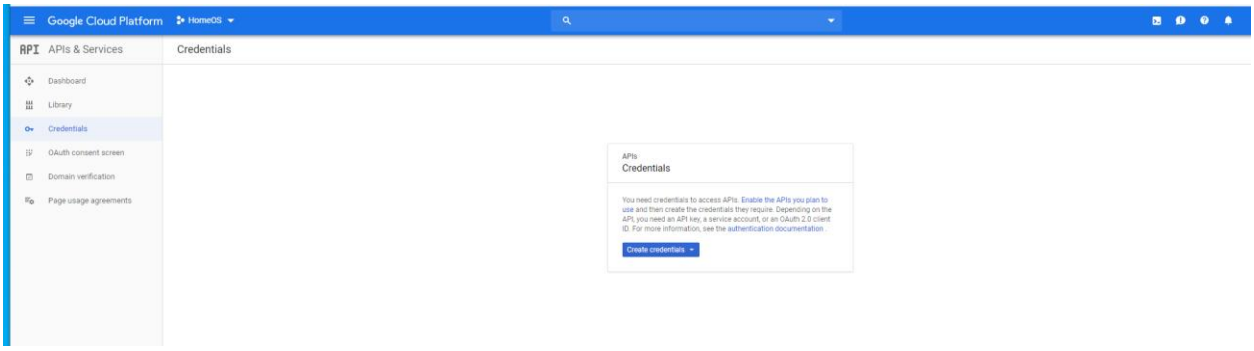
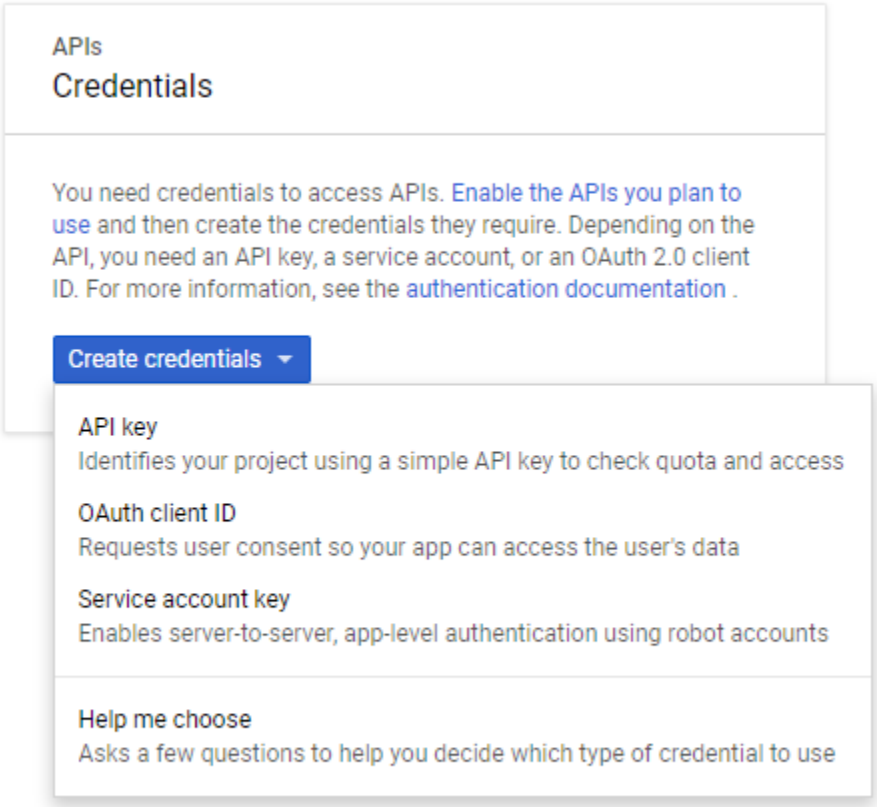
1. Go to https://console.cloud.google.com/apis/credentials
2. Please note this may look a little different due to person google vs GSuite
3. Click Create Credentials



4. Go to OAuth Client ID



5. Configure Consent Screen

OAuth consent screen

Before your users authenticate, this consent screen will allow them to choose whether they want to grant access to their private data, as well as give them a link to your terms of service and privacy policy. This page configures the consent screen for all applications in this project.

Verification status

Not published

Application name
The name of the app asking for consent

SOW SPA

Application logo
An image on the consent screen that will help users recognize your app

Local file for upload | Browse

Support email
Shown on the consent screen for user support

jeremiahs1079@hotmail.com

Scopes for Google APIs
Scopes allow your application to access your user's private data. Learn more

If you add a sensitive scope, such as scopes that give you full access to Gmail or Drive, Google will verify your consent screen before it's published.

- email
- profile
- openid

Add scope

Authorized domains
To protect you and your users, Google only allows applications that authenticate using OAuth to use Authorized Domains. Your applications' links must be hosted on Authorized Domains. Learn more

example.com

Type in the domain and press Enter to add it

Application Homepage link
Shown on the consent screen. Must be hosted on an Authorized Domain.

https:// or http://

Application Privacy Policy link
Shown on the consent screen. Must be hosted on an Authorized Domain.

https:// or http://

Application Terms of Service link (Optional)
Shown on the consent screen. Must be hosted on an Authorized Domain.

https:// or http://

Save | Submit for verification | Cancel

About the consent screen

The consent screen tells your users who is requesting access to their data and what kind of data you're asking to access.

OAuth verification

To protect you and your users, your consent screen and application may need to be verified by Google. Verification is required if your app is marked as **Public** and at least one of the following is true:

- Your app uses a sensitive and/or restricted scope
- Your app displays an icon on its OAuth consent screen
- Your app has a large number of authorized domains
- You have made changes to a previously-verified OAuth consent screen

The verification process may take up to several weeks, and you will receive email updates as it progresses. Learn more about verification.

Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your app will behave before it's verified.

Let us know what you think about our OAuth experience.

OAuth grant limits

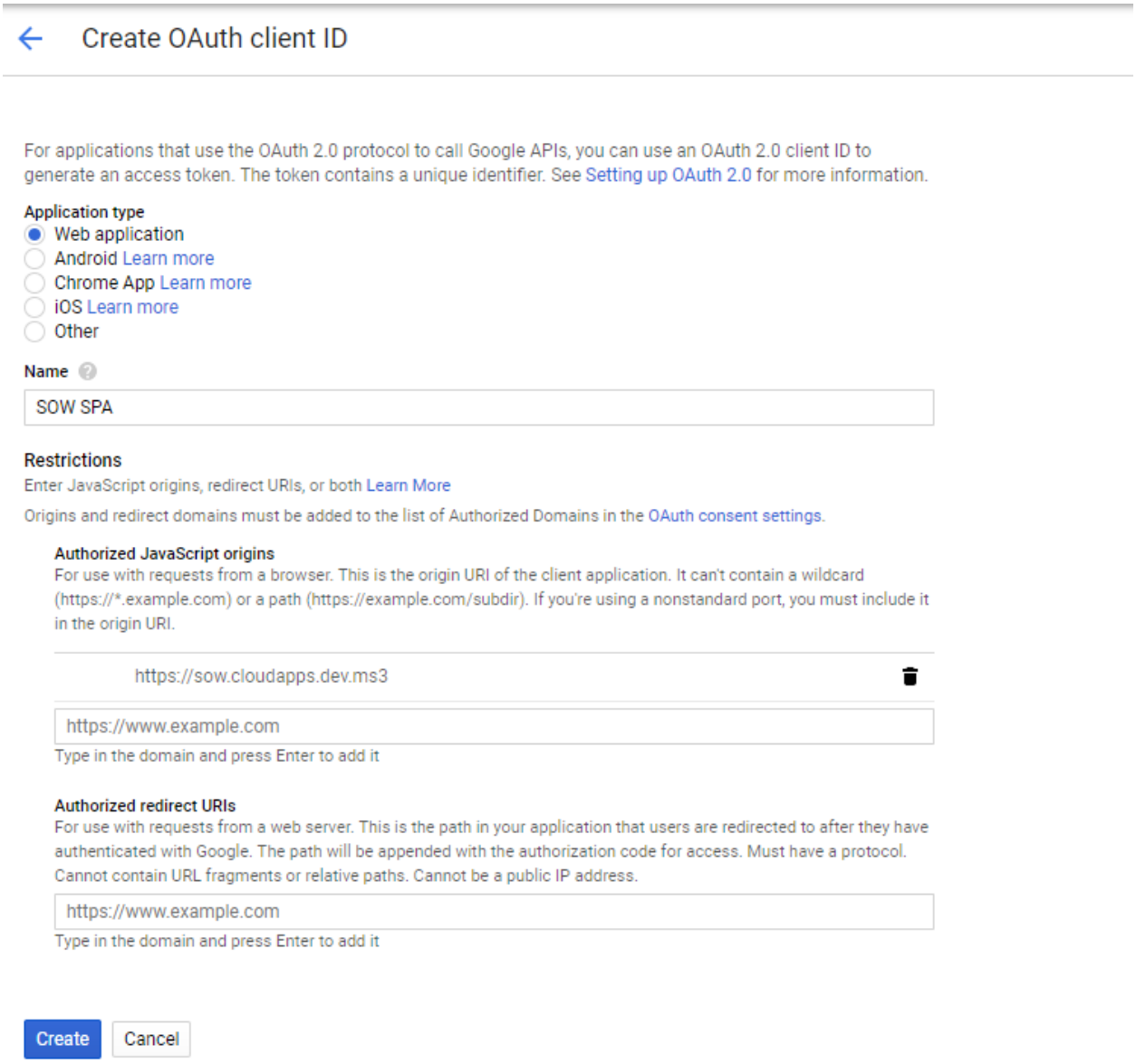
Token grant rate

Your current per minute token grant rate limit is 100 grants per minute. The per minute token grant rate resets every minute. Your current per day token grant rate limit is 10,000 grants per day. The per day token grant rate resets every day.

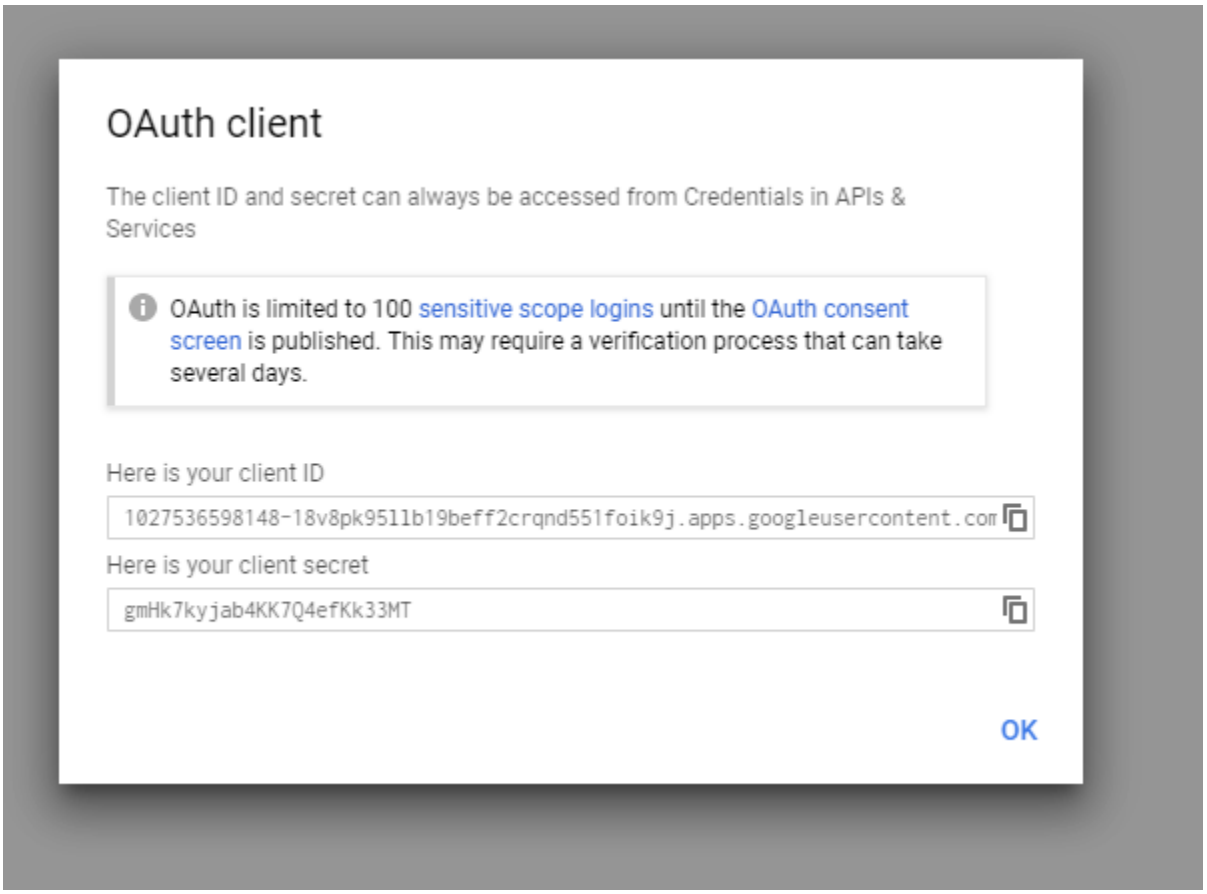
Raise limit

1h | 6h | 1d | 7d | 30d

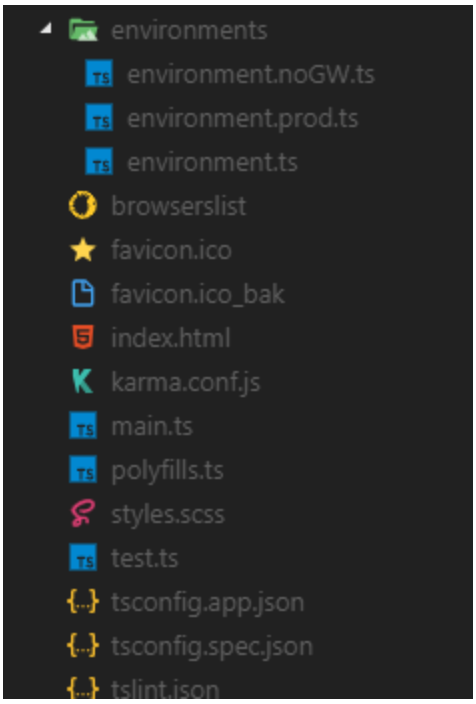
6. As far as I know the only required is the application name and support email. The default scopes are fine. Authorized domains would be @ms3-inc.com
7. Save
8. Create Web Application OAuth Client ID
9. The Authorized JavaScript is the link to the sow app. This should also go into Authorized redirect URI's



10. Record Client ID



11. This will go into the sow environment file for prod and regular


environments
environment.noGW.ts
environment.prod.ts
environment.ts
browserslist
favicon.ico
favicon.ico_bak
index.html
karma.conf.js
main.ts
polyfills.ts
styles.scss
test.ts
tsconfig.app.json
tsconfig.spec.json
tslint.json

12. Done.