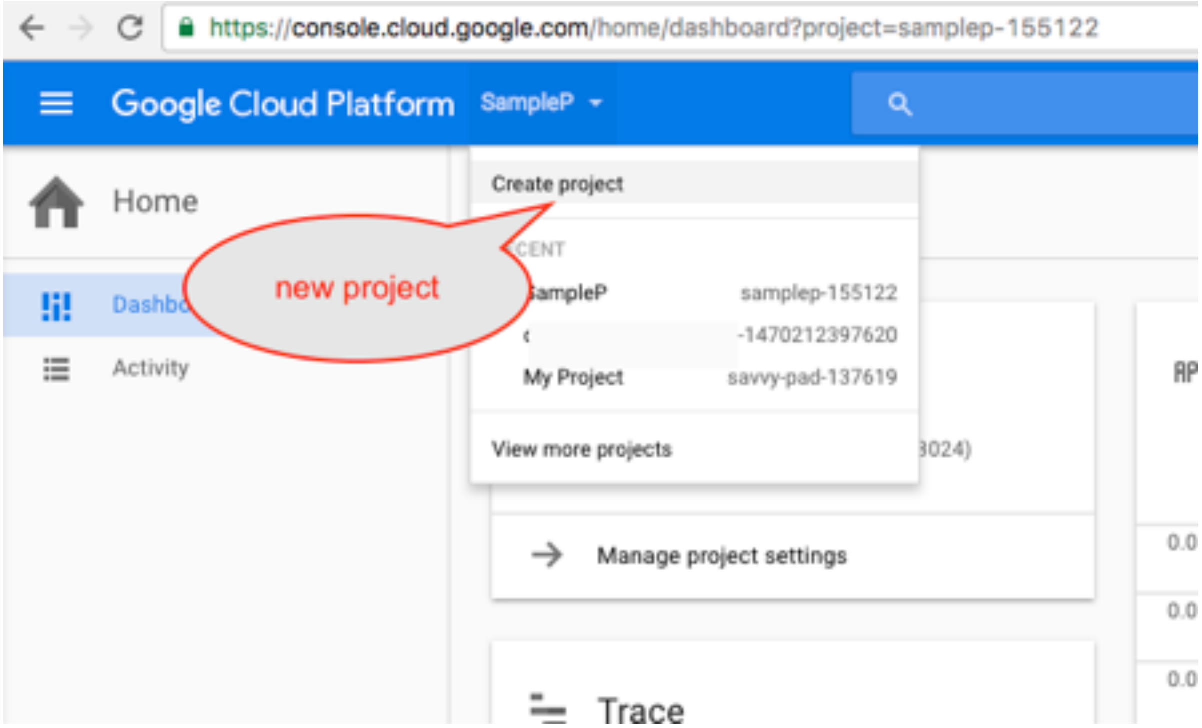
Google Configuration and System Setup

To use the system, you must have a valid Google Service Account that has Domain Wide Delegation enabled. And an OAuth 2.0 Client of the type: Service Account Client

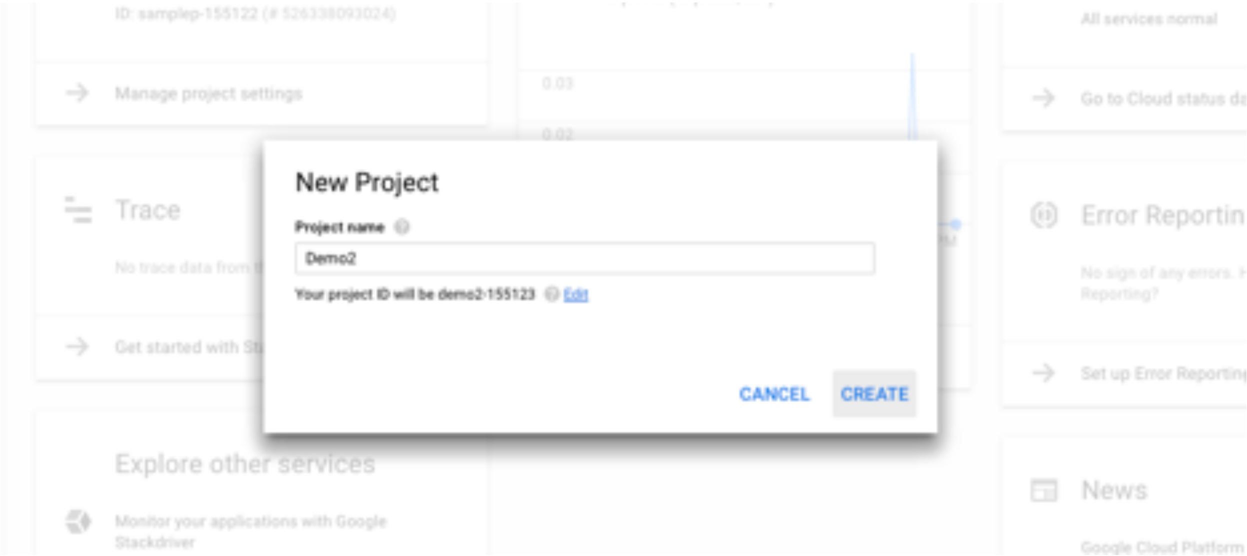
Within the Google Admin Security settings, you must also authorize the OAuth Client, to manage the provisioning of your google groups and users.

The steps related to this are outlined below. Screen shots were taken on January 9, 2017.

https://console.cloud.google.com



new project



New Project

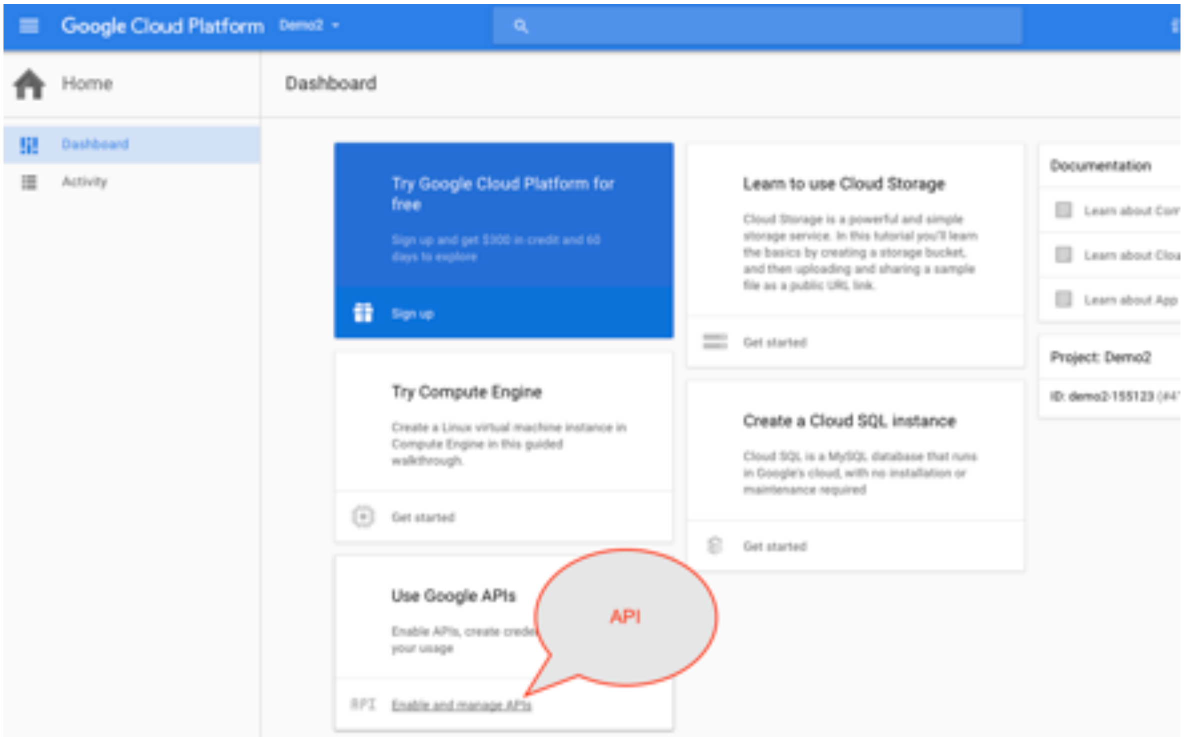
Project name: Demo2

Your project ID will be demo2-155123 Edit

CANCEL CREATE

Go to APIs dashboard

https://console.cloud.google.com/apis/dashboard?



Try Google Cloud Platform for free

Sign up and get $300 in credit and 60 days to explore

Try Compute Engine

Create a Linux virtual machine instance in Compute Engine in this guided walkthrough.

Learn to use Cloud Storage

Cloud Storage is a powerful and simple storage service. In this tutorial you'll learn the basics by creating a storage bucket, and then uploading and sharing a sample file as a public URL link.

Create a Cloud SQL instance

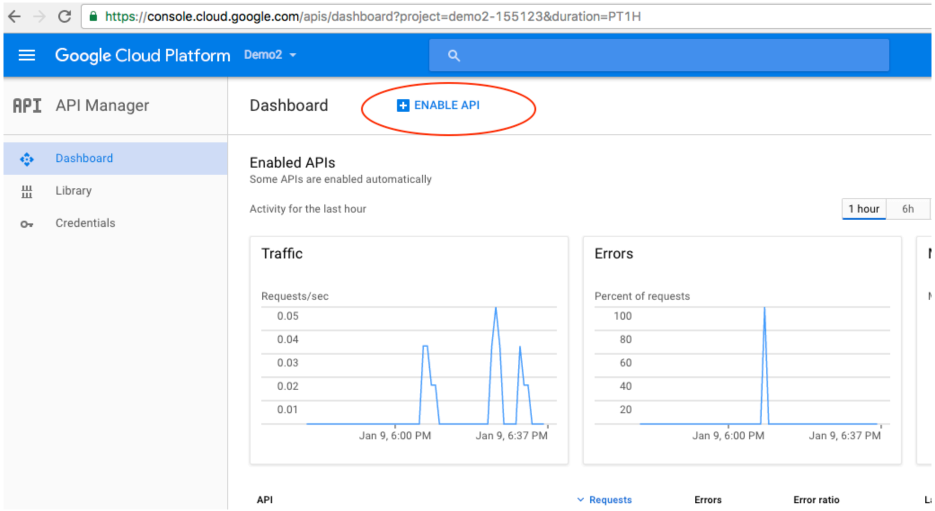
Cloud SQL is a MySQL database that runs in Google's cloud, with no installation or maintenance required

Use Google APIs

Enable APIs, create crede your usage

https://console.cloud.google.com/apis/api/admin/overview

Now select Enable API



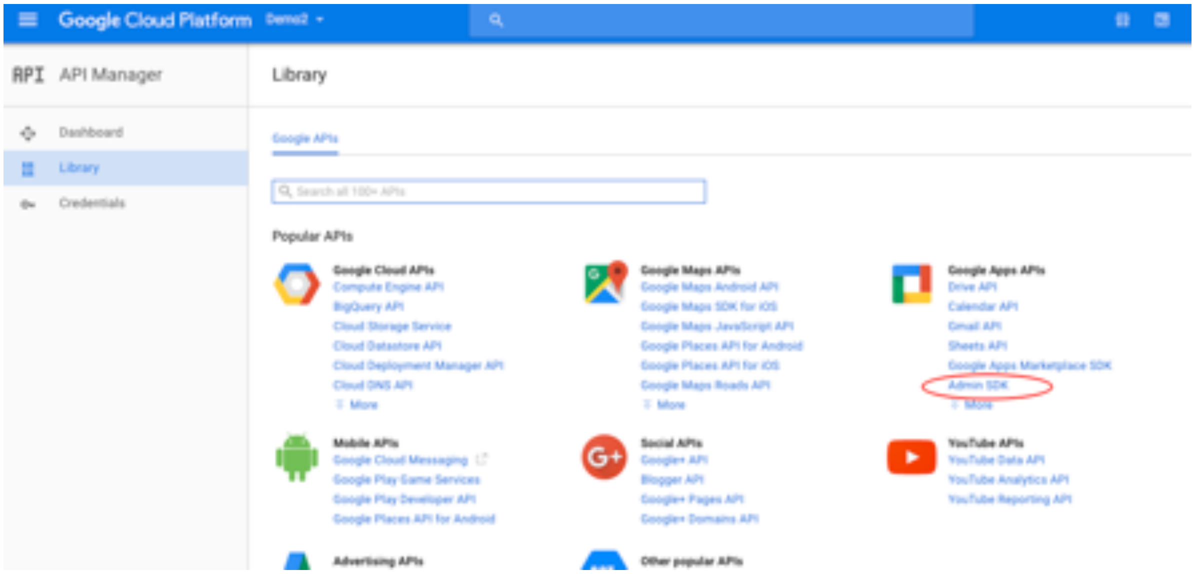
https://console.cloud.google.com/apis/dashboard?project=demo2-155123&duration=PT1H

Enabled APIs

Some APIs are enabled automatically

Activity for the last hour

https://console.cloud.google.com/apis/library



Library

Google APIs

Search all 100+ APIs

Popular APIs

Google Cloud APIs
- Compute Engine API
- BigQuery API
- Cloud Storage Service
- Cloud Datastore API
- Cloud Deployment Manager API
- Cloud DNS API
- More

Google Maps APIs
- Google Maps Android API
- Google Maps SDK for iOS
- Google Maps JavaScript API
- Google Places API for Android
- Google Places API for iOS
- Google Maps Roads API
- More

Google Apps APIs
- Drive API
- Calendar API
- Gmail API
- Sheets API
- Google Apps Marketplace SDK
- Admin SDK
- More

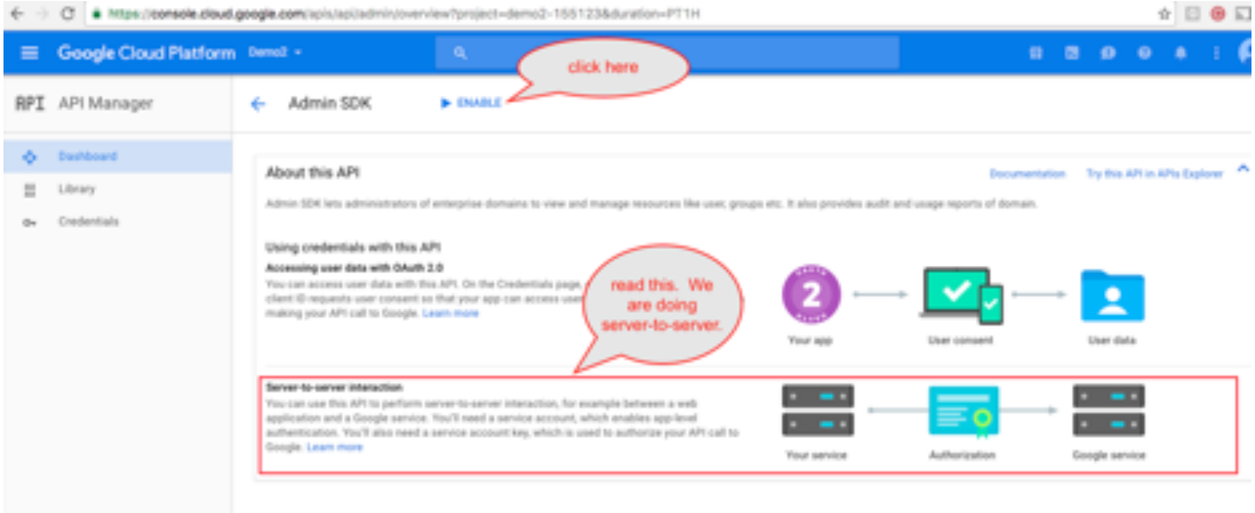
Mobile APIs
- Google Cloud Messaging
- Google Play Game Services
- Google Play Developer API
- Google Places API for Android

Social APIs
- Google+ API
- Blogger API
- Google+ Pages API
- Google+ Domains API

YouTube APIs
- YouTube Data API
- YouTube Analytics API
- YouTube Reporting API

Advertising APIs

Other popular APIs



About this API

Admin SDK lets administrators of enterprise domains to view and manage resources like user, groups etc. It also provides audit and usage reports of domain.

Using credentials with this API

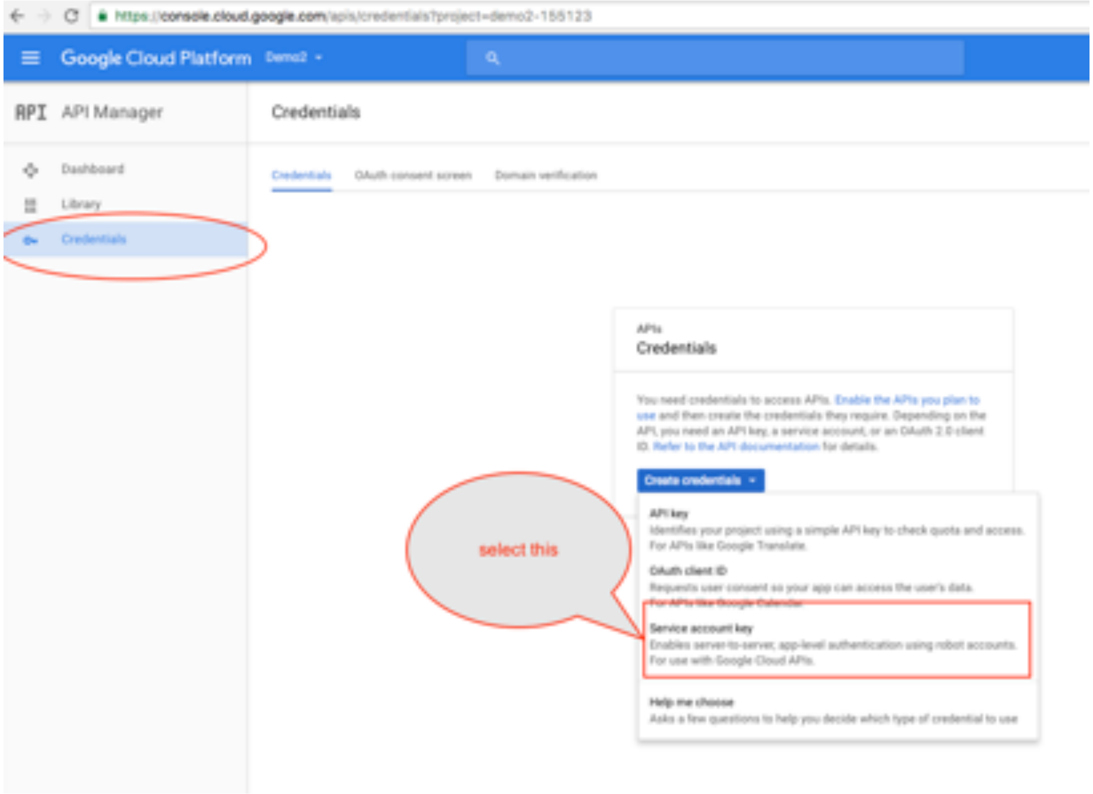
Accessing user data with OAuth 2.0

You can access user data with this API. On the Credentials page, client ID requests user consent so that your app can access use making your API call to Google. Learn more

Server-to-server interaction

You can use this API to perform server-to-server interaction, for example between a web application and a Google service. You'll need a service account, which enables app-level authentication. You'll also need a service account key, which is used to authorize your API call to Google. Learn more https://console.cloud.google.com/apis/credentials

The service account will allow us to have full access to the google groups and users.



You need credentials to access APIs. Enable the APIs you plan to use and then create the credentials they require. Depending on the API, you need an API key, a service account, or an OAuth 2.0 client ID. Refer to the API documentation for details.

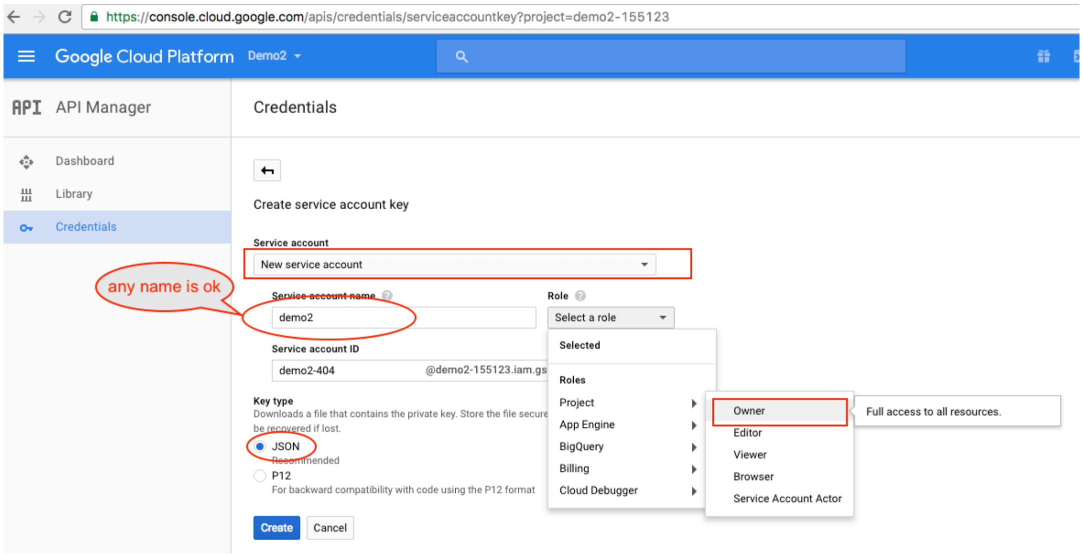
API key
Identifies your project using a simple API key to check quota and access. For APIs like Google Translate.

OAuth client ID
Requests user consent so your app can access the user's data. For APIs like Google Calendar.

Service account key
Enables server-to-server, app-level authentication using robot accounts. For use with Google Cloud APIs.

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

https://console.cloud.google.com/apis/credentials/serviceaccountkey



Create service account key

Service account: New service account

Service account name: demo2

Role: Select a role

Service account ID: demo2-404 @demo2-155123.iam.gs

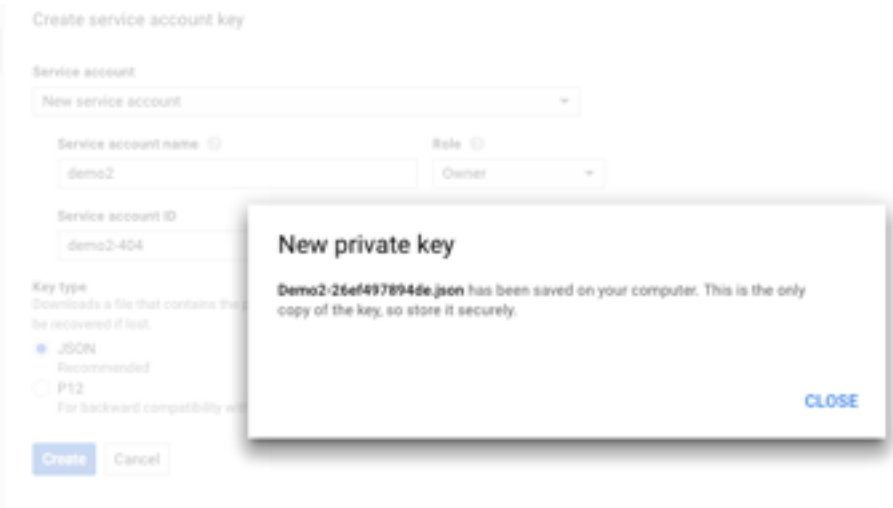
Key type
Downloads a file that contains the private key. Store the file secure be recovered if lost.

● JSON
Recommended

○ P12
For backward compatibility with code using the P12 format

Full access to all resources.

The Private JSON key will be downloaded. Save this to a special place. You will use this to configure the system.



Create service account key

Service account: New service account

Service account name: demo2

Role: Owner

Service account ID: demo2-404

Key type

Downloads a file that contains the p… be recovered if lost.

● JSON Recommended

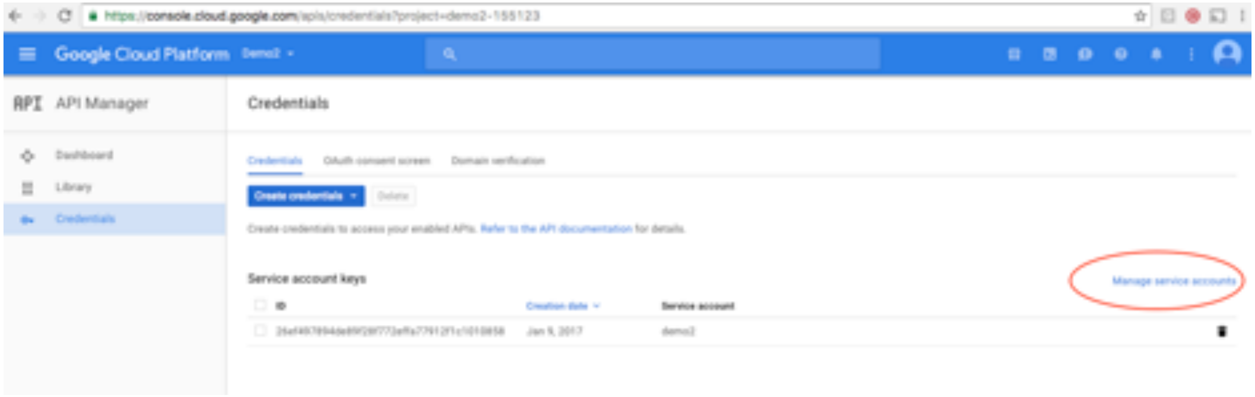
○ P12 For backward compatibility wi…

New private key

Demo2-26ef497894de.json has been saved on your computer. This is the only copy of the key, so store it securely.

In this case, the file name is: Demo2-5884231b5df8.json   *** make a note of this, because you will need to use this file to setup the system.

The service account is created. Now you need to enable DOMAIN WIDE DELEGATION (DWD) .



https://console.cloud.google.com/apis/credentials?project=demo2-155123

Credentials

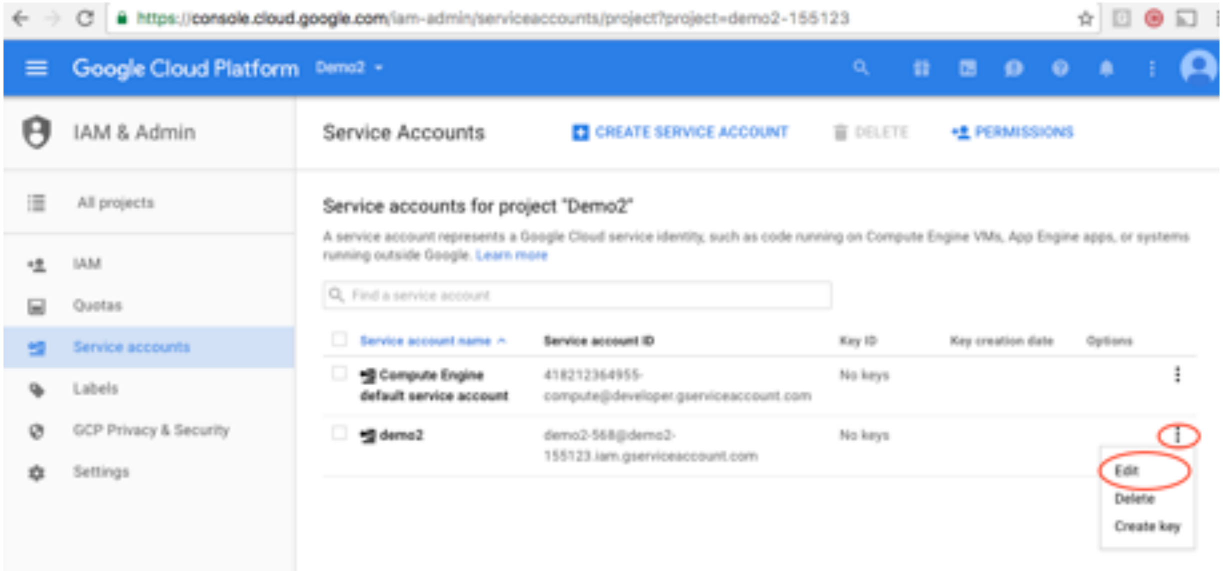
Create credentials to access your enabled APIs. Refer to the API documentation for details.

Service account keys

ID	Creation date	Service account
26ef497894de89f28f772effa77912f1c1010858	Jan 9, 2017	demo2

https://console.cloud.google.com/iam-admin/serviceaccounts/project

Now edit the project

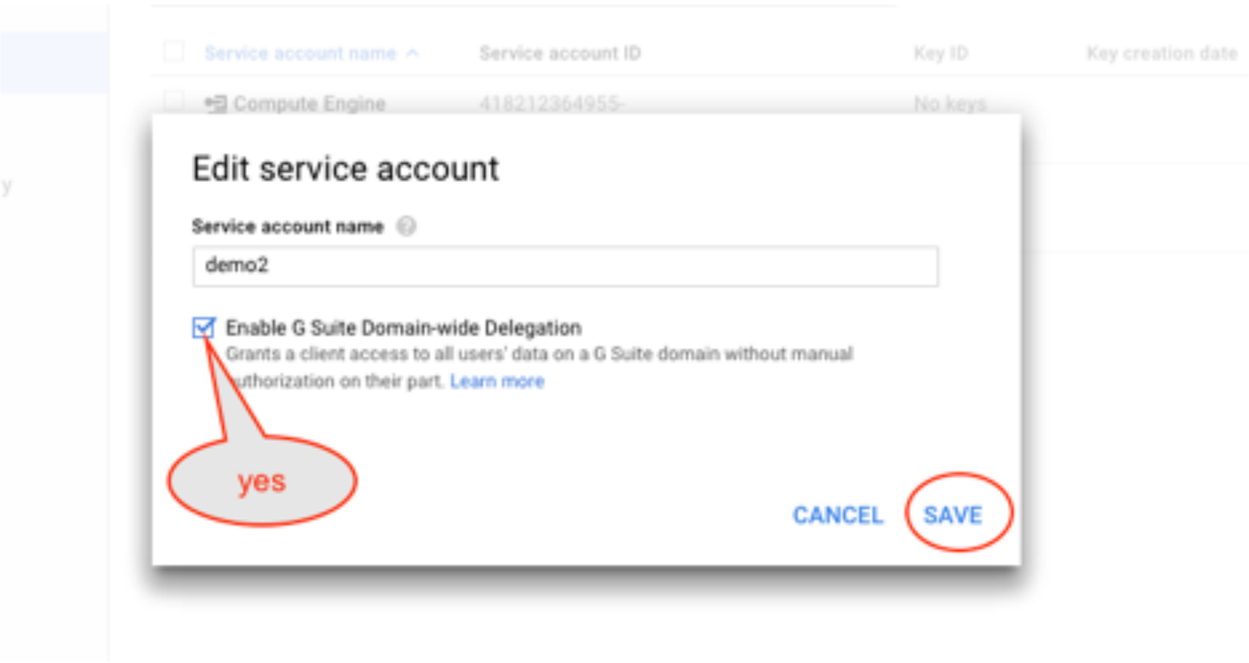


Service accounts for project "Demo2"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more

Service account name	Service account ID	Key ID	Key creation date	Options
Compute Engine default service account	418212364955-compute@developer.gserviceaccount.com	No keys		⋮
demo2	demo2-568@demo2-155123.iam.gserviceaccount.com	No keys		⋮

enable DOMAIN WIDE DELEGATION (DWD) .



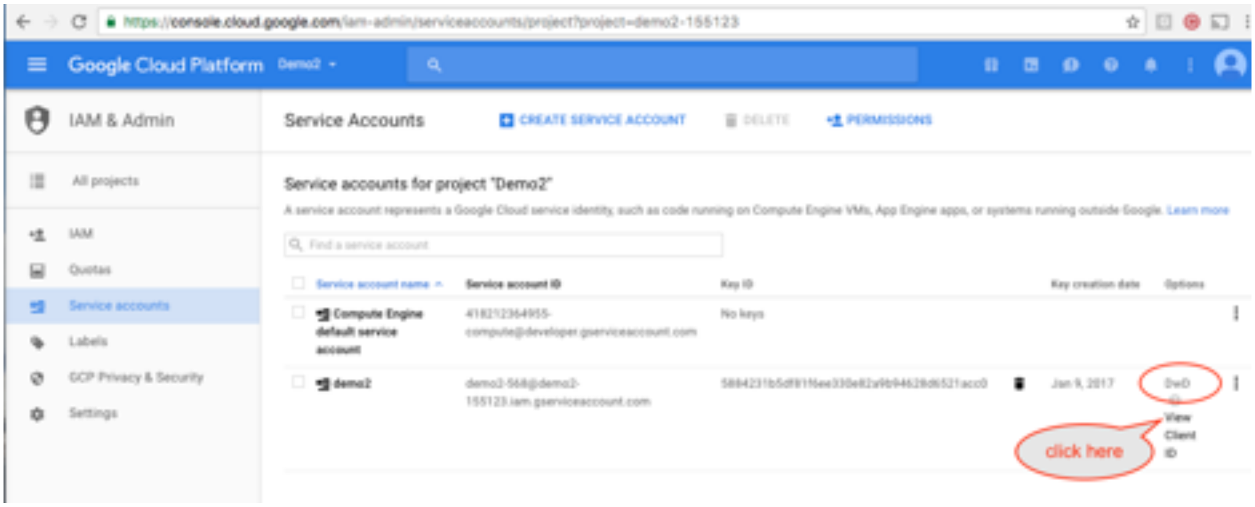
Edit service account

Service account name: demo2

☑ Enable G Suite Domain-wide Delegation

Grants a client access to all users' data on a G Suite domain without manual authorization on their part. Learn more

Notice now that the service account has DwD Options turned on.



https://console.cloud.google.com/iam-admin/serviceaccounts/project?project=demo2-155123

Service Accounts

Service accounts for project "Demo2"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more

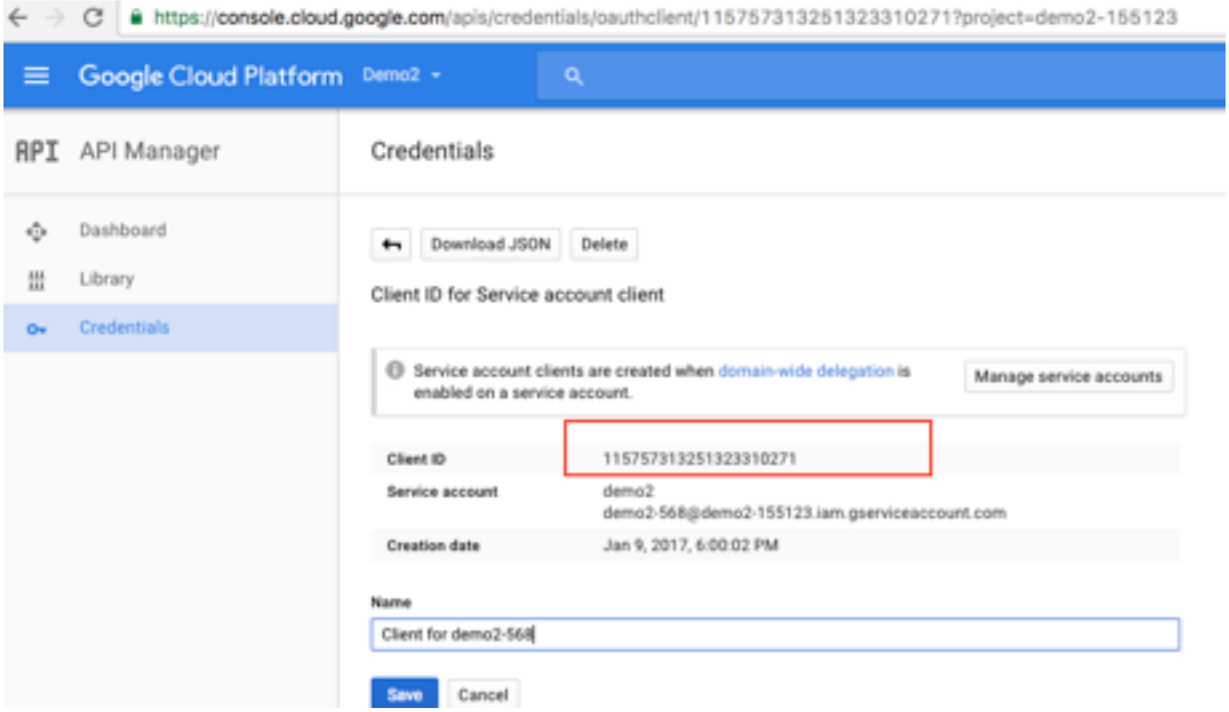
□	Service account name	Service account ID	Key ID	Key creation date	Options
□	Compute Engine default service account	418212364955-compute@developer.gserviceaccount.com	No keys		
□	demo2	demo2-568@demo2-155123.iam.gserviceaccount.com	5884231b5df81f6ee330e82a9b94628d6521acc0	Jan 9, 2017	DwD View Client ID

It also created a CLIENT ID.   Click to view the client ID. We need the ID value.

https://console.cloud.google.com/apis/credentials/oauthclient/115757313251323310271

The Client ID is: 115757313251323310271

The service account name is: demo2-568@demo2-155123.iam.gserviceaccount.com



https://console.cloud.google.com/apis/credentials/oauthclient/115757313251323310271?project=demo2-155123

Credentials

Client ID for Service account client

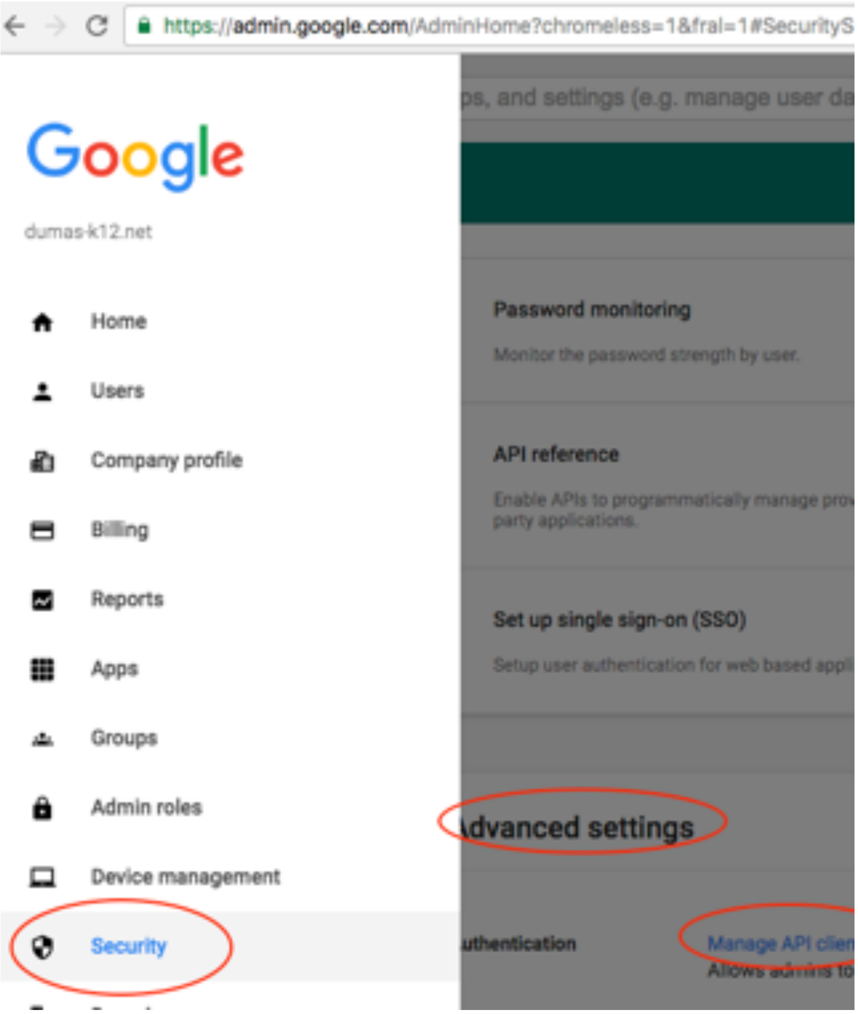
Service account clients are created when domain-wide delegation is enabled on a service account.

Client ID	115757313251323310271
Service account	demo2 demo2-568@demo2-155123.iam.gserviceaccount.com
Creation date	Jan 9, 2017, 6:00:02 PM

Name

Client for demo2-568

Now you need go to the Google Admin, and get into Security - Advanced Settings to Manage the API client access for our client ID: 115757313251323310271


https://admin.google.com/AdminHome?chromeless=1&fral=1#SecurityS
ps, and settings (e.g. manage user da
Google
dumas-k12.net
Home
Users
Company profile
Billing
Reports
Apps
Groups
Admin roles
Device management
Security
Password monitoring
Monitor the password strength by user.
API reference
Enable APIs to programmatically manage prov
party applications.
Set up single sign-on (SSO)
Setup user authentication for web based appl
dvanced settings
uthentication
Manage API clien
Allows admins to

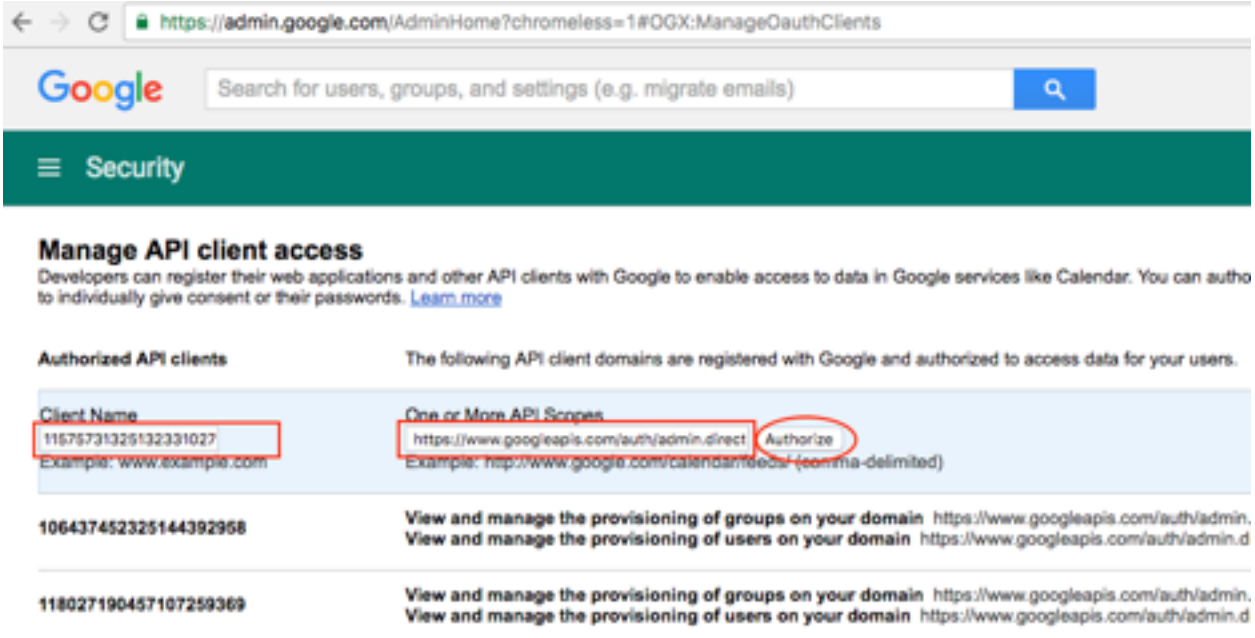
https://admin.google.com/AdminHome?chromeless=1#OGX:ManageOauthClients

Enter the Client ID into the Client Name text box.

And enter both of these into the API Scopes text box. Separated by a comma.

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

Then Authorize Button.   They will then appear in the list below as Authorized.



https://admin.google.com/AdminHome?chromeless=1#OGX:ManageOauthClients

Google
Search for users, groups, and settings (e.g. migrate emails)
Security

Manage API client access

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Calendar. You can autho
to individually give consent or their passwords. Learn more

Authorized API clients The following API client domains are registered with Google and authorized to access data for your users.

Client Name: 11575731325132331027
Example: www.example.com

One or More API Scopes: https://www.googleapis.com/auth/admin.direct
Example: http://www.google.com/calendar/feeds/ (comma-delimited)

106437452325144392958	**View and manage the provisioning of groups on your domain** https://www.googleapis.com/auth/admin. **View and manage the provisioning of users on your domain** https://www.googleapis.com/auth/admin.d
118027190457107259369	**View and manage the provisioning of groups on your domain** https://www.googleapis.com/auth/admin. **View and manage the provisioning of users on your domain** https://www.googleapis.com/auth/admin.d

The Google setup is now completed.

Now you need to Setup and configure the system.   To do that follow these instructions.

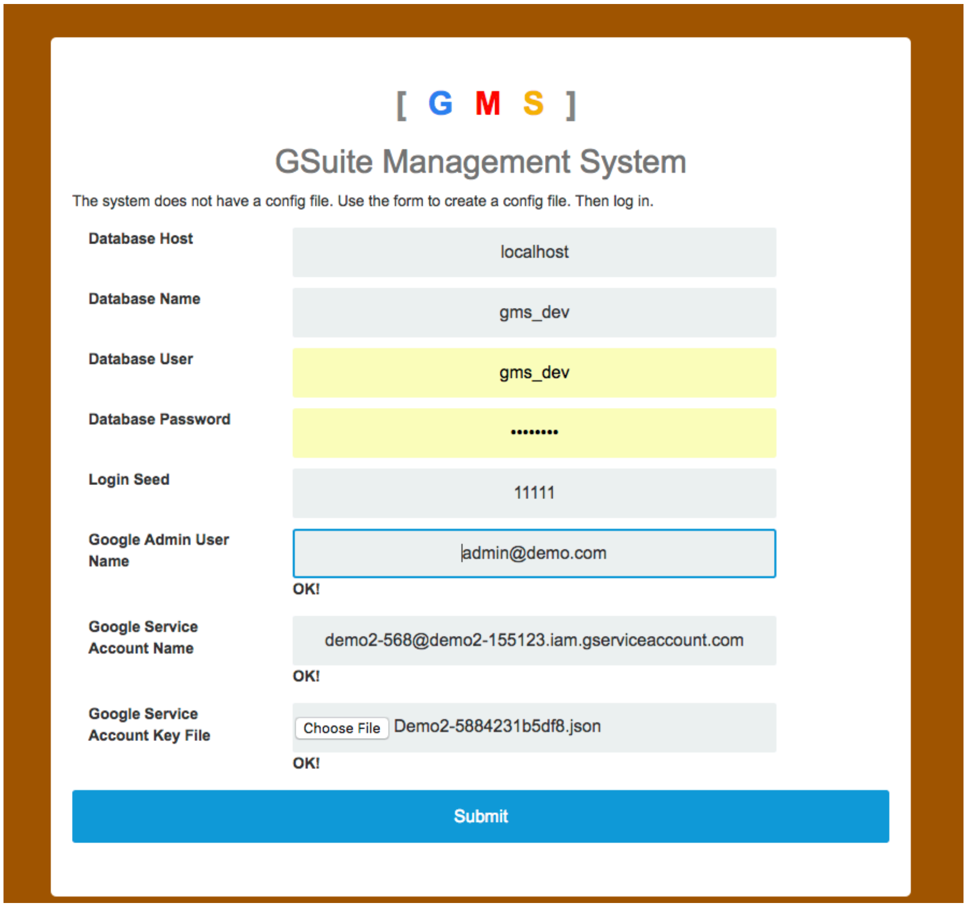
Install the source code in your web root.
Create a mysql database and initialize it with the database schema in APP/SQL/DATABASE.sql   **** this must be done before you do the next step below.

Make this writable directory 1 directory above your web root: gms_etc
This directory will be used to hold the system config.ini and your Google Service Account key file (the .json file you downloaded from google).

To setup the system, you need 3 things from Google (above).

admin user email: admin@demo.com
service account name: demo2-568@demo2-155123.iam.gserviceaccount.com
service account key file name: Demo2-5884231b5df8.json

Go to a browser and go to the default index.php page.   Because you do not yet have a config.ini file, this index page will redirect you to the 1 time setup.php page. You will use this setup page to create a config.ini file that will be used by the system going forward.



[G M S]

GSuite Management System

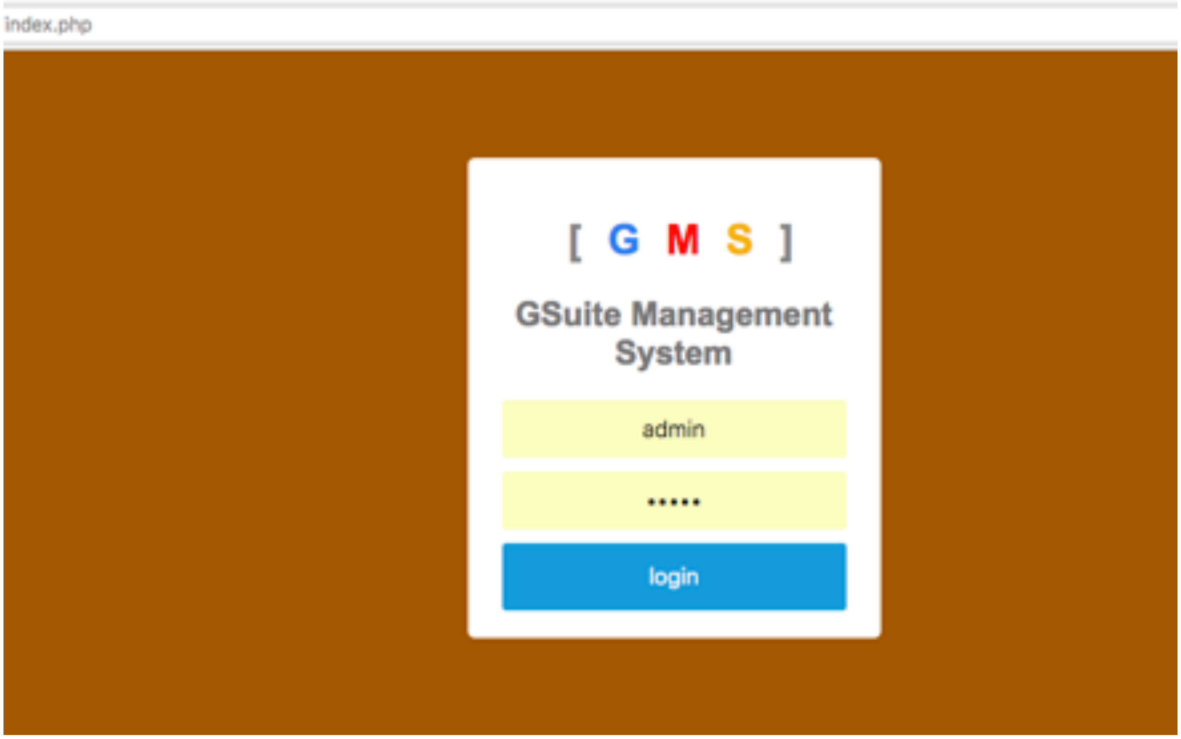
The system does not have a config file. Use the form to create a config file. Then log in.

Database Host	localhost
Database Name	gms_dev
Database User	gms_dev
Database Password	••••••••
Login Seed	11111
Google Admin User Name	admin@demo.com OK!
Google Service Account Name	demo2-568@demo2-155123.iam.gserviceaccount.com OK!
Google Service Account Key File	Choose File Demo2-5884231b5df8.json OK!

The setup page will create the config.ini file and store it in the directory ../gms_etc. It will also store the service account key file in that same directory.

The setup also creates 1 admin user in the database with a default password of: admin

You can now login:



GSuite Management System

admin

•••••

To verify that your system is properly initialized, use the menu and navigate to:
Google Groups -> Standard Groups.

If your system is properly setup, then this page will show you a list of any existing google groups from your Google Admin account.