

Google Analytics API Provider Setup

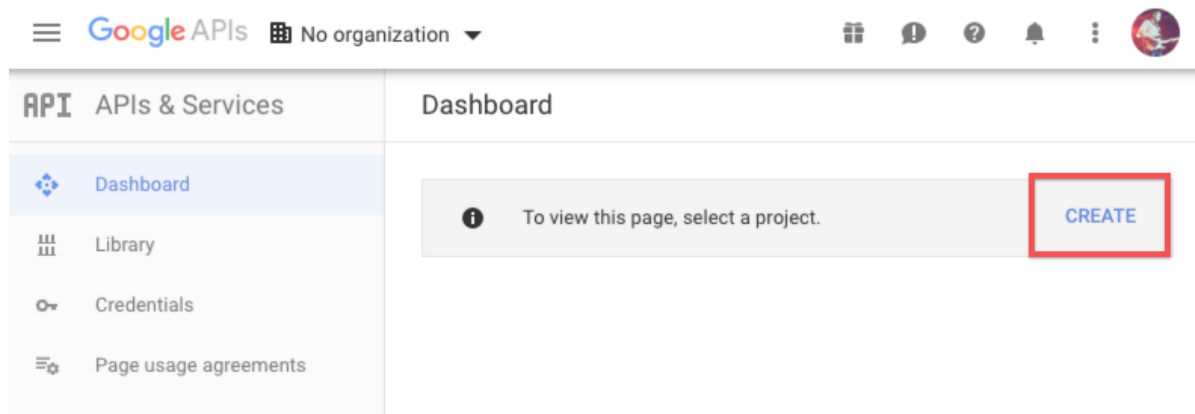
Last Modified on 05/05/2020 5:31 pm EDT

Before you can authenticate an instance of the Google Analytics connector, you must first complete these tasks:

- [Create and register an Analytics project](#)
- [Generate OAuth credentials](#)
- (Optional; only required if authenticating via API) [Record the project's account ID](#)


Creating and Registering an Analytics Project

1. In a web browser, navigate to the [Google APIs Console](#) and sign in to your account.
2. From the Google APIs Dashboard, click Create.




3. On the New Project page, enter a name for your project and select a parent organization or folder (or select [No Organization](#)) from the Location menu. Record the project name that you enter, as you will use it as the Account Name value during authentication. When you are finished, click Create.


New Project

 You have 12 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)

[MANAGE QUOTAS](#)

Project name *
myCoolProject 

Project ID: mycoolproject-250421. It cannot be changed later. [EDIT](#)

Location *
 No organization [BROWSE](#)

Parent organization or folder

[CREATE](#) [CANCEL](#)


After your project is created, the APIs & Services page appears.


- Click Enable APIs and Services.


Google APIs myCoolProject


APIs & Services [+ ENABLE APIS AND SERVICES](#)

APIs & Services

 Dashboard

 Library

 Credentials

 You don't have any APIs available to use yet. To get started, click "Enable APIs and services" or go to the [API library](#)

- On the API Library page, navigate to and select the Google Analytics Reporting API.

Google APIs myCoolProject


Search Google Analytics Reporting API


Filter by 2 results

CATEGORY

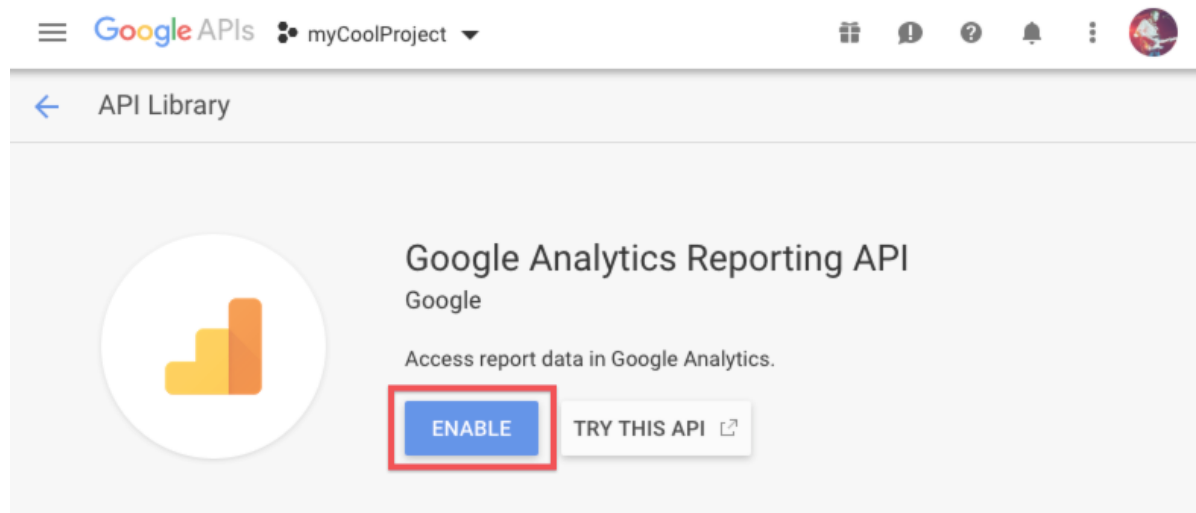
Advertising (1)

YouTube (1)

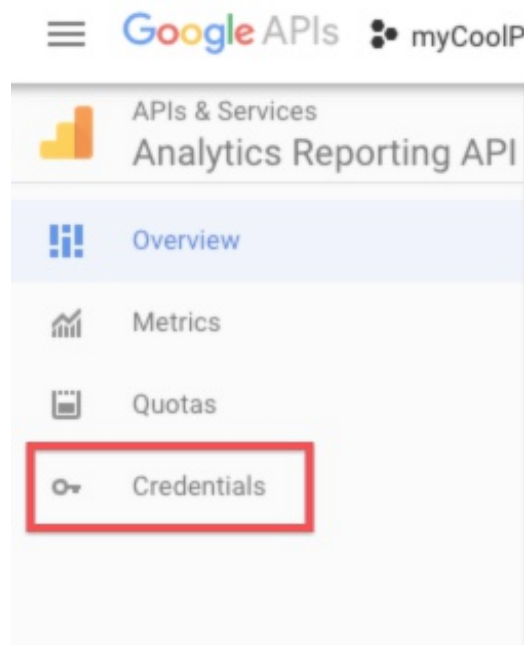
 **Google Analytics Reporting API**
Google
Access report data in Google Analytics.

 **YouTube Reporting API**
Google
Schedules reporting jobs containing your YouTube Analytics data and downlo

6. On the Google Analytics Reporting API page, click Enable.



7. On the left-side navigation bar, click Credentials.




8. On the Credentials page, click Configure Consent Screen.

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

Credentials compatible with this API

To view all credentials or create new credentials visit [Credentials in APIs & Services](#)

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

OAuth 2.0 Client IDs


<input type="checkbox"/>	Name	Creation Date	Type	Client ID	Service-specific Usage (last 30 days) ?	Total Usage (last 30 days) ?
No rows to display						









- Enter a name for your application, and optionally add an application logo.
- Under Scopes for Google APIs, click Add Scope and then click the option to manually paste your scopes. Enter the following scopes into the field, and then click Add:
 - <https://www.googleapis.com/auth/analytics.manage.users.readonly>
 - <https://www.googleapis.com/auth/analytics.manage.users>
 - <https://www.googleapis.com/auth/analytics.edit>
 - <https://www.googleapis.com/auth/analytics.readonly>
- The Scopes for Google APIs section should look like this:

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.

 Because you've added a sensitive scope, your consent screen requires verification by Google before it's published. [Learn more](#)

email	
profile	
openid	
 ../auth/analytics.manage.users.readonly	
 ../auth/analytics.manage.users	
 ../auth/analytics.edit	
 ../auth/analytics.readonly	


Note: As explained in the above screenshot, your application will need to be verified by Google before it will be published. For more information about the application verification process, see [Google's documentation](#).





- In the Authorized Domains field, add cloudelements.io and cloud-elements.com as

approved domains.

Authorized domains [?]

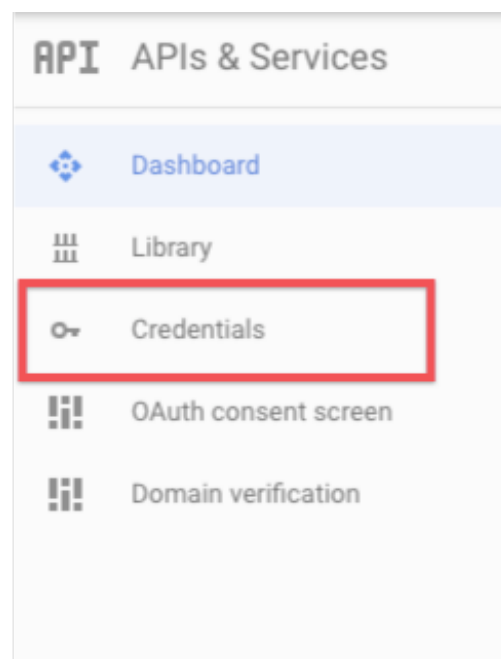
To protect you and your users, Google only allows applications that authenticate using OAuth to use Authorized Domains. Your applications' links must be hosted on Authorized Domains. [Learn more](#)

 Because you've added a sensitive scope, your consent screen requires verification by Google before it's published. [Learn more](#)

	cloudelements.io	
	cloud-elements.com	

Type in the domain and press Enter to add it

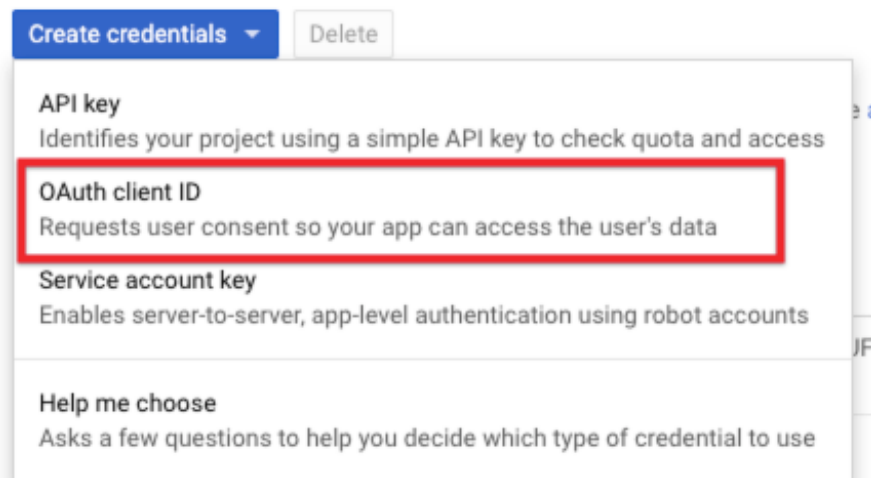
13. Click Save, and then click Credentials from the left-side navigation bar.



Generating OAuth Credentials

1. On the Credentials page, click Create Credentials, and then click OAuth client ID.

Credentials



2. On the Create OAuth client ID page, click Web application, and enter a name for your application.
3. In the Authorized JavaScript Origins field, add the following domains:
 - <https://staging.cloud-elements.com>
 - <https://cloud-elements.com>
 - <https://cloudelements.io>
 - <https://staging.cloudelements.io>
4. In the Authorized Redirect URIs field, add `https://auth.cloudelements.io/oauth`

Your Create OAuth Client ID page should look like this:

Create OAuth client ID

For applications that use the OAuth 2.0 protocol to call Google APIs, you can use an OAuth 2.0 client ID to generate an access token. The token contains a unique identifier. See [Setting up OAuth 2.0](#) for more information.

Application type

- ☒ Web application
- ☐ Android [Learn more](#)
- ☐ Chrome App [Learn more](#)
- ☐ iOS [Learn more](#)
- ☐ Other

Name

My Cool Application

Restrictions

Enter JavaScript origins, redirect URIs, or both [Learn More](#)

Origins and redirect domains must be added to the list of Authorized Domains in the [OAuth consent settings](#).

Authorized JavaScript origins

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (https://*.example.com) or a path (<https://example.com/subdir>). If you're using a nonstandard port, you must include it in the origin URI.

<https://staging.cloud-elements.com>



<https://cloud-elements.com>



<https://cloudelements.io>



<https://staging.cloudelements.io>



Type in the domain and press Enter to add it

Authorized redirect URIs

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

<https://auth.cloudelements.io/oauth>



Type in the domain and press Enter to add it

Create

Cancel

5. Click Create.
6. On the OAuth client window, record your client ID and secret, both of which you will use during authentication.

OAuth client

The client ID and secret can always be accessed from Credentials in APIs & Services

i OAuth is limited to 100 [sensitive scope logins](#) until the [OAuth consent screen](#) is published. This may require a verification process that can take several days.

Here is your client ID

[Pixelated Client ID] 

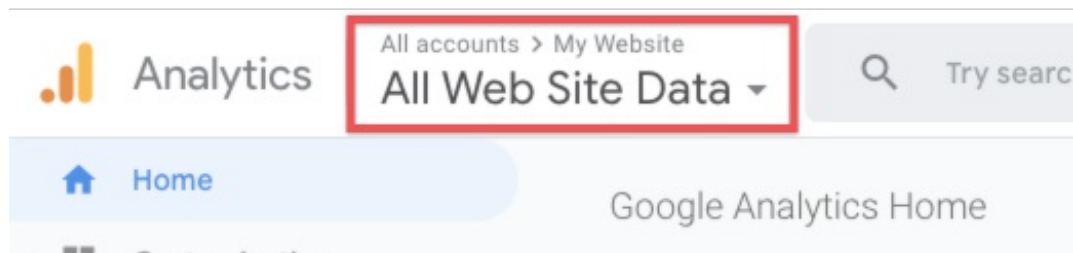
Here is your client secret

[Pixelated Client Secret] 

OK

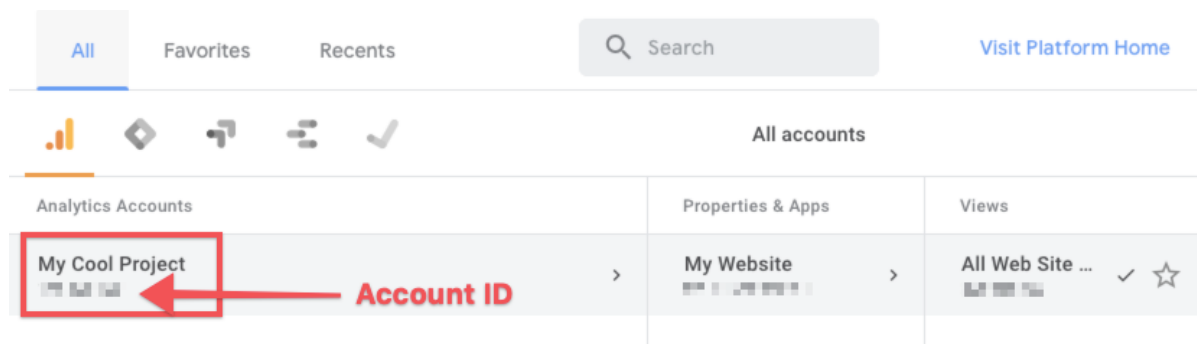
Recording the Project's Account ID

1. Navigate to <https://analytics.google.com/> and sign in to your account.
2. On the Analytics Home page, click your account from the top navigation bar.



The Accounts window appears.

3. Under the Analytics column, identify the account for the project you're authenticating with, and record the numeric ID beneath the account name.



Note: in the above screenshot, the account ID and other fields are pixelated for security; the displayed value will be a numeric string.

Required Information

After completing these instructions, you should now have the following information on hand for authentication:

- Account name
 - API key
 - API secret
 - (optional) Account ID, if authenticating via API and not the SAP Cloud Platform Open Connectors UI
-