd6db25d2498.jar
tyrus-standalone-client-1.13.jar
src
app.iml
build.gradle
google-services.json
proguard-rules.pro
project.properties
app-lib
BarcodescannerLib
com.oracle.bots.client.sdk.android.core-20.8.1
com.oracle.bots.client.sdk.android.ui-20.8.1
cordova
CordovaLib
customizations
gradle
obdxcore
obdxwear
obdxwear-lib
oracle.live.api-release
android.iml
android.json
build.gradle
4: Run
TODO
Profiler
6: Logcat
Terminal
Event Log

9. Un-comment LiveExperienceActivity and NetverifyActivity from zigbank\platforms\android\app\src\main\AndroidManifest.xml



```
            <activity
                android:configChanges="keyboard|keyboardHidden|screenLayout|screenSize|orientation"
                android:label="ZigBank"
                android:name="com.facebook.FacebookActivity" />
            <!--    For Live Experience
            <activity android:name="com.ofss.live.LiveExperienceActivity"/>

            <activity
                android:name="com.jumio.nv.NetverifyActivity"
                android:configChanges="orientation|screenSize|screenLayout|keyboardHidden"
                android:hardwareAccelerated="true"
                android:theme="@style/Theme.Netverify"
                android:windowSoftInputMode="adjustResize"/>-->

        </application>
</manifest>
```

```
Use '--warning-mode all' to show the individual deprecation warnings.
See https://docs.gradle.org/6.1.1/userguide/command_line_interface.html#sec:command_line_warnings

CONFIGURE SUCCESSFUL in 11s
```

android: successful at 1/11/2021 7:50 PM 28 s 593 ms

Gradle sync finished in 28 s 330 ms (2 minutes ago)

[Home](#)

9. Adding Custom Cordova Plugin

Step 1 -

Create java folder and add yout package under app(zigbank\platforms\android\app)

Create java file under your package which will extends CordovaPlugin

Override execute method with JsonArray as a parameter

Retrive jsonobject from JsonArray and get the data which passed from js file

Example:

```
public class GetDirectionMapPlugin extends CordovaPlugin {
    @Override
    public boolean execute(String action, JSONArray args, CallbackContext callbackContext)
            throws JSONException {
        try{
            JSONObject object = args.getJSONObject(0);
            String yourKey = object.getString("your_key");
        }catch (Exception e){
            Log.e(TAG,e.getMessage());
        }
        return true;
    }
}
```

Step 2 –

Create plugin file under plugins folder of

www(zigbank\platforms\android\service\workspace\app\src\main\assets\www\plugins)

Example:

```
        cordova.define("cordova-plugin-getdirection", function(require, exports, module) {
    var exec = cordova.require('cordova/exec');
```

```
        exports.navigate = function(args, successCallback, errorCallback) {
            cordova.exec(successCallback, errorCallback, "GetDirectionMapPlugin", "direction",
                    [args]);
        };
    });
```

cordova-plugin-getdirection.getDirectionPlugin -> user defined id from cordova_plugin.js(zigbank\platforms\android\service\workspace\app\src\main\assets\www\cordova_plugin.js)

GetDirectionMapPlugin-> name of java plugin class

direction -> action

navigate -> this can be use in js file to this function

Step 3 –

Make entry of plugin in cordova_plugin.js(zigbank\platforms\android\service\workspace\zigbank\platforms\android\app\src\main\assets\www) as below ->

Example:

```
    {
        "id": "cordova-plugin-getdirection.getDirectionPlugin", -> user defined id
        "file": "plugins/cordova-plugin-getdirection/www/mapgetdirection.js", -> path of plugin js
        file
        "pluginId": "cordova-plugin-getdirection",
            "clobbers": [
        "window.getDirection" -> this can be used in js file to call plugin
 ]
    }
```

Step 4 -

Make entry of java plugin class in config.xml(zigbank\platforms\android\service\workspace\zigbank\platforms\android\app\src\main\res\xml) file of app as below -

Example:

```
<feature name="GetDirectionMapPlugin">
<param name="android-package" value="Your_Plugin_Java_Class_Path" />
</feature>
```

GetDirectionMapPlugin -> Name of java plugin class

Step 5 -

Plugin calling in js file ->

Example:

```
        window.getDirection.navigate({
    originLatLng: origin,
            destinationLatLng: location
})
```

window.getDirection -> clobber define in the cordova_plugin.js file

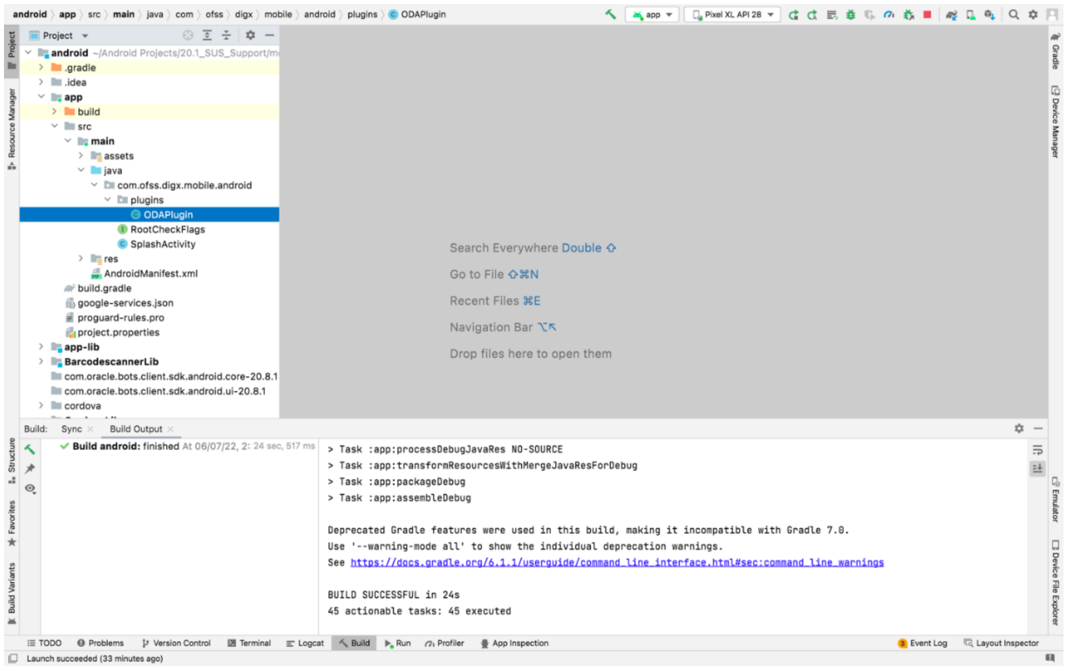
navigate -> name of the function defined in plugin js file

Home

10. ODA Chatbot Inclusion

To enable ODA Chatbot services in the mobile app, the following changes needs to be made:

1. Copy ODAPlugin.java from workspace_installer/AppExtension/oda to workspace_installer/zigbank/platforms/android/app/src/main/java/com/ofss/digx/mobile/android/plugins/



android › app › src › main › java › com › ofss › digx › mobile › android › plugins › ODAPlugin
Project
android ~/Android Projects/20.1_SUS_Support/m
.gradle
.idea
app
build
src
main
assets
java
com.ofss.digx.mobile.android
plugins
ODAPlugin
RootCheckFlags
SplashActivity
res
AndroidManifest.xml
build.gradle
google-services.json
proguard-rules.pro
project.properties
app-lib
BarcodescannerLib
com.oracle.bots.client.sdk.android.core-20.8.1
com.oracle.bots.client.sdk.android.ui-20.8.1
cordova
Search Everywhere Double ⇧
Go to File ⇧⌘N
Recent Files ⌘E
Navigation Bar ⌥↖
Drop files here to open them
Build: Sync Build Output
Build android: finished At 06/07/22, 2: 24 sec, 517 ms
TODO Problems Version Control Terminal Logcat Build Run Profiler App Inspection Event Log Layout Inspector
Launch succeeded (33 minutes ago)

```
> Task :app:processDebugJavaRes NO-SOURCE
> Task :app:transformResourcesWithMergeJavaResForDebug
> Task :app:packageDebug
> Task :app:assembleDebug

Deprecated Gradle features were used in this build, making it incompatible with Gradle 7.0.
Use '--warning-mode all' to show the individual deprecation warnings.
See https://docs.gradle.org/6.1.1/userguide/command_line_interface.html#sec:command_line_warnings

BUILD SUCCESSFUL in 24s
45 actionable tasks: 45 executed
```

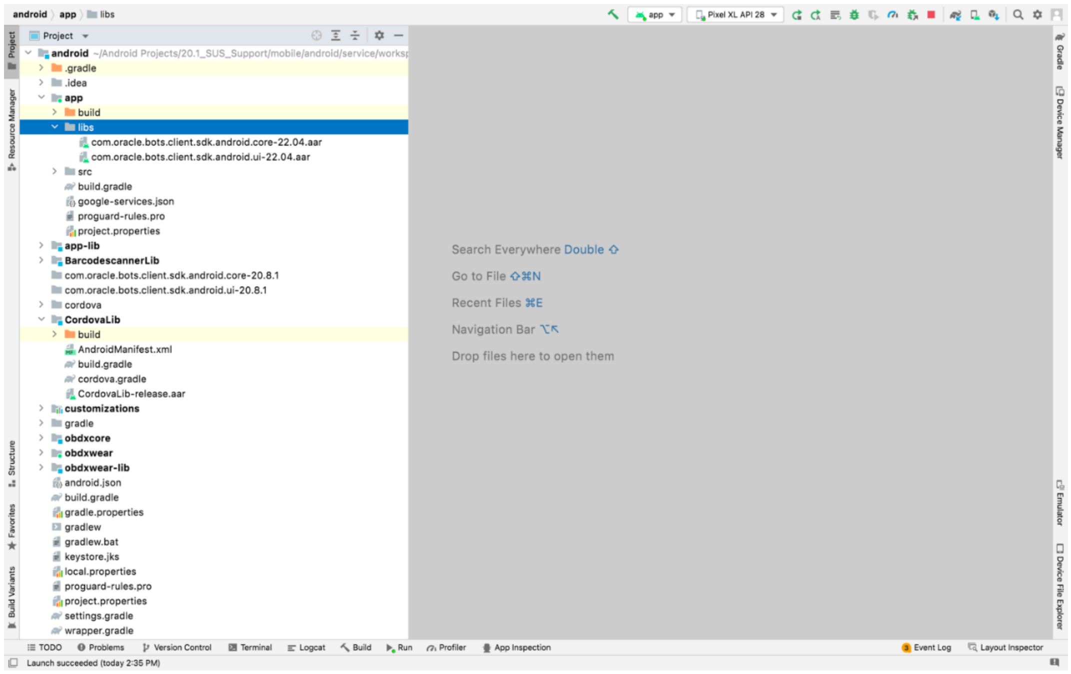
2. Download ODA Android sdk from below link-

https://www.oracle.com/downloads/cloud/amce-downloads.html

3. Add libs folder at zigbank\platforms\android\app and copy below files from downloaded sdk folder in it.

   a. com.oracle.bots.client.sdk.android.core-xx.aar

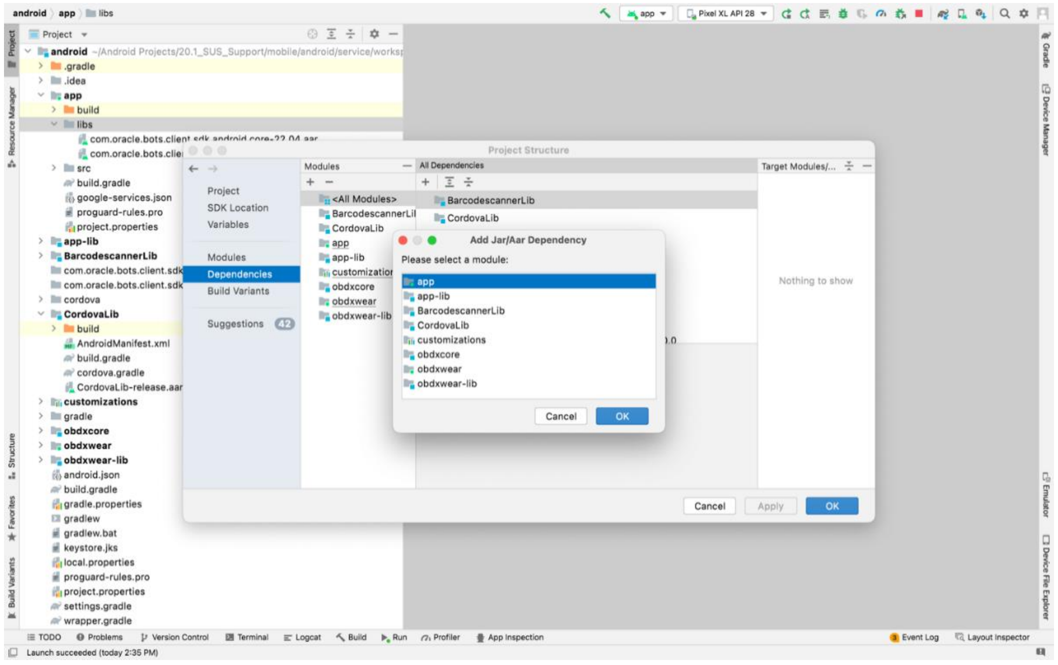
   b. com.oracle.bots.client.sdk.android.ui-22.04.aar



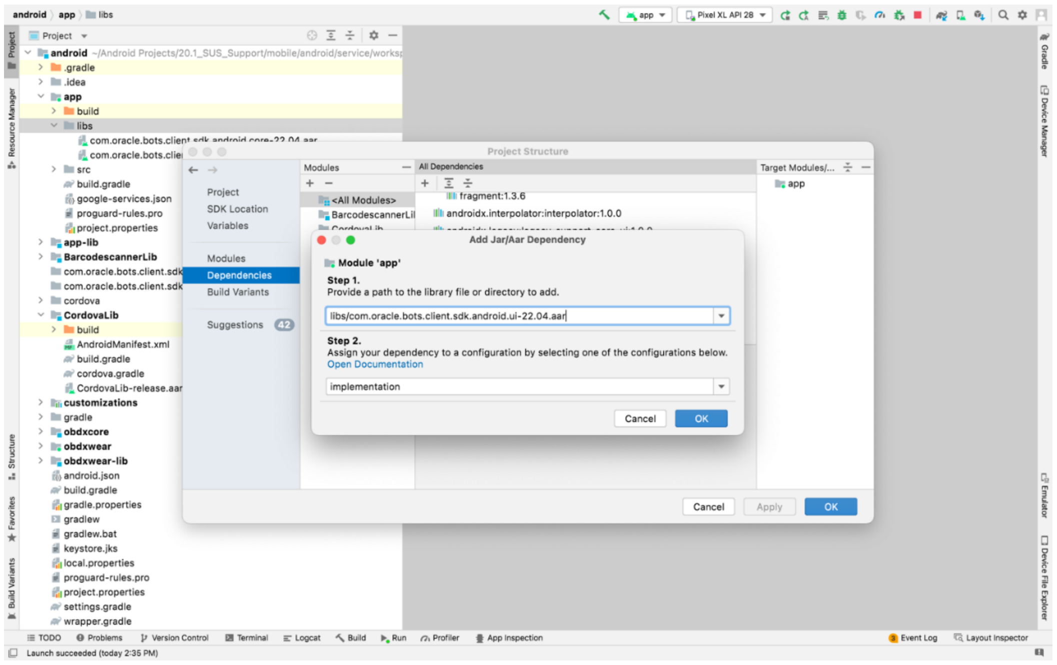
4. In Android Studio follow below steps-

File -> Project Structure -> Dependencies

5. Click on "+" icon and select JR/AAR Dependency and select app module and click Ok.



6. Add both .aar file paths from step3. Then click Apply and Ok.



Add Jar/Aar Dependency

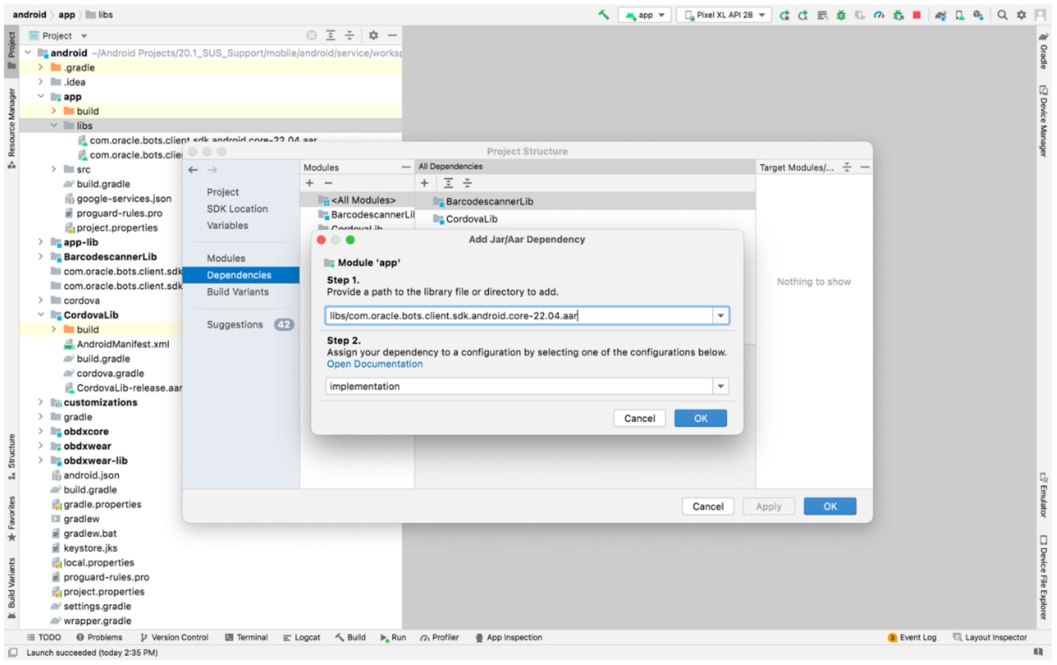
Module 'app'

Step 1.
Provide a path to the library file or directory to add.

libs/com.oracle.bots.client.sdk.android.ui-22.04.aar

Step 2.
Assign your dependency to a configuration by selecting one of the configurations below.
Open Documentation

implementation



Add Jar/Aar Dependency

Module 'app'

Step 1.
Provide a path to the library file or directory to add.

libs/com.oracle.bots.client.sdk.android.core-22.04.aar

Step 2.
Assign your dependency to a configuration by selecting one of the configurations below.
Open Documentation

implementation

7. Add Chatbot ID and Chatbot URL in app.properties.xml(zigbank\platforms\android\customizations\src\main\res\values)

```
<string name="CHATBOT_ID">@@CHATBOT_ID</string>

<string name="CHATBOT_URL">@@CHATBOT_URL</string>
```

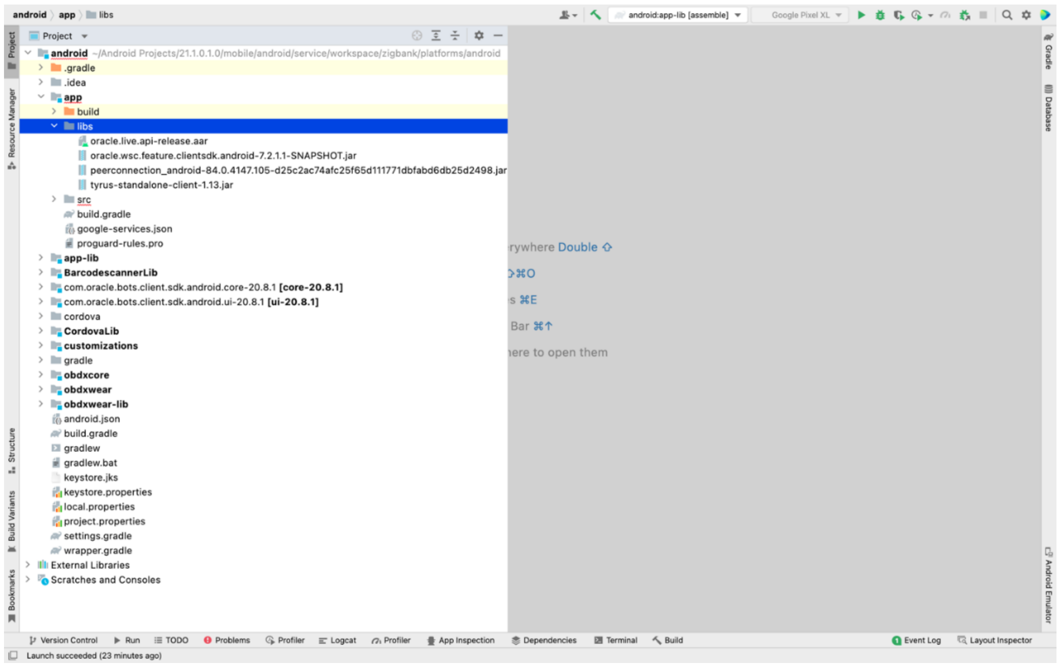
11. Live Experience Integration

1. Download live experience android sdk from below download link.

   https://www.oracle.com/downloads/cloud/oracle-live-experience-downloads.html

2. Add libs folder at zigbank\platforms\android\app and copy below jars from downloaded sdk folder in it.

   - oracle.wsc.feature.clientsdk.android-7.2.1.1-SNAPSHOT.jar
   - peerconnection_android-84.0.4147.105-25c2ac74afc25f65d111771dbfabd6db25d2498.jar
   - tyrus-standalone-client-1.13.jar
   - oracle.live.api-release.aar



3. Add Live Experience Client ID and Cloud Address in below two properties under

   app.properties.xml(zigbank\platforms\android\customizations\src\main\res\values)

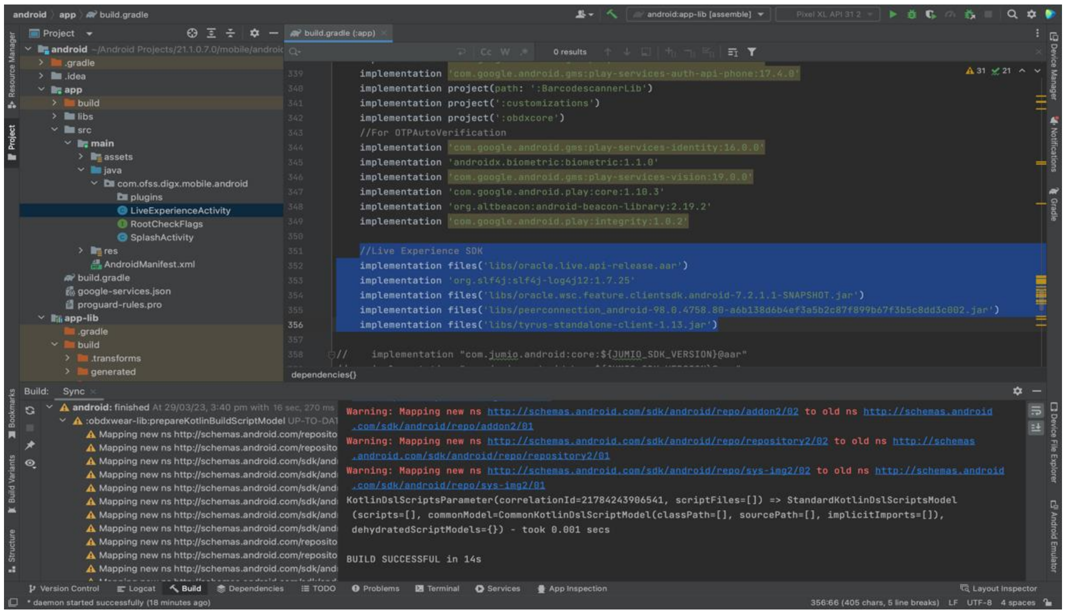
   <string name="LX_CLIENT_ID">@@CLIENT_ID</string>

   <string name="LX_ADDRESS">@@ADDRESS</string>

   Note: Add LX_ADDRESS without https://

   For example. If the LX_ADDRESS is https://live.oraclecloud.com then add only live.oraclecloud.com.

4. Un-comment the Live Experience SDK's from zigbank\platforms\android\app\build.gradle.

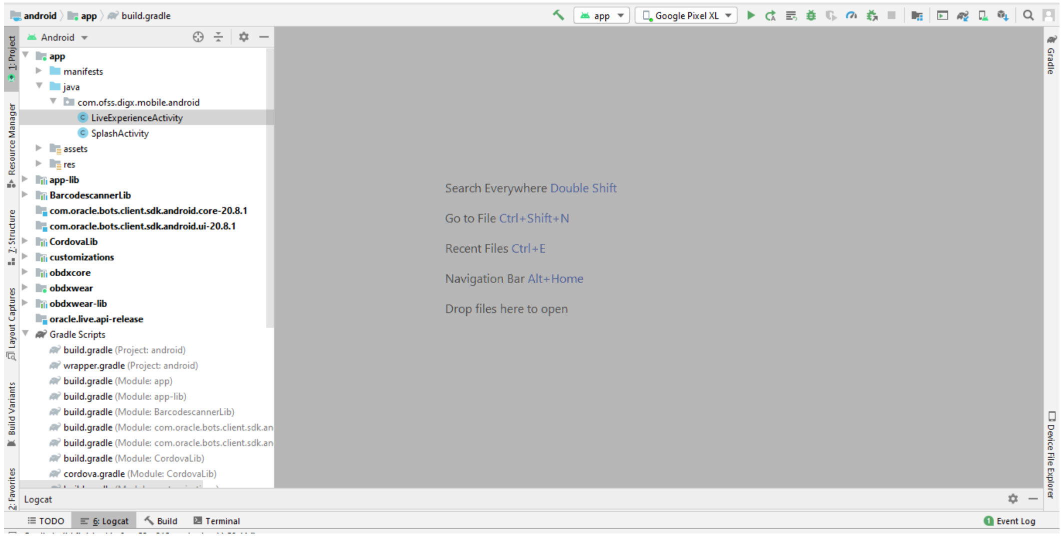


```
    implementation 'com.google.android.gms:play-services-auth-api-phone:17.4.0'
    implementation project(path: ':BarcodescannerLib')
    implementation project(':customizations')
    implementation project(':obdxcore')
    //For OTPAutoVerification
    implementation 'com.google.android.gms:play-services-identity:16.0.0'
    implementation 'androidx.biometric:biometric:1.1.0'
    implementation 'com.google.android.gms:play-services-vision:19.0.0'
    implementation 'com.google.android.play:core:1.10.3'
    implementation 'org.altbeacon:android-beacon-library:2.19.2'
    implementation 'com.google.android.play:integrity:1.0.2'

    //Live Experience SDK
    implementation files('libs/oracle.live.api-release.aar')
    implementation 'org.slf4j:slf4j-log4j12:1.7.25'
    implementation files('libs/oracle.wsc.feature.clientsdk.android-7.2.1.1-SNAPSHOT.jar')
    implementation files('libs/peerconnection_android-98.0.4758.80-a6b138d6b4ef3a5b2c87f899b67f3b5c8dd3c002.jar')
    implementation files('libs/tyrus-standalone-client-1.13.jar')

//    implementation "com.jumio.android:core:${JUMIO_SDK_VERSION}@aar"
```

```
Warning: Mapping new ns http://schemas.android.com/sdk/android/repo/addon2/02 to old ns http://schemas.android
 .com/sdk/android/repo/addon2/01
Warning: Mapping new ns http://schemas.android.com/sdk/android/repo/repository2/02 to old ns http://schemas
 .android.com/sdk/android/repo/repository2/01
Warning: Mapping new ns http://schemas.android.com/sdk/android/repo/sys-img2/02 to old ns http://schemas.android
 .com/sdk/android/repo/sys-img2/01
KotlinDslScriptsParameter(correlationId=21784243906541, scriptFiles=[]) => StandardKotlinDslScriptsModel
 (scripts=[], commonModel=CommonKotlinDslScriptModel(classPath=[], sourcePath=[], implicitImports=[]),
 dehydratedScriptModels={}) - took 0.001 secs

BUILD SUCCESSFUL in 14s
```

android > app > build.gradle
android:app-lib [assemble]
Pixel XL API 31 2
Project
build.gradle (:app)
0 results
android ~/Android Projects/21.1.0.7.0/mobile/android
.gradle
.idea
app
build
libs
src
main
assets
java
com.ofss.digx.mobile.android
plugins
LiveExperienceActivity
RootCheckFlags
SplashActivity
res
AndroidManifest.xml
build.gradle
google-services.json
proguard-rules.pro
app-lib
.gradle
build
.transforms
generated
dependencies{}
Build: Sync
android: finished At 29/03/23, 3:40 pm with 16 sec, 270 ms
:obdxwear-lib:prepareKotlinBuildScriptModel UP-TO-DATE
Mapping new ns http://schemas.android.com/reposito
Version Control
Logcat
Build
Dependencies
TODO
Problems
Terminal
Services
App Inspection
Layout Inspector
daemon started successfully (18 minutes ago)
356:66 (405 chars, 5 line breaks) LF UTF-8 4 spaces

5. Add LiveExperienceActivtiy.java folder from AppExtensions\live experience\ at zigbank\platforms\android\app\src\main\java\com\ofss\digx\mobile\android


android > app > build.gradle
app
Google Pixel XL
Android
app
manifests
java
com.ofss.digx.mobile.android
LiveExperienceActivity
SplashActivity
assets
res
app-lib
BarcodescannerLib
com.oracle.bots.client.sdk.android.core-20.8.1
com.oracle.bots.client.sdk.android.ui-20.8.1
CordovaLib
customizations
obdxcore
obdxwear
obdxwear-lib
oracle.live.api-release
Gradle Scripts
build.gradle (Project: android)
wrapper.gradle (Project: android)
build.gradle (Module: app)
build.gradle (Module: app-lib)
build.gradle (Module: BarcodescannerLib)
build.gradle (Module: com.oracle.bots.client.sdk.an
build.gradle (Module: com.oracle.bots.client.sdk.an
build.gradle (Module: CordovaLib)
cordova.gradle (Module: CordovaLib)
Search Everywhere Double Shift
Go to File Ctrl+Shift+N
Recent Files Ctrl+E
Navigation Bar Alt+Home
Drop files here to open
Logcat
TODO
Logcat
Build
Terminal
Event Log

6. Un-comment LiveExperienceActivity from zigbank\platforms\android\app\src\main\AndroidManifest.xml

12. Push Notification 2FA configuration

If Push notification 2fa is enabled at bank side for any transaction then, the screen displays message to wait for the push notification to accept/reject the transaction authentication. The message as well contains a timer of 5 minutes displayed on the UI. This value is set in the UI code. If bank needs to change this value, bank needs to update the value in UI code:

File path: channel/metadata/user-components/push-out-of-band/push-out-of-band/hook.js

Code to be changed: const mins = <<value>>;

Update the value to what bank needs to set it. This value is in minutes.

So, ideally 5 minutes (existing value in base UI code) is an ideal time. Any changes made in this value should satisfy below pre-condition.

1. There is an OTP expiration time set in “digx_fw_config_ALL_b” table.
2. Also, there is business policy check set to 10 minutes for validation of the generated 2fa token. Bank can write their own business policy where they can modify the 10 minutes time.

So, the time in UI code should not exceed 10 minutes and OTP expiration time in “digx_fw_config_ALL_b” table.

Home