Oracle Banking Digital Experience

Mobile Application Builder Guide – Android
Release 19.2.0.0.0

Part No. F25153-01

December 2019

Mobile Application Builder Guide – Android

December 2019

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/

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

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

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

Table of Contents

1. Preface

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=accandid=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=accandid=info or visit

http://www.oracle.com/pls/topic/lookup?ctx=accandid=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:

- Prerequisites
- Configuration / Installation.

1.5 Related Information Sources

For more information on Oracle Banking Digital Experience Release 19.2.0.0.0, refer to the following documents:

- Oracle Banking Digital Experience Licensing Guide

2. OBDX Servicing Application

2.1 Prerequisites

OBDX Android App is supported on Android 6 and above versions.

App will not work for Android 5 and below versions

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. Cordova Version: 6.x

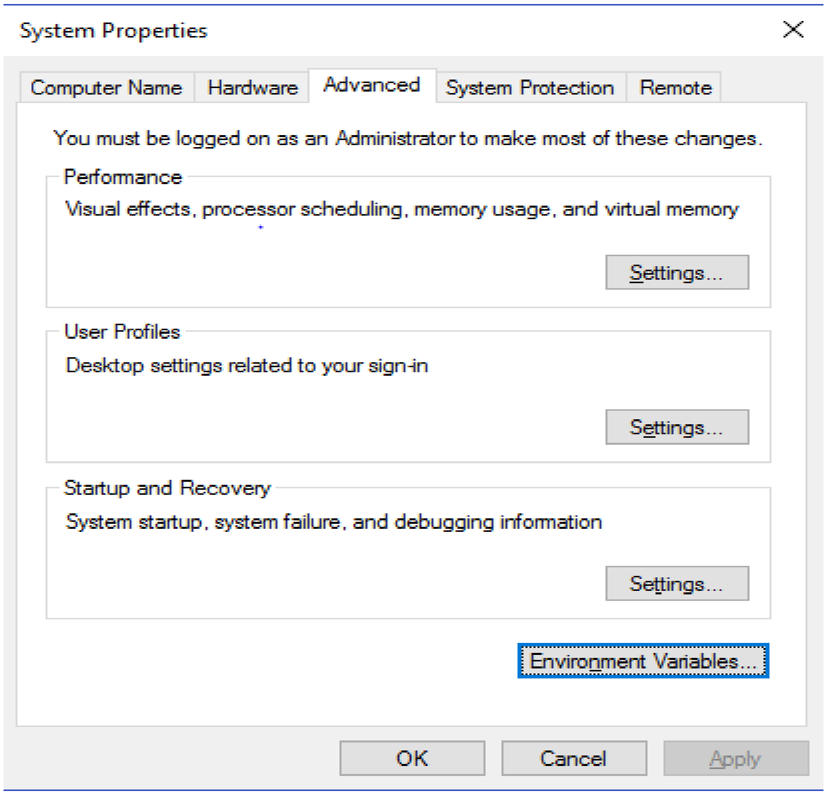
h. Gradle Version: gradle-4.6

i. Android Gradle Plugin Version (3.2.1): 'com.android.tools.build:gradle:3.2.1'

j. **Set Environment variables**

k. 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



System Properties

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

Performance

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

User Profiles

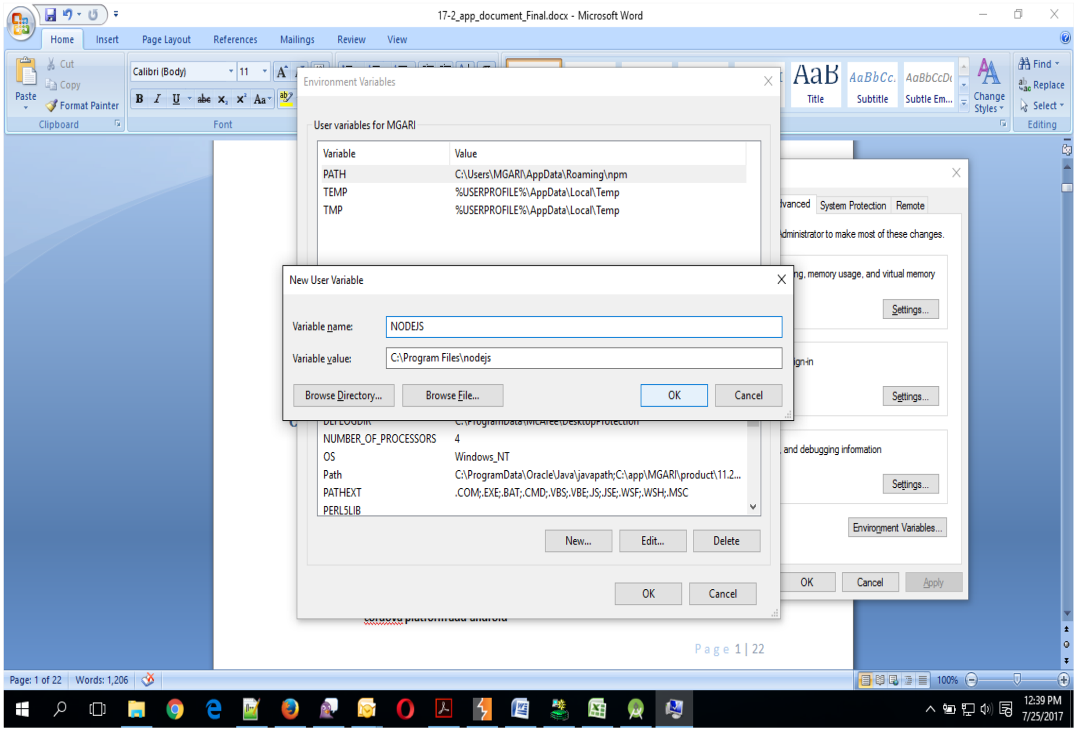
Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

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

l. Add the above variables in "*PATH*" system variable.



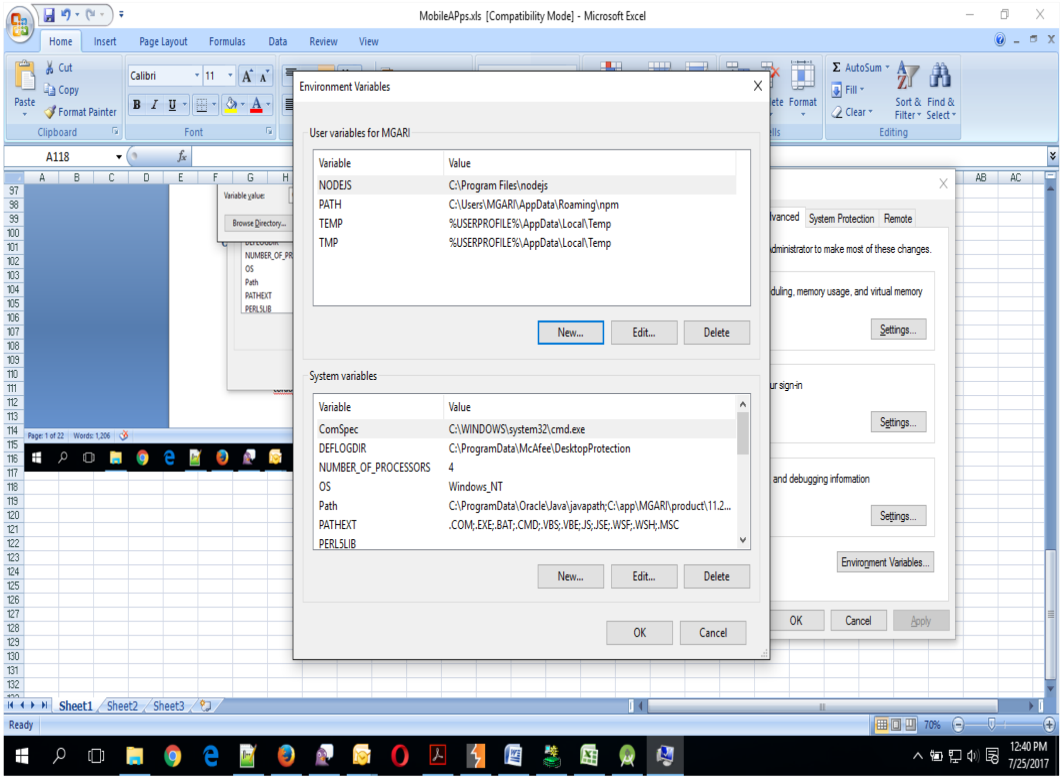
User variables for MGARI

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

Variable name: NODEJS

Variable value: C:\Program Files\nodejs

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	



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

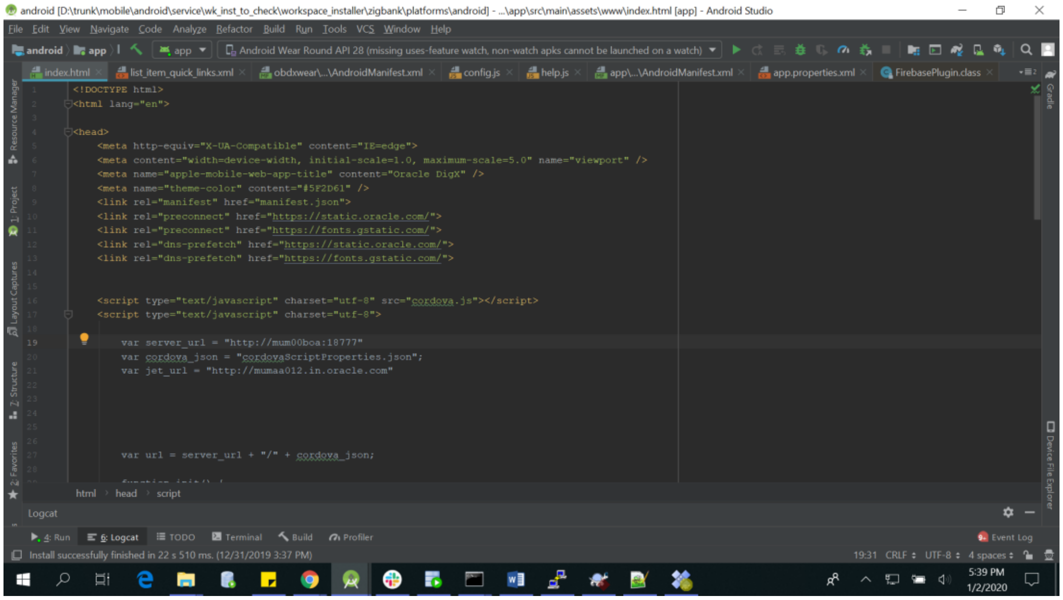
System variables

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 19.2, you can create app in two ways-using local UI or using remote UI (if want to create using remote go to 2.2 else directly to 2.3)

2.2 Create project using Remote UI

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



android [D:\trunk\mobile\android\service\wk_inst_to_check\workspace_installer\zigbank\platforms\android] - ...\app\src\main\assets\www\index.html [app] - Android Studio

File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help
android app app
Android Wear Round API 28 (missing uses-feature watch, non-watch apks cannot be launched on a watch)
index.html list_item_quick_links.xml obdxwear\...\AndroidManifest.xml config.js help.js app\...\AndroidManifest.xml app.properties.xml FirebasePlugin.class

```
<!DOCTYPE html>
<html lang="en">

<head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta content="width=device-width, initial-scale=1.0, maximum-scale=5.0" name="viewport" />
    <meta name="apple-mobile-web-app-title" content="Oracle DigX" />
    <meta name="theme-color" content="#5F2D61" />
    <link rel="manifest" href="manifest.json">
    <link rel="preconnect" href="https://static.oracle.com/">
    <link rel="preconnect" href="https://fonts.gstatic.com/">
    <link rel="dns-prefetch" href="https://static.oracle.com/">
    <link rel="dns-prefetch" href="https://fonts.gstatic.com/">


    <script type="text/javascript" charset="utf-8" src="cordova.js"></script>
    <script type="text/javascript" charset="utf-8">

        var server_url = "http://mum00boa:18777"
        var cordova_json = "cordovaScriptProperties.json";
        var jet_url = "http://mumaa012.in.oracle.com"





        var url = server_url + "/" + cordova_json;
```

html › head › script
Logcat
4: Run 6: Logcat TODO Terminal Build Profiler Event Log

Install successfully finished in 22 s 510 ms. (12/31/2019 3:37 PM)

1. In var server_url ,put the same KEY_SERVER_URL to be used in app.properties.xml
2. In var jet_url , put the url where your JET libraries are hosted or if not hosted on any particular server use: https://static.oracle.com/cdn

after this proceed to **2.4 Importing in Android Studio** directly

2.3 Local UI

2.3.1 Adding UI to workspace.

Use any 1 option below

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

Refer to User Interface Guide and then create a copy of index.html in the same folder and rename it to home.html.

Note: When copying to www, index.html already present in the workspace should be replaced)

B. Using built UI (out of box shipped with installer)

i. Go to path OBDX_Patch_Installer/installables/ui/deploy

ii. Create a copy of index.html and rename the copy to home.html

iii. Copy folders(components,extensions,framework,images,flows,json,lzn,home.html ,partials,resource, index.html,build.fingerprint) to workspace (platforms/android/app/android/app/src/main/assets/www/)

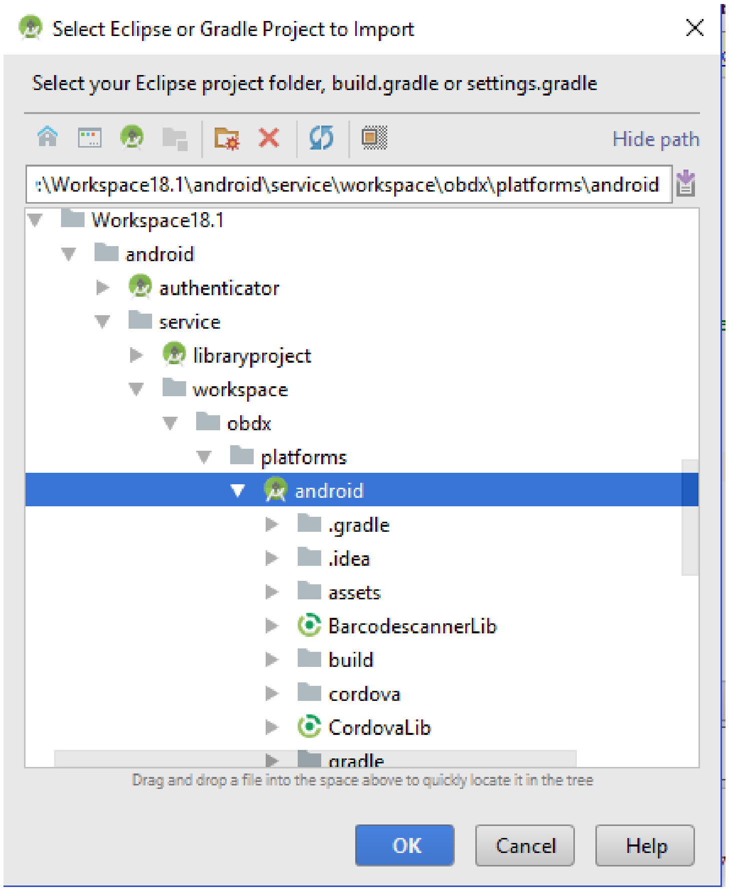
iv. Replace the index.html present in the workspace_installer folder

Ensure webhelp folder is not copied.

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

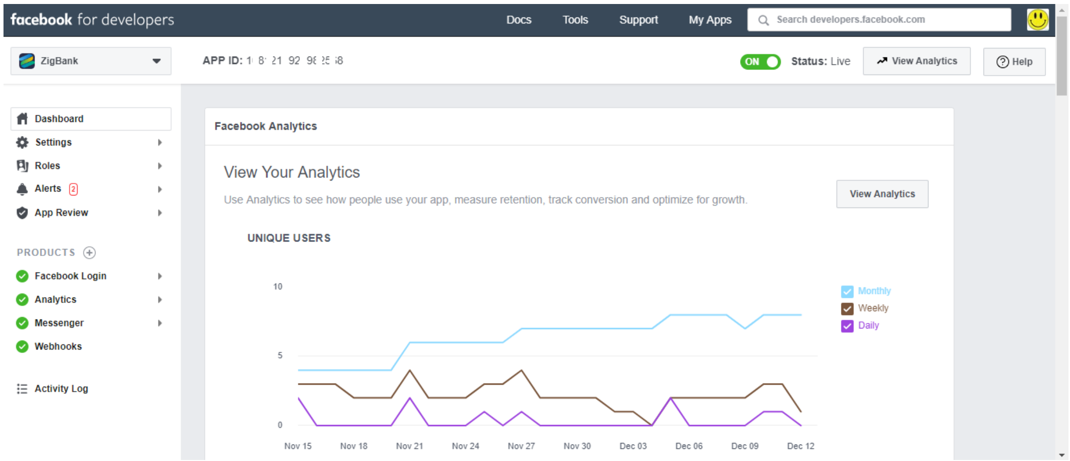
:\Workspace18.1\android\service\workspace\obdx\platforms\android

- 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. For Adding Facebook (Required for social payments only)
   a. Open facebookconnect.xml
   b. Replace FB_APP_ID with your fb app id generated from facebook developer console
   c. Replace FB_APP_NAME with the App name

As shown below



facebook for developers

Docs Tools Support My Apps

Search developers.facebook.com

ZigBank

APP ID: [redacted]

ON Status: Live

View Analytics

Help

- Dashboard
- Settings
- Roles
- Alerts 2
- App Review

PRODUCTS

- Facebook Login
- Analytics
- Messenger
- Webhooks

Activity Log

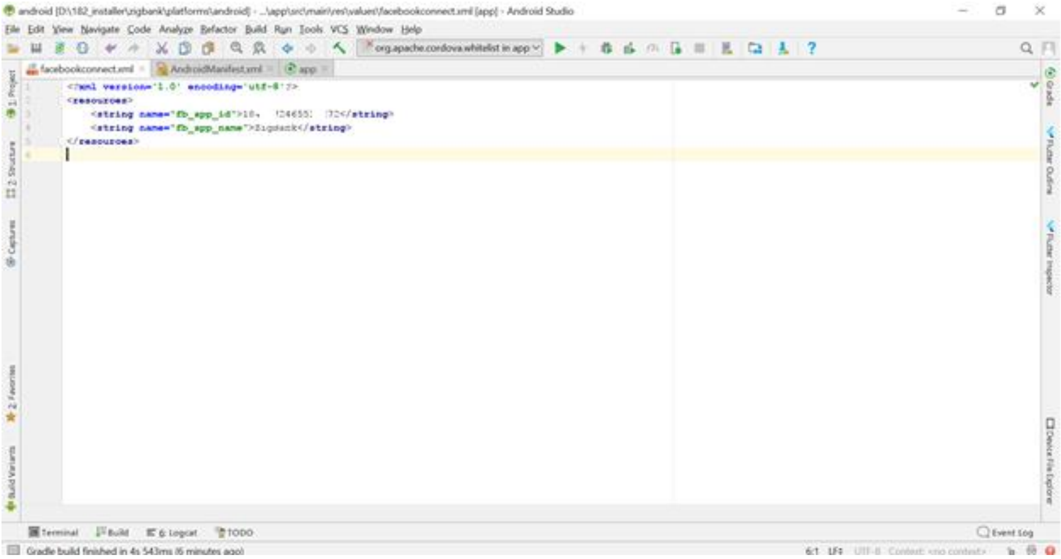
Facebook Analytics

View Your Analytics

Use Analytics to see how people use your app, measure retention, track conversion and optimize for growth.

View Analytics

UNIQUE USERS



android [D:\182_installer\zigbank\platforms\android] - ...\app\src\main\res\values\facebookconnect.xml [app] - Android Studio

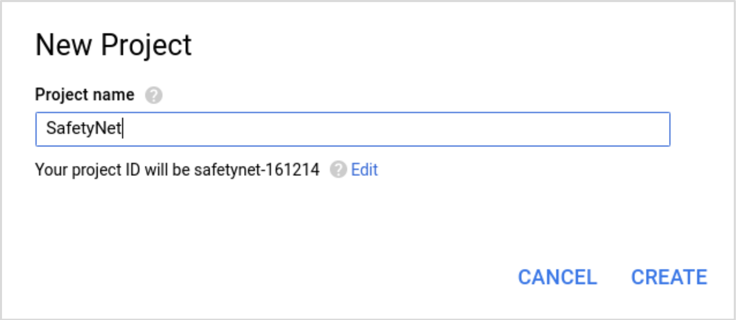
```
<?xml version='1.0' encoding='utf-8'?>
<resources>
    <string name="fb_app_id">[redacted]</string>
    <string name="fb_app_name">Zigbank</string>
</resources>
```

Gradle build finished in 4s 543ms (6 minutes ago)

3. Google Play Integrity

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

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



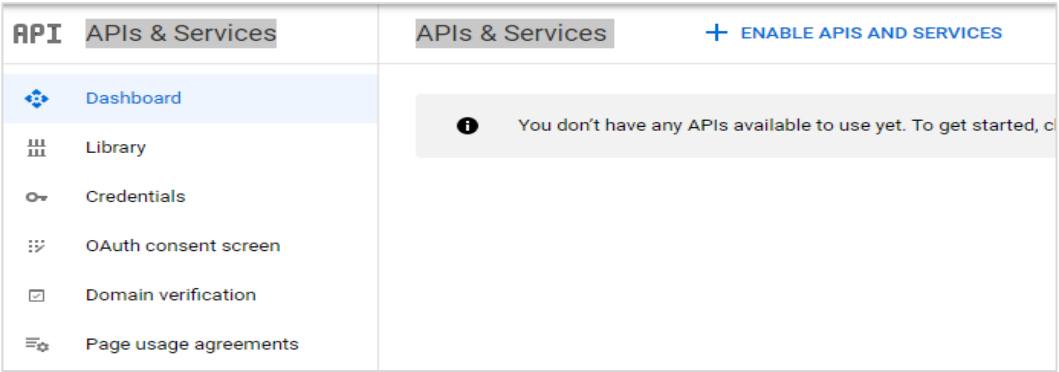
New Project

Project name: SafetyNet

Your project ID will be safetynet-161214

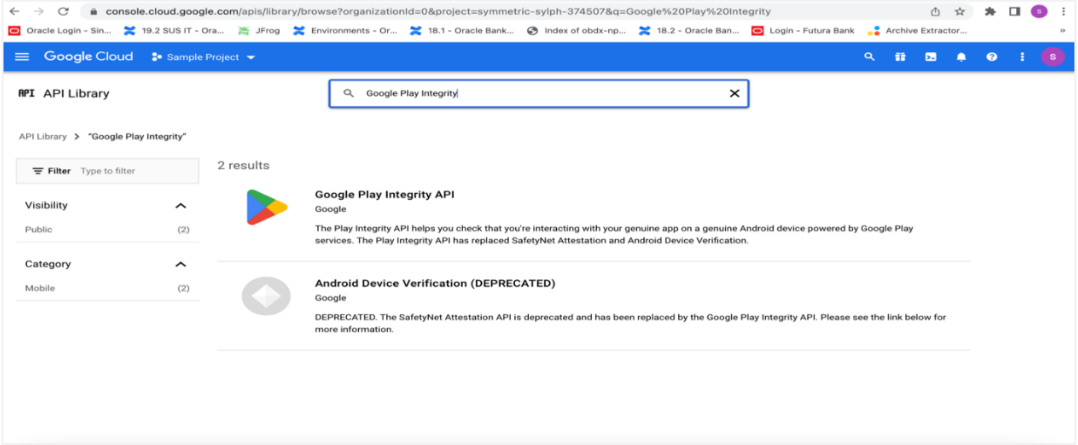
c. Choose **'API's & Services'** option from side bar.

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

Search: Google Play Integrity

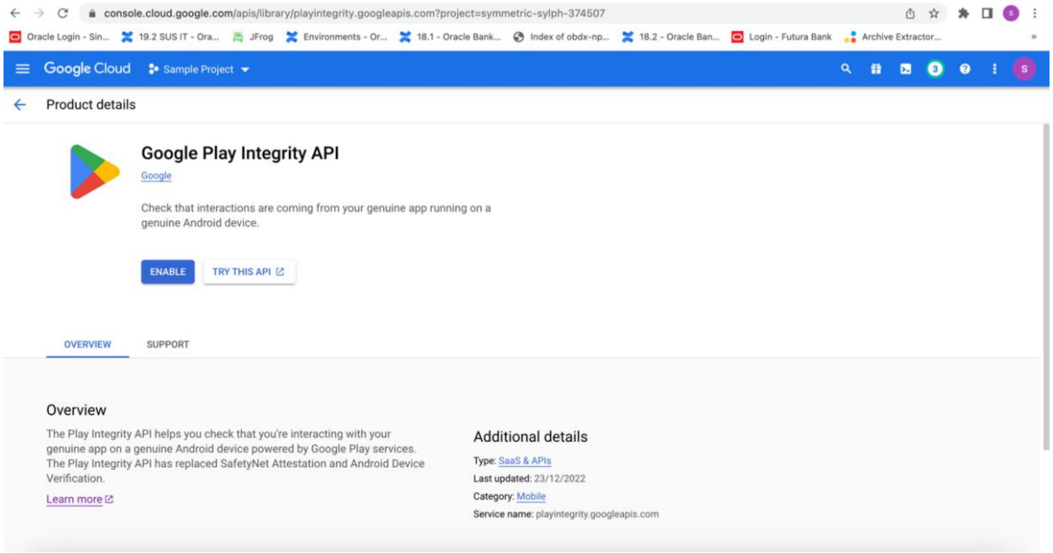
API Library > "Google Play Integrity"

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.



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

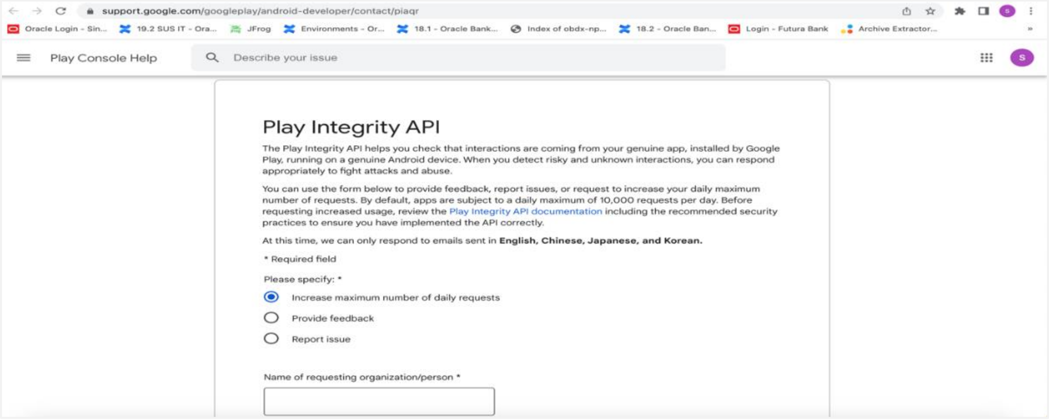
Last updated: 23/12/2022

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



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

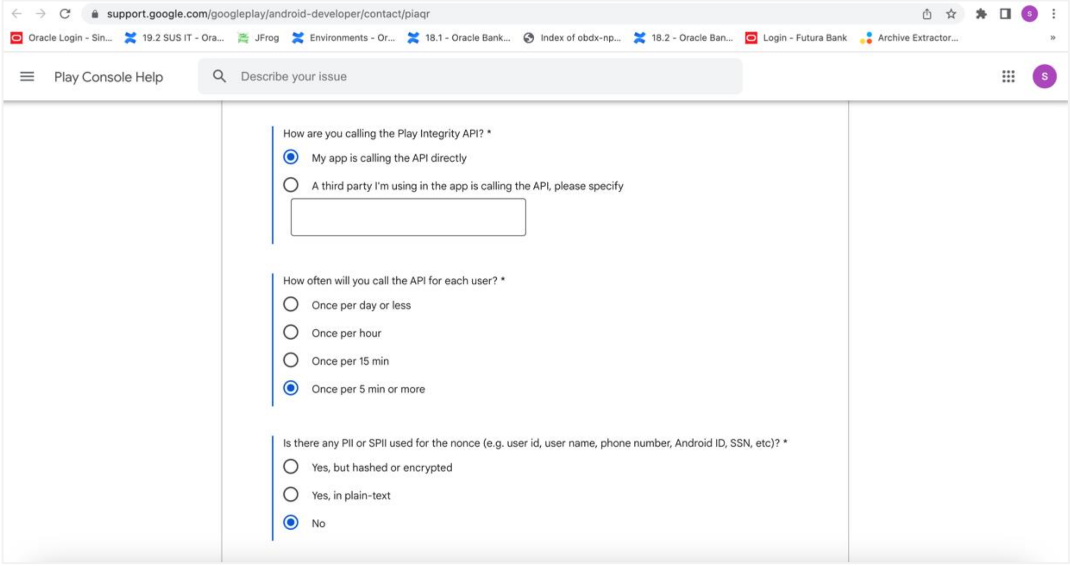
Please specify: *

● Increase maximum number of daily requests

○ Provide feedback

○ Report issue

Name of requesting organization/person *



How are you calling the Play Integrity API? *

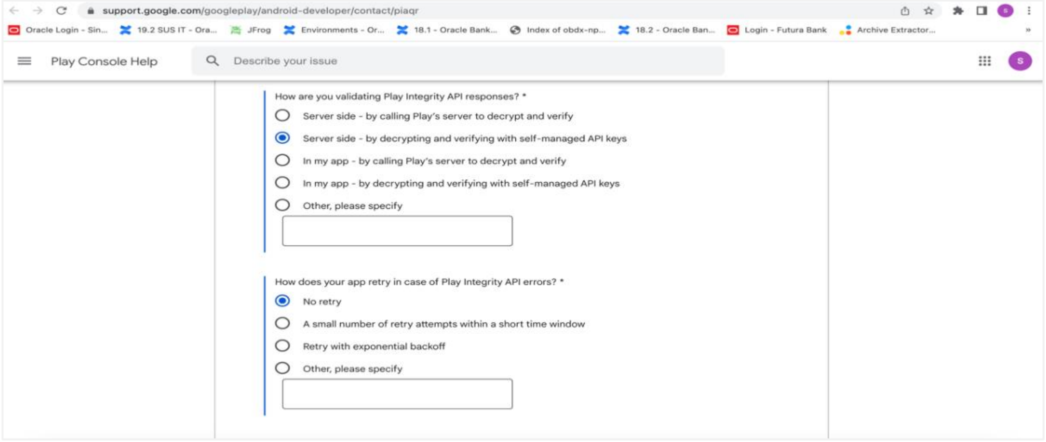
- ● My app is calling the API directly
- ○ A third party I'm using in the app is calling the API, please specify

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

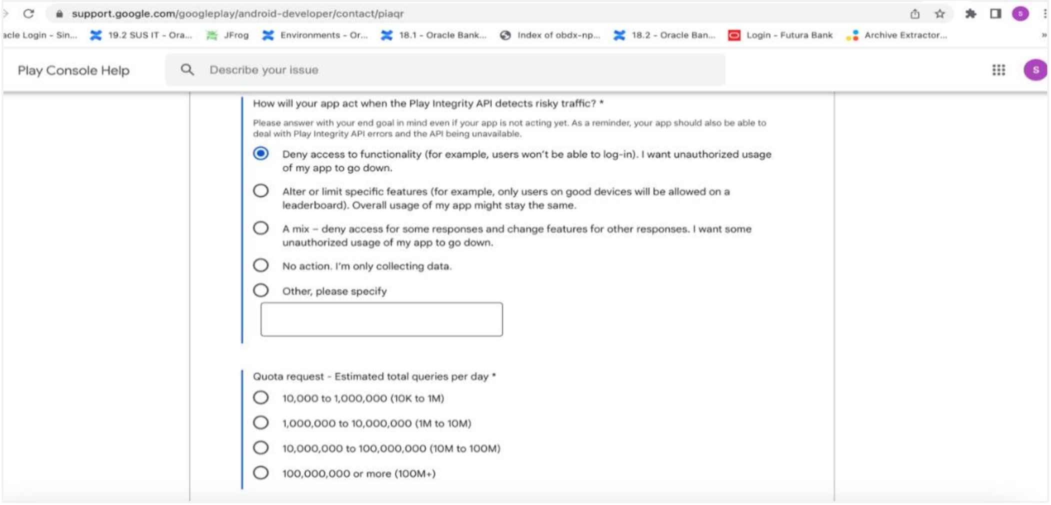


How are you validating Play Integrity API responses? *

- ○ 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 *

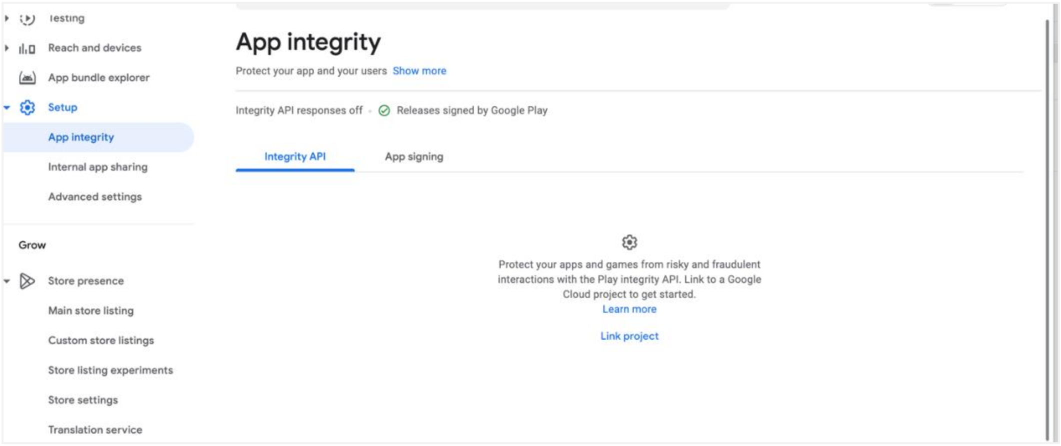
- ○ 10,000 to 1,000,000 (10K to 1M)
- ○ 1,000,000 to 10,000,000 (1M to 10M)
- ○ 10,000,000 to 100,000,000 (10M to 100M)
- ○ 100,000,000 or more (100M+)

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



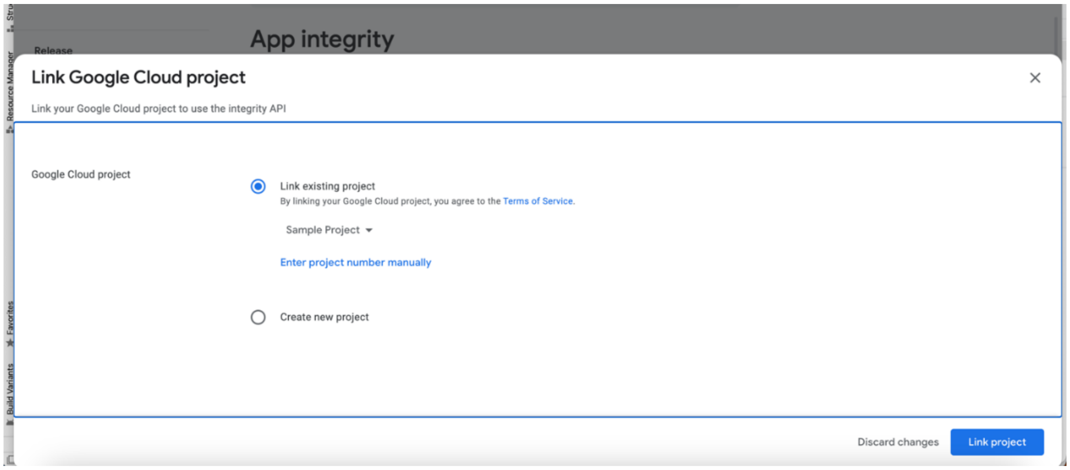
App integrity

Protect your app and your users Show more

Integrity API responses off · Releases signed by Google Play

Protect your apps and games from risky and fraudulent interactions with the Play integrity API. Link to a Google Cloud project to get started.

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



Link Google Cloud project

Link your Google Cloud project to use the integrity API

Google Cloud project

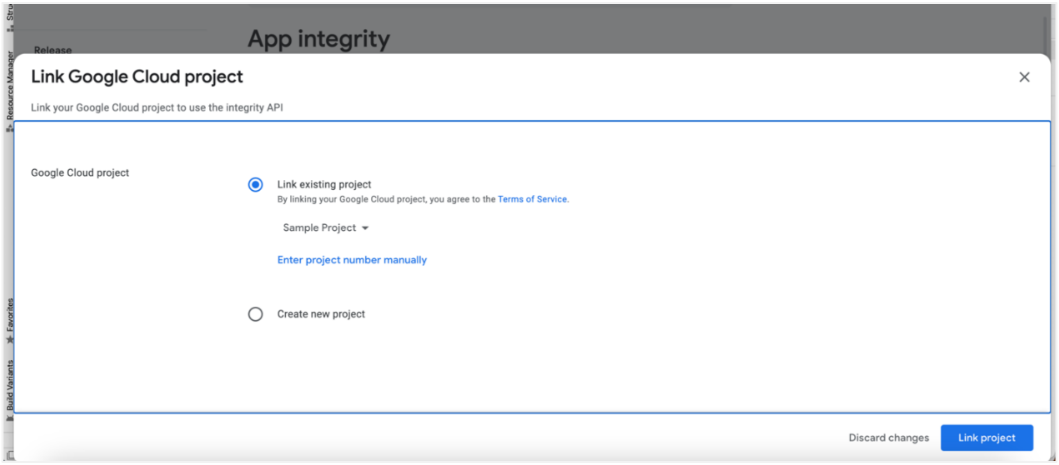
● Link existing project

By linking your Google Cloud project, you agree to the Terms of Service.

Sample Project

Enter project number manually

○ Create new project



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 ▾

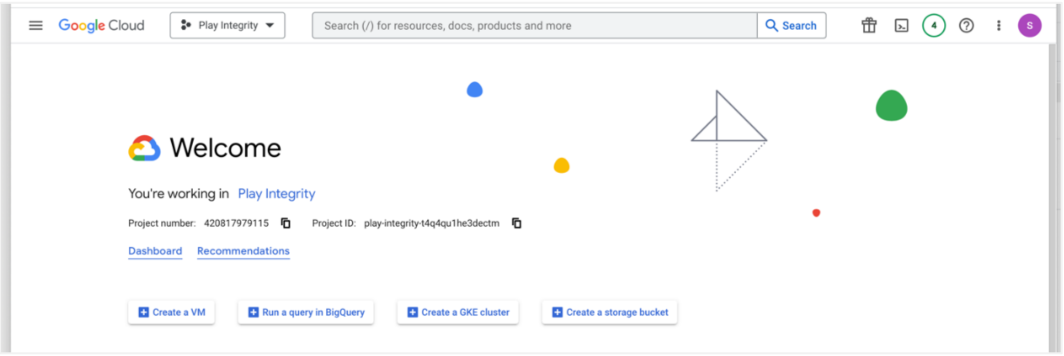
Enter project number manually

○ Create new project

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.



Welcome

You're working in Play Integrity

Project number: 420817979115

Project ID: play-integrity-t4q4qu1he3dectm

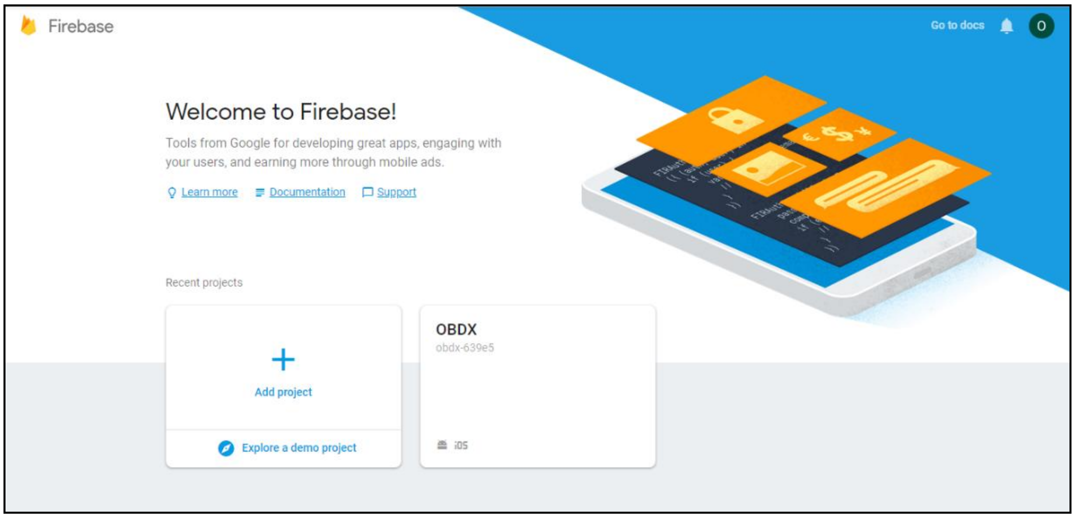
j. Mention the time in seconds to which app can hit the play integrity api. By default it is 300 seconds but you can configure as per the requirement. Please use below property in RootCheckFlags.java(workspace_installer/zigbank/platforms/android/app/src/main/java/com/ofss/digx/mobile/android/)

```
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



Welcome to Firebase!

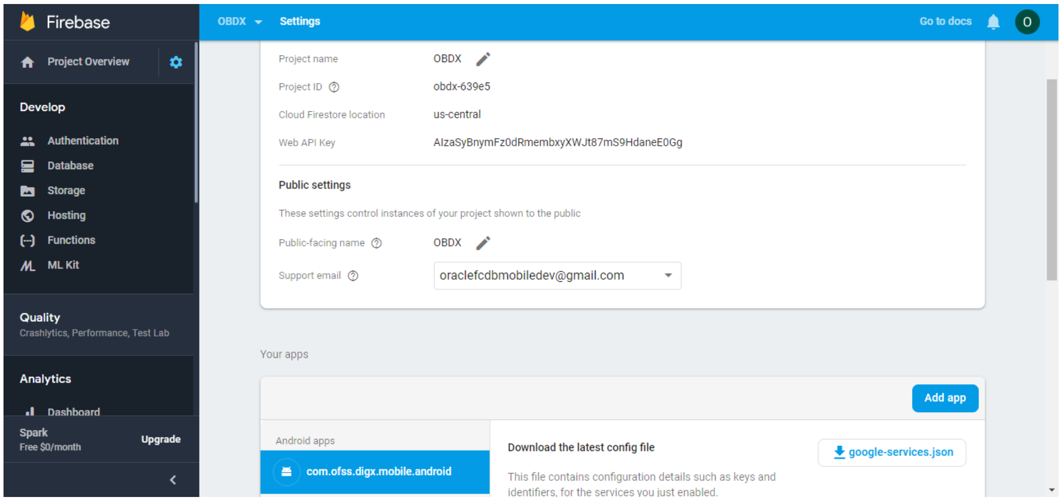
Tools from Google for developing great apps, engaging with your users, and earning more through mobile ads.

Recent projects

OBDX
obdx-639e5

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

Your apps

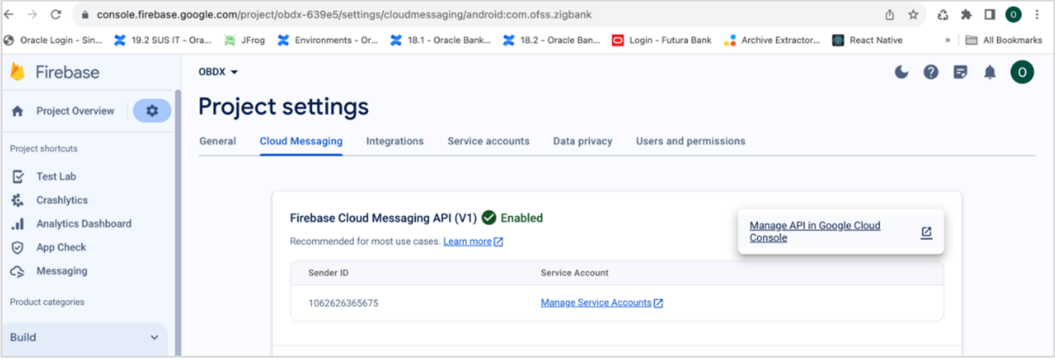
Android apps

com.ofss.digx.mobile.android

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.



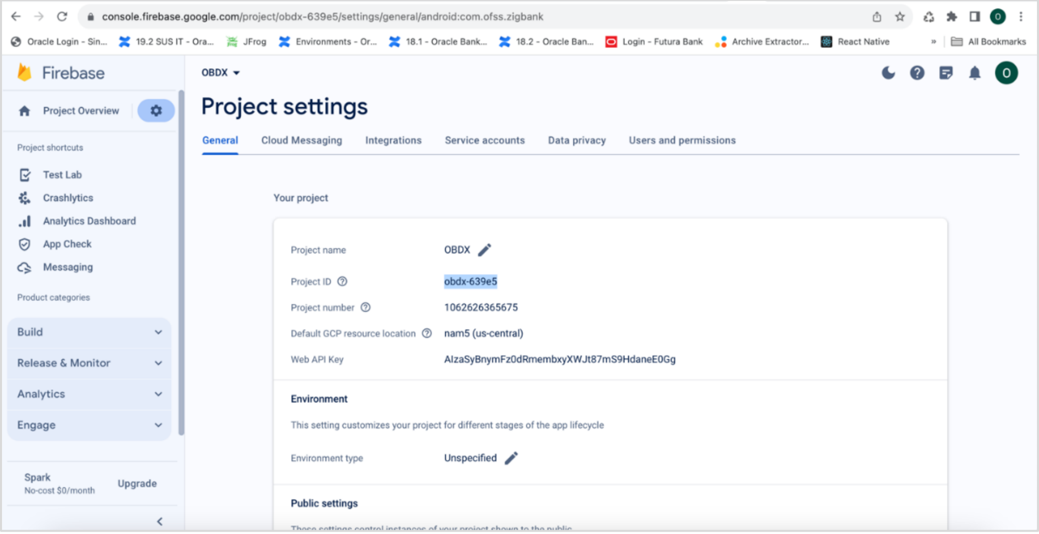
Project settings

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

These settings control instances of your project shown to the public

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**

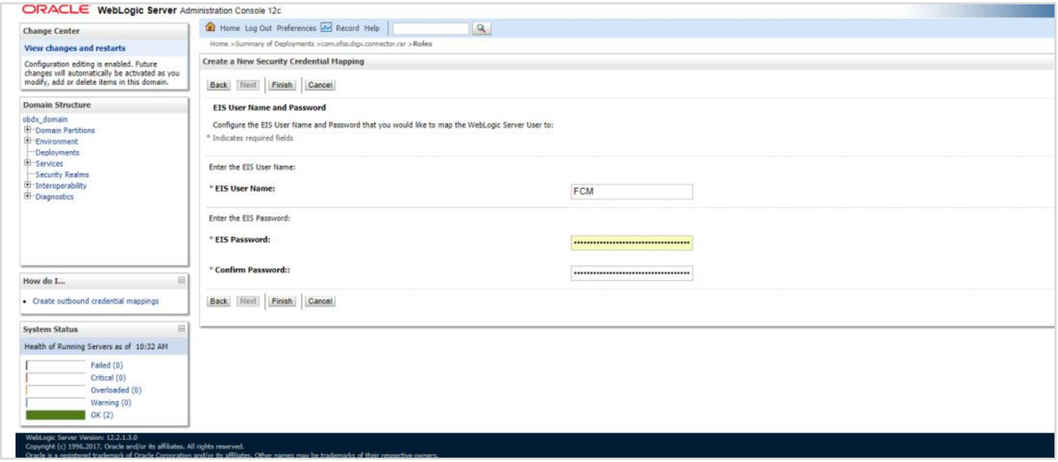
- Click **Generate New Private Key**, then confirm by clicking **Generate Key**

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



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

Health of Running Servers as of 10:32 AM

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: ••••••••••••••••••••••••••••••••••••

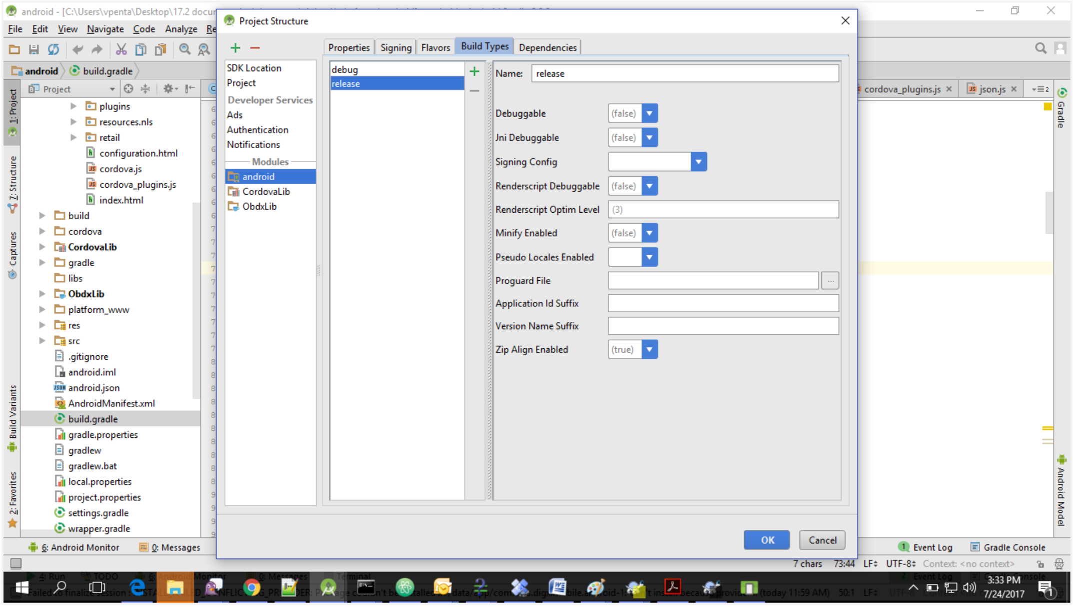
* Confirm Password:: ••••••••••••••••••••••••••••••••••••

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.

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**

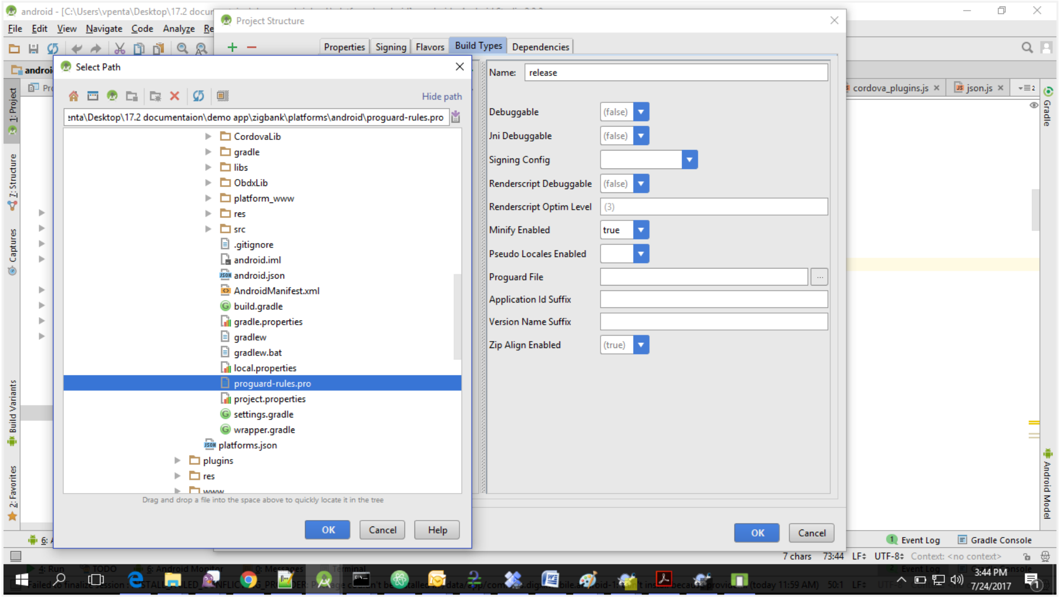


Project Structure — Build Types

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)

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



Select Path: `...nta\Desktop\17.2 documentaion\demo app\zigbank\platforms\android\proguard-rules.pro`

Name	release
Minify Enabled	true

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

SERVER_TYPE	OAUTH3
KEY_SERVER_URL	Eg. http://whf00bpp.in.oracle.com:17778
WEB_URL	Eg. http://whf00bpp.in.oracle:17777
KEY_OAUTH_PROVIDER_URL	E.g.http://whf00ebe.in.oracle.com:15100/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 **Application Security Configuration (For SSL Pinning) section- 7**
REDIRECT_URI	zigbank://oauthredirect

c. IDCS Setup

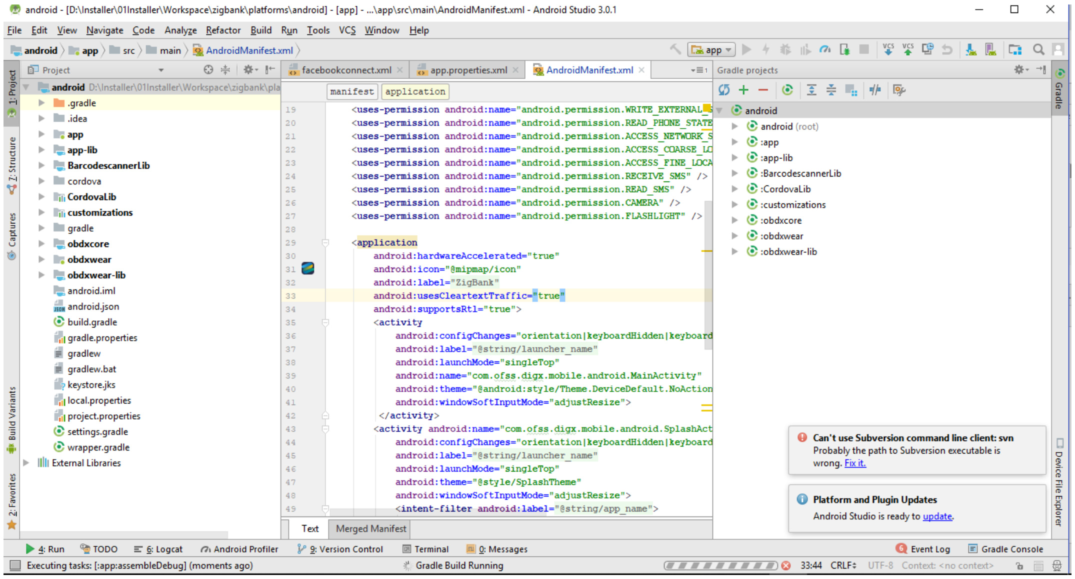
SERVER_TYPE	IDCS
KEY_SERVER_URL	Eg. https://mumaa012.in.oracle.com:18443 (This URL must be of OHS without webgate)
WEB_URL	Eg. https://mumaa012.in.oracle.com:18443
KEY_OAUTH_PROVIDER_UR	http://obdx-tenant01.identity.c9dev0.oc9qadev.com/oauth2/v1/toke

L	n
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. Adding chatbot support to mobile application (Optional)

CHATBOT_ID	The tenant ID
CHATBOT_URL	The web socket URL for the ChatApp application in IBCS

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



```
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_S
    <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">
```

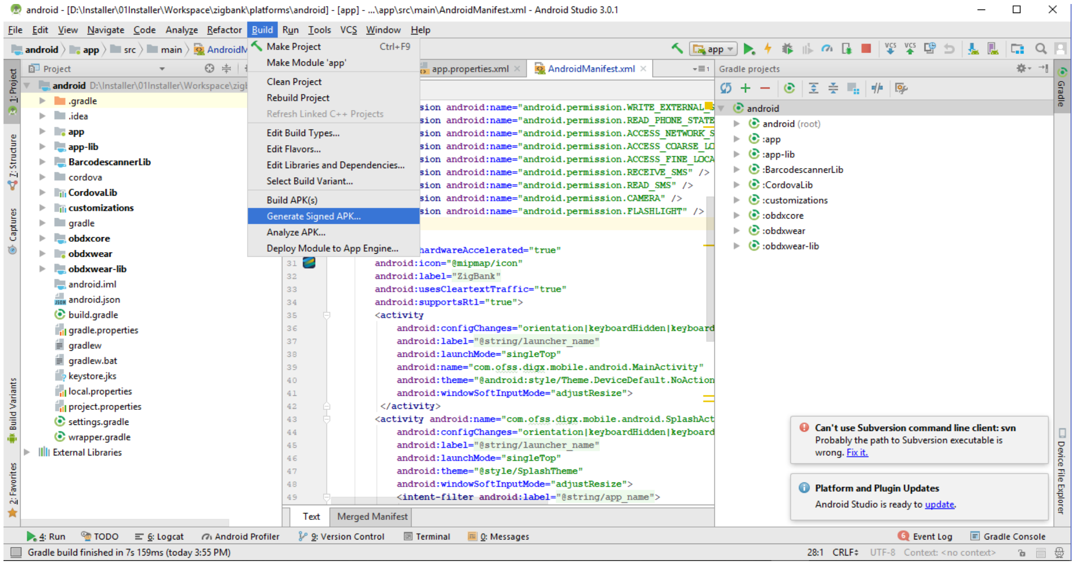
Can't use Subversion command line client: svn
Probably the path to Subversion executable is wrong. Fix it.

Platform and Plugin Updates
Android Studio is ready to update.

Executing tasks: [:app:assembleDebug] (moments ago)

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

On menu bar click on Build -> Generate Signed Apk

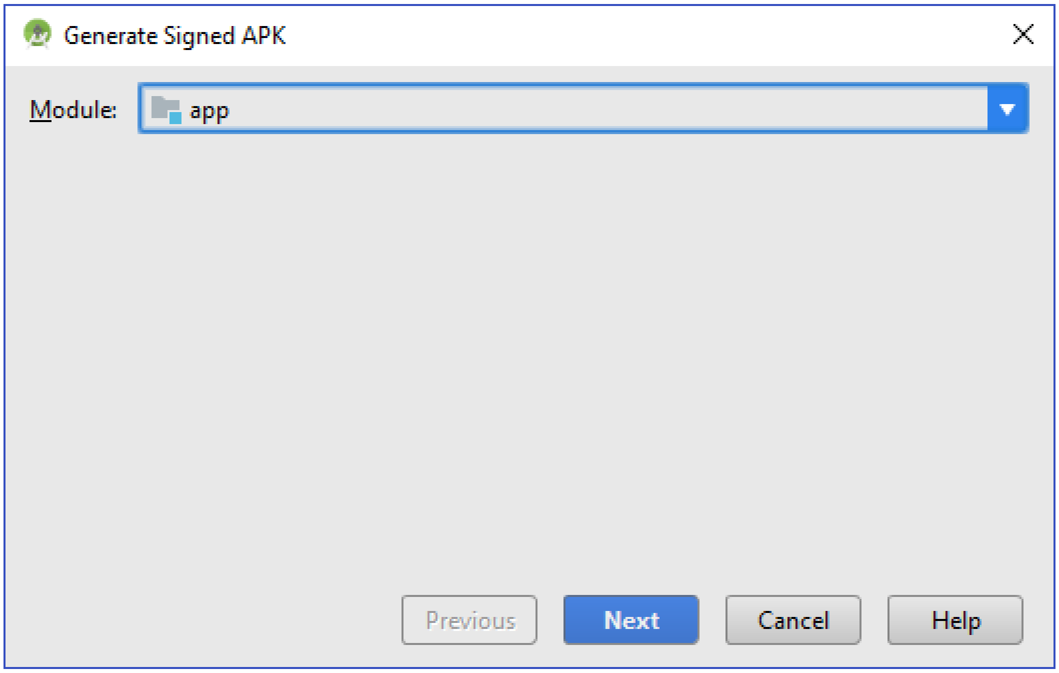


```
sion android:name="android.permission.WRITE_EXTERNAL_
sion android:name="android.permission.READ_PHONE_STATE
sion android:name="android.permission.ACCESS_NETWORK_S
sion android:name="android.permission.ACCESS_COARSE_LO
sion android:name="android.permission.ACCESS_FINE_LOCA
sion android:name="android.permission.RECEIVE_SMS"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

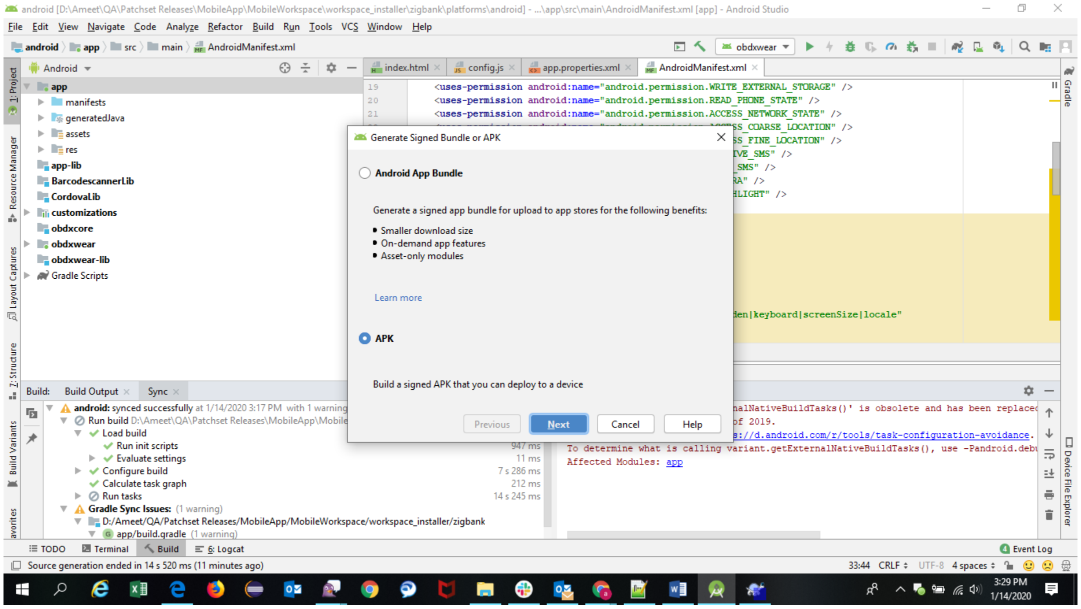
Can't use Subversion command line client: svn
Probably the path to Subversion executable is wrong. Fix it.

Platform and Plugin Updates
Android Studio is ready to update.

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



Module: app



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

Generate Signed Bundle or APK

○ **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

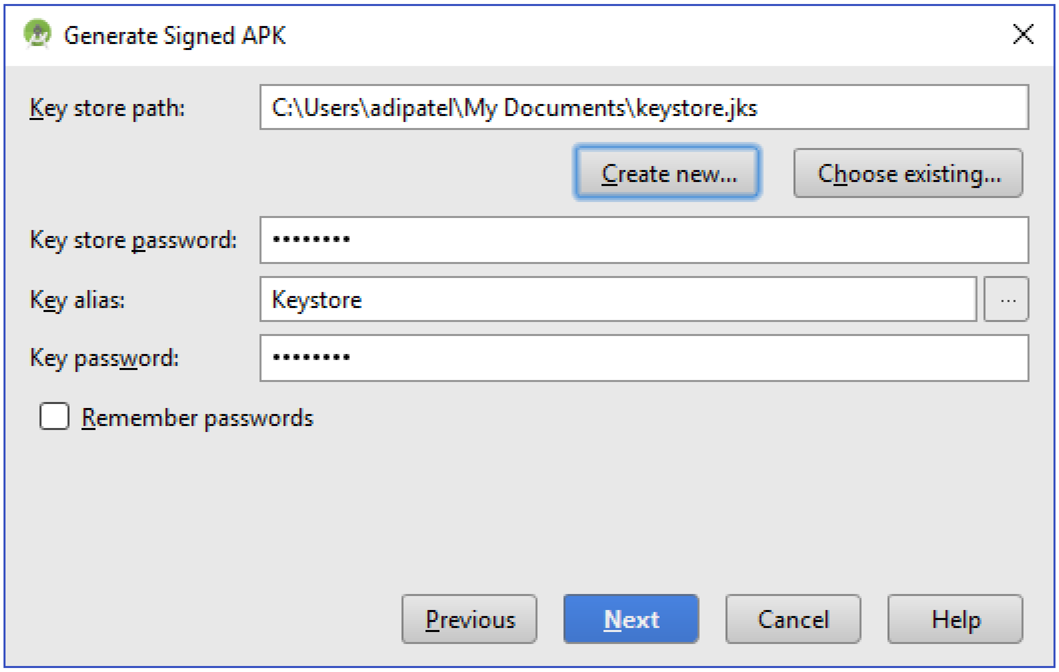
● **APK**

Build a signed APK that you can deploy to a device

```
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)
```

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

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



Generate Signed APK

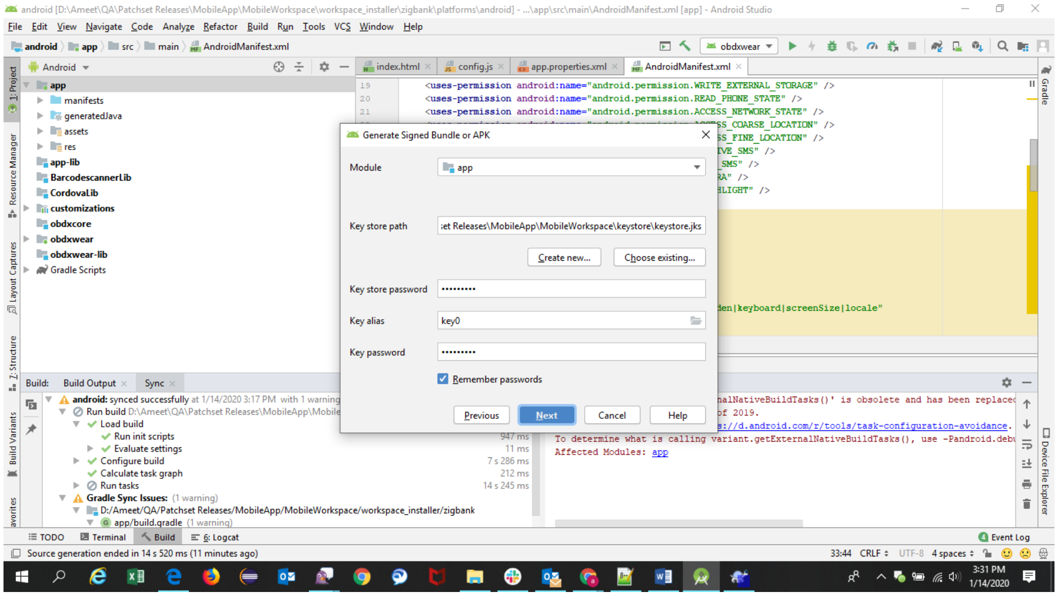
Key store path: C:\Users\adipatel\My Documents\keystore.jks

Key store password: ••••••••

Key alias: Keystore

Key password: ••••••••

□ Remember passwords



Generate Signed Bundle or APK

Module: app

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

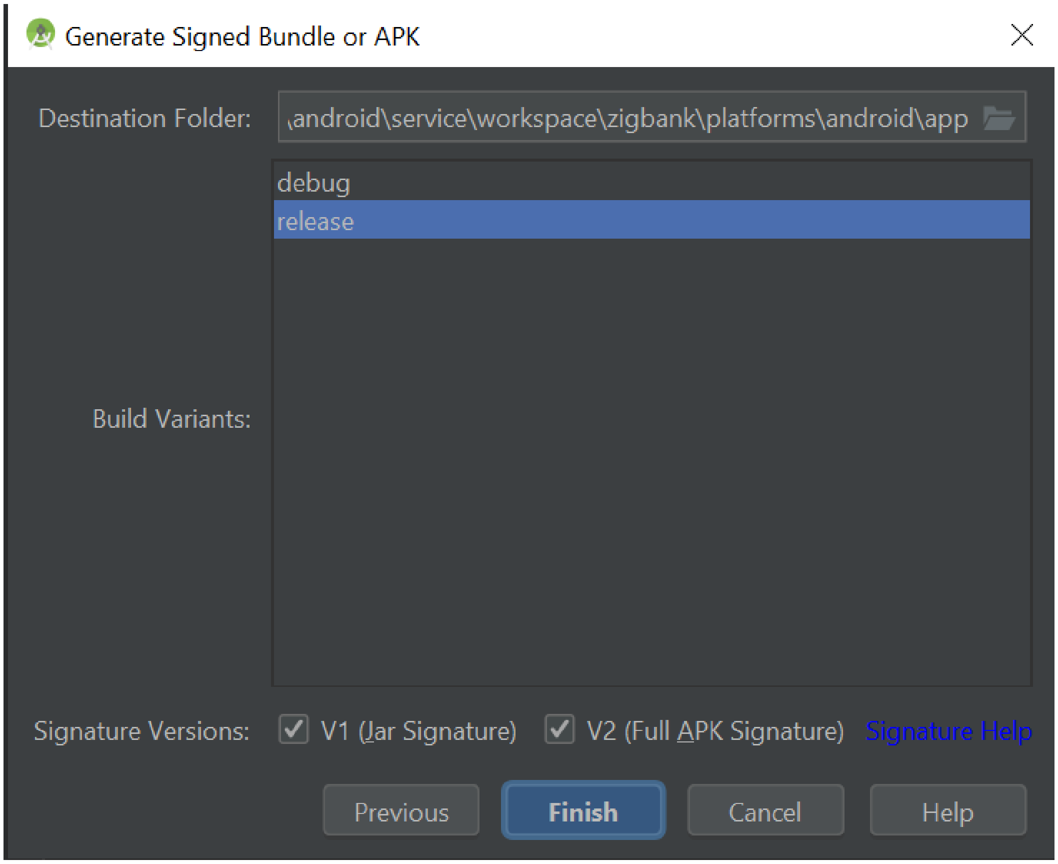
Key store password: ••••••••••

Key alias: key0

Key password: ••••••••••

☑ Remember passwords

10. 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



Generate Signed Bundle or APK

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

Build Variants:
debug
release

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

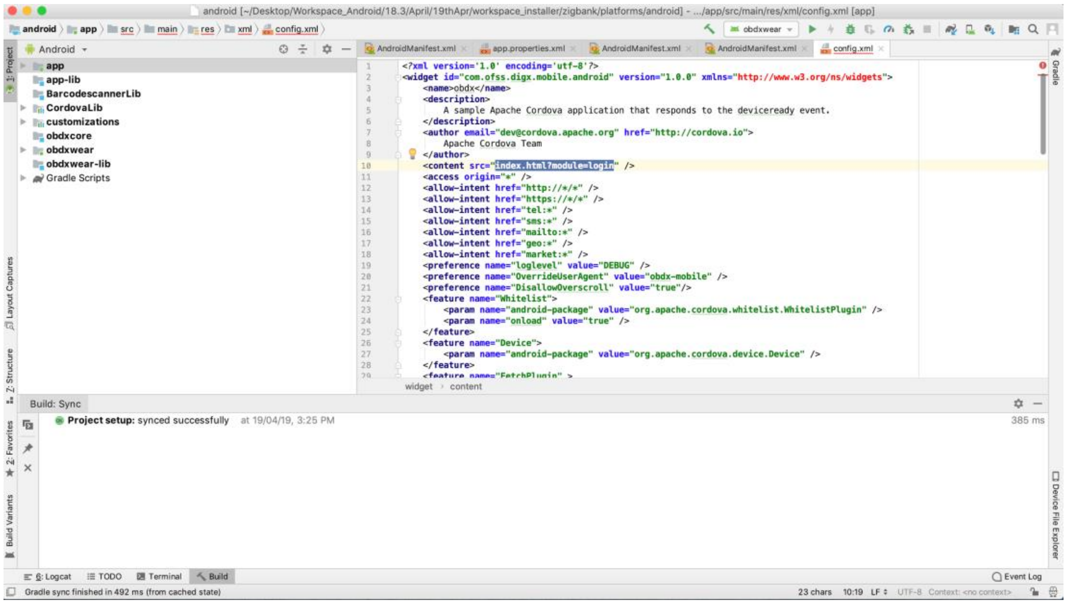
11. This will generate APK by the given name and destination folder. Default APK Destination folder is **zigbank\platforms\android\app\release**

12. Run the App and select Device or Simulator.

13. **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.

14. 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>
    <feature name="FetchPlugin" >
```

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

Gradle sync finished in 492 ms (from cached state)

15. 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 replace below code block 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>
```

With below one as,

```
<IfModule mod_headers.c>
```

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

        Header edit Set-Cookie "SameSite=Strict" ""

    </If>

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

        Header edit Set-Cookie "SameSite=Strict" ""

    </If>

</IfModule>
```

Note: We strongly recommend you to use https setup with sdk 31 only, as google play store won’t allow app’s   below sdk 31.

6. OBDX Authenticator Application

6.1 Authenticator UI (Follow any one step below)

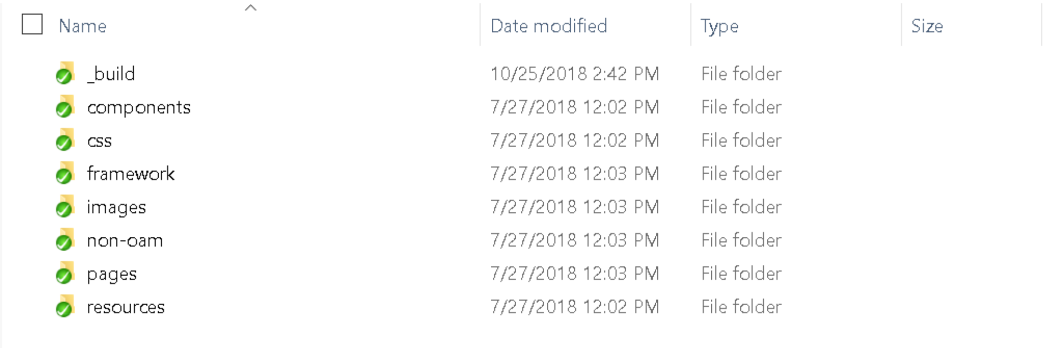
6.1.1 Using built UI

For Non-OAM - Unzip dist.tar.gz directory from OBDX_Patch_Mobile\authenticator\non-oam

For OAM - Unzip dist.tar.gz directory from OBDX_Patch_Mobile\authenticator\oam

6.1.2 Building UI manually

1. Extract authenticator_ui.tar.gz from OBDX_Patch_Mobile\authenticator\unbuilt_ui. The folder structure is as shown:



□ Name	Date modified	Type	Size
_build	10/25/2018 2:42 PM	File folder	
components	7/27/2018 12:02 PM	File folder	
css	7/27/2018 12:02 PM	File folder	
framework	7/27/2018 12:03 PM	File folder	
images	7/27/2018 12:03 PM	File folder	
non-oam	7/27/2018 12:03 PM	File folder	
pages	7/27/2018 12:03 PM	File folder	
resources	7/27/2018 12:02 PM	File folder	

2. Build UI based on selected Authentication mechanism.

a. OAM based Authentication

- Open command prompt at "_build" level.
- Run following command :

```
npm install -g grunt-cli

npm install

node render-requirejs/render-requirejs.js

grunt authenticator --verbose
```

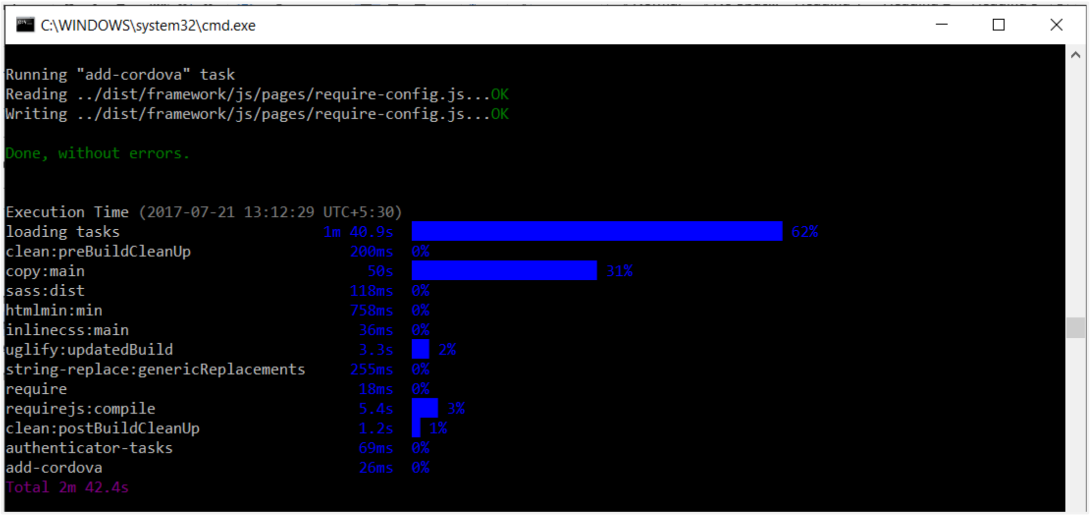
- After running above commands and getting result as "Done, without errors." a new folder will be created in "ui" with name as "dist".

b. NON-OAM Based Authentication

- Copy "non-oam /login" folder and paste it at location "components/modules" location. This will replace existing "login" folder.
- Open command prompt at "_build" level.
- Run following command :

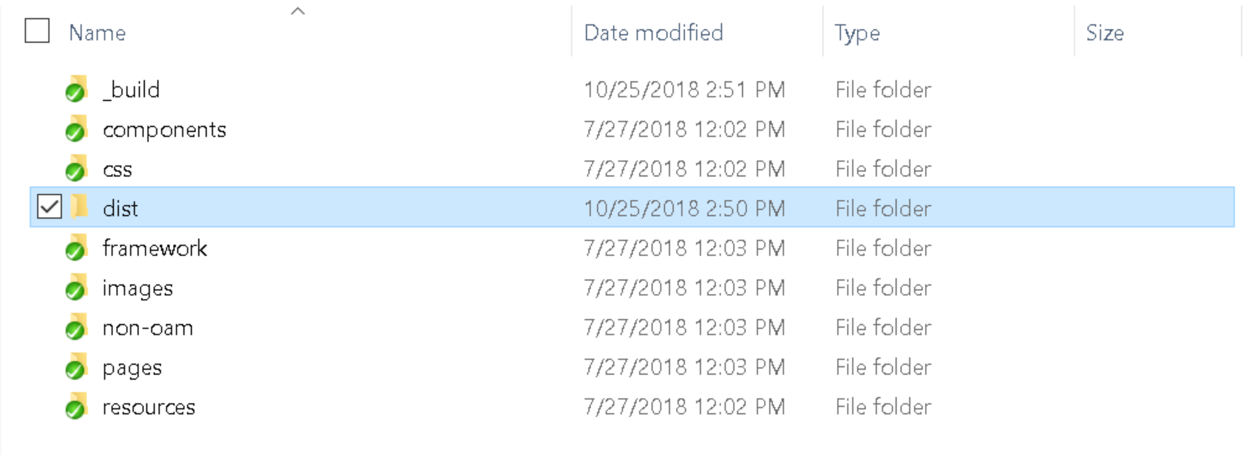
```
npm install -g grunt-cli

npm install

node render-requirejs/render-requirejs.js

grunt authenticator --verbose
```

- After running above commands and getting result as “Done, without errors.” a new folder will be created in “ui” folder with name as “dist”.



C:\WINDOWS\system32\cmd.exe

```
Running "add-cordova" task
Reading ../dist/framework/js/pages/require-config.js...OK
Writing ../dist/framework/js/pages/require-config.js...OK

Done, without errors.


Execution Time (2017-07-21 13:12:29 UTC+5:30)
loading tasks                         1m 40.9s                                           62%
clean:preBuildCleanUp                    200ms  0%
copy:main                                  50s                      31%
sass:dist                                118ms  0%
htmlmin:min                              758ms  0%
inlinecss:main                            36ms  0%
uglify:updatedBuild                       3.3s    2%
string-replace:genericReplacements       255ms  0%
require                                   18ms  0%
requirejs:compile                         5.4s     3%
clean:postBuildCleanUp                    1.2s   1%
authenticator-tasks                       69ms  0%
add-cordova                               26ms  0%
Total 2m 42.4s
```

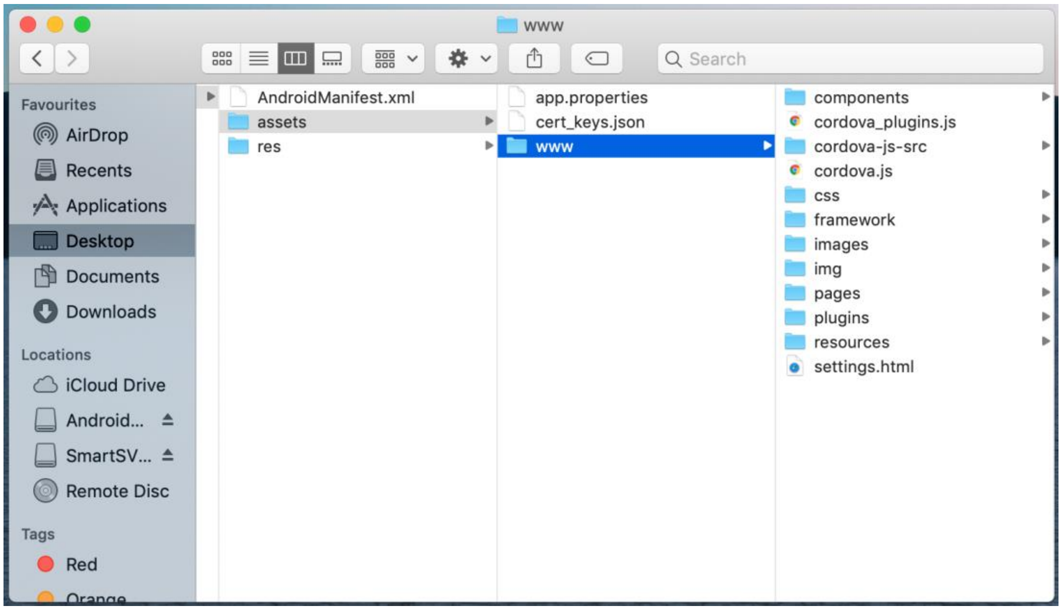


□ Name	Date modified	Type	Size
_build	10/25/2018 2:51 PM	File folder	
components	7/27/2018 12:02 PM	File folder	
css	7/27/2018 12:02 PM	File folder	
☑ dist	10/25/2018 2:50 PM	File folder	
framework	7/27/2018 12:03 PM	File folder	
images	7/27/2018 12:03 PM	File folder	
non-oam	7/27/2018 12:03 PM	File folder	
pages	7/27/2018 12:03 PM	File folder	
resources	7/27/2018 12:02 PM	File folder	

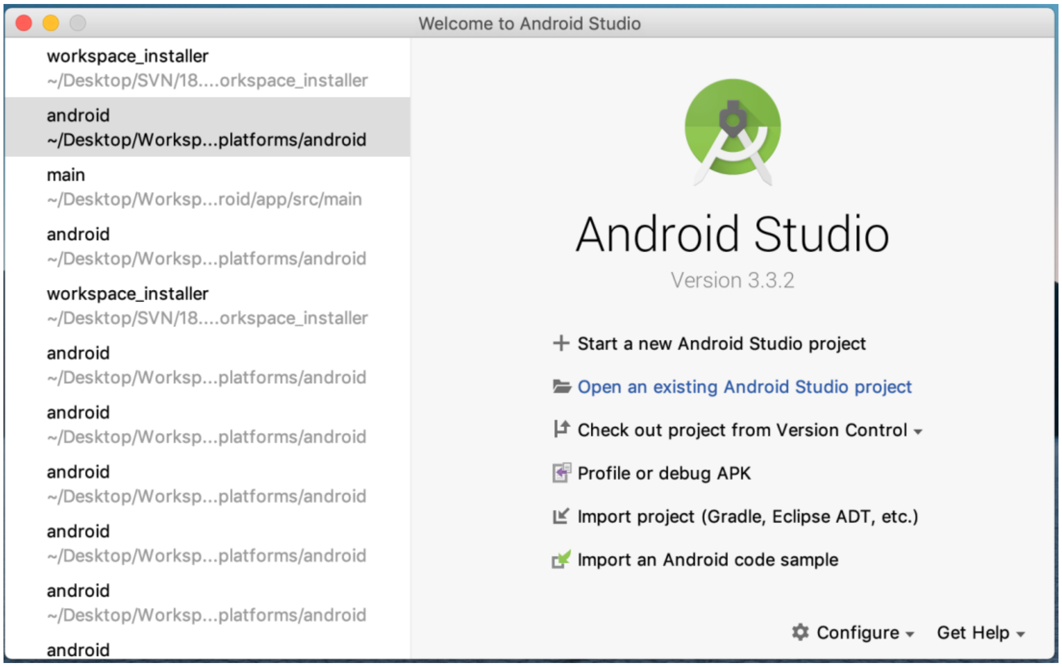
6.2 Authenticator Application Workspace Setup

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

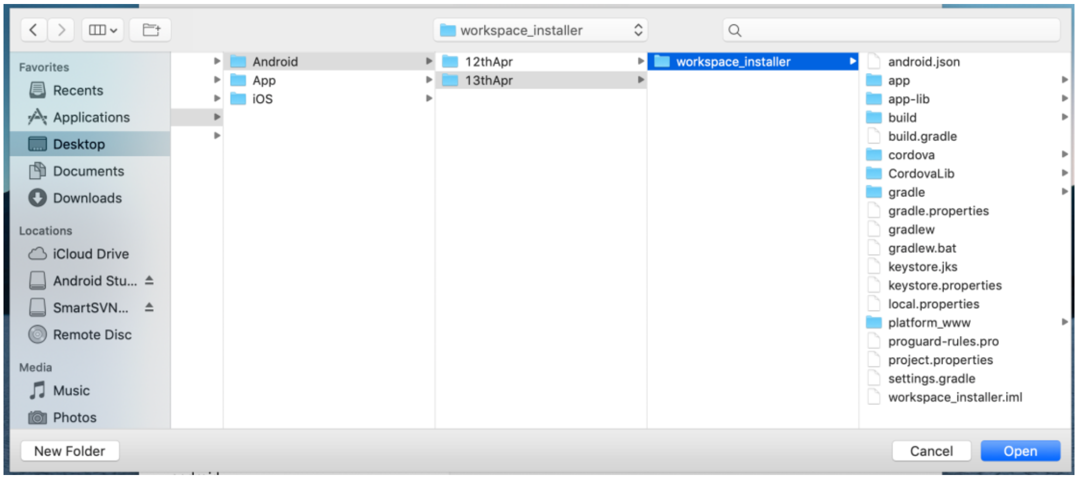
   In case any popup appears, click replace



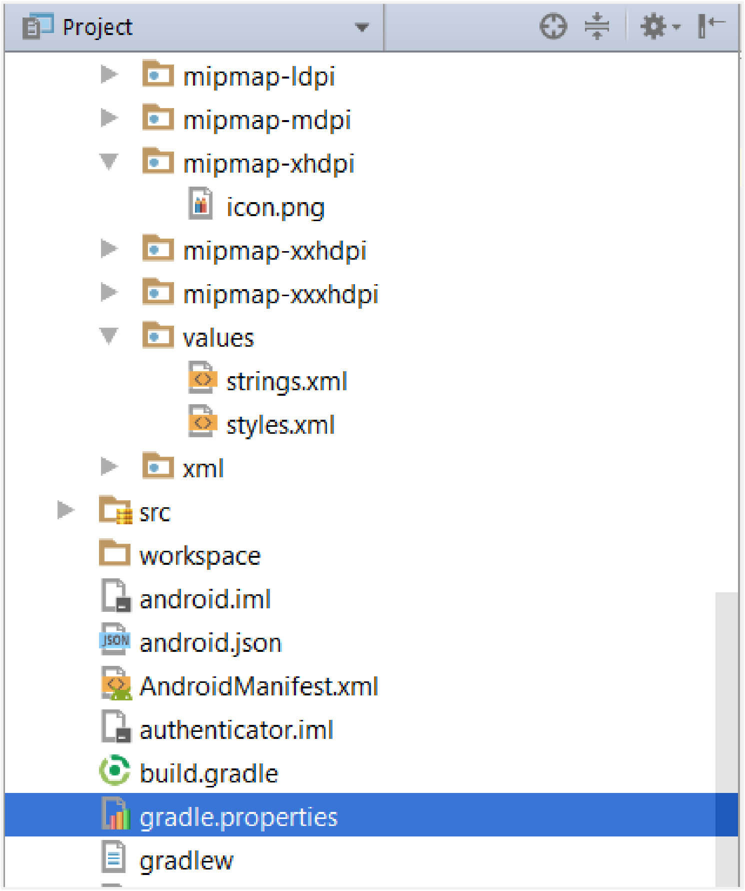
2. Launch Android Studio and open existing project


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.

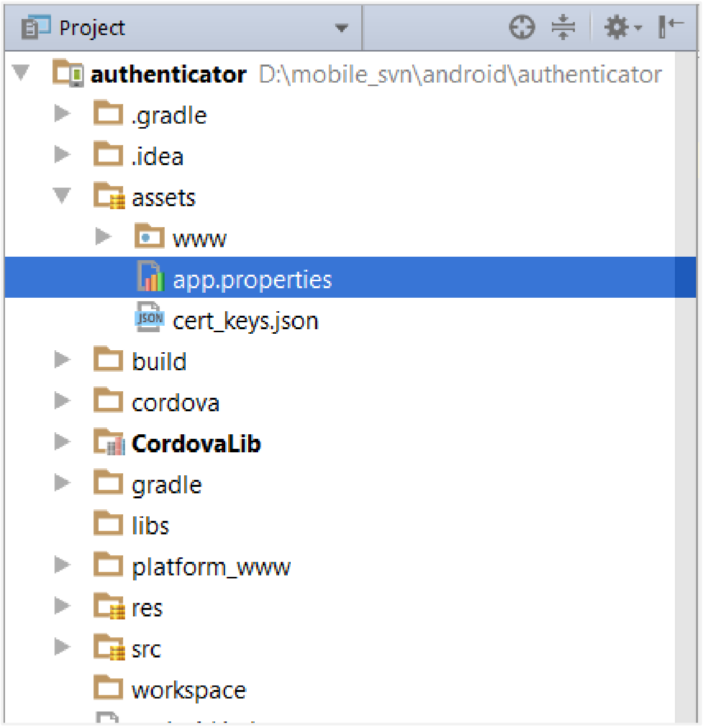


4. Open gradle.properties file and update following properties with relevant proxy address if required

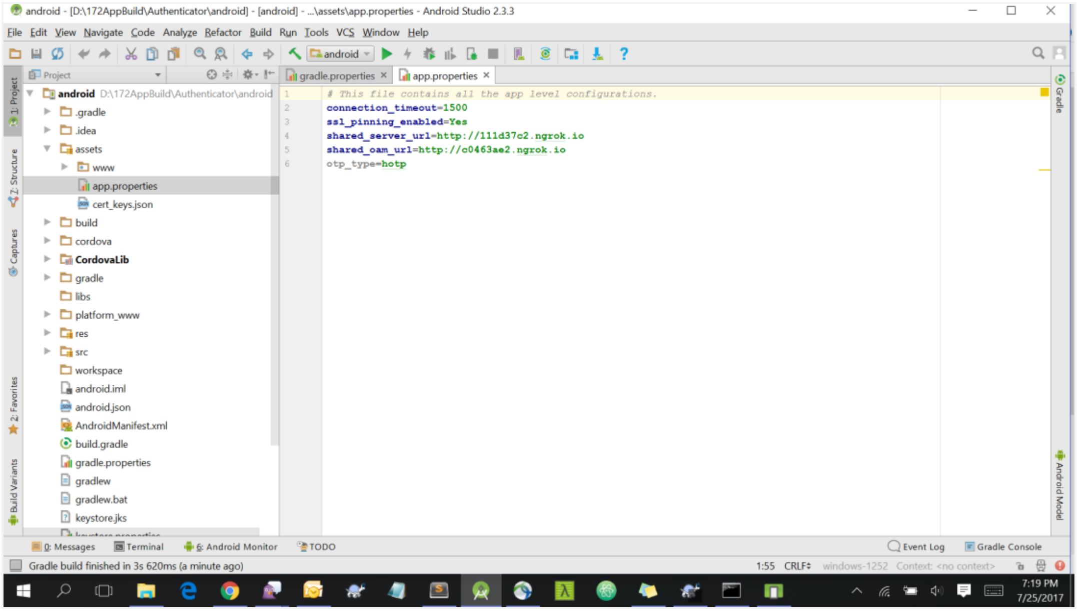


```
systemProp.http.proxyHost = <proxy_address>
systemProp.https.proxyPort = <port_number>
systemProp.https.proxyHost = <proxy_address>
systemProp.http.proxyPort = <port_number>
android.enableJetifier=true
android.useAndroidX=true
```

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



```
connection_timeout = <timeout_in_milliseconds>
ssl_pinning_enabled = <YES or NO>
shared_server_url = <server_url>
shared_oam_url = <oam_url>
otp_type = <HOTP or TOTP>
```



```
# This file contains all the app level configurations.
connection_timeout=1500
ssl_pinning_enabled=Yes
shared_server_url=http://111d37c2.ngrok.io
shared_oam_url=http://c0463ae2.ngrok.io
otp_type=hotp
```

Gradle build finished in 3s 620ms (a minute ago)

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.

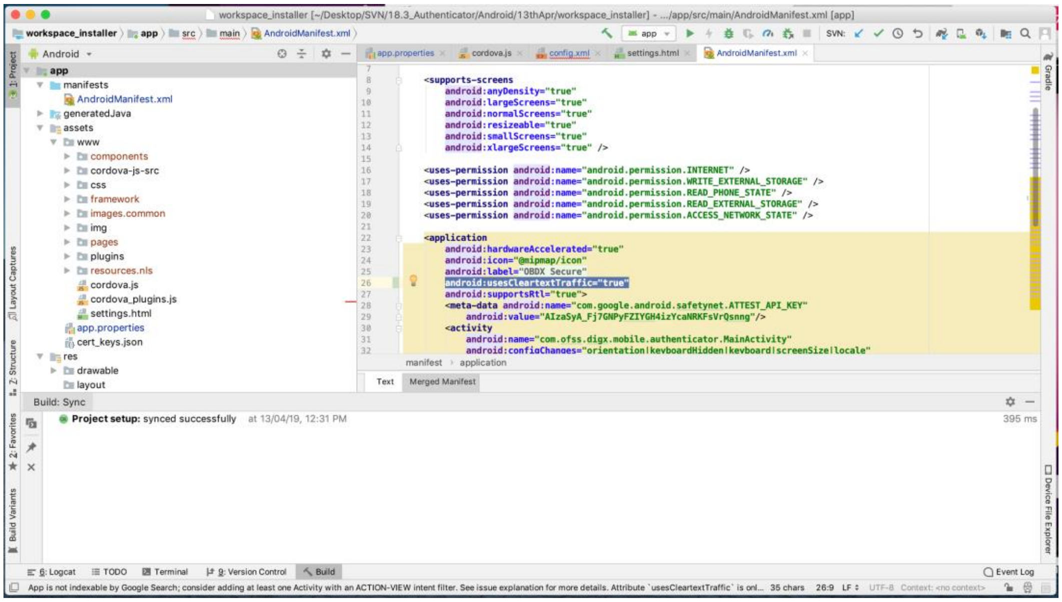
7. Click on Build → Edit Build Type → app → release

   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



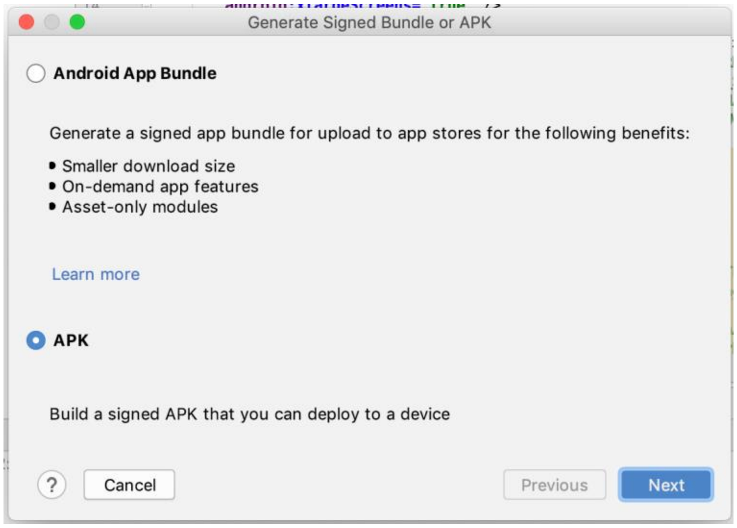
```
    <supports-screens
        android:anyDensity="true"
        android:largeScreens="true"
        android:normalScreens="true"
        android:resizeable="true"
        android:smallScreens="true"
        android:xlargeScreens="true" />

    <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...

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

   On menu bar click on Build -> Generate Signed Apk



Generate Signed Bundle or APK

○ **Android App Bundle**

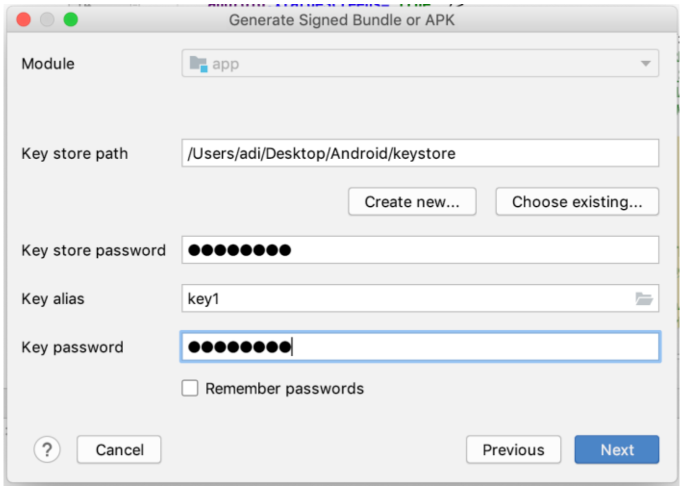
Generate a signed app bundle for upload to app stores for the following benefits:

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

Learn more

● **APK**

Build a signed APK that you can deploy to a device



Generate Signed Bundle or APK

Module: app

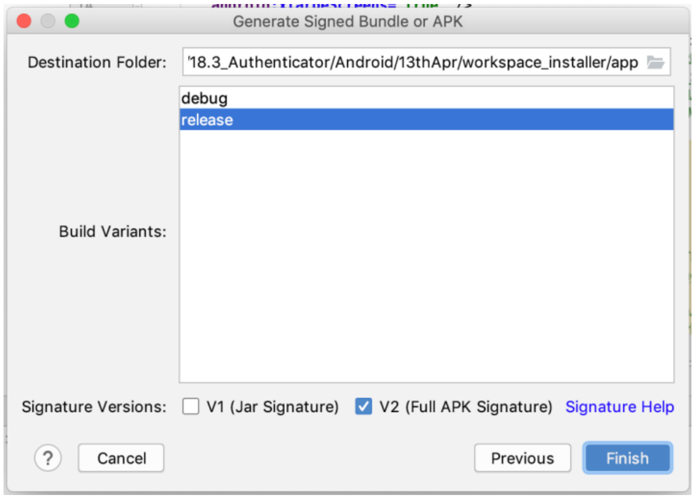
Key store path: /Users/adi/Desktop/Android/keystore

Key store password: ●●●●●●●●

Key alias: key1

Key password: ●●●●●●●●

□ Remember passwords



Generate Signed Bundle or APK

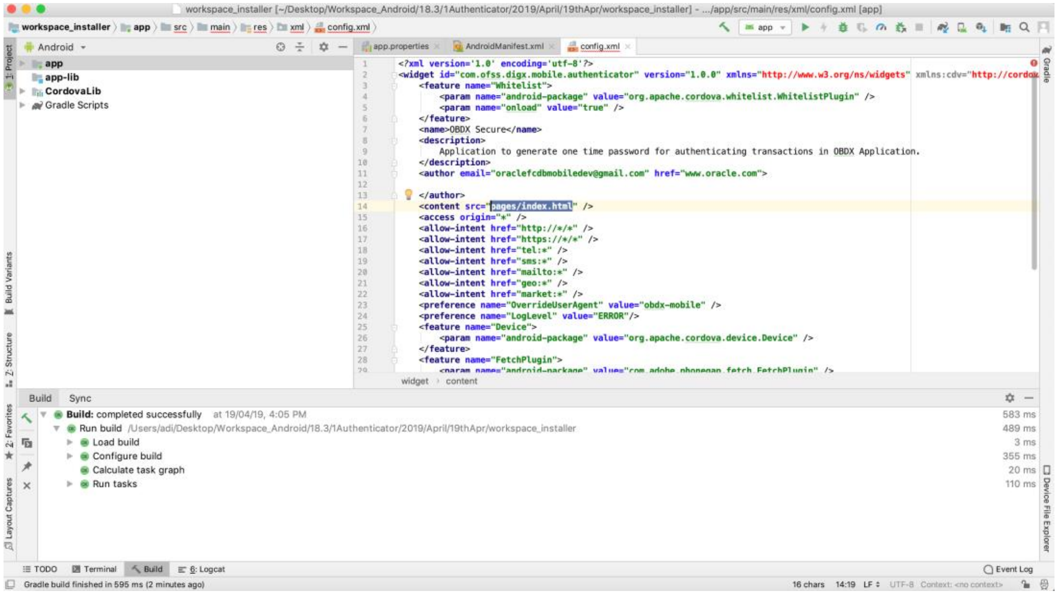
Destination Folder: '18.3_Authenticator/Android/13thApr/workspace_installer/app

Build Variants: debug, release (selected)

Signature Versions: □ V1 (Jar Signature) ☑ V2 (Full APK Signature) Signature Help

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 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)

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';

1. 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>
```