

Setting up Google Play Developer API Access

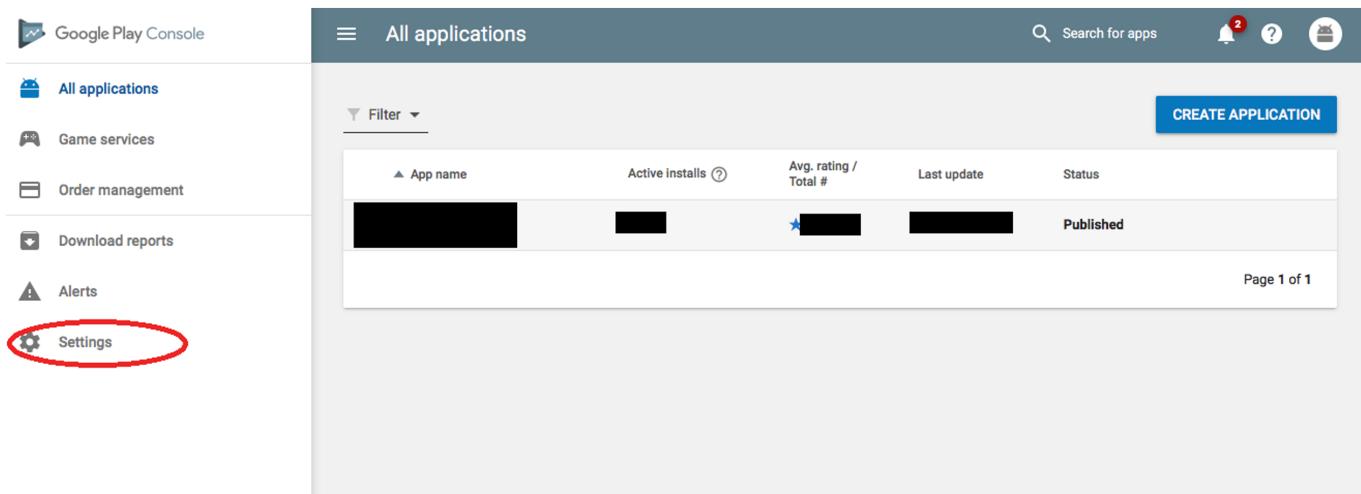
Setting up Google Play Developer API Access

Modified on: Wednesday, 20 Feb, 2019 at 3:41 PM

In order to publish and update your Android branded app, we need access to your Play Store account via the Google Play Developer API. This access must be granted via your Google developer account, as well as on the Google Play Console. **If possible, simply provide our support team with the login details for your Google developer account and we'll set this up for you.** No need to read further in that case :) However, if you cannot provide us with these login details - e.g., because of corporate policy or two-factor authorization being enabled - then you must follow the steps below to grant us the required access.

Please note that while we have tried to make the screenshots and instructions as generic as possible, what you actually see in your browser may be slightly different because of settings and other projects that may be in your Google account.

1. Open a web browser and navigate to the following URL: <http://play.google.com/apps/publish>
2. Log in with your Google developer account credentials
3. Once logged in, you should see the following page. Click on “Settings” in the left-hand side menu.



4. In the Account Details area, click on “API access” in the left-hand side menu.

Google Play Console

Account details

Developer Profile

Developer name *

Physical address

Email address *

The developer name is displayed to users under your application name. Changes to the developer name will be reviewed by Google and can take up to 7 days.

Fields marked with * need to be filled before saving.

11/50

API access

Linked accounts

Payments settings

Developer page

Manage testers

Preferences

5. In the API access page, click on “**CREATE SERVICE ACCOUNT**.” Please note that this page may look slightly different based on what has been set up in your Google account to date.

Google Play Console

All applications

Developer account

Account details

Users & permissions

Activity log

API access

Linked accounts

Payments settings

Developer page

Manage testers

Preferences

API access

Note on security

API users have access to perform actions similar to those available through this console. Your API credentials should be kept secure at all times and managed with the same care as other Google Play Console access credentials. Users' permissions as configured in 'User Accounts & Rights' also apply to API requests.

Linked Project

Google Play Android Developer UNLINK

Games Services Publishing API ON

OAuth Clients

An OAuth client is required to build interactive apps where users can log in and perform publishing actions using their own credentials. API actions will be attributed to the user. Users' permissions are configured through the 'User Accounts & Rights' page.

There are no OAuth clients associated with your project.

CREATE OAUTH CLIENT

Service Accounts

Service accounts allow access to the Google Play Developer Publishing API on behalf of an application rather than an end user. Service accounts are ideal for accessing the API from an unattended server, such as an automated build server (e.g. Jenkins). All actions will be shown as originating from the service account. You can configure fine grained permissions for the service account on the 'User Accounts & Rights' page.

There are no service accounts associated with your project.

CREATE SERVICE ACCOUNT

6. This will result in the following modal window appearing. Click on the “**Google API Console**” link.

Create Service Account

1. Navigate to the [Google API Console](#).
2. Click 'Create Service Account'.
3. Fill in the details for the service account and click 'Create'.

At this point, you will have the option to create a private key. The private key is downloaded to your machine and is the only copy of this key. You must keep the private key secure, it will be needed by your application to make API calls using your service account.

4. Click "Done" below and ensure the new service account appears in the list.

CANCEL **DONE**

7. This will open up a new page in the Google API Console. Click on "**CREATE SERVICE ACCOUNT**." *Please note that this page may look slightly different based on what all has been set up in your Google account.*

The screenshot shows the Google API Console interface. On the left, there's a sidebar with various project settings like IAM, Identity & Organization, Organization policies, Quotas, and Service accounts (which is currently selected). The main area is titled 'Service accounts' and shows a table with columns: Email, Name, Description, Key ID, Key creation date, and Action. A red circle highlights the '+ CREATE SERVICE ACCOUNT' button at the top of the table. To the right, there's a 'Permissions' section with a note about allowing specific users to manage service accounts, and another note about assigning project roles to service accounts. A message at the bottom says 'Please select at least one resource.'

8. This will bring up the following page. Please fill in the fields to match the screenshot. If you are blocked from using the *publishapp* as the "Service account name," then just make it *publishapp2* instead.

After you have filled in details as above, click on "**CREATE.**"

IAM & admin Create service account

- IAM
- Identity & Organization
- Organization policies
- Quotas
- Service accounts**
- Labels
- Settings
- Cryptographic keys
- Identity-Aware Proxy
- Roles
- Audit Logs

1 Service account details

— 2 Grant this service account access to project (optional) —

3 Grant users access to this service account (optional)

Service account details

Service account name: **publishapp**

Display name for this service account:

Service account email: **publishapp@ap[REDACTED].iam.gserviceaccount.com**

Service account description: **Google Play Developer**

Describe what this service account will do:

CREATE CANCEL

9. This will then take you to step 2 - “Grant this service account access to project.” Here, set the role of the Service account to the Owner of the Project, as shown in the screenshot below:

IAM & admin Create service account

- IAM
- Identity & Organization
- Organization policies
- Quotas
- Service accounts**
- Labels
- Settings
- Cryptographic keys
- Identity-Aware Proxy
- Roles
- Audit Logs

Service account permissions (optional)

Grant this service account access to Google Play Android Developer so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Role	Project	Editor	Owner	Viewer
Android Management				
App Engine			Owner	
AutoML				
BigQuery				
Billing				
Binary Authorization				
Cloud Asset				
MANAGE ROLES				

10. Verify the “Role” has been successfully set as “Owner” and click on “CONTINUE.”

The screenshot shows the Google Cloud IAM & admin interface. On the left, there's a sidebar with various options: IAM, Identity & Organization, Organization policies, Quotas, Service accounts (which is selected and highlighted in blue), Labels, Settings, Cryptographic keys, Identity-Aware Proxy, Roles, and Audit Logs. The main content area is titled "Create service account". It has three steps: 1. Service account details (checked), 2. Grant this service account access to project (optional) (step 2 is shown), and 3. Grant users access to this service account (optional). Step 2 includes a section for "Service account permissions (optional)" where "Owner" is selected from a dropdown menu. A red circle highlights the "CONTINUE" button at the bottom.

11. The following page will then appear for step 3 - “Grant users access to this service account.” Click on “**CREATE KEY**.”

IAM & admin

- IAM
- Identity & Organization
- Organization policies
- Quotas
- Service accounts**
- Labels
- Settings
- Cryptographic keys
- Identity-Aware Proxy
- Roles
- Audit Logs

Create service account

Service account details

Grant this service account access to project (optional)

Grant users access to this service account (optional)

Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account.

[Learn more](#)

Service account users role

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

Grant users the permission to administer this service account

Create key (optional)

Download a file that contains the private key. Store the file securely because this key can't be recovered if lost. However, if you are unsure why you need a key, skip this step for now.

+ CREATE KEY

DONE **CANCEL**

12. This will bring up a modal window on the side to create the key. Make sure “Key type” is set to **JSON**, then click on “**CREATE**.”

Your free trial is waiting: activate now to get \$300 credit to explore Google Cloud products. [Learn more](#)

Google APIs **Google Play Android Developer** [Q](#)

IAM & admin

- IAM
- Identity & Organization
- Organization policies
- Quotas
- Service accounts**
- Labels
- Settings
- Cryptographic keys
- Identity-Aware Proxy
- Roles
- Audit Logs

Create service account

Service account details

Grant this service account access to project (optional)

Grant users access to this service account (optional)

Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account.

[Learn more](#)

Service account users role

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

Grant users the permission to administer this service account

Create key (optional)

Download a file that contains the private key. Store the file securely because this key can't be recovered if lost. However, if you are unsure why you need a key, skip this step for now.

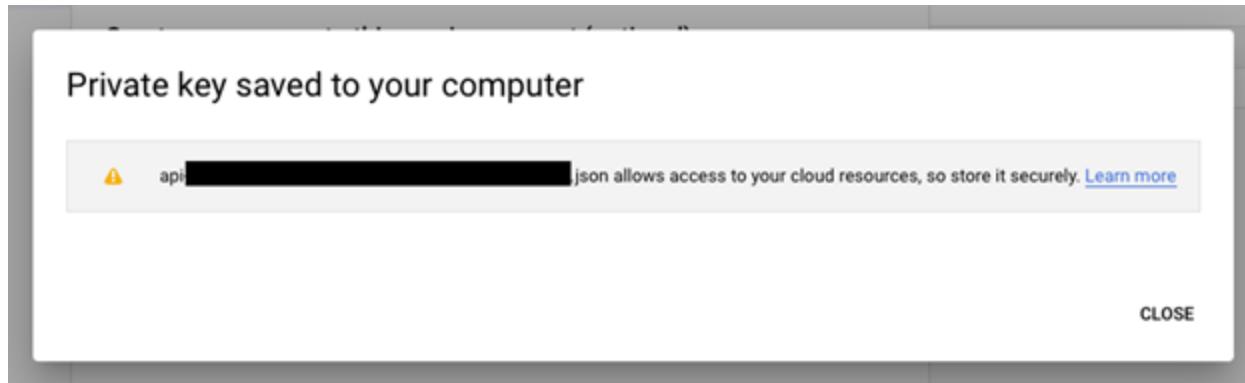
Key type

JSON Recommended

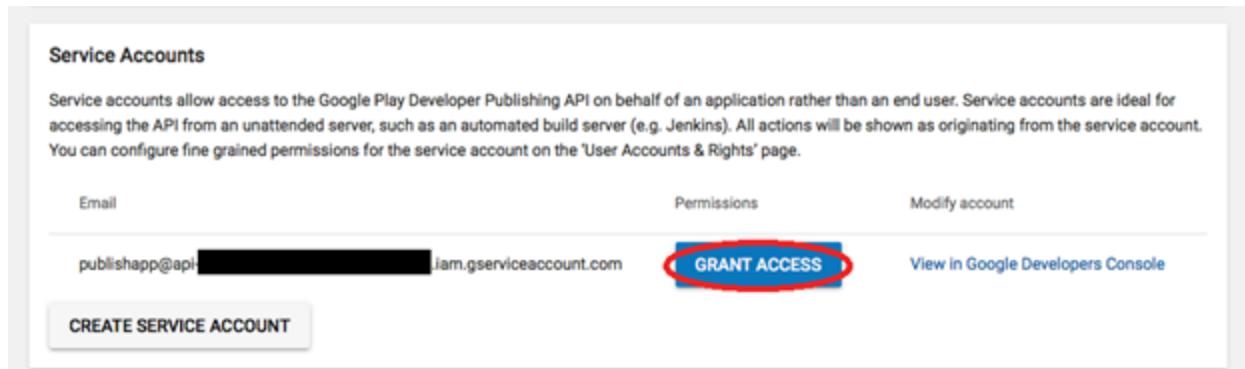
P12 For backward compatibility with code using the P12 format

CREATE **CANCEL**

13. The following modal window will appear and a JSON file should automatically be downloaded to your computer. **Please keep this key file somewhere safe as you will need to send it to us after you have completed all steps.**



14. Go back to the Google Play Console. If you have closed the window or tab for it, then follow steps 1 – 7 to load it again and navigate to the “API access” settings. You may need to refresh the page, but the “Service Accounts” section will now be updated to show the account you just created. Click on “**GRANT ACCESS**.”



15. This will bring up a modal window. Configure access for the service account as per the screenshot below. Make sure the “Access expiry date” is set to “Never” and the “Role” is “Release Manager.” Once you have confirmed that these settings are correct, click on “**ADD USER**.”

Add a new user

Email * publishapp@[REDACTED].iam.gserviceaccount.com

Access expiry date * Never On: [REDACTED]

Role * Release manager

PERMISSIONS	GLOBAL	Add an app ▾
ACCESS LEVEL		
View app information ⓘ	<input checked="" type="checkbox"/>	
Create & edit draft apps ⓘ	<input checked="" type="checkbox"/>	
Manage user permissions ⓘ	<input type="checkbox"/>	
FINANCIAL DATA		
View financial data ⓘ	<input type="checkbox"/>	
Manage orders ⓘ	<input type="checkbox"/>	
RELEASE MANAGEMENT		
Manage production releases ⓘ	<input checked="" type="checkbox"/>	
Manage testing track releases ⓘ	<input checked="" type="checkbox"/>	
Manage testing track configuration ⓘ	<input checked="" type="checkbox"/>	
STORE PRESENCE		
Edit store listing, pricing & distribution ⓘ	<input checked="" type="checkbox"/>	
USER FEEDBACK		
Reply to reviews ⓘ	<input checked="" type="checkbox"/>	
GOOGLE PLAY GAMES SERVICES		
Create & edit games ⓘ	<input checked="" type="checkbox"/>	
Publish games ⓘ	<input checked="" type="checkbox"/>	

Permissions granted at the global level will automatically be granted at the per-app level.

CANCEL ADD USER

16. You will now see that the "GRANT ACCESS" button has been changed to a "View permissions" link.

publishapp@[REDACTED].iam.gserviceaccount.com

[View permissions](#)

[View in Google Developers Console](#)

17. Please send the JSON file you downloaded earlier to our support team. We will then verify everything has been set up correctly and can proceed with updating your application.