

# Lepide Active Directory Self Service

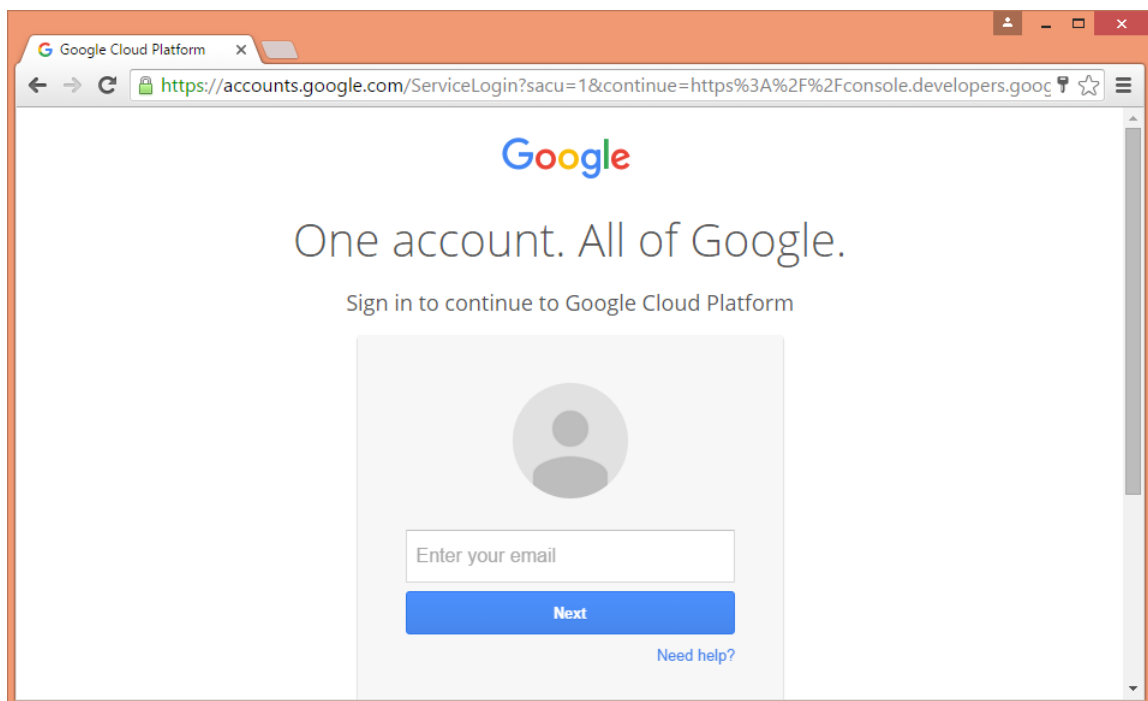


## How to generate P12 key

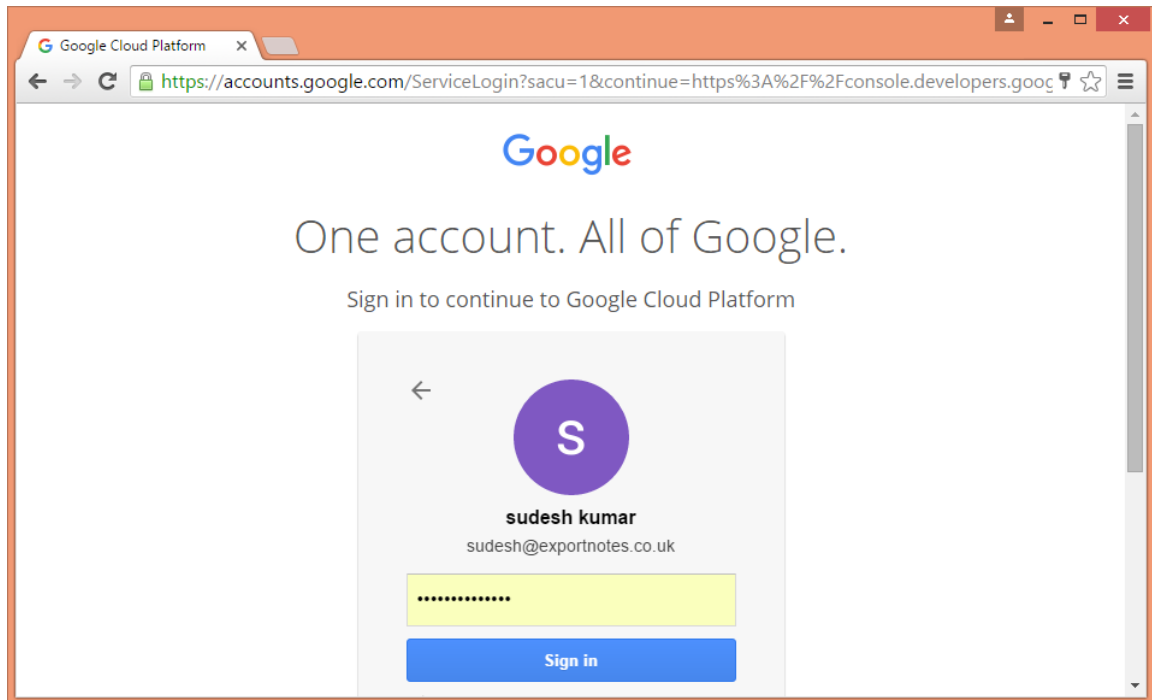
Lepide Active Directory Self Service allows Password Synchronization of Google Apps and IBM accounts. In order to enable Google Apps Password synchronization, you need to generate a P12 key by making certain settings in your Google service account.

Follow the below mentioned steps to generate the P12 key for Google App Service Account.

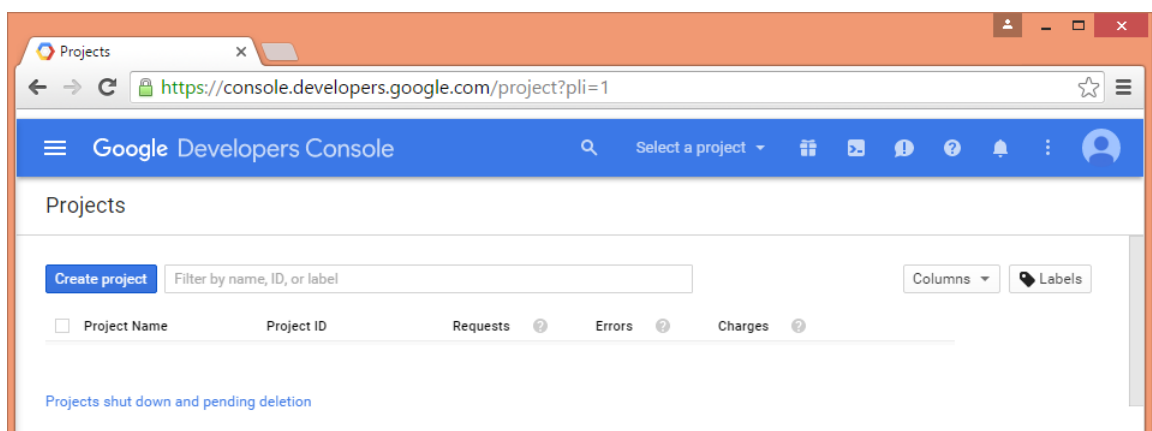
1. Open Google Developer Console Project for Google Cloud Platform - <https://console.developers.google.com/project> in Web browser, preferably Google Chrome.



2. Enter the email address of your Google Service Account and click "Next".



3. Enter the password of your Google Service Account and click "Sign In". It takes you to the Google Service Projects page.



4. Click "Create Project" to access "New Project" pop-up.

### New Project

**Project name** ?

Your project ID will be based on your project name ? [Edit](#)

[Show advanced options...](#)

- The Project ID is assigned as per the project name. If you want to provide a manual project ID, click "Edit" link. You can also click "Show advanced options..." to access the advanced options.

### New Project

**Project name** ?

**Project ID** ?

[Hide advanced options...](#)

**App Engine location** ?

us-central

- Enter the Project Name, Project ID, and select the advanced option. Click "Create" to create the project.

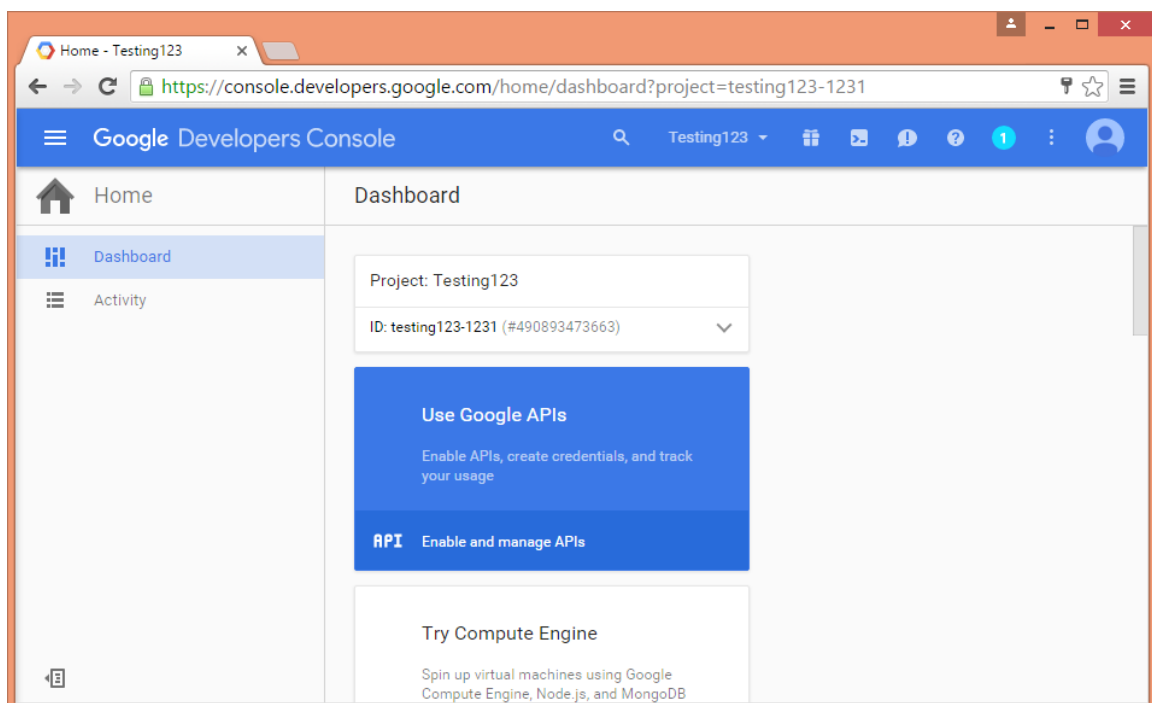
### New Project

**Project name** ?

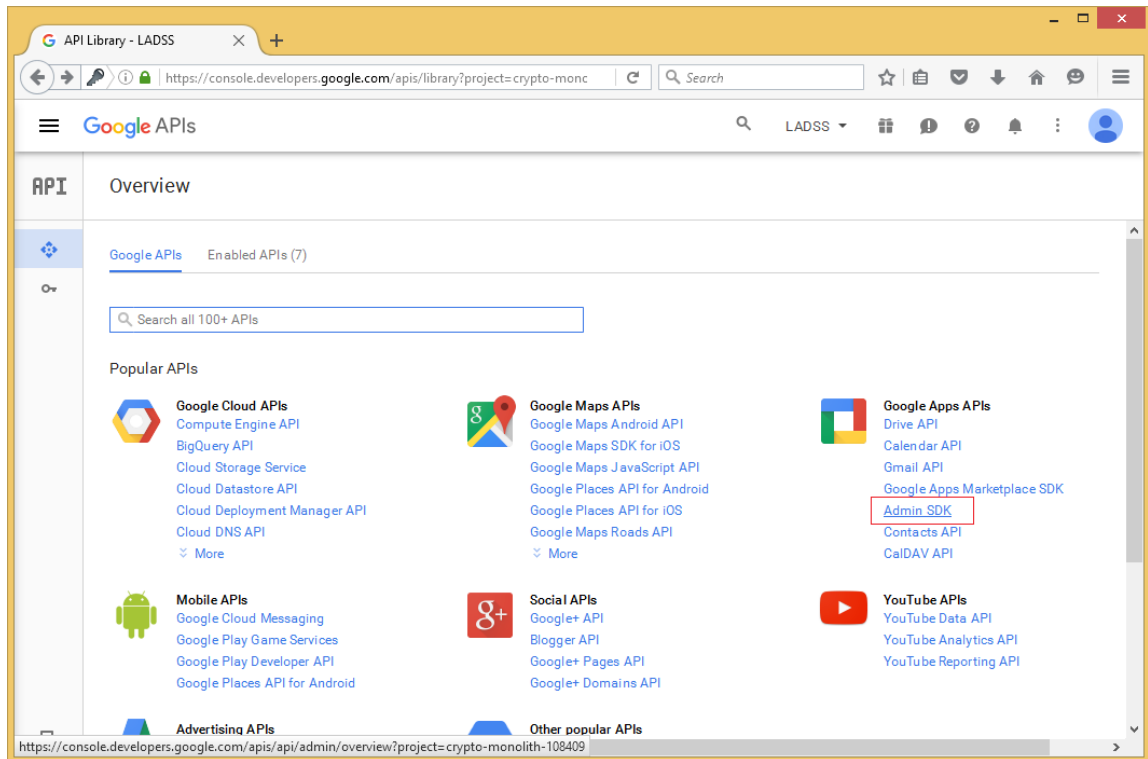
  
**Project ID** ?  
[Hide advanced options...](#)  
**App Engine location** ?  

CreateCancel

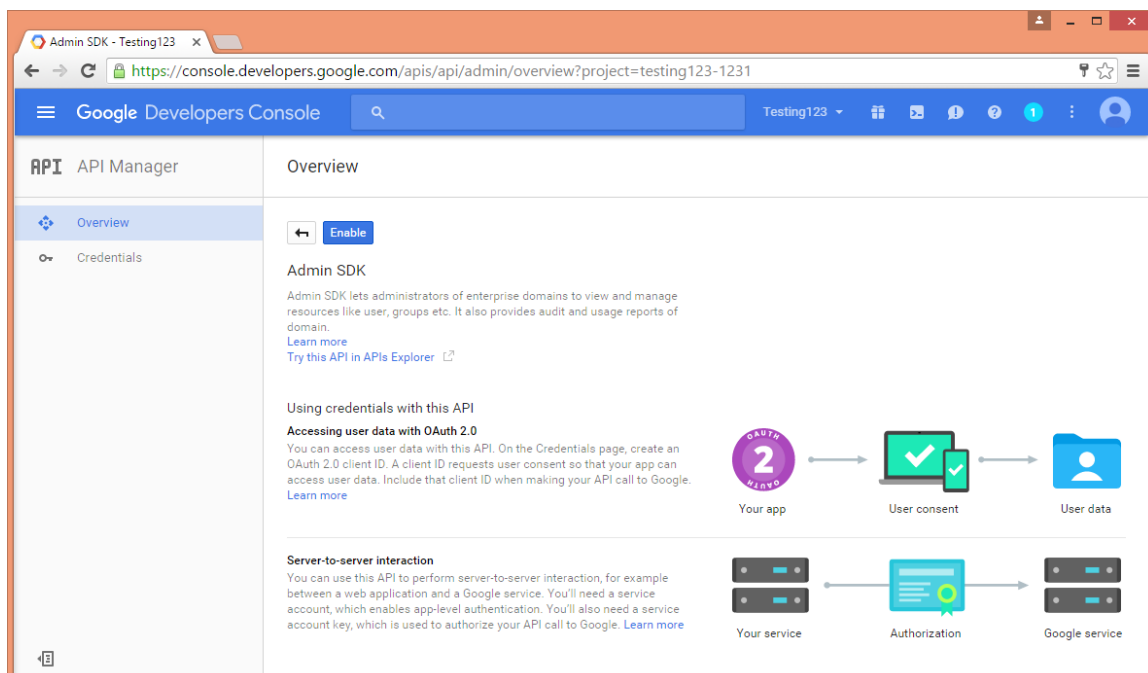
- Once created, the dashboard comes up. Click "Enable and Manage APIs" in "Use Google APIs" section. It displays the popular APIs.



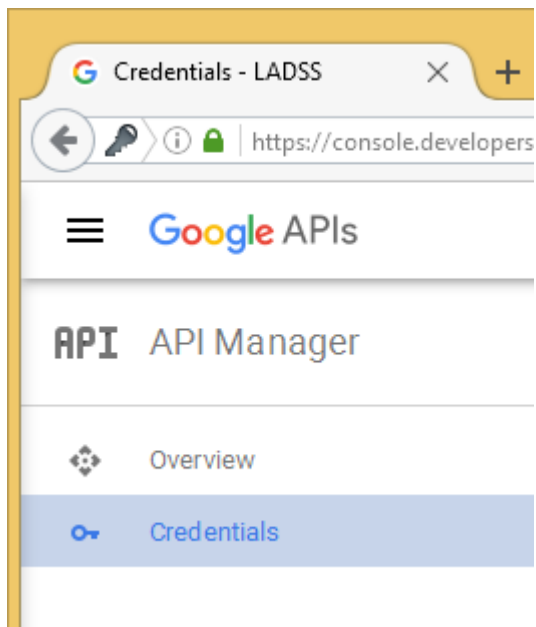
- Click 'Admin SDK' API link to access its settings.



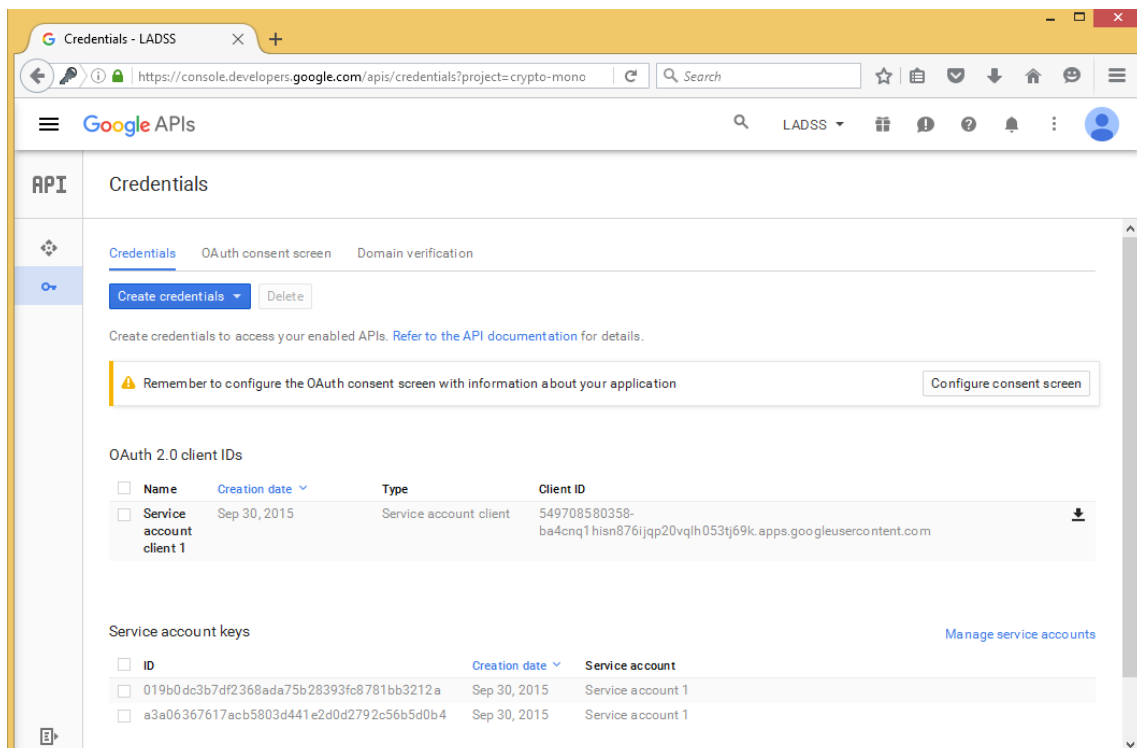
9. Click the **Enable** button to enable Admin SDK API for the service account.



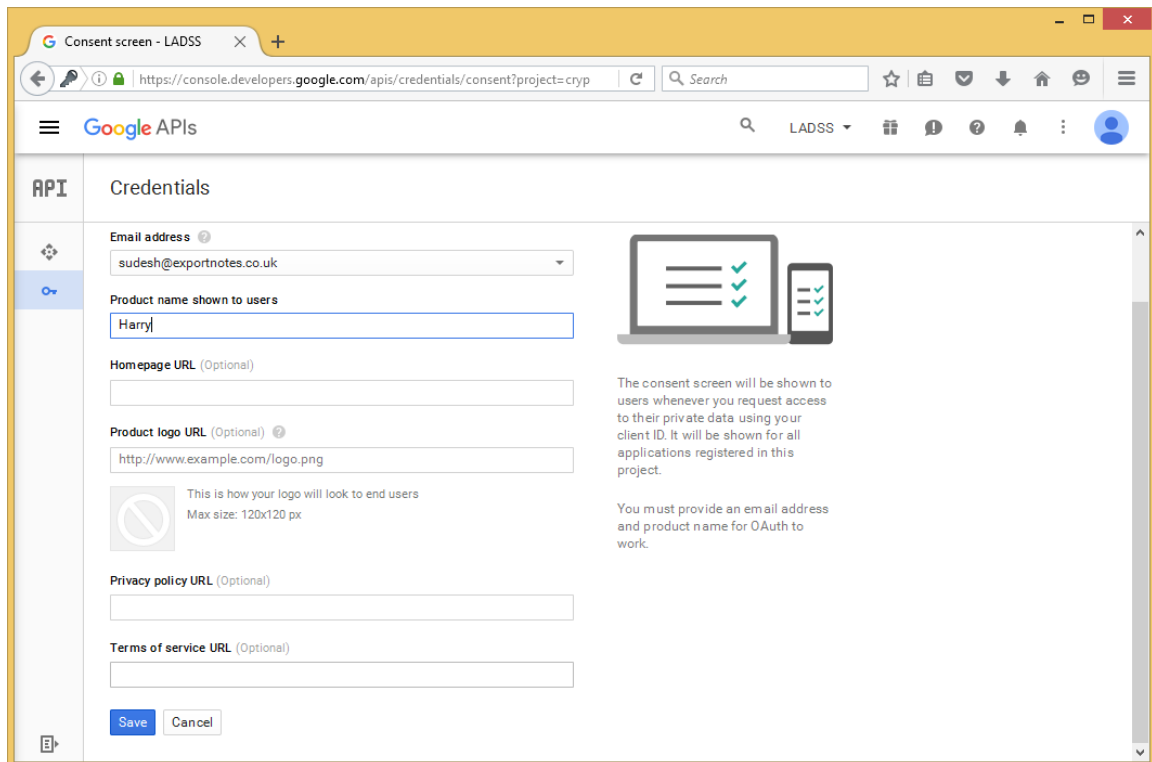
10. Now from the left pane of API Manager select credential.



11. The following page will open up. Click on the "OAuth consent screen" tab.



12. In the "OAuth consent screen" page, fill the form to complete the project registration. Click "Save".



The screenshot shows the "Consent screen - LADSS" page in the Google API Console. The page is titled "Credentials" and contains a form for configuring an OAuth consent screen. The form fields are as follows:

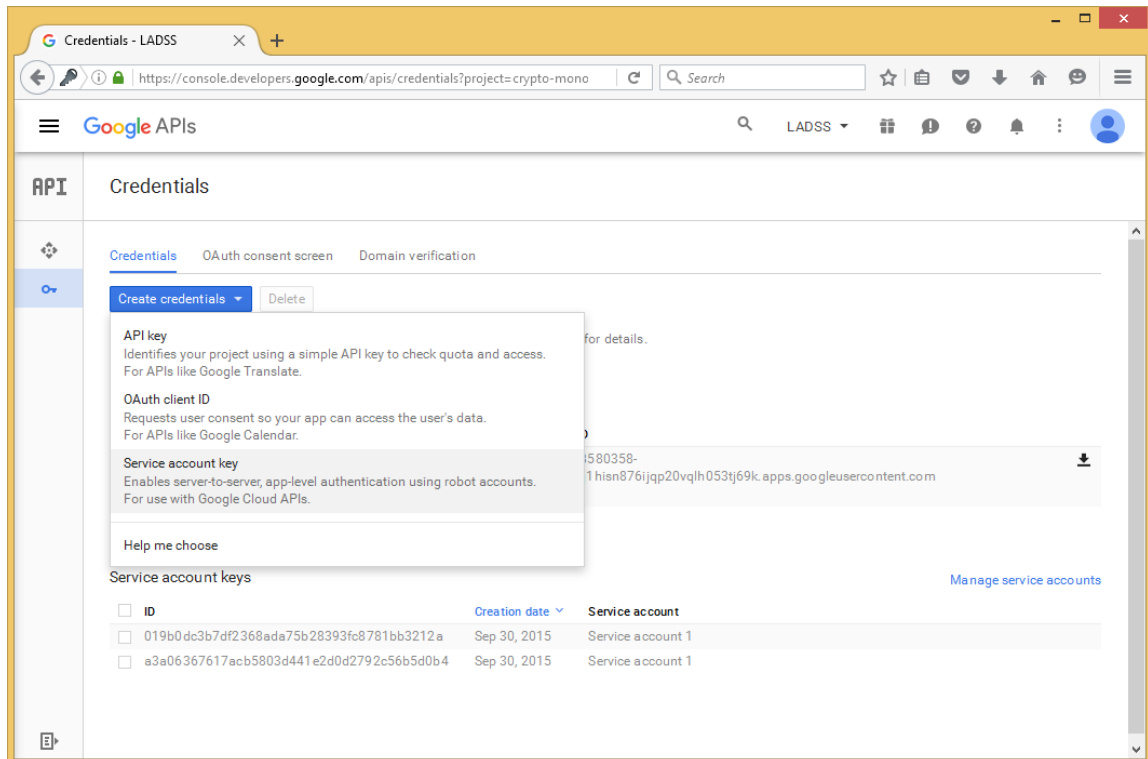
- Email address:** A dropdown menu with the selected value "suresh@exportnotes.co.uk".
- Product name shown to users:** A text input field containing the text "Harry".
- Homepage URL (Optional):** An empty text input field.
- Product logo URL (Optional):** A text input field containing the URL "http://www.example.com/logo.png".
- Privacy policy URL (Optional):** An empty text input field.
- Terms of service URL (Optional):** An empty text input field.

Below the form fields are two buttons: "Save" and "Cancel".

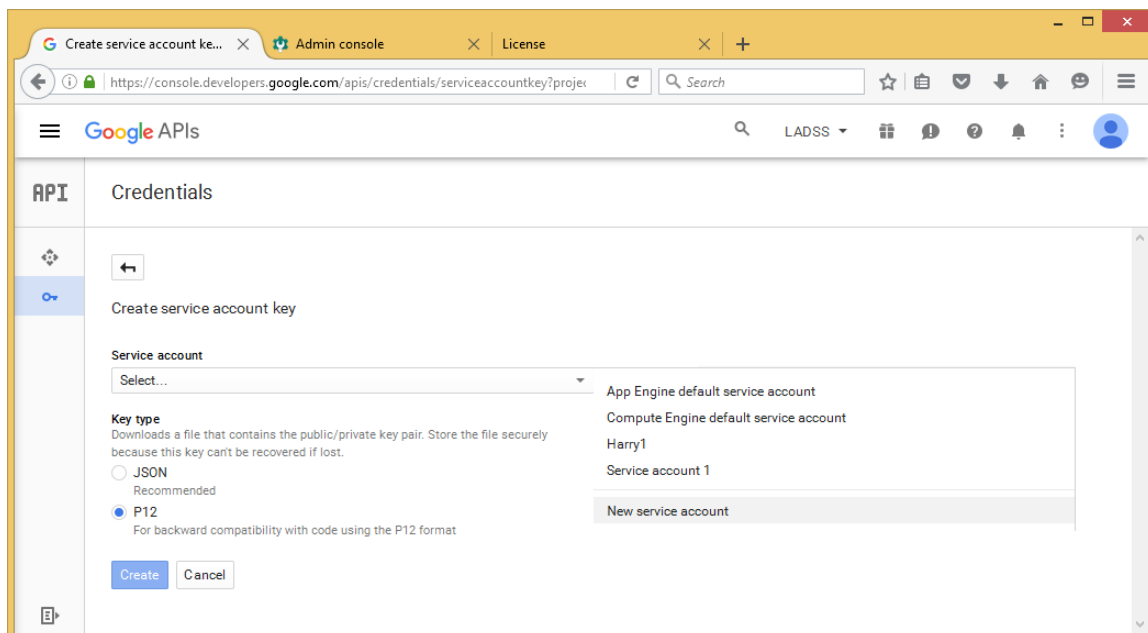
On the right side of the form, there is a graphic of a laptop and a smartphone displaying checkmarks, indicating successful configuration. Below this graphic, there is a note: "The consent screen will be shown to users whenever you request access to their private data using your client ID. It will be shown for all applications registered in this project." Below this note, there is another note: "You must provide an email address and product name for OAuth to work."

13. You will be redirected back to the Credentials tab. Now, click on "Create credential" and select service account key from the dropdown menu.





14. Select P12 as the key type and create a new service account by selecting it from the 'service account' dropdown menu.

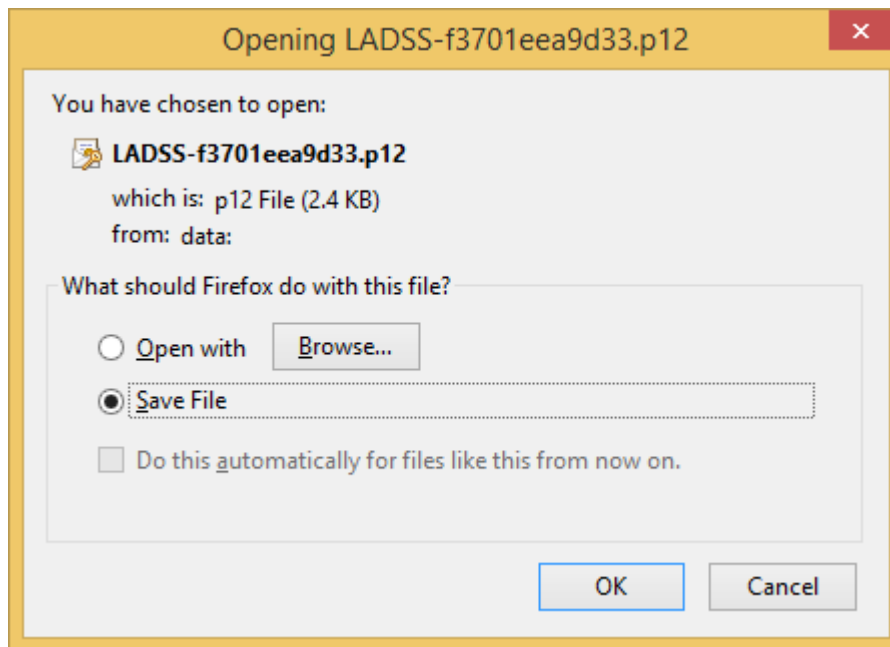


15. Enter the service account name and service account ID. Click "Create".

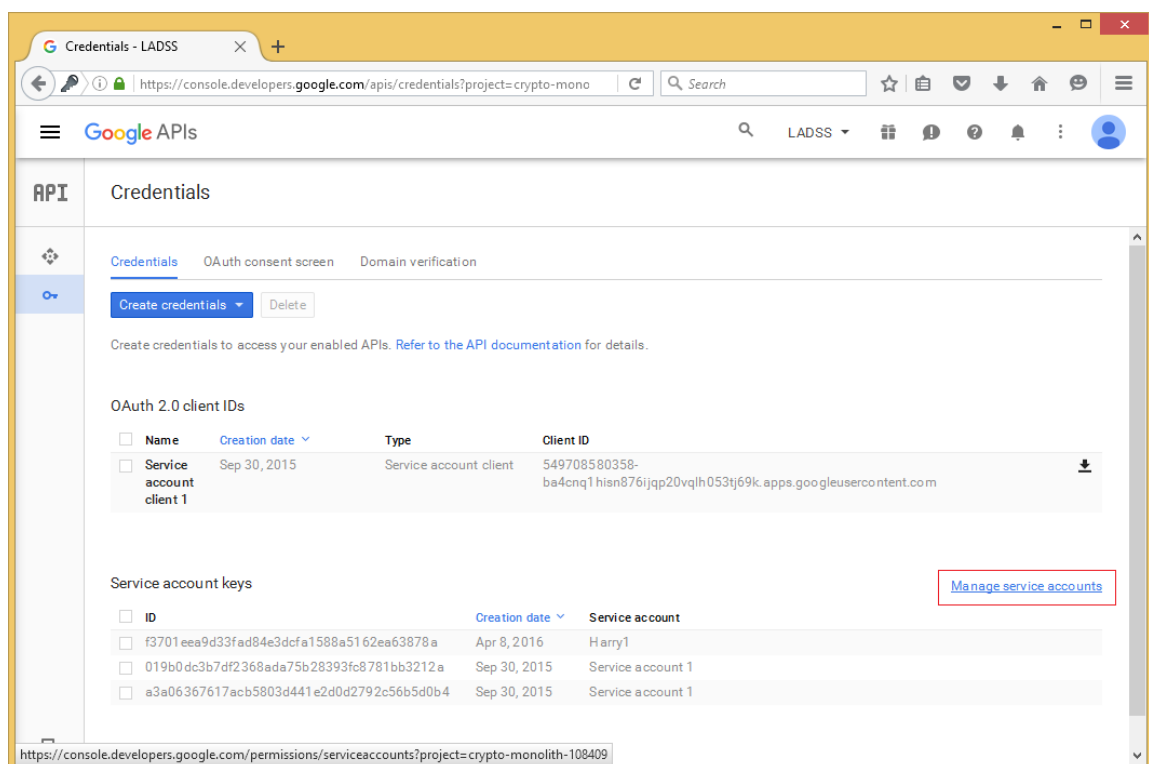
The screenshot shows the Google Cloud Platform console for creating a service account key. The 'Service account name' is 'Harry1' and the 'Service account ID' is 'harry1@crypto-monolith-108409.iam.gserviceaccount.com'. The 'Key type' is set to 'P12' (Recommended). The 'Create' button is visible at the bottom.

16. As soon as the service account is created, a P12 key file is generated. Save the generated p12 file to a safe location.

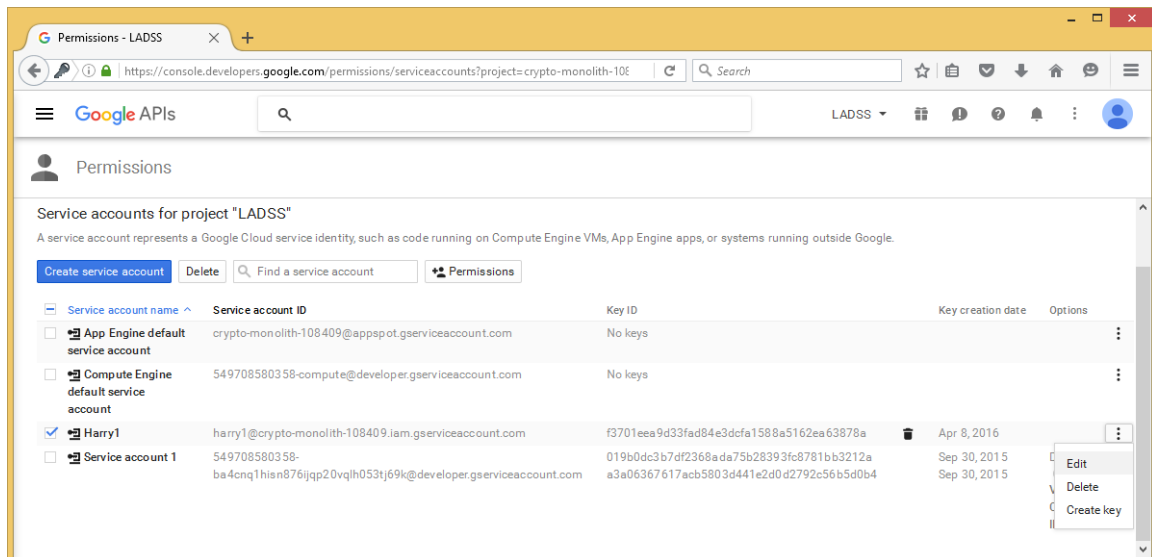
**Note:** This is the P12 key file which you need to browse while adding Google Apps for password synchronization.



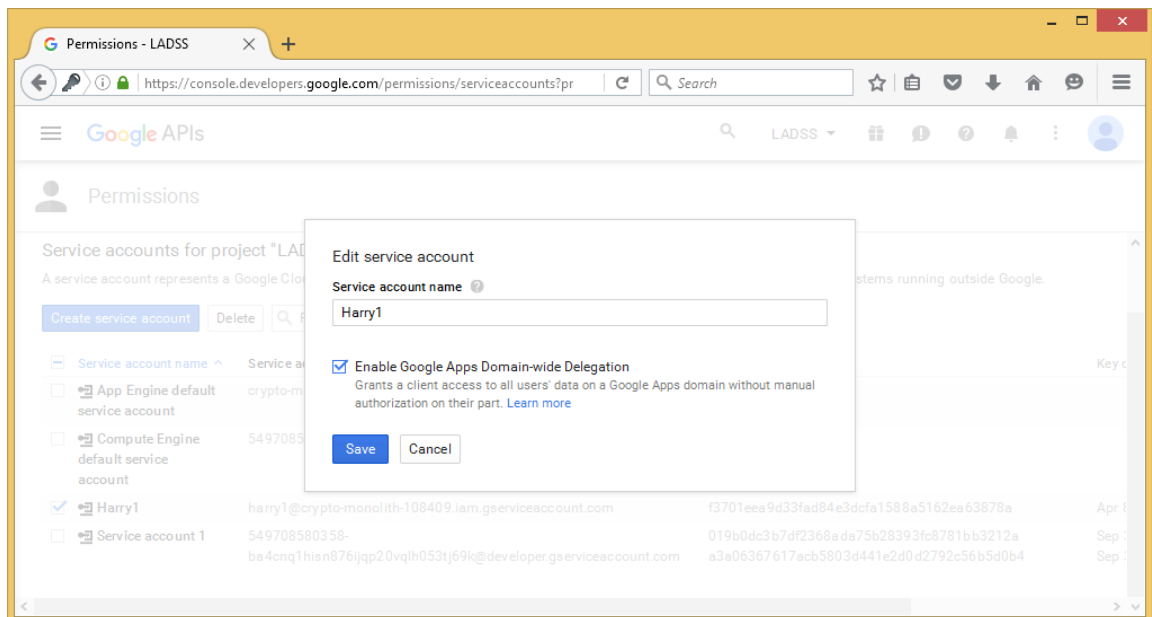
17. You will be redirected back to the Credentials tab. Now, click on "Manage service accounts".



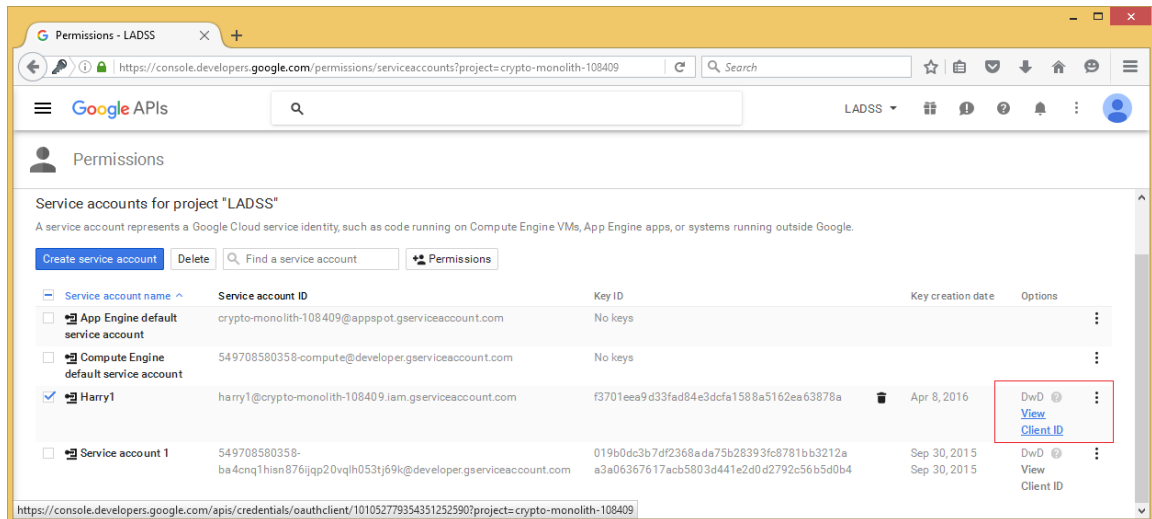
18. Select the service account created and click edit from options (three vertical dots at the end of account record).



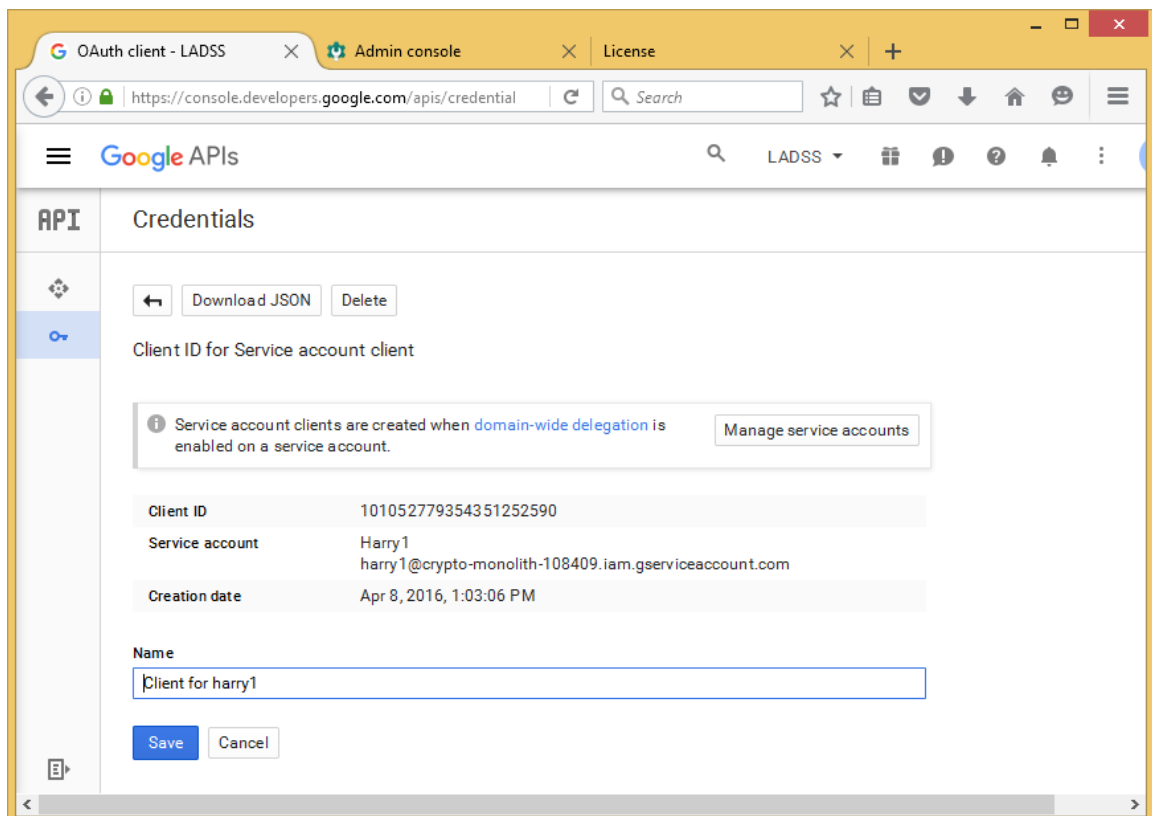
19. Select "Enable-Google Apps Domain-wide Delegation" to grant domain wide access without logging to the service account. See this link for more details: [https://developers.google.com/admin-sdk/directory/v1/guides/delegation#delegate\\_domain-wide\\_authority\\_to\\_your\\_service\\_account](https://developers.google.com/admin-sdk/directory/v1/guides/delegation#delegate_domain-wide_authority_to_your_service_account)



20. Now click on View Client ID.

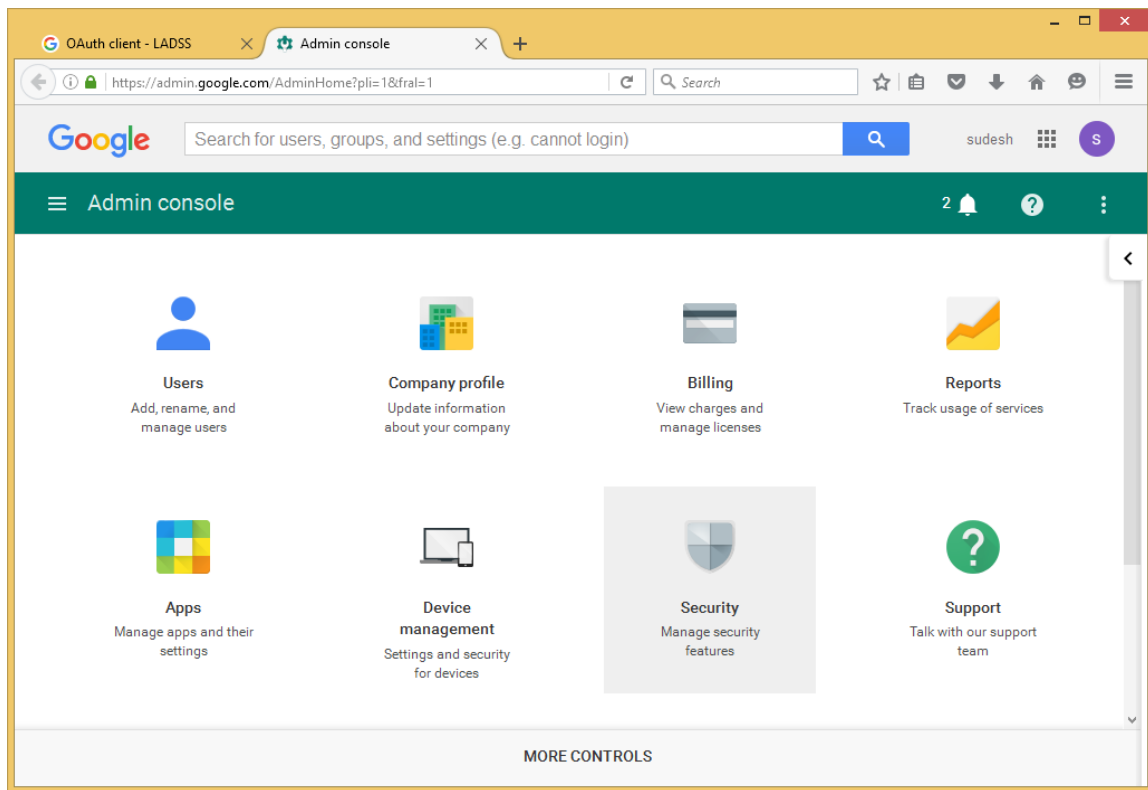


21. Copy the Client ID and Service account email in a safe location for further use.



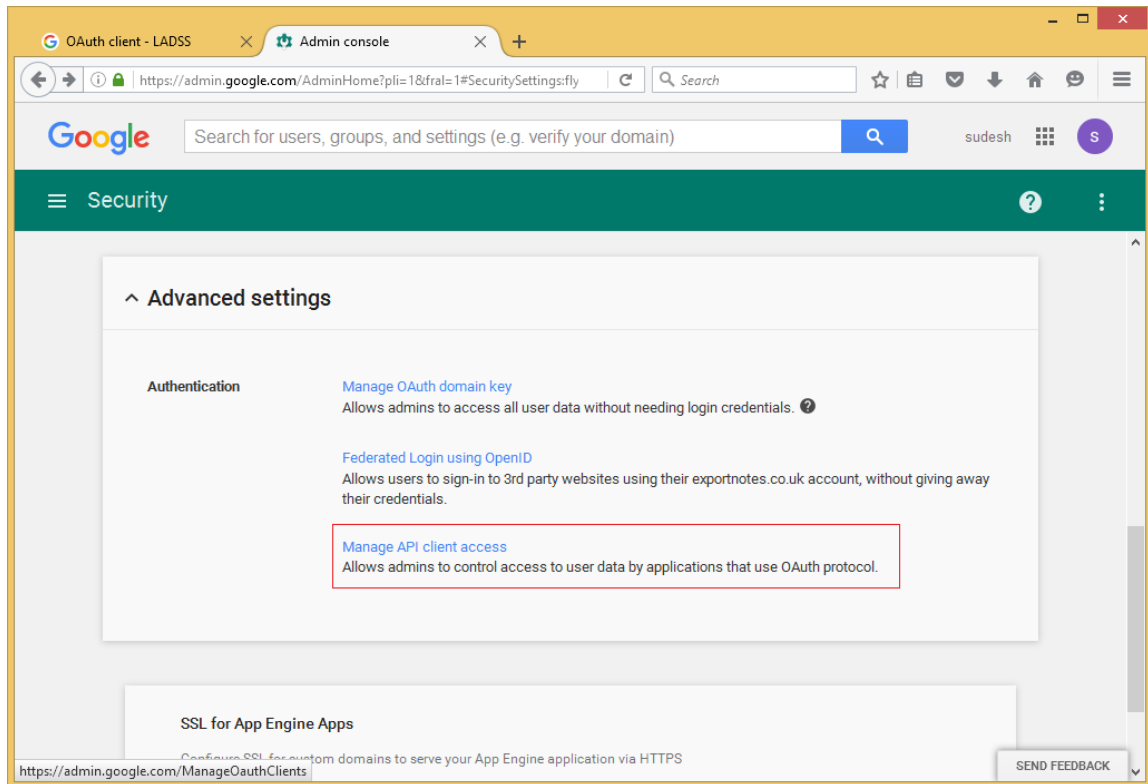
22. Now go to Google Admin Console (<https://admin.google.com>) and login using your Google Apps Administrator account.

23. Click on security tile.



24. Click show more and go to Advanced Setting.

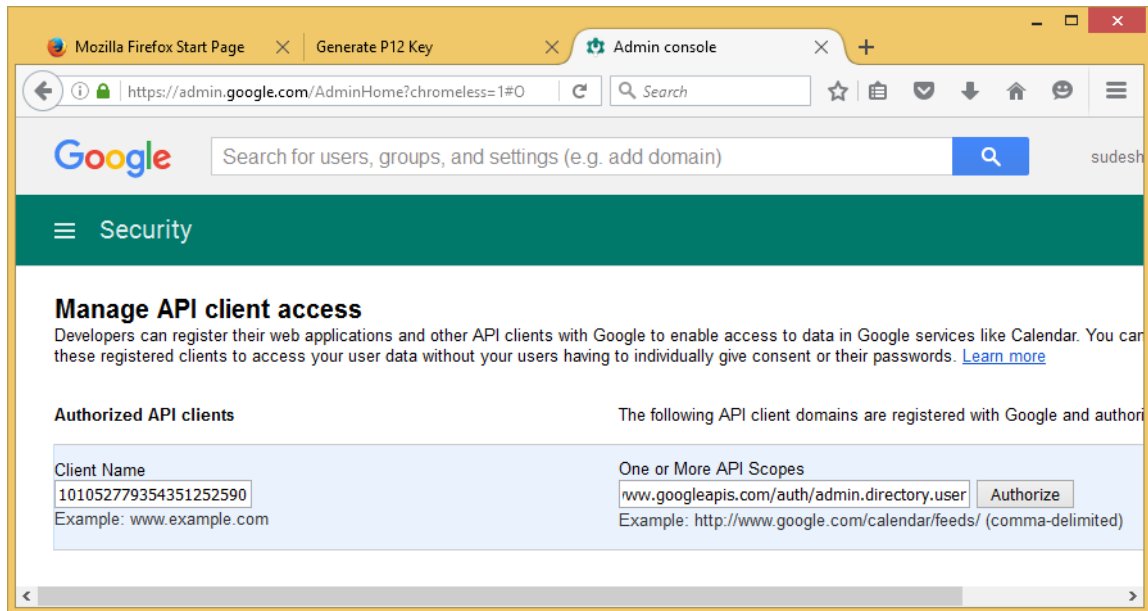
25. Click on Manage API Access.



26. Enter the Client ID generated earlier from developer console in client name and enter the following scopes in the scope field (use comma to separate them).

*<https://www.googleapis.com/auth/admin.directory.user>, <https://www.googleapis.com/auth/admin.directory.group>*

27. Click 'Authorize'.



28. That's it. You can start using the details in the Software.

Once the Password Synchronization settings are completed, Google Apps password resets can be successfully performed by end users.