

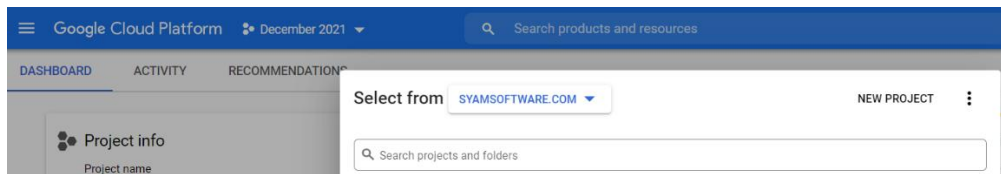


---

## Configuring the Google Service Account

Log into Google Cloud Platform <https://console.cloud.google.com/>

From the top menu select the drop-down box to the right of Cloud Platform and select one of the existing projects



Click New Project

---

### New Project

**Project name \***  
SyAM Chromebook Integration ?

Project ID: storied-myth-334613. It cannot be changed later. [EDIT](#)

**Organization \***  
syamsoftware.com ?

Select an organization to attach it to a project. This selection can't be changed later.

**Location \***  
syamsoftware.com [BROWSE](#)

Parent organization or folder

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

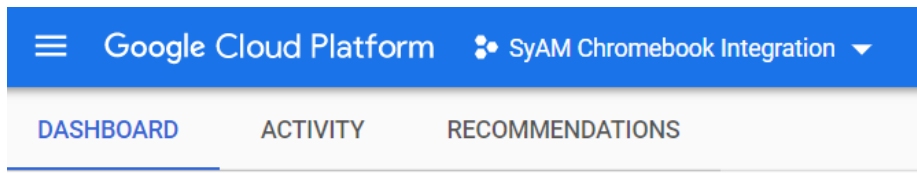
Give the Project a name and click Create

This will take you back to the Dashboard

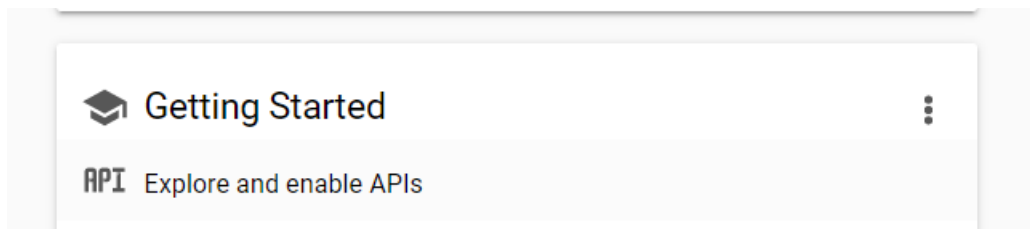


## Quick Reference Chromebook Integration

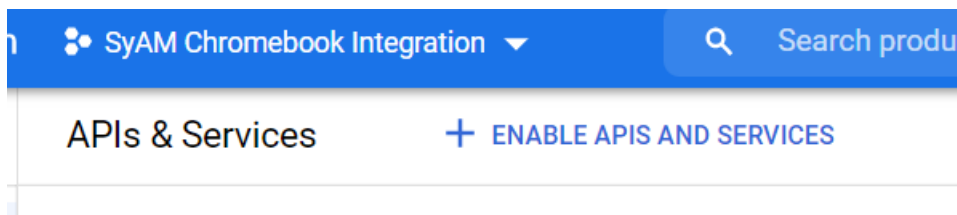
Now select the new project from the drop down next to Cloud



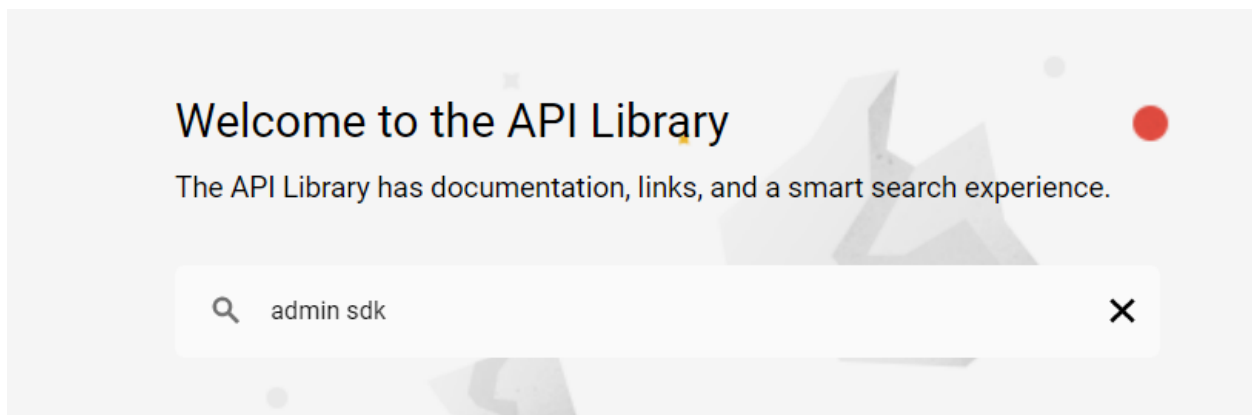
Scroll down the page and under Getting Started select API Explore and enable APIs



Now click on enable APIs



Enter admin sdk in the search box





# Quick Reference Chromebook Integration

## Select Admin SDK API

“admin sdk”

2 results



### Admin SDK API

Google Enterprise 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.

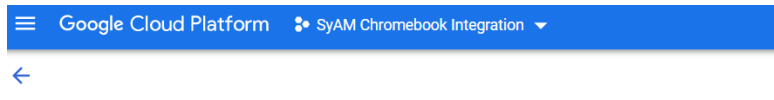


### Cloud Identity

Google Enterprise API

Cloud Identity is the most secure platform for managing your company's users, devices and applications in the cloud. Stay secure on the same infrastructure Google uses to manage billions of enterprise and consumer identities. Backed by Google Cloud, you can scale from prototype to planet-scale without having to think about capacity. Cloud Identity features include user lifecycle management, account security, single sign-on...

## Click Enable



### Admin SDK API

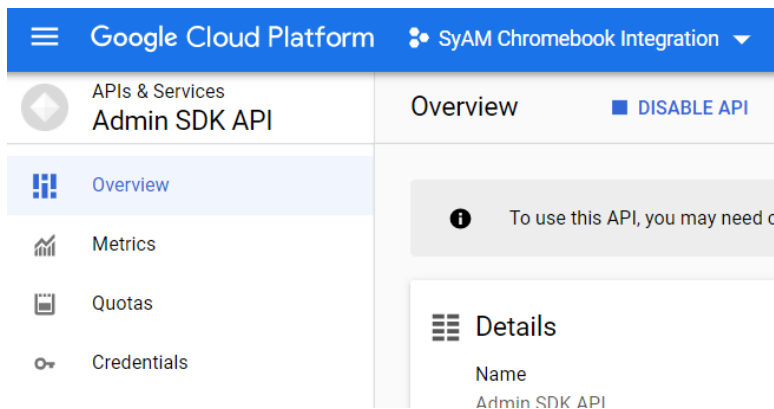
Google Enterprise API

Admin SDK lets administrators of enterprise domains to view and manage resources like user,...

ENABLE

TRY THIS API

## Now select Credentials from the left menu





Click Create Credentials

Search products

Credentials + CREATE CREDENTIALS DELETE

**Credentials compatible with this API**

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

Select Service Account

+ CREATE CREDENTIALS DELETE

**OAuth client ID**  
Requests user consent so your app can access the user's data

**Service account**  
Enables server-to-server, app-level authentication using robot accounts

Give the service account a name and click Create and Continue

Create service account

### 1 Service account details

Service account name \*  
Chromebook Integration  
Display name for this service account

Service account ID \*  
chromebook-integration @storied-myth-334613.iam.gserviceaccou X C

Service account description  
Describe what this service account will do

CREATE AND CONTINUE

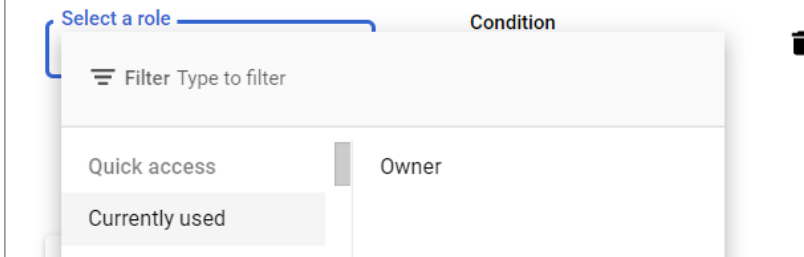


Under Roles select Currently Used – Owner then click to continue

✓ **Service account details**

2 **Grant this service account access to project (optional)**

Grant this service account access to SyAM Chromebook Integration so that it has permission to complete specific actions on the resources in your project. [Learn more](#)



Leave the Grant User access to this service account empty, press Done

Create service account

✓ **Service account details**

✓ **Grant this service account access to project (optional)**

3 **Grant users access to this service account (optional)**

Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role ⓘ

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role ⓘ

Grant users the permission to administer this service account

**DONE** CANCEL



# Quick Reference Chromebook Integration

Once back at the Credentials Menu click on the service account

The screenshot shows the Google Cloud Platform 'Credentials' page for 'SyAM Chromebook Integration'. The left sidebar contains navigation options: Dashboard, Library, Credentials (selected), OAuth consent screen, Domain verification, and Page usage agreements. The main content area is divided into three sections: 'API Keys' (empty), 'OAuth 2.0 Client IDs' (empty), and 'Service Accounts'. The 'Service Accounts' section contains one entry with the email 'chromebook-integration@storied-myth-334613.iam.gserviceaccount.com' and the name 'Chromebook Integration'. A 'CONFIGURE CONSENT SCREEN' button is visible at the top right of the main content area.

Copy the email and unique id to notepad as we need to paste this data into the SyAM MDM.

The screenshot shows the 'Service account details' page for 'Chromebook Integration'. The page has a breadcrumb 'Chromebook Integration' and tabs for 'DETAILS', 'PERMISSIONS', 'KEYS', 'METRICS', and 'LOGS'. The 'Name' field is 'Chromebook Integration' with a 'SAVE' button. The 'Description' field is empty with a 'SAVE' button. The 'Email' field is 'chromebook-integration@storied-myth-334613.iam.gserviceaccount.com'. The 'Unique ID' field is '104914023858068432931'. The 'Service account status' section shows 'Account currently active' with a green checkmark and a 'DISABLE SERVICE ACCOUNT' button. At the bottom, there is a 'SHOW ADVANCED SETTINGS' link.


Click on Keys and then select Create New Key



← Chromebook Integration

DETAILS   PERMISSIONS   **KEYS**   METRICS   LOGS

### Keys

 Service account keys could pose a security risk if compromised. We recommend you av about the best way to authenticate service accounts on Google Cloud [here](#) .

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using [organization policies](#).  
[Learn more about setting organization policies for service accounts](#)

**ADD KEY** ▾

- Create new key
- Upload existing key

Key creation date	Key expiration date
-------------------	---------------------

Select P12 and Create the key file

### Create private key for "Chromebook Integration"

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

Key type

JSON

Recommended

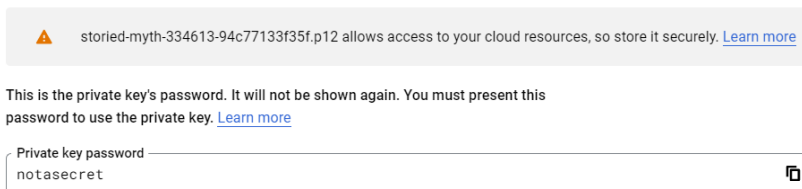
P12

For backward compatibility with code using the P12 format

CANCEL   CREATE

Press Close and it will save the file, you will need to upload this into the SyAM MDM

Private key saved to your computer



storied-myth-334613-94c77133f35f.p12 allows access to your cloud resources, so store it securely. [Learn more](#)

This is the private key's password. It will not be shown again. You must present this password to use the private key. [Learn more](#)

Private key password  
notasecret

CLOSE

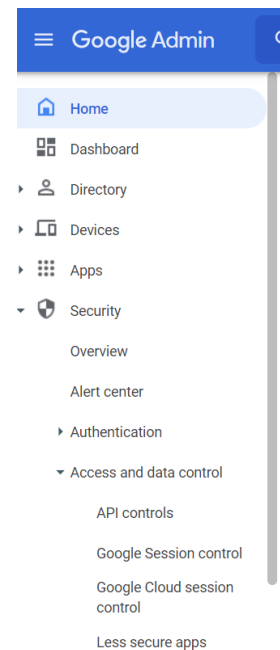
You can now log out of the Google Cloud Platform.

### Update the Google Admin Console

Next we need to enable this new service account in Google Admin Console.

Login to your Google Apps Admin console. <https://admin.google.com>

Expand Security – Access and data control from the left menu and select API controls







# Quick Reference Chromebook Integration

Scroll down the page and  
select Manage Domain  
Wide Delegation

## API controls

Use these controls to enable or restrict access to Google Workspace APIs for customer-owned and third-party applications and service accounts. Reduce the risk associated with third-party access to Google Workspace APIs by limiting access to only trusted apps.

Message (300 characters limit)

- Block all third-party API access  
Requests by third-party apps are denied access to user data. This setting blocks all OAuth scopes, except for those explicitly granted to the app.
- Trust internal, domain-owned apps  
Internal, domain-owned apps will be exempt from the API access control list.

Apps you trust on the [Google Workspace Market](#) trusted on your App access control list.

## Domain wide delegation

Developers can register their web applications and other API clients with Google to access your user data without your users having to enter their passwords. [Learn more](#)

[MANAGE DOMAIN WIDE DELEGATION](#)

Security > API Controls > Domain-wide Delegation

**i** Developers can register their web applications and other API clients to access your user data without your users having to enter their passwords.

API clients [Add new](#) [Download client info](#)

+ Add a filter

Click Add New



## Quick Reference Chromebook Integration

Select Manage API client access in the Authentication section. In the Client Name field enter the service account's Client ID. (This is the Unique ID from the Service Account Details we had pasted into notepad)

**Add a new client ID**

Client ID  
104914023858068432931

Overwrite existing client ID ?

OAuth scopes (comma-delimited) ×  
<https://www.googleapis.com/auth/admin.directory.>

OAuth scopes (comma-delimited)

CANCEL AUTHORIZE

Paste in the following under OAuth scopes

<https://www.googleapis.com/auth/admin.directory.device.chromeos>,  
<https://www.googleapis.com/auth/admin.directory.group.member>,  
<https://www.googleapis.com/auth/admin.directory.user>,  
<https://www.googleapis.com/auth/admin.directory.orgunit>,  
<https://www.googleapis.com/auth/admin.directory.group>,  
<https://www.googleapis.com/auth/apps.licensing>,  
<https://www.googleapis.com/auth/chromewebstore.readonly>,<https://www.googleapis.com/auth/admin.reports.audit.readonly>,  
<https://www.googleapis.com/auth/admin.reports.usage.readonly>,<https://www.googleapis.com/auth/admin.directory.rolemanagement>,<https://www.googleapis.com/auth/admin.directory.userschema>,<https://www.googleapis.com/auth/classroom.courses>,  
<https://www.googleapis.com/auth/classroom.rosters>

Then Click Authorize

Log out of Google Admin Console






## Log into the SyAM MDM Interface

Click on the left menu Managed Devices – select ChromeOS

Upload the P12 file and paste in the ID and email from your Service Account Details

Press Next

SERVICE ACCOUNT SETUP

 service account       API Key       impersonation

Service Account Certificate (.p12)




No file chosen

File Saved

Skip the key for Static Maps by pressing Next

Enter the domain and the user email address that was used to Authorize the Service API in Google Admin Console and press Save

SERVICE ACCOUNT SETUP

 service account       API Key       impersonation

GSuite User Impersonation



---

Press Sync

After it completes the Sync, it will present that data retrieved from Google.

### Service Account Settings

Sync

**Last Updated** December 09 2021 08:45:13 AM



## Quick Reference Chromebook Integration

You can now set the Polling Interval for the GAC Sync and the Site Manager Asset Update

Auto Sync ✔ Running

✔ Management Utility URL:

Sync with GAC every

✔ SiteManager URL and PORT:

Upload to SiteManager every



---

### Possible reasons why the error Authorization Status 401 Unauthorized can occur

Incorrect Role chose for the service account – it must be set to Project – Service Account Actor

- To resolve, delete the two sets of settings in the Chrome OS page in Management Utilities, delete the service account and start the process again, creating a new service account and then add the new service account into Google Admin Console with the URLs.

Incorrect Google Apps Email Address, possibly a typo or the email account used was not the account used when logging into Google Admin Console to add in the URLs to the Service account.

- To resolve delete the Google Apps Domain information in the Chrome OS page in Management Utilities, then enter the correct email address and press save.

### Likely reason the error Authorization Status 403 Unauthorized can occur

Service Account Created but the API was not enabled

To resolve, log back into the Google Cloud, <https://console.cloud.google.com/> select your project and click to enable APIs