

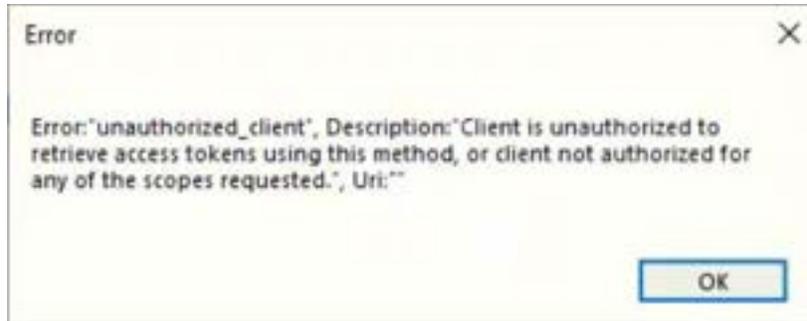
Kernel G Suite Backup

Troubleshooting Guide



'Unauthorized Client Error' in Kernel G Suite Backup Tool

When the Kernel G Suite Backup tool finds that the client does not have the sufficient authority to process the request, then the software gives an error:

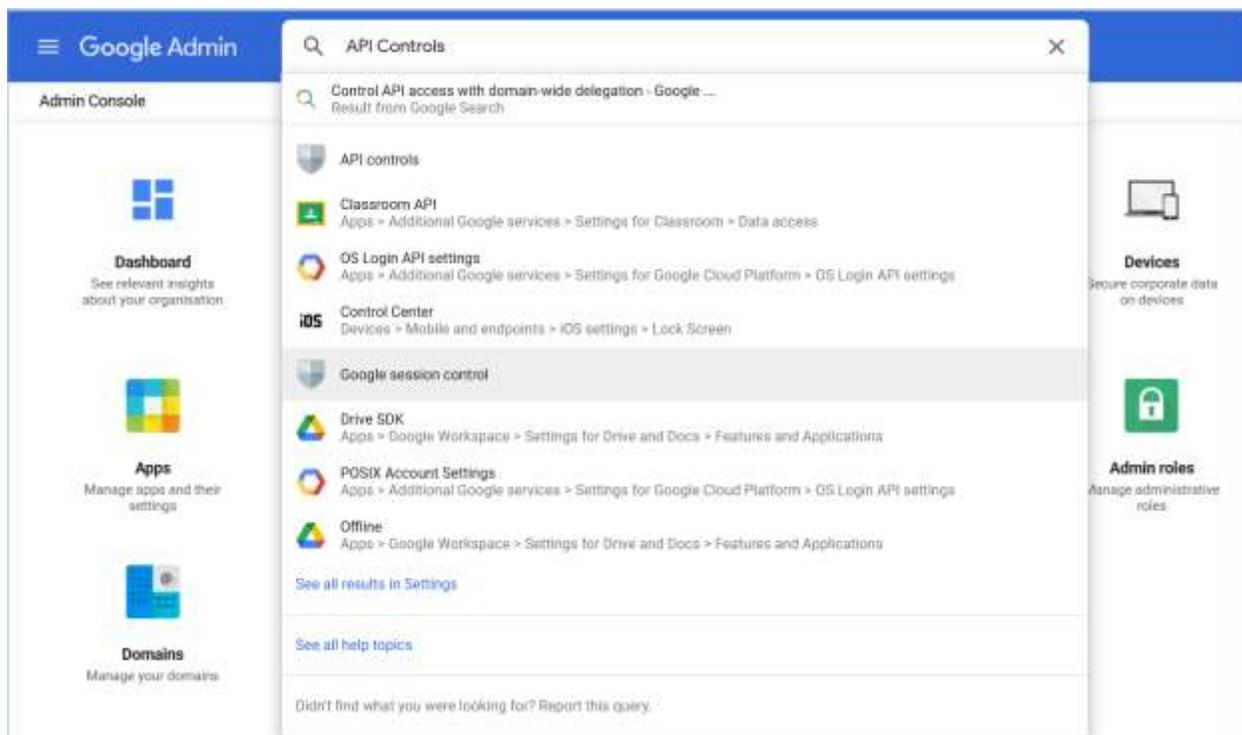


Here is the complete process to overcome the error-

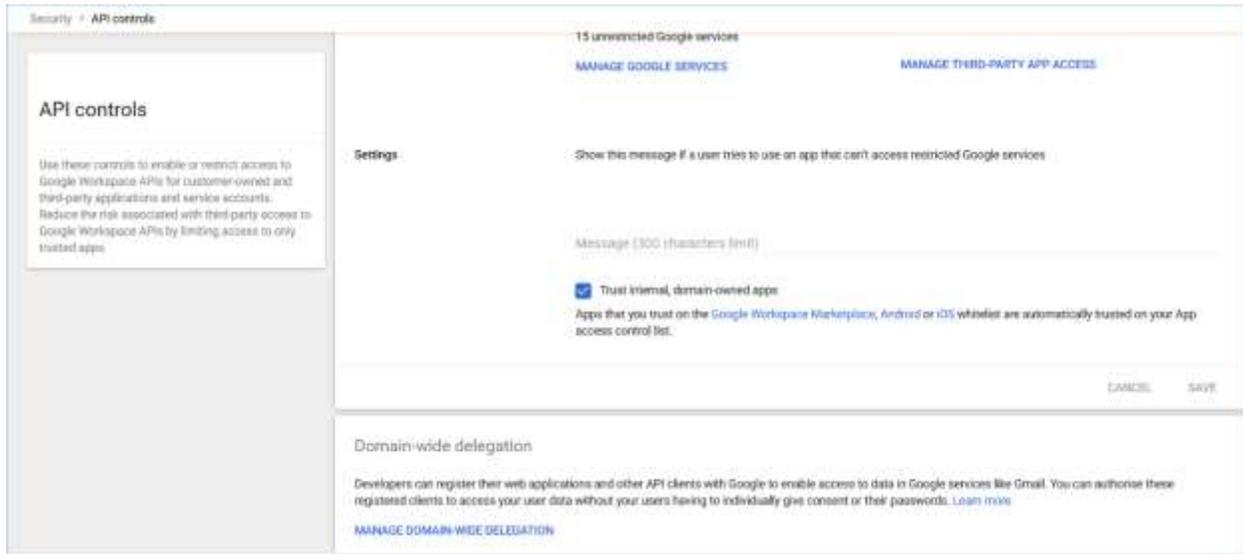
1. Login to Admin console of the G Suite account with the URL – <https://admin.google.com>



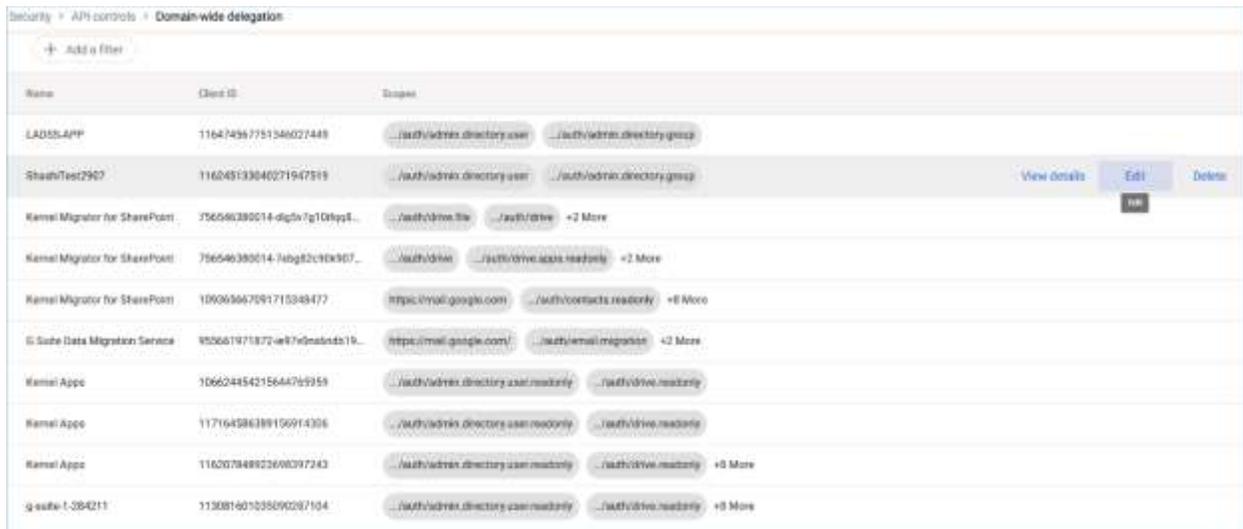
2. In the search bar, type **API Controls** and click it.



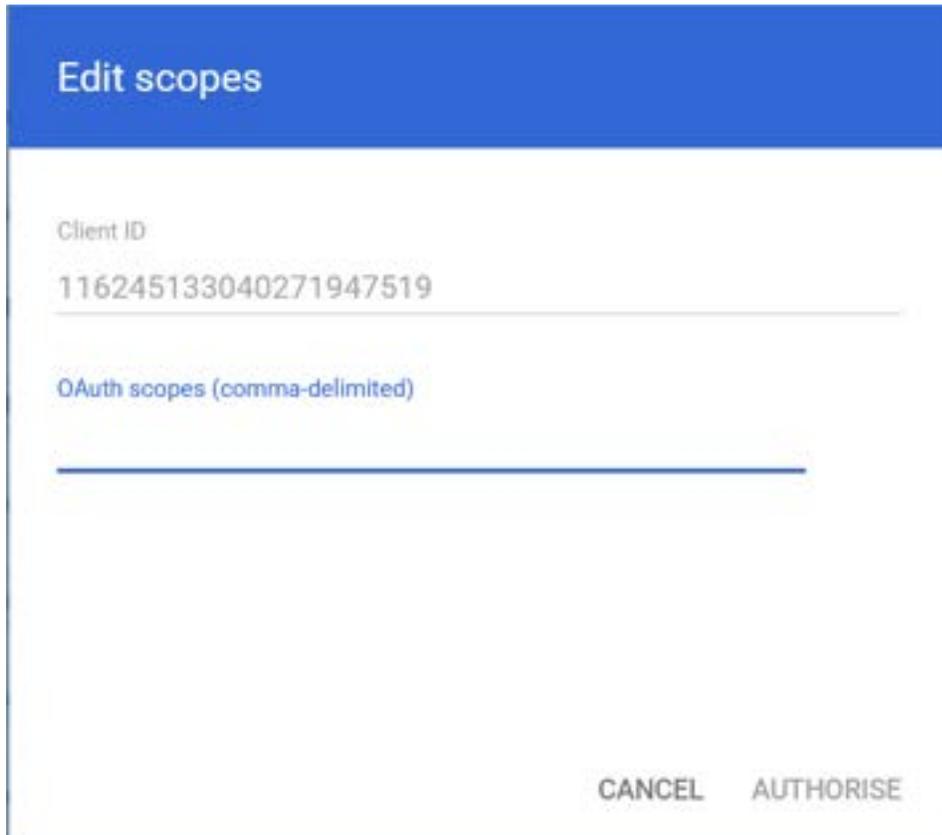
3. Click the option 'Manage Domain-wide delegation' under **Domain-wide delegation**.



4. Choose the service account and click the **Edit** option.

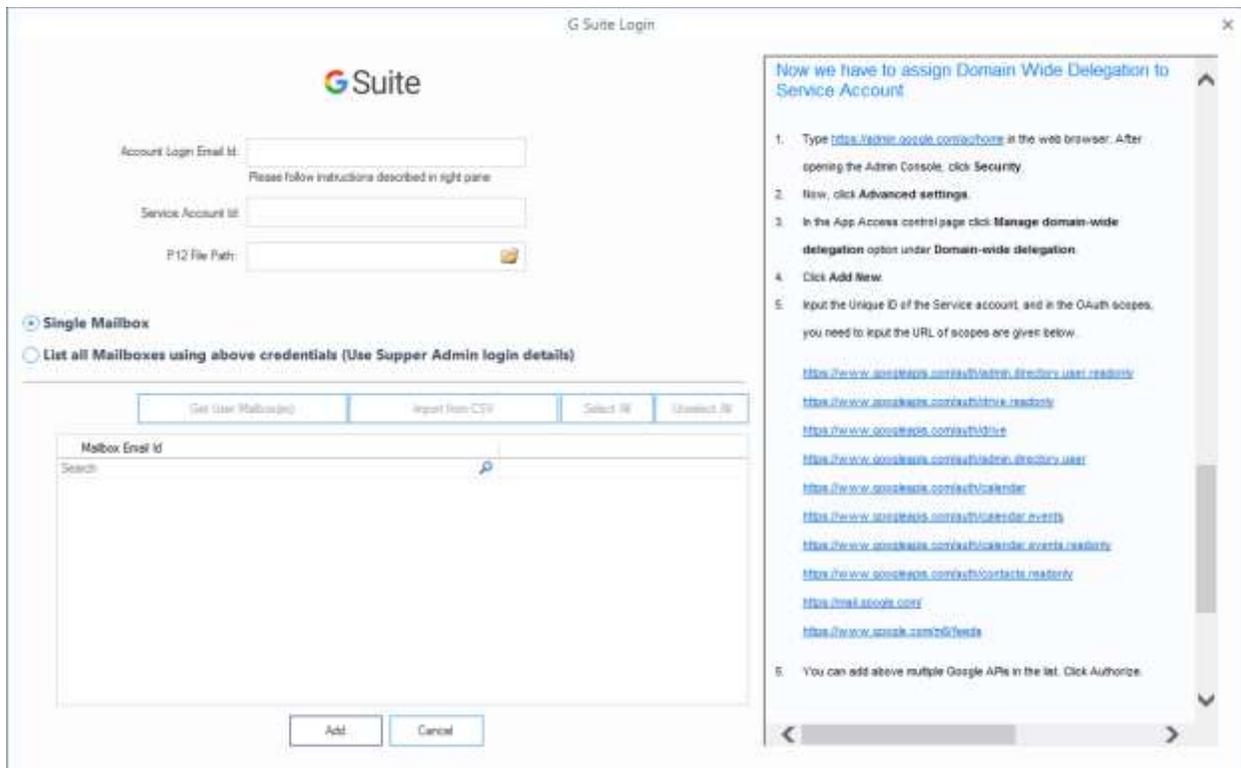


5. You need to fill the **OAuth scopes** field.



The screenshot shows a dialog box titled "Edit scopes" with a blue header. It contains a "Client ID" field with the value "116245133040271947519". Below it is an empty "OAuth scopes (comma-delimited)" field. At the bottom right, there are two buttons: "CANCEL" and "AUTHORISE".

6. Come back to the **G Suite Login** page of the Kernel software and copy the URLs in the help window.



The screenshot shows the "G Suite Login" page. On the left, there are input fields for "Account Login Email Id", "Service Account Id", and "P12 File Path". Below these are radio buttons for "Single Mailbox" (selected) and "List all Mailboxes using above credentials (Use Supper Admin login details)". A table with columns "Get User Mailbox(es)", "Input from CSV", "Select All", and "Unselect All" is visible. Below the table is a "Mailbox Email Id" search box. At the bottom are "Add" and "Cancel" buttons. On the right, a help window is open with the title "Now we have to assign Domain Wide Delegation to Service Account". It contains a numbered list of steps and several URLs for domain-wide delegation.

Now we have to assign Domain Wide Delegation to Service Account

1. Type <https://www.google.com/apps> in the web browser. After opening the Admin Console, click Security.
2. Now, click Advanced settings.
3. In the App Access control page click Manage domain-wide delegation option under Domain-wide delegation.
4. Click Add New.
5. Input the Unique ID of the Service account, and in the OAuth scopes, you need to input the URL of scopes are given below.

<https://www.google.com/apps/admin/directory/user/readonly>

<https://www.google.com/apps/admin/readonly>

<https://www.google.com/apps/admin>

<https://www.google.com/apps/admin/directory/user>

<https://www.google.com/apps/admin/calendar>

<https://www.google.com/apps/admin/calendar/event>

<https://www.google.com/apps/admin/calendar/event/readonly>

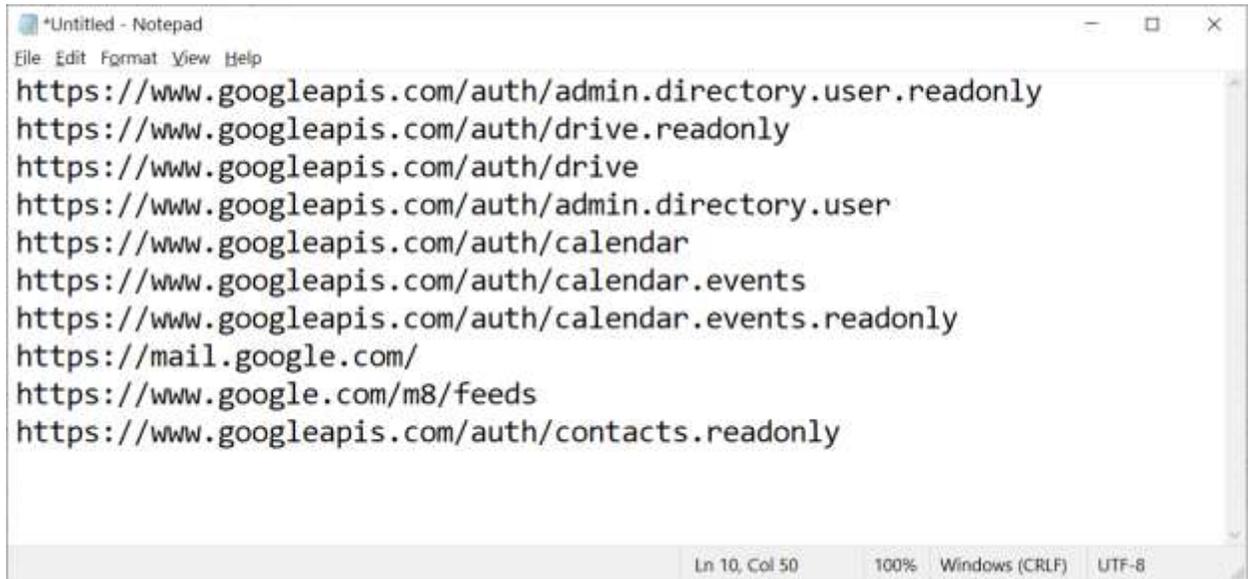
<https://www.google.com/apps/admin/contacts/readonly>

<https://mail.google.com/>

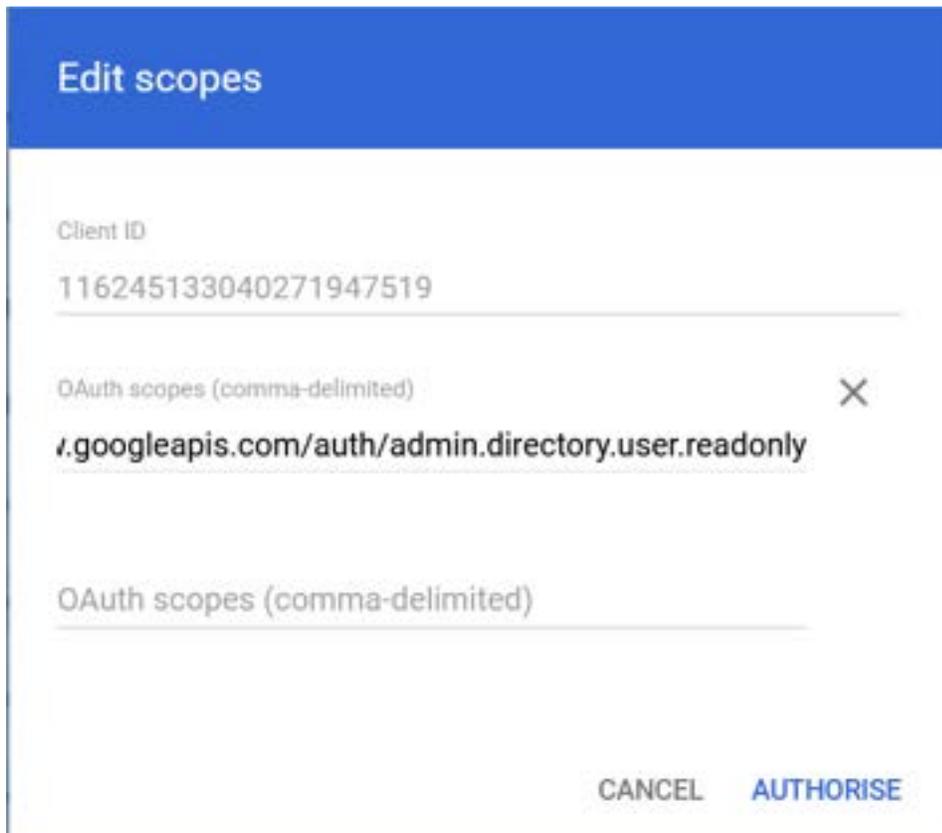
<https://www.google.com/calendar/feeds>

5. You can add above multiple Google APIs in the list. Click Authorize.

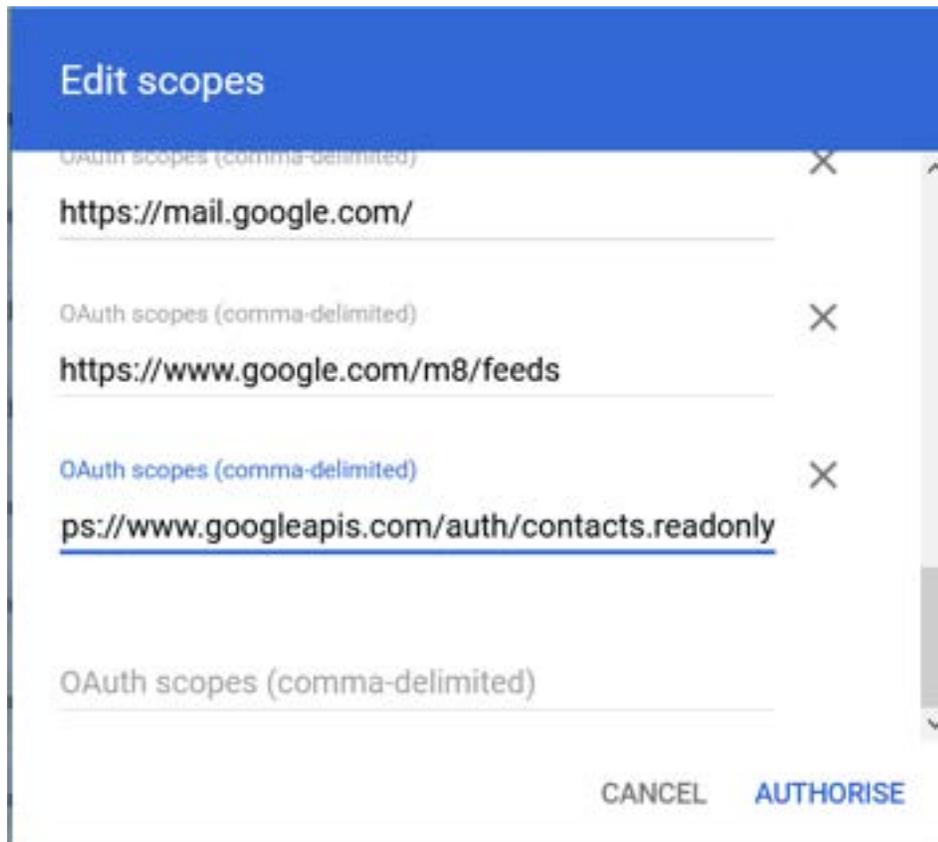
7. Paste all the selected URLs in a Notepad file as it will be easier to select them from there.



8. Copy and paste the first API URL in the **OAuth Scope** field.



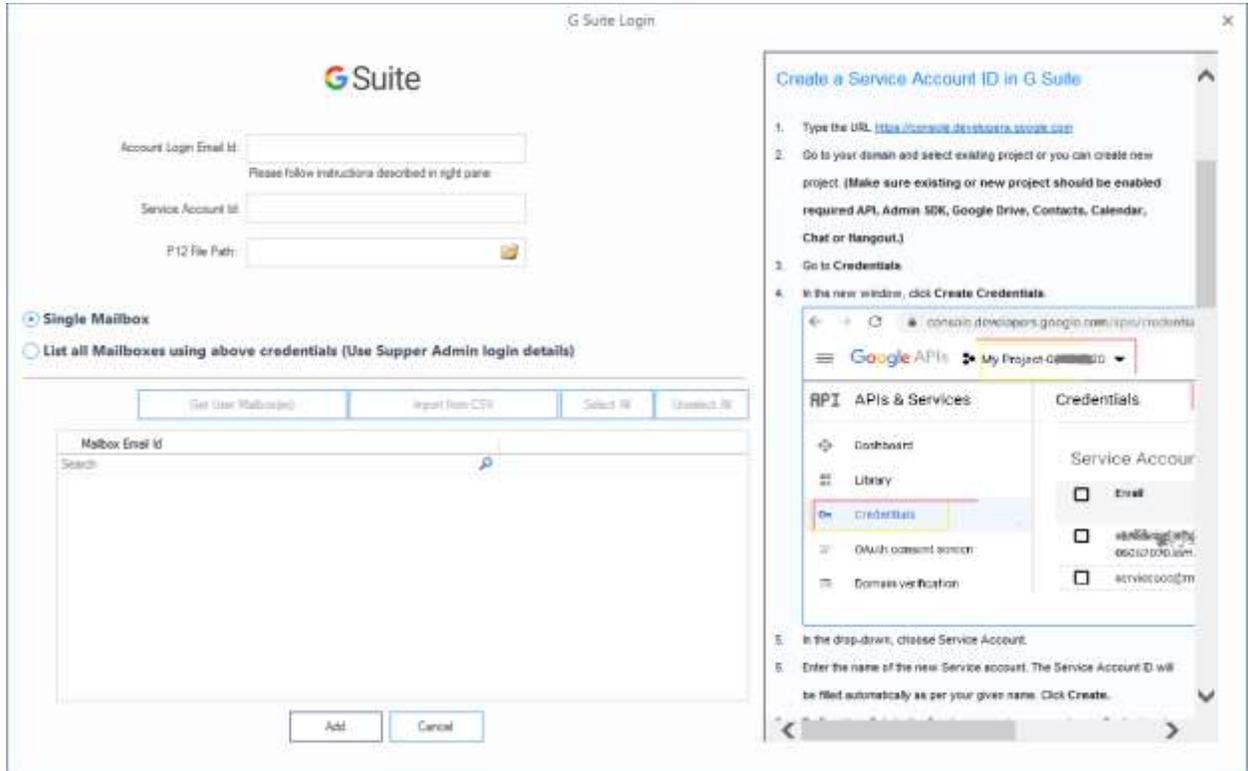
9. Perform the same copy & paste operation to include all the API URLs in the **OAuth Scope** field. Then click the **Authorize** button.



10. A message appears at the bottom of the screen that the client is now updated with 10 scopes.

The OAuth client 116245133040271947519 is now updated with 10 scopes

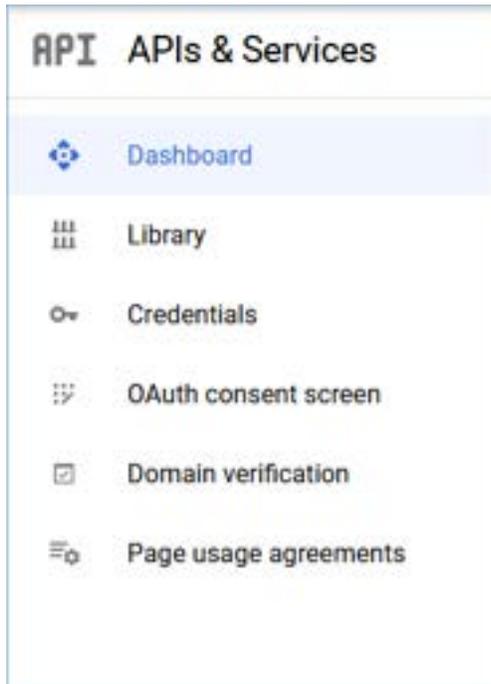
11. Go back to the software window and copy the developer URL from the help section.



12. Open the developer console using the URL – <https://console.developers.google.com>



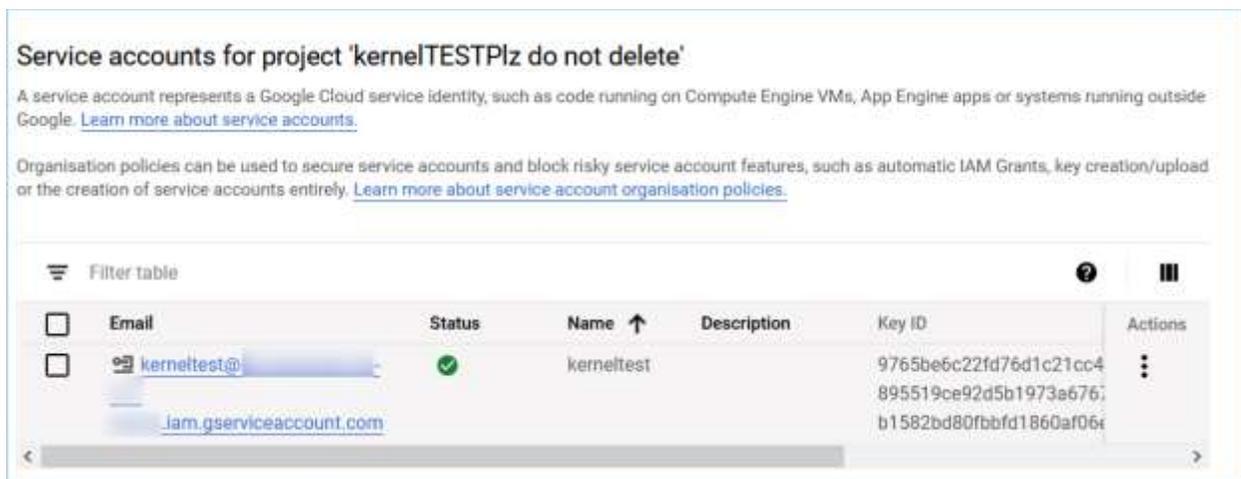
13. Under the **APIs & Services** section, click **Credentials**.



14. Select the service account from the list and click **Manage Service Accounts**.



15. Double-click on the service account.



16. Go to the **Keys** section and click **Add Key**. Then choose the **Create new key** option.

Keys

Add a new key pair or upload a public key certificate from an existing key pair. Please note that public certificates need to be in RSA_X509_PEM format. [Learn more about upload key formats](#)

ADD KEY ▾

- Create new key
- Upload existing key

	Key	Key creation date	Key expiry date	
	9765be6c22fd76d1c21cc4fe8f02d2b3cf364a30	19 Jan 2021	1 Jan 10000	🗑️
🔍	✓ Active 895519ce92d5b1973a67676032e4a09ba29b929a	19 Jan 2021	1 Jan 10000	🗑️
🔍	✓ Active b1582bd80fbbfd1860af06ebdb784944741d4a1d	19 Jan 2021	1 Jan 10000	🗑️

17. Select the second option of **P 12** and click **Create**.

Create private key for 'kerneltest'

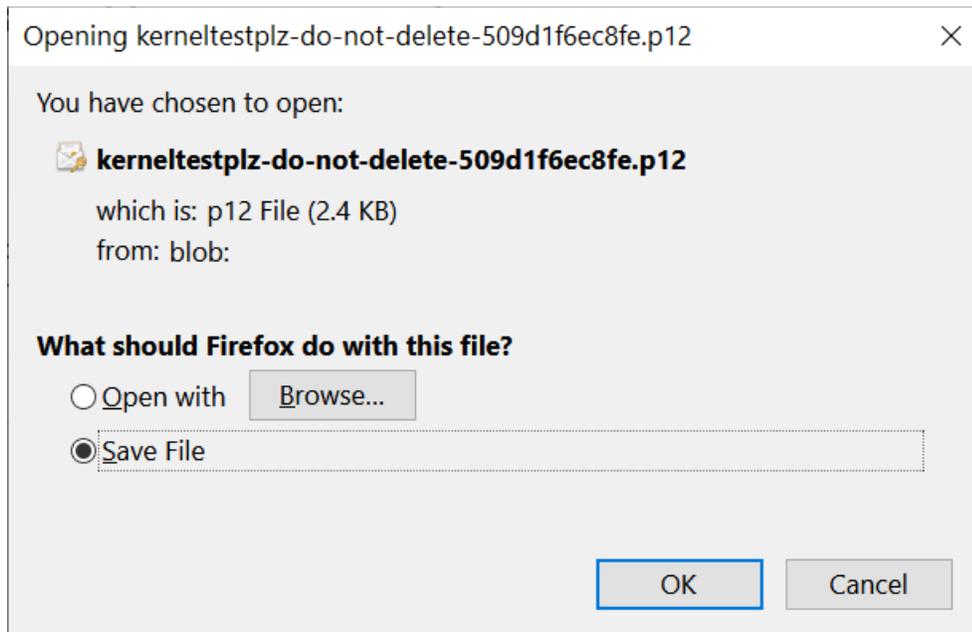
Downloads a file that contains the private key. Store the file securely because this key cannot be recovered if lost.

Key type

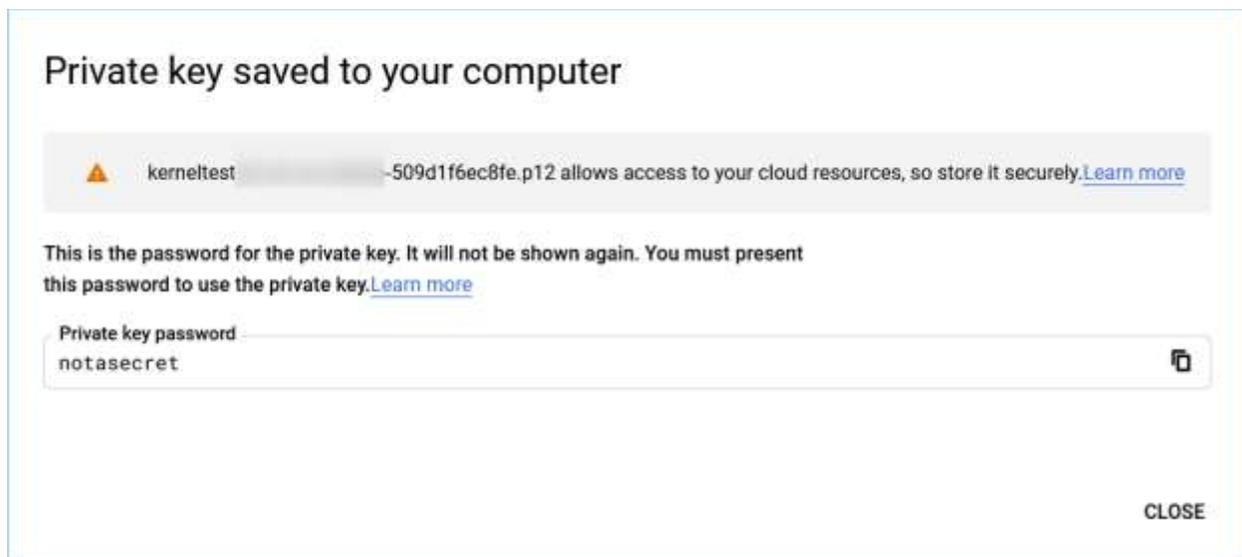
- JSON
Recommended
- P12
For backward compatibility with code using the P12 format

CANCEL CREATE

18. Save the P 12 key. Click OK.



19. A new P 12 key is saved on the local computer. Click Close.



20. Go to **Service account details** on the same page and copy the email address of the service account.

Service account details

Name
kerneltest

Description

Email
kerneltest@.iam.gserviceaccount.com

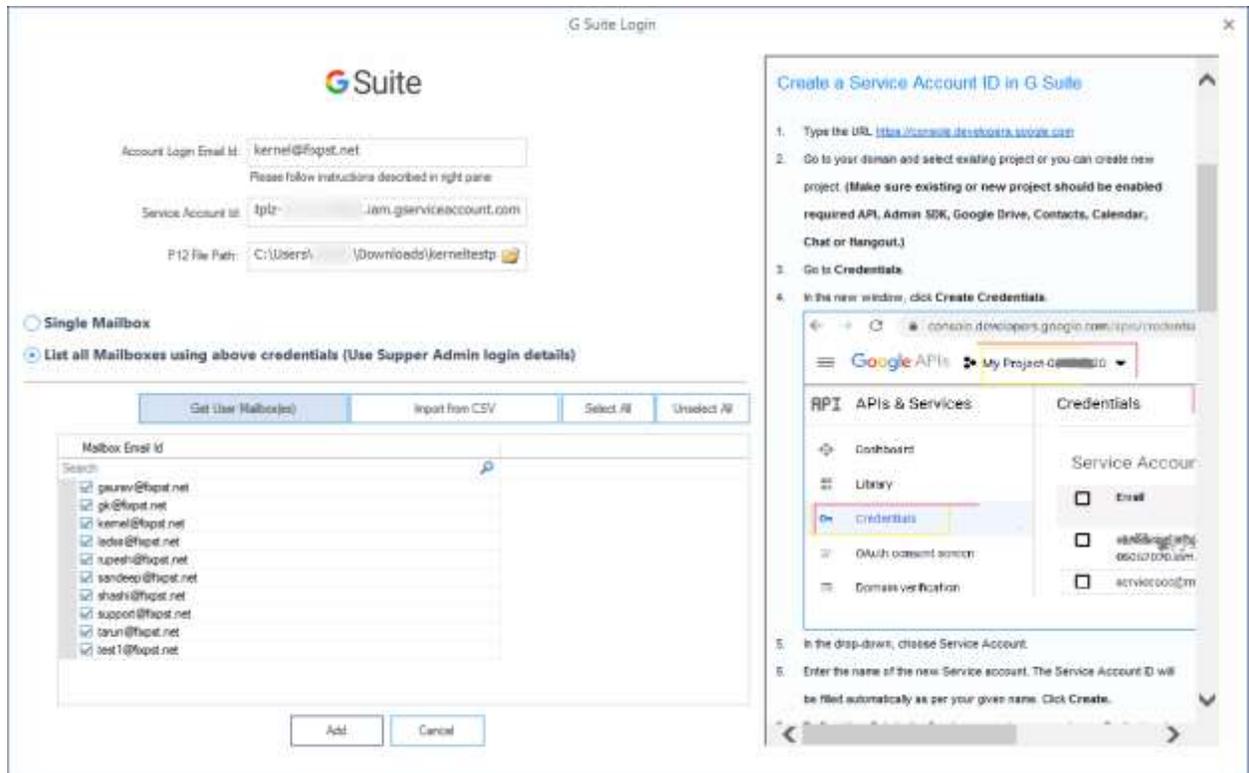
Unique ID
109365667091715348477

Service account status

Disabling your account allows you to preserve your policies without having to delete it.

 Account currently active

21. Finally, come back to the **G Suite Login** page of the software and provide the Super Administrator credentials, the selected service account, and the newly created P 12 key. Then select the second option – **List all mailboxes using above credentials**. Then click the button **Get User Mailboxes**.



The software has successfully retrieved all the G Suite mailboxes without any error.

Contact Us



1-866-348-7872
0-808-189-1438



Support@nucleustechnologies.com
Sales@nucleustechnologies.com



[Talk to Product Specialist](#)

