

Key Steps -

1. Google Cloud Console

- a. Create Project
- b. API Enable
- c. Create Credentials
- d. Auth 2.0 Client Id
- e. Service Account - download
 - i. Key - P12
 - ii. Key – JSON

2. Salesforce

- a. Convert the P12 File to JKS File
- b. Identity Provider - Enable
- c. Certificate and Key Management - Import from KeyStore - JKS File

3. Salesforce With Google Drive

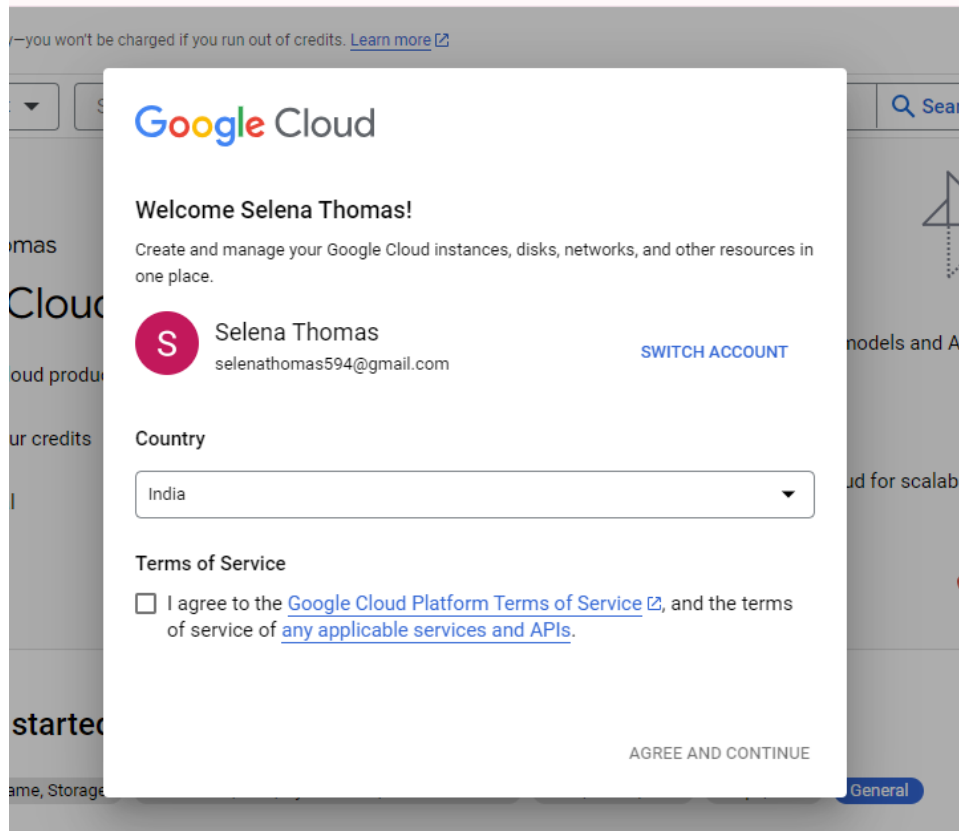
- a. Salesforce - AUTH Provider
- b. Google Cloud - Credential - OAuth 2.0 Client IDs
 - i. Callback URL
- c. Salesforce - Named Credential Authentication
 - i. Update the Certificate
- d. Salesforce Custom Metadata Update with Google Drive JSON File
 - i. Private Key
 - ii. Client Email
- e. Salesforce - Trusted URL
- f. Google Drive - Main Folder
 - i. Google Drive - Main Folder Share with Client Email
 - ii. Google Drive - Main Folder - General Access - Anyone with This Link
- g. Add your domain in API Restriction to secure your domain

4. Salesforce - Custom Metadata

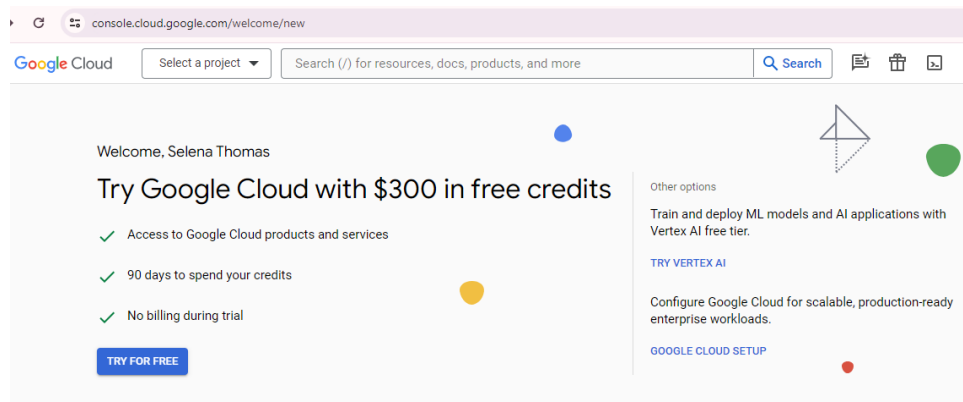
- a. Update Main Folder Id
- b. Update the Client Email Field with Google JSON
- c. Update the Private Key Field with Google JSON File

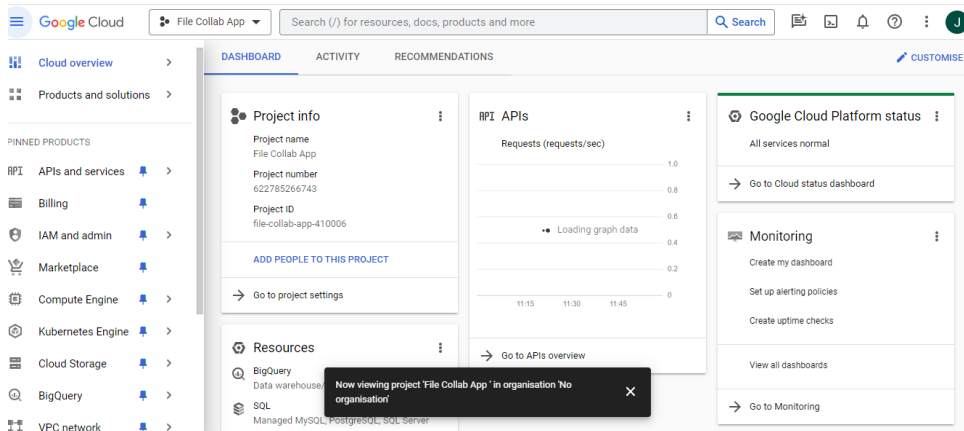
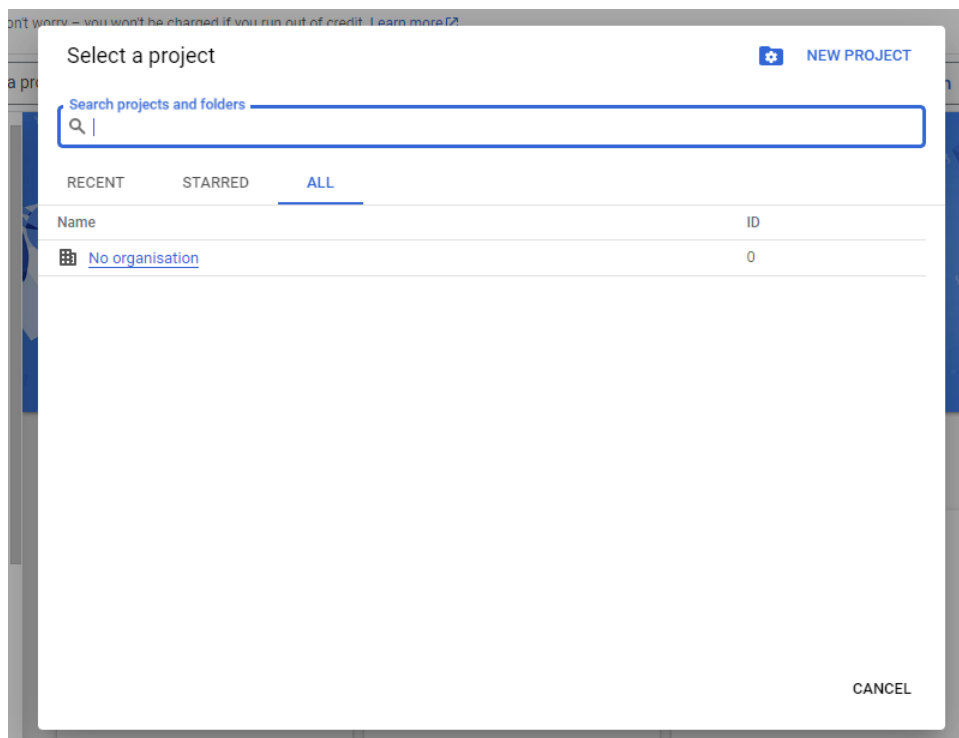
Detailed Steps -

- Go to - <https://console.cloud.google.com/>

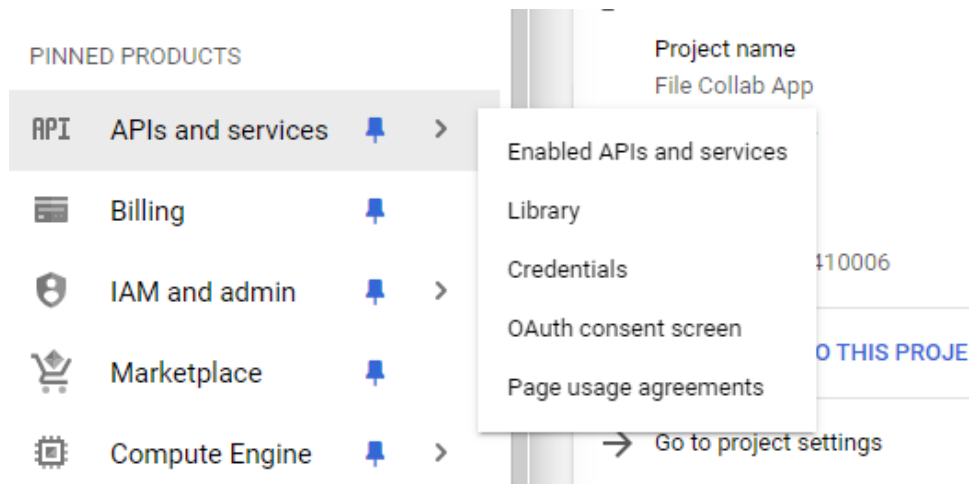


- Click on – Select a Project → Click on **New Project** → Enter Project Name - > Create

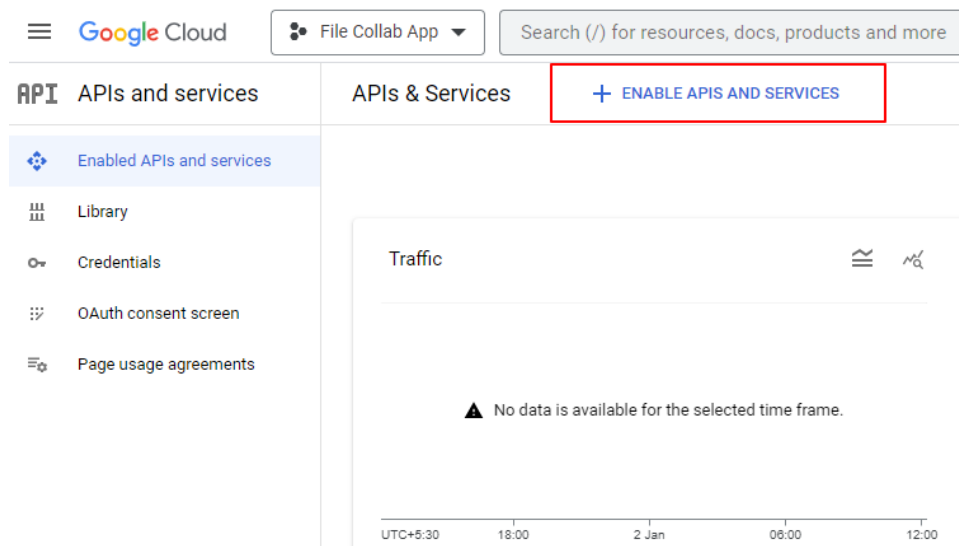




- Go to - APIs and services



- **Enabled APIs and SERVICES**



- Search For - “Google Drive API” and ‘Enable’ it –

The screenshot shows the Google API Library interface. At the top, a search bar contains the text "Google Drive API". Below the search bar, a list of 11 results is displayed. The first result, "Google Drive API", is highlighted with a red box. It is a Google Enterprise API that allows access to Google Drive resources. Below the search results, the "Product details" page for the "Google Drive API" is shown. The "ENABLE" button is highlighted with a red box. The page also includes tabs for "OVERVIEW", "DOCUMENTATION", "SUPPORT", and "RELATED PRODUCTS".

- Go to **Credential** and Click on **CREATE CREDENTIAL** Button

The screenshot shows the Google Cloud Platform "APIs & Services" page. The "Credentials" tab is selected and highlighted with a red box. The page displays a list of credentials, including "Traffic", "Errors", and "Median latency". Each credential has a "CREATE CREDENTIAL" button. The "Traffic" and "Errors" credentials show a message: "No data is available for the selected time frame." The "Median latency" credential is partially visible at the bottom.

- Create an **API Key** Credential

Google Cloud

File Collab App

Search (/) for resources, docs, products and more

Search

🗨️ 🗑️ 📄 2 ? ⋮ 👤

APIs and services

Enabled APIs and services

Library

Credentials

OAuth consent screen

Page usage agreements

Credentials

+ CREATE CREDENTIALS

🗑️ DELETE

↶ RESTORE DELETED CREDENTIALS

Create credentials to access your enabled APIs. [Learn more](#)

Remember to configure the OAuth consent screen with information about your application. [CONFIGURE CONSENT SCREEN](#)

API key

identifies your project using a simple API key to check quota and access

OAuth client ID

Requests user consent so that your app can access the user's data.

Service account

Enables server-to-server, app-level authentication using robot accounts

Help me choose

Asks a few questions to help you decide which type of credential to use

Restrictions

Actions

OAuth 2.0 Client IDs

☐	Name	Creation date	Type	Client ID	Actions
No OAuth clients to display					

Service Accounts

[Manage service accounts](#)

☐	Email	Name	Actions
No service accounts to display			

APIs and services

Enabled APIs and services

Library

Credentials

OAuth consent screen

Page usage agreements

Credentials

+ CREATE CREDENTIALS

🗑️ DELETE

↶ RESTORE DELETED CREDENTIALS

Create credentials to access your enabled APIs. [Learn more](#)

Remember to configure the OAuth consent screen with information about your application. [CONFIGURE CONSENT SCREEN](#)

API keys

☐	Name	Creation date	Restrictions	Actions
☐	API key 1	2 Jan 2024	None	SHOW KEY

Google Cloud

File Collab Review

Search (/) for resources, docs, products, and more

Q Search

APIs & Services

Enabled APIs & services

Library

Credentials

OAuth consent screen

Page usage agreements

Edit API key

REGENERATE KEY

DELETE

Name *

API key 1

Key restrictions

Restricting where and for which APIs this key can be used helps prevent unauthorized use. [Learn more](#)

Set an application restriction

Application restrictions limit an API key's usage to specific websites, IP addresses, Android applications, or iOS applications. You can set one application restriction per key.

None

Webistes

IP addresses

Android apps

IOS apps

Website restrictions

Restrict key usage requests to the specified websites.

⚠ If left blank, your API key will accept requests from any website.

ADD

Filter

Enter property name or value

Status

Website

Edit

https://blucursor8-dev-ed.develop.lightning.force.com/

API restrictions

API restrictions specify the enabled APIs that this key can call

Don't restrict key

This key can call any API

Restrict key

1 API

Selected APIs:

Google Drive API

Note: It may take up to 5 minutes for settings to take effect

SAVE CANCEL

Additional information

API Key

AIzaSyA7Q9Str28e2SGRaaymSh2HveAjJ1fSI3g

Use this key in your application by passing it with key=API_KEY parameter.

Creation date

March 15, 2024 at 7:21:20 PM GMT+5

How do I restrict my API key to specific websites?

Use a website to restrict the URLs that can use an API key. [Learn more](#)

Here are some examples of URLs that you can allow to set up a website:

- Any URL in a single domain with no subdomains: <https://example.com>
- Any URL in a single subdomain: <https://sub.example.com>
- Any subdomain in a single domain, using a wildcard asterisk (*): https://*.example.com
- A domain and all its subdomains, using a wildcard asterisk (*):
 - <https://example.com>
 - https://*.example.com
- A URL with a non-standard port: <http://www.example.com:8000>

Note: query parameters and fragments are not currently supported; they will be ignored if you include them in a website.

Additional information

API Key

AIzaSyA7Q9Str28e2SGRaaymSh2HveAjJ1fSI3g

Add the API Key – Custom Metadata of Salesforce ‘googleDrive -> Field Name –’ Google API Key’)

- Create an OAuth Client ID Credentials

APIs and services

Credentials [+ CREATE CREDENTIALS](#) [DELETE](#) [RESTORE DELETED CREDENTIALS](#)

Enabled APIs and services

Library

Credentials

OAuth consent screen

Page usage agreements

Create credentials to access your project

Remember this credential

API key

API key identifies your project using a simple API key to check quota and access

OAuth client ID

Requests user consent so that your app can access the user's data.

Service account

Enables server-to-server, app-level authentication using robot accounts

Help me choose

Asks a few questions to help you decide which type of credential to use

Configure consent screen

SHOW KEY

OAuth 2.0 Client IDs

Name	Creation date	Type	Client ID	Actions
No OAuth clients to display				

- Click on **Configure Consent Screen** and Click on **External**

Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

To create an OAuth client ID, you must first configure your consent screen

[CONFIGURE CONSENT SCREEN](#)

OAuth consent screen

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

User Type

☐ Internal ?

Only available to users within your organisation. You will not need to submit your app for verification. [Learn more about user type](#)

☒ External ?

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)

[CREATE](#)

Click on **Create** and you will navigate to **Edit app registrations** page. Enter the **App Name**, **User support email**, enter the **Authorized domain** as "salesforce.com". Also enter the required email field in the end and click on **Save and Continue** button

Edit app registration

1 OAuth consent screen

2 Scopes

3 Test users

4 Summary

App information

This shows in the consent screen, and helps end users know who you are and contact you

App name *

File Collab App

The name of the app asking for consent

User support email *

jazmincrown@gmail.com

For users to contact you with questions about their consent. [Learn more](#)

App logo

This is your logo. It helps people to recognise your app and is displayed on the OAuth consent screen.
After you upload a logo, you will need to submit your app for verification unless the app is configured for internal use only or has a publishing status of 'Testing'. [Learn more](#)

Logo file to upload

BROWSE

Upload an image, not larger than 1 MB on the consent screen that will help users recognise your app. Allowed image formats are JPG, PNG and BMP. Logos should be square and 120px by 120px for the best results.

App domain

To protect you and your users, Google only allows apps using OAuth to use Authorised Domains. The following information will be shown to your users on the consent screen.

Application home page

Provide users a link to your home page

Application privacy policy link

Provide users a link to your public privacy policy

Application Terms of Service link

Provide users a link to your public Terms of Service

Authorised domains

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the [Google Search Console](#) to check if your domains are authorised. [Learn more](#) about the authorised domain limit.

Authorised domain 1 *

salesforce.com

+ ADD DOMAIN

Developer contact information

Email addresses *

jazmincrown@gmail.com

These email addresses are for Google to notify you about any changes to your project.

SAVE AND CONTINUE

CANCEL

- After Click on Save and Continue -> Click on **ADD OR REMOVE SCOPES**

File Collab App

Search (/) for resources, docs

Update selected scopes

1

Only scopes for enabled APIs are listed below. To add a missing scope to this screen, find and enable the API in the [Google API Library](#) or use the Pasted Scopes text box below. Refresh the page to see any new APIs you enable from the Library.

Filter

Enter property name or value

☐	API	Scope	User-facing description
☐		.../auth/userinfo.email	See your primary Google Account email address
☐		.../auth/userinfo.profile	See your personal info, including any personal info you've made publicly available
☐		openid	Associate you with your personal info on Google
☐	BigQuery API	.../auth/bigquery	View and manage your data in Google BigQuery and see the email address for your Google Account
☐	BigQuery API	.../auth/cloud-platform	See, edit, configure and delete your Google Cloud data and see the email address for your Google Account.
☐	BigQuery API	.../auth/bigquery.readonly	View your data in Google BigQuery
☐	BigQuery API	.../auth/cloud-platform.read-only	View your data across Google Cloud services and see the email address of your Google Account
☐	BigQuery API	.../auth/devstorage.full_control	Manage your data and permissions in Cloud Storage and see the email address for your Google Account
☐	BigQuery API	.../auth/devstorage.read_only	View your data in Google Cloud Storage

Edit app registration

OAuth consent screen

Scopes

Scopes express the permissions that you request your app and allow your project to access specific data from their Google Account. [Learn more](#)

ADD OR REMOVE SCOPES

Your non-sensitive scopes

API

Scope

User-facing description

No rows to display

Your sensitive scopes

Sensitive scopes are scopes that request access to private information.

- Click On **Update** Button at the End

After selecting all the scopes, the screen will look something like this. Make sure you have selected all drive scopes and click on **Save and Continue**

- Your non-sensitive scopes
- Your sensitive scopes
- Your restricted scopes
- Gmail scopes

Once everything is filled you will be able to see **Back to Dashboard** as shown in the screenshot below

APIs and services

Enabled APIs and services

Library

Credentials

OAuth consent screen

Page usage agreements

Edit app registration

API	Scope	User-facing description
	...read-only	address or your Google Account
BigQuery API	.../auth/devstorage.full_control	Manage your data and permissions in Cloud Storage and see the email address for your Google Account
BigQuery API	.../auth/devstorage.read_only	View your data in Google Cloud Storage
BigQuery API	.../auth/devstorage.read_write	Manage your data in Cloud Storage and see the email address of your Google Account

Rows per page:

10

1 - 10 of 40

Test users

EDIT

0 users (0 test, 0 other) / 100 user cap

Filter

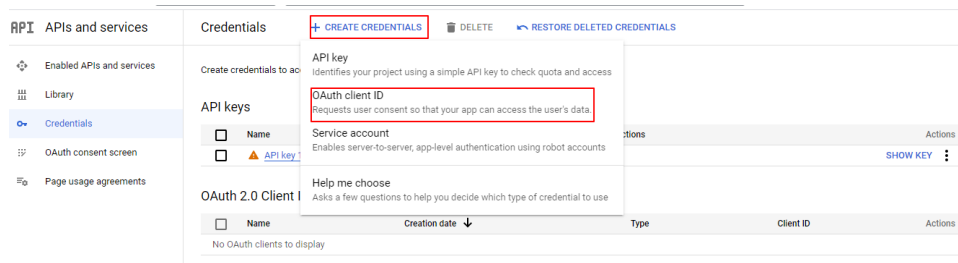
Enter property name or value

User information

No rows to display

BACK TO DASHBOARD

- Go Back to **Credentials** and select **OAuth Client Id**



- Select the Application type as **Web Application** and Click on Create Button

← Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *
Web application ▼

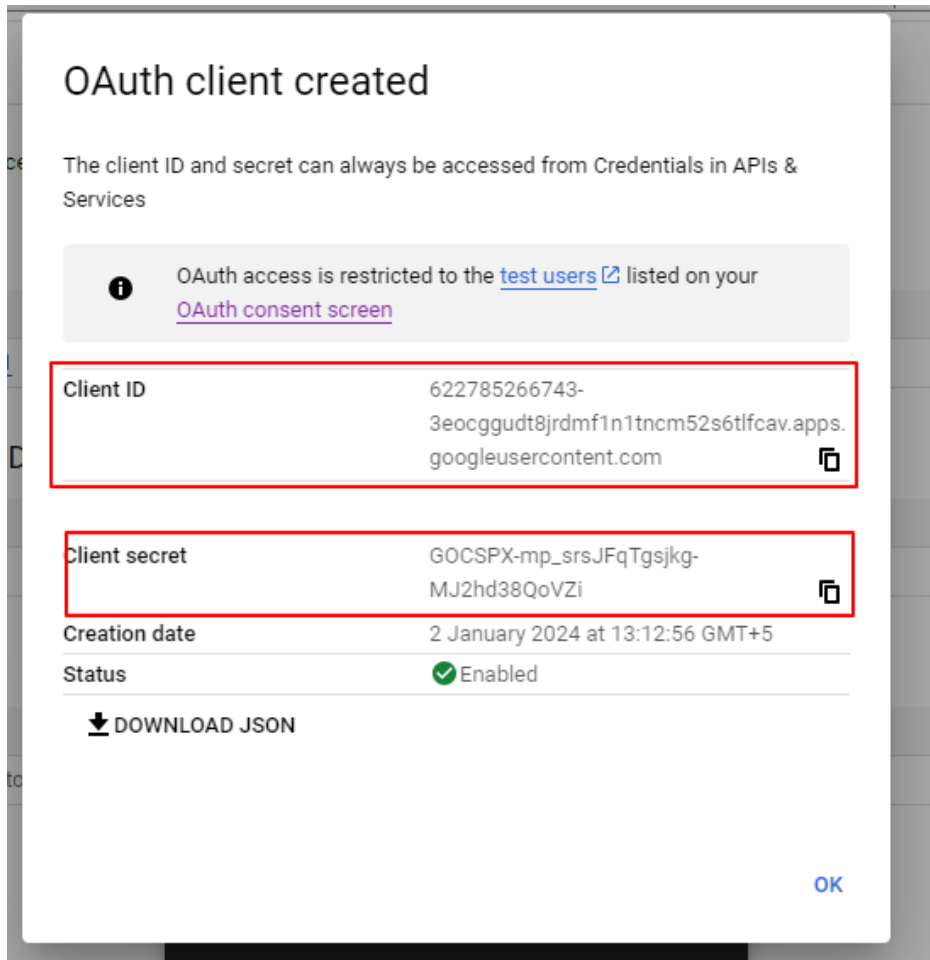
Name *
Web client 1

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.



The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorised domains](#).

- Click on Create button and Dialog box will appear with Client ID and Client Secret



Copy the Client Id and Client Secret and go back to Salesforce Org. Enter both the keys in Auth Provider.

Enter Client Id in **Consumer Key** and Client Secret key in **Consumer Secret** in Auth Provider in Salesforce

- **Create an Auth Provider in Salesforce from Setup**
 - Enter Auth Provider in Setup
 - Click New
 - Select 'Google' in Picklist

Auth. Provider Edit

Provider Type: Google

Name:

URL Suffix:

Consumer Key:

Consumer Secret:

Authorize Endpoint URL: <https://accounts.google.com/o/oauth2/auth>

Token Endpoint URL: <https://accounts.google.com/o/oauth2/token>

User Info Endpoint URL: <https://www.googleapis.com/oauth2/v3/userinfo>

Use Proof Key for Code Exchange (PKCE) Extension: ☒

Default Scopes:

Include Consumer Secret in SOAP API Responses: ☒

Custom Error URL:

Custom Logout URL:

Registration Handler: [Automatically create a registration handler template](#)

Execute Registration As:

Portal: --None--

Icon URL: [Choose one of our sample icons](#)

Use Salesforce MFA for this SSO Provider: ☐

Save Save & New Cancel

- Add Auth Name - ' Google_Auth '
- URL Suffix - ' Google_Auth '
- Consumer Key – From OAuth Client Id
- Consumer Secret – From OAuth Client Secret
- Authorize Endpoint URL - 'https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force'
- Token EndPoint URL - '<https://accounts.google.com/o/oauth2/token>'
- User Info Endpoint URL - '<https://www.googleapis.com/oauth2/v3/userinfo>'
- Default Scopes - ' openid email profile <https://www.googleapis.com/auth/drive> '
- Include Consumer Secret in SOAP API Responses – Checkbox Checked
- Click to Save Button

Auth. Provider	
Auth. Provider Detail	
Auth. Provider ID	0SO2t000000gcyX
Provider Type	Google
Name	Google Auth
URL Suffix	Google_Auth
Consumer Key	
Consumer Secret	Click to reveal
Authorize Endpoint URL	https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force
Token Endpoint URL	https://accounts.google.com/o/oauth2/token
User Info Endpoint URL	https://www.googleapis.com/oauth2/v3/userinfo
Use Proof Key for Code Exchange (PKCE) Extension	☐
Default Scopes	openid email profile https://www.googleapis.com/auth/drive
Include Consumer Secret in SOAP API Responses	☒
Custom Error URL	

Now Go back to Salesforce Org and Navigate to Setup -> Auth Provider -> **Google Auth**

And copy the **Callback URL**

Auth. Providers

Get into Lightning URL: <https://www.googleapis.com/oauth2/v2/authorize>

Use Proof Key for Code Exchange (PKCE) Extension: ☐

Default Scopes: openid email profile <https://www.googleapis.com/auth/drive>

Include Consumer Secret in SOAP API Responses: ☒

Custom Error URL:

Custom Logout URL:

Registration Handler:

Execute Registration As: Portal

Icon URL:

Use Salesforce MFA for this SSO Provider: ☐

Salesforce Configuration

Test-Only Initialization URL	https://testabccom3-dev-ed.develop.my.salesforce.com/services/auth/test/Google_Auth
Existing User Linking URL	https://testabccom3-dev-ed.develop.my.salesforce.com/services/auth/link/Google_Auth
OAuth-Only Initialization URL	https://testabccom3-dev-ed.develop.my.salesforce.com/services/auth/oauth/Google_Auth
Callback URL	https://testabccom3-dev-ed.develop.my.salesforce.com/services/authcallback/Google_Auth
Single Logout URL	https://testabccom3-dev-ed.develop.my.salesforce.com/services/auth/rp/oidc/logout

[Edit](#) [Delete](#) [Clone](#)

Callback URL - https://testabccom3-dev-ed.develop.my.salesforce.com/services/authcallback/Google_Auth

Authorised Javascript origins - <https://testabccom3-dev-ed.develop.my.salesforce.com>

Enter the URL till salesforce.com as shown in screenshot below

Authorised redirect URIs - Enter the Same copied URL

- Add the Trusted URL Side for in Salesforce

- URL - <https://www.googleapis.com>

Trusted URLs

Specify the URLs that you trust to interact with your users and network. You can use Content Security Policy (CSP) directives to control the types of resources that Lightning components, third-party APIs, and WebSocket connections can load from each trusted URL. If you enabled the Permissions-Policy HTTP header in Session Settings, you can control which URLs can access browser features from Salesforce.

Related Policies

Content Security Policy (CSP). Use CSP directives to specify whether Lightning components, your CSP-secured [App or LWC files](#), third-party APIs, and WebSockets connections can load scripts, fonts, images, media, or stylesheets from each trusted URL. The main objective of CSP is to help prevent cross-site scripting (XSS) and other code injection attacks.

Permissions Policy. Control access to browser features such as cameras and microphones. To use this policy, enable the Permissions-Policy HTTP header under Browser Feature Permissions in [Session Settings](#).

Trusted URLs

View: [Full](#) [Compact](#) [New View](#)

Action	API Name *	URL	Active	CSP Context	Created By	Created Date	Last Modified By	Last Modified Date
Edit Del	GoogleAPI	https://www.googleapis.com	✓	All	Full	21/02/2024, 11:25 pm	Full	21/02/2024, 11:31 pm

Authorised JavaScript origins ?

For use with requests from a browser

URIs 1 *
https://testabccom3-dev-ed.develop.my.salesforce.com

+ ADD URI

Authorised redirect URIs ?

For use with requests from a web server

URIs 1 *
https://testabccom3-dev-ed.develop.my.salesforce.com/services/authcallback

+ ADD URI

- Go back to Google Drive and Click on Create Credentials -> Service Account

APIs and services

Credentials [+ CREATE CREDENTIALS](#) [DELETE](#) [RESTORE DELETED CREDENTIALS](#)

Create credentials to access your APIs

API keys

- ☐ Name
- ☐ [API key](#)

OAuth 2.0 Client IDs

- ☐ Name
- ☐ [Web client 1](#)

Service account

Enables server-to-server, app-level authentication using robot accounts

Name	Creation date	Type	Client ID
Web client 1	2 Jan 2024	Web application	62278526

- Enter the Service account Name and Click on Done.

← Create service account

- Service account details**

Service account name
File Collab
Display name for this service account

Service account ID *
file-collab
X ↺

Email address: file-collab@file-collab-app-410006.iam.gserviceaccount.com

Service account description
Describe what this service account will do

CREATE AND CONTINUE
- Grant this service account access to the project (optional)**
- Grant users access to this service account (optional)**

DONE
CANCEL

Once you have configured all the things correctly the credentials page will look like this.

- API Keys
- OAuth 2.0 Client IDs
- Service Accounts

APIs and services

Enabled APIs and services

Library

Credentials

OAuth consent screen

Page usage agreements

Credentials

+ CREATE CREDENTIALS

DELETE

RESTORE DELETED CREDENTIALS

Create credentials to access your enabled APIs. [Learn more](#)

API keys

☐	Name	Creation date ↓	Restrictions	Actions
☐	API key 1	2 Jan 2024	None	SHOW KEY ⋮

OAuth 2.0 Client IDs

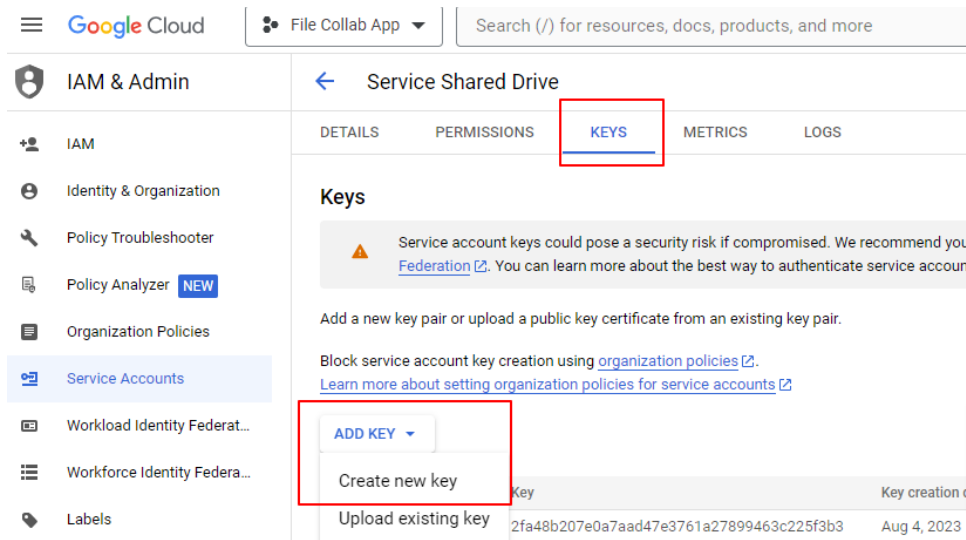
☐	Name	Creation date ↓	Type	Client ID	Actions
☐	Web client 1	2 Jan 2024	Web application	622785266743-3e0c...	🔗 🗑️ ⬇️

Service Accounts

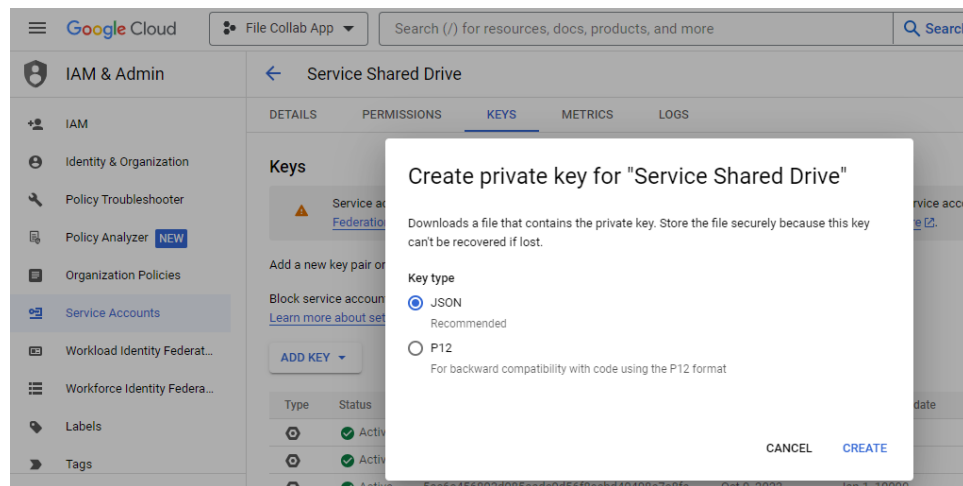
☐	Email	Name ↑	Actions
☐	file-collab@file-collab-app-410006.iam.gserviceaccount.com	File Collab	🔗 🗑️

[Manage service accounts](#)

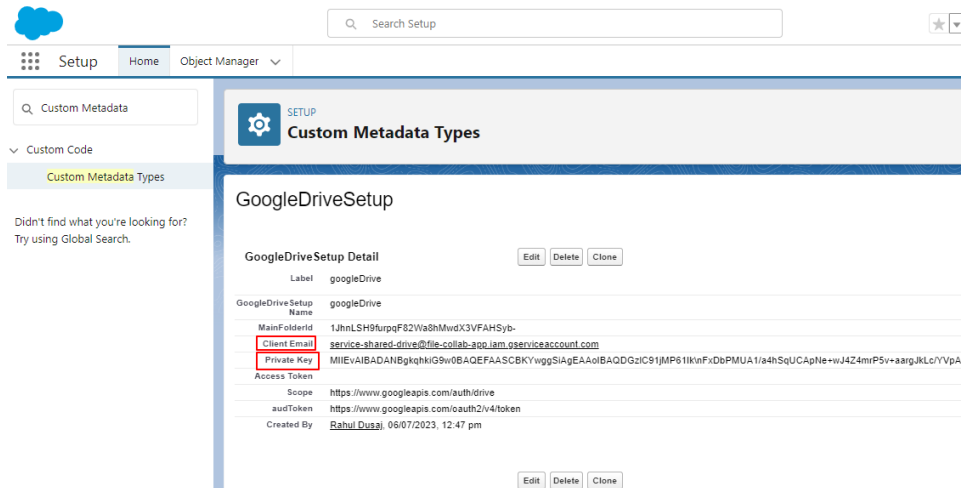
- Now Click on Service Account - > Email - > KEYS



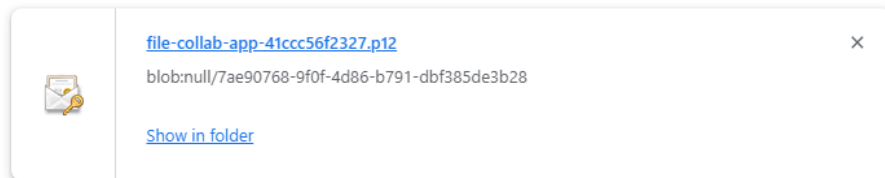
- Now Create a new Key – Create Two Files **JSON** and **P12** Files and **Save the Password of P12 File**



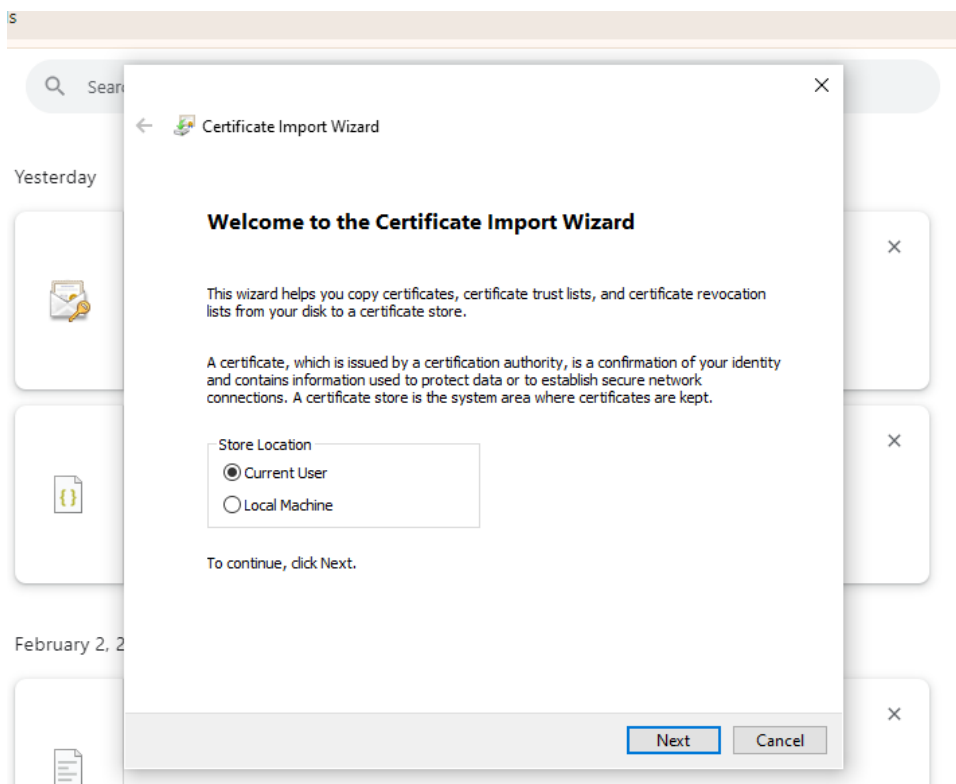
- ON JSON File – You will get – Private Key, Client Email (Note – Please Do not Share this anyone)
- Salesforce – Update the Private Key, Client Email from JSON File, Download from OAuth Client 2.0 Id in Custom Metadata 'GoogleDriveSetup' of Salesforce



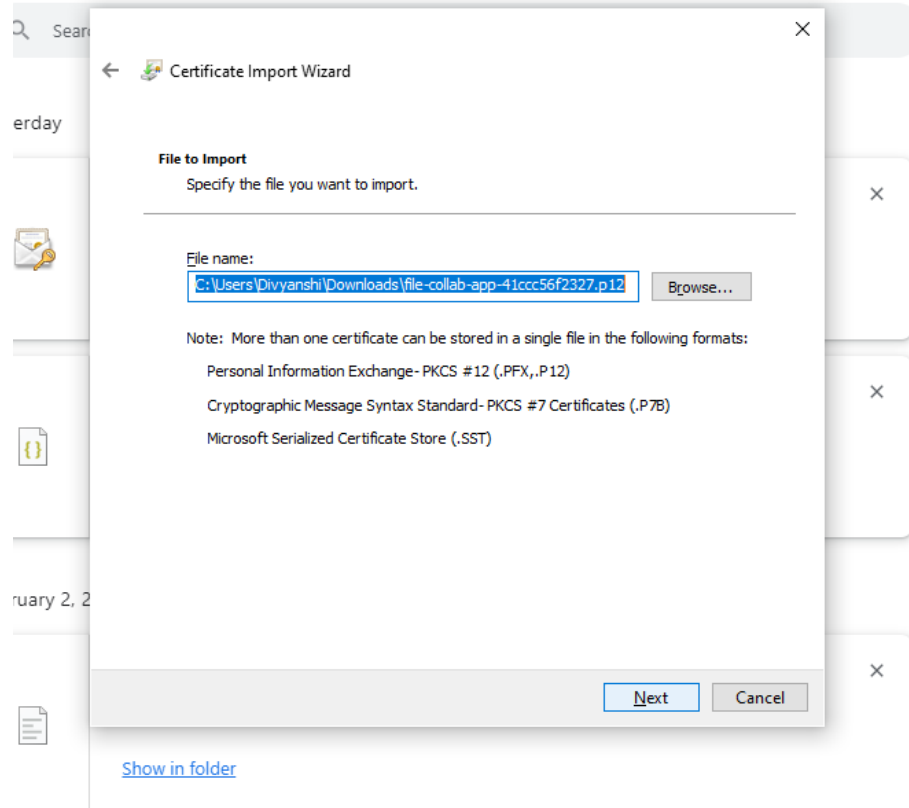
- On P12 File –
 - On Download Section – Click on P12 File
 - 1.



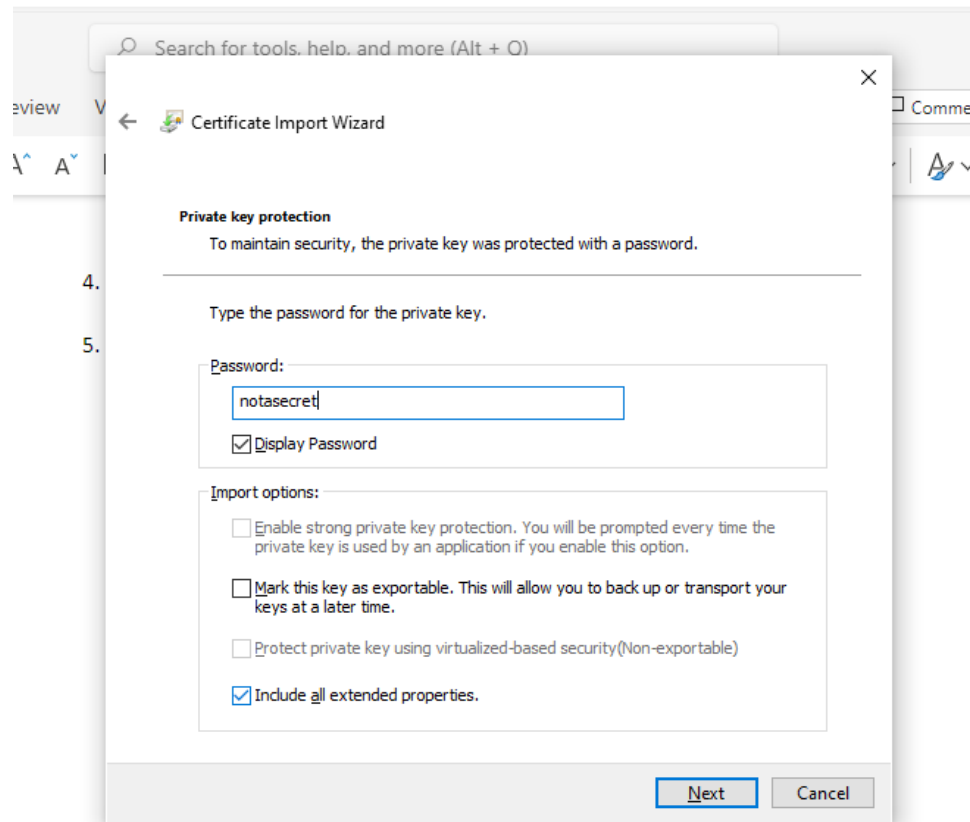
- Select Local Machine



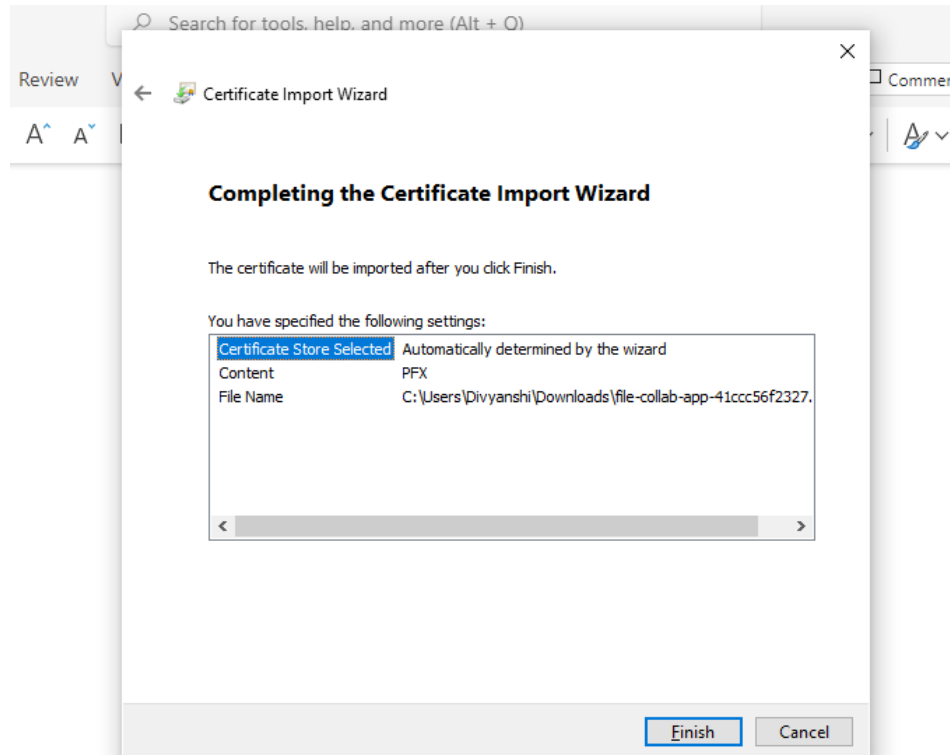
3. Click on Next Button



4. Now Type the Password of P12 File Which is came at download P12 File and Click on Next

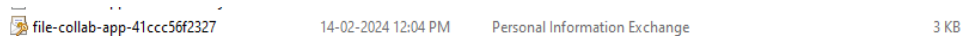


5. Click on Finish Button



6. Now P12 File Will View in your local system

1.



7. If You Have JDK in your system you are ready to go in next step

(System Should Have JDK Environment If not install JDK and Set in Enviroment Variables - <https://www.oracle.com/in/java/technologies/downloads/#jdk21-windows>)

8. Command – Run this command Where You Have downloaded your P12 File - >
To Convert P12 File to JSK File

```
keytool -importkeystore -srckeystore ./yourP12FileName.p12 -destkeystore  
yourP12FileName.jks -srcstorepass notasecret -srcalias privatekey -  
srcstoretype pkcs12 -deststoretype jks -destalias yourP12FileName -  
deststorepass notasecret
```

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Divyanshi\Downloads>keytool -importkeystore -srckeystore ./file-collab-app-41ccc56f2327.p12 -destkeystore file-collab-app-41ccc56f2327.jks -srcstorepass notasecret -srcaalias privatekey -srcstoretype pkcs12 -deststoretype jks -destalias file-collab-app-41ccc56f2327 -deststorepass notasecret
Importing keystore ./file-collab-app-41ccc56f2327.p12 to file-collab-app-41ccc56f2327.jks...

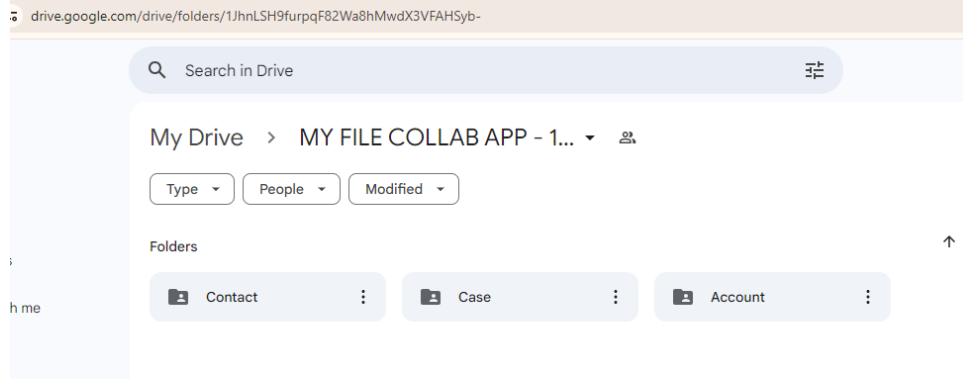
Warning:
[file-collab-app-41ccc56f2327] uses the SHA1withRSA signature algorithm which is considered a security risk.
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore file-collab-app-41ccc56f2327.jks -destkeystore file-collab-app-41ccc56f2327.jks -deststoretype pkcs12".

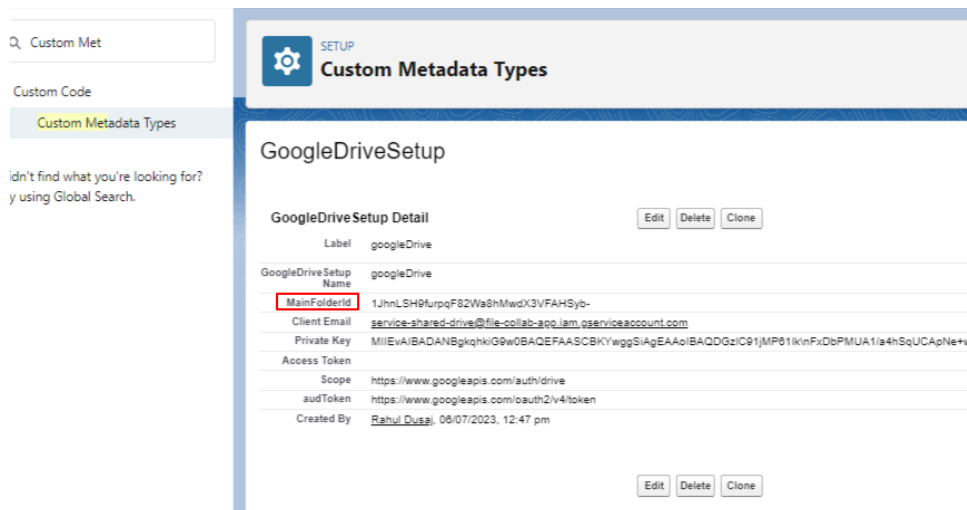
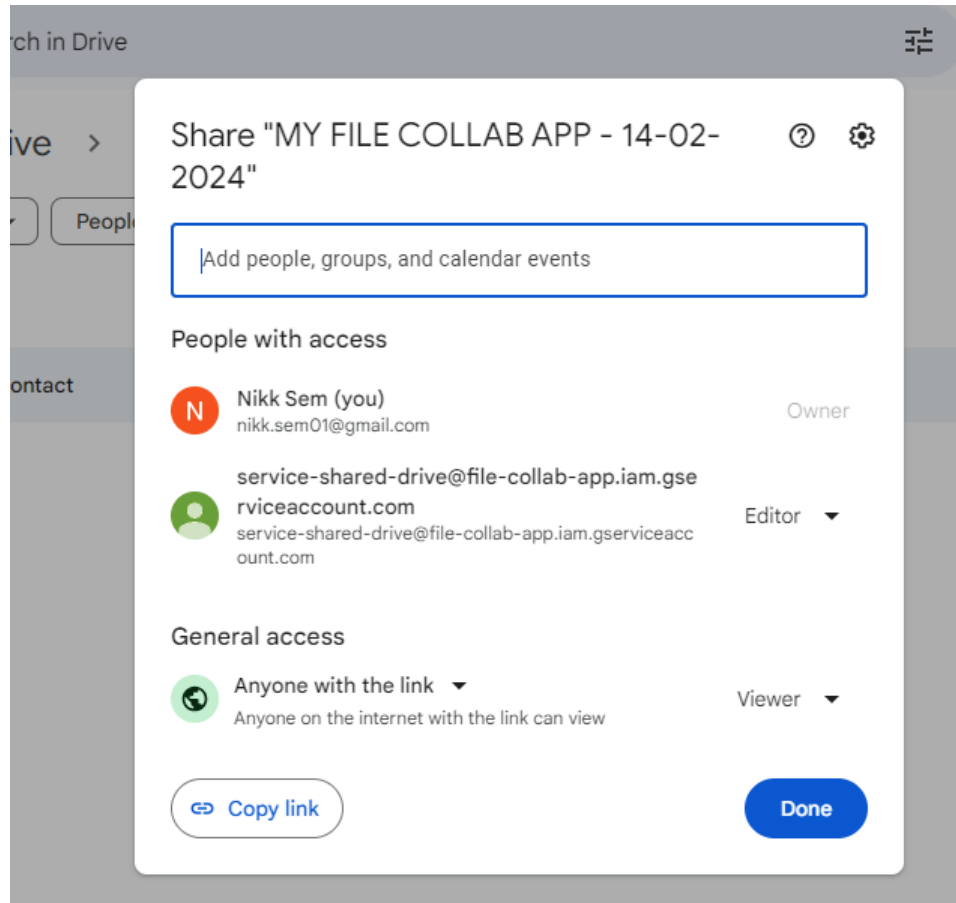
C:\Users\Divyanshi\Downloads>
```

PC > Downloads

Name	Date modified	Type	Size
Today (1)			
file-collab-app-41ccc56f2327.jks	15-02-2024 12:47 PM	JKS File	5 KB

9. Create a Folder in Google Drive and Share the Folder with client Email and Update the Folder Id in Custom Metadata - " of Salesforce

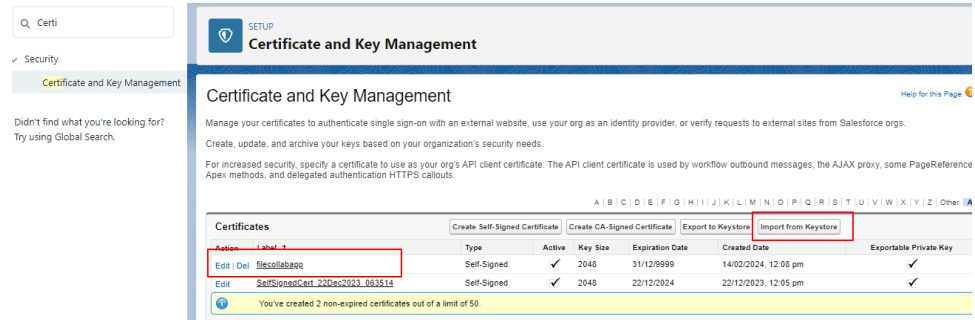




10. Now Go to Salesforce -

1. Enable Identity Provide from Setup Side
2. Go to Certificate and Key Management from Setup

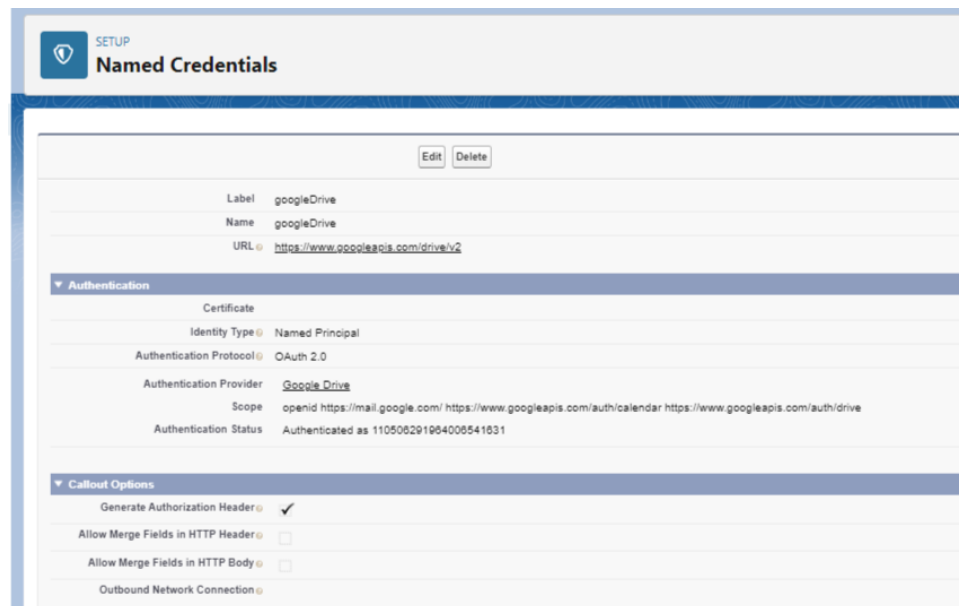
3. Click on Import from Key Store – Upload your JKS File – Type the P12 Password



4. Go to Named Credential from Setup -> Click googleDrive Named Credential – Edit -> Add the Auth Provider -> Check the checkbox of Generate Authorization Header -> Save

Scope -

'openid https://mail.google.com/https://www.googleapis.com/auth/calendar
https://www.googleapis.com/auth/drive'



After the on save button - Follow - Step 7

5. Named Credential – DeleteNamed – Add the JKS File Certificate on Certificate Section -> Add the Auth Provider -> Unchecked the checkbox of **Generate Authorization Header** in Callout Options

Scope - openid

<https://mail.google.com/https://www.googleapis.com/auth/calendar>

<https://www.googleapis.com/auth/drive>

The screenshot shows the 'Named Credential: DeletNamed' configuration page in Salesforce. The page includes a title bar, a description, a 'Back to Named Credentials' link, and an 'Edit' button. The configuration is divided into three main sections: 'Authentication', 'Callout Options', and 'Outbound Network Connection'. The 'Authentication' section shows the 'Certificate' as 'googlebottle', 'Identity Type' as 'Named Principal', 'Authentication Protocol' as 'OAuth 2.0', 'Authentication Provider' as 'Google Auth', 'Scope' as 'openid https://mail.google.com/ https://www.googleapis.com/auth/calendar https://www.googleapis.com/auth/drive', and 'Authentication Status' as 'Authenticated as 11050829195400541831'. The 'Callout Options' section shows four checkboxes: 'Generate Authorization Header' (unchecked), 'Allow Merge Fields in HTTP Header' (unchecked), 'Allow Merge Fields in HTTP Body' (unchecked), and 'Outbound Network Connection' (unchecked).

Named Credential: DeletNamed	
Specify the callout endpoint's URL and the authentication settings that are required for Salesforce to make callouts to the remote system.	
Back to Named Credentials	
Edit	
Label	DeletNamed
Name	DeletNamed
URL	https://www.googleapis.com/drive/v3/files
Authentication	
Certificate	googlebottle
Identity Type	Named Principal
Authentication Protocol	OAuth 2.0
Authentication Provider	Google Auth
Scope	openid https://mail.google.com/ https://www.googleapis.com/auth/calendar https://www.googleapis.com/auth/drive
Authentication Status	Authenticated as 11050829195400541831
Callout Options	
Generate Authorization Header	☐
Allow Merge Fields in HTTP Header	☐
Allow Merge Fields in HTTP Body	☐
Outbound Network Connection	☐

After Save Button - Follow Step - 7

6. Named Credential - "Service_Drive" -> Click Edit -> Add Certificate Generate Authorization Header -> Add the Auth Provider -> Check the Chekbox of Generate Authorization Header

Scope -

openid <https://mail.google.com/https://www.googleapis.com/auth/calendar>

<https://www.googleapis.com/auth/drive>

SETUP
Named Credentials

Edit Delete

Label	Service Drive
Name	Service_Drive
URL	https://www.googleapis.com/oauth2/v4/token

Authentication

Certificate	googlecsfile
Identity Type	Named Principal
Authentication Protocol	OAuth 2.0
Authentication Provider	Google Drive
Scope	openid https://mail.google.com/ https://www.googleapis.com/auth/calendar https://www.googleapis.com/auth/drive
Authentication Status	Authenticated as 110506291984006541631

Callout Options

Generate Authorization Header	☒
Allow Merge Fields in HTTP Header	☐
Allow Merge Fields in HTTP Body	☐
Outbound Network Connection	☐

7. Enter your Google Drive Email Id and Password

Sign in with Google

Sign in
to continue to [salesforce.com](https://www.salesforce.com)

Email or phone

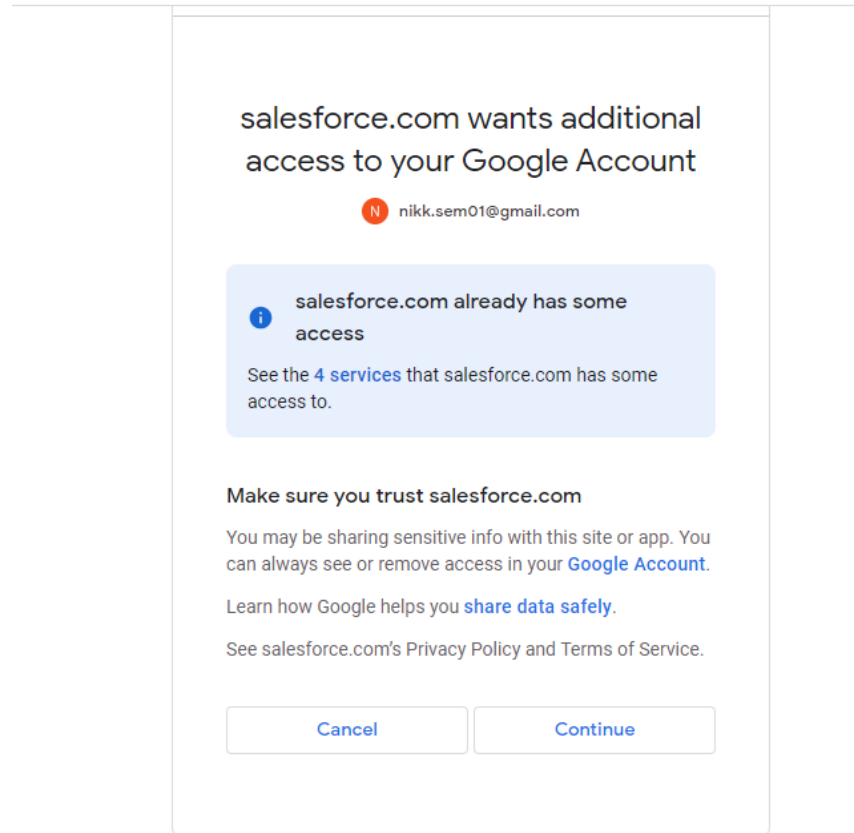
[Forgot email?](#)

To continue, Google will share your name, email address, language preference, and profile picture with salesforce.com.

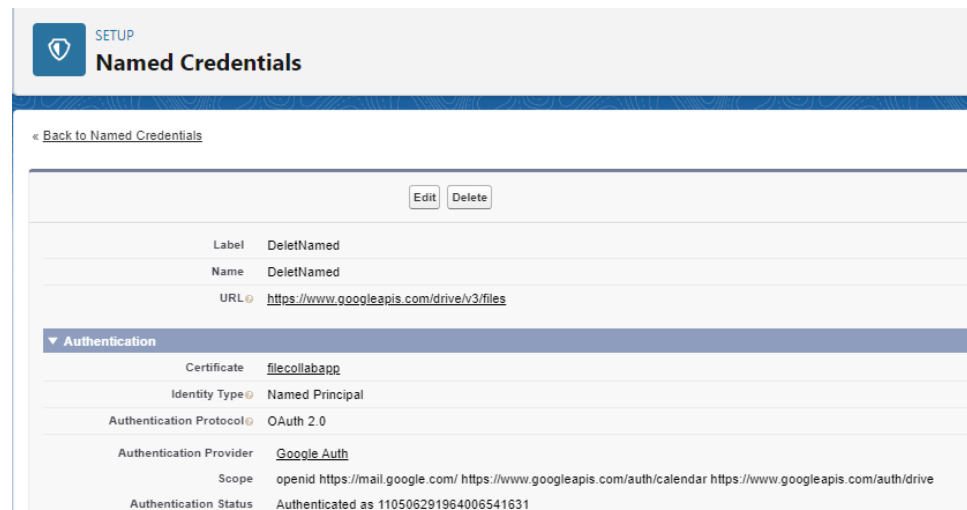
Next

8. Click on Advance – Click on Go to Salesforce.com (Safe) - Continue

nore modern look and feel



9. Now You are Redirect to Salesforce and Check Authenticated Status should be like this



10. Now please do same process for further two named credential as well
11. Go to Remote Site Setting -> Enter the URL - <https://www.googleapis.com>

12. Now Drop the File Collab Component – Go to App Launcher -> Select Object -> Record -> Click on Edit Page -> Drop 'CustomFileUploadLWC' From Search Box