

Integrating Google with SecurityCoach

In this article, you will learn how to integrate Gmail, Google Drive, and Google IAM with SecurityCoach. Once you set up this integration, data provided by Google will be available under the **SecurityCoach** tab of your KMSAT console. This data can be viewed in SecurityCoach reports and used to create detection rules for real-time coaching campaigns.

Click the links below to learn how to integrate these Google products with SecurityCoach. For general information about SecurityCoach, see our [SecurityCoach Product Manual](#).

Jump to:

[Set Up the Integration in Your Google Cloud Platform](#)

[Set Up the Integration in Your KMSAT Console](#)

[Assign Domain-Wide Delegation and Scopes](#)

Set Up the Integration in Your Google Cloud Platform

Before you can set up the SecurityCoach integration in your KMSAT console, you will need to set up the integration in your Google Cloud platform by creating a project and a service account. You will also need to enable APIs for your project and obtain a JSON file and unique ID from your service account.

To jump to the article subsection for each of these steps, click the links below:

- [Create a Project](#)
- [Enable APIs for Your Project](#)
- [Create a Service Account](#)
- [Obtain the JSON File and Unique ID of a Service Account](#)

Create a Project

To create a project in your Google Cloud platform, follow the steps below:

1. Log in to your Google Cloud platform and navigate to **IAM & Admin > Create a Project**.

Start your Free Trial with \$300 in credit. Don't worry—you won't be charged

Google Cloud Platform

Home

View all products

PINNED

IAM & Admin

Billing

APIs & Services

Marketplace

Compute Engine

Cloud Storage

VPC network

Kubernetes Engine

BigQuery

SQL

IAM

Identity & Organization

Policy Troubleshooter

Policy Analyzer

Organization Policies

Service Accounts

Workload Identity Federation

Labels

Tags

Settings

Privacy & Security

Identity-Aware Proxy

Roles

Audit Logs

Manage Resources

Create a Project

Asset Inventory

Essential Contacts

Groups

Early Access Center

2. Enter "KB4VendorIntegration" as the **Project name**. The **Organization** and **Location** fields will automatically populate for you.
3. Click **CREATE**.

← → ↻ console.cloud.google.com/projectcreate?project=knowbe4securitawareness

Google Cloud Platform Search Products, resources

New Project

Project name *
KB4VendorIntegration ?

Project ID: kb4vendorintegration. It cannot be changed later. [EDIT](#)

Organization *
sa-demo.com ▼ ?

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

Location *
sa-demo.com [BROWSE](#)

Parent organization or folder

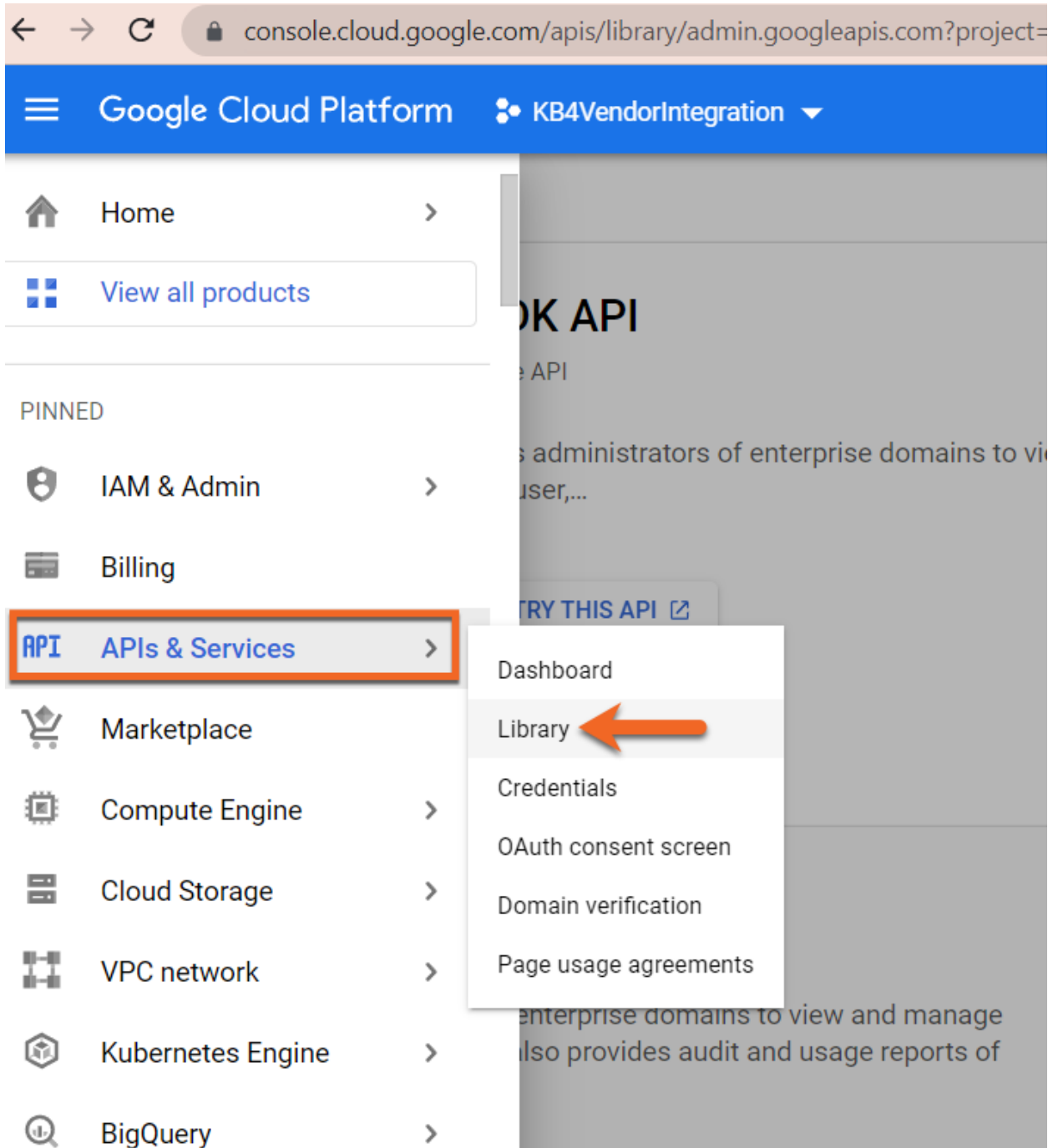
CREATE CANCEL

[Back to top](#)

Enable APIs for Your Project

To enable APIs for the project you created in the [Create a Project](#) section above, follow the steps below:

1. At the top of your Google Cloud platform, click the drop-down arrow and select **KB4VendorIntegration** as the current project.
2. Navigate to **APIs & Services > Library**.



3. Enter "Admin SDK API" into the search bar and press the **Enter** key on your keyboard.
4. From the search results, click **Admin SDK API**.

Google Cloud Platform

KB4VendorIntegration

API API Library

admin sdk api

API Library > "admin sdk api"

Filter by

CATEGORY

Developer tools (1)

Google Enterprise APIs (2)

Security (1)

Google Workspace (1)

"admin sdk api"

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,...

VPC network

Kubernetes Engine

BigQuery

Page usage agreements

enterprise domains to view and manage

also provides audit and usage reports of

5. Click **ENABLE**.

Google Cloud Platform

KB4VendorIntegration

Admin SDK API

Google Enterprise API

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

ENABLE

TRY THIS API

OVERVIEW

DOCUMENTATION

Overview

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.

Additional details

Type: [SaaS & APIs](#)

Last updated: 7/23/21

Category: [Google Workspace](#), [Google Enterprise APIs](#)

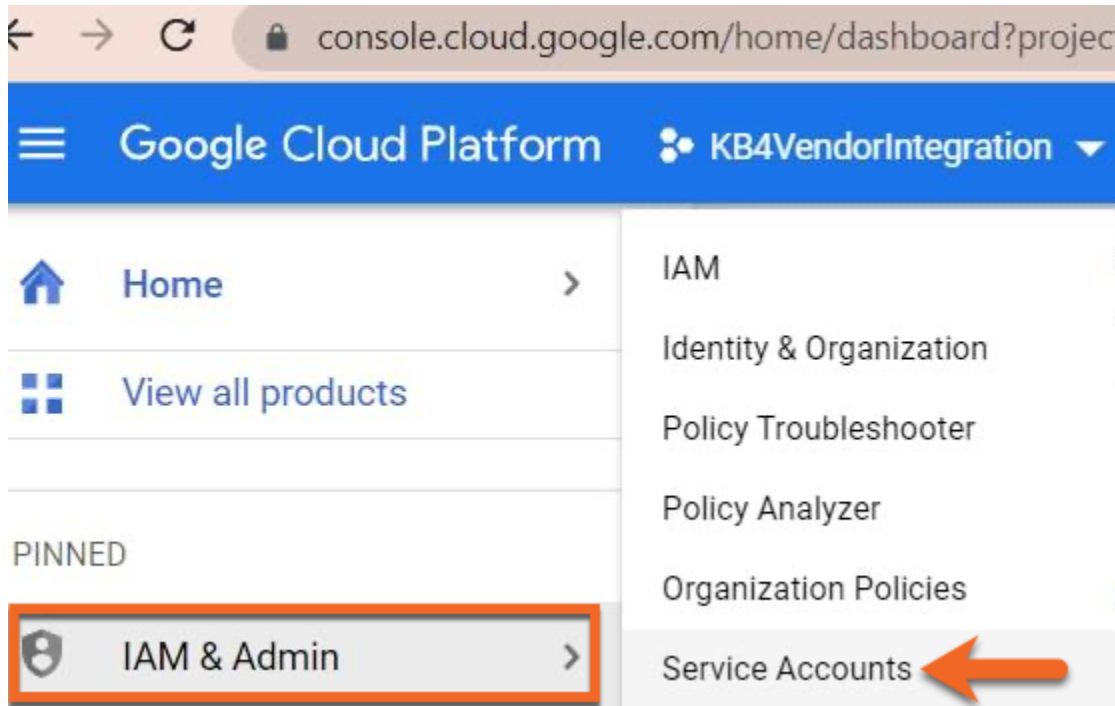
Service name: admin.googleapis.com

Back to top

Create a Service Account

To create a service account in your Google Cloud platform, follow the steps below:

1. At the top of your Google Cloud platform, click the drop-down arrow and select **KB4VendorIntegration** as the current project.
2. Navigate to **IAM & Admin** > **Service Accounts**.



3. In the menu bar at the top of the page, click + **CREATE SERVICE ACCOUNT**.

console.cloud.google.com/iam-admin/serviceaccounts?project=kb4vendorintegration

Google Cloud Platform KB4VendorIntegration

Search Products, resources, docs (/)

IAM & Admin

Service accounts + CREATE SERVICE ACCOUNT DELETE MANAGE ACCESS REFRESH

Service accounts for project "KB4VendorIntegration"

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

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation, [account organization policies](#).

Filter Enter property name or value

☐	Email	Status	Name ↑	Description	Key ID	Key creation date	OAuth 2 Client ID ?
No rows to display							

4. Enter a name for your new service account. We recommend "KB4MyOrganizationGSuiteServiceAcc", with "MyOrganization" being your organization's name.
5. For the **Service account description**, enter "This is the service account for integration with KnowBe4".
6. Click **CREATE AND CONTINUE**.

Google Cloud Platform

KB4VendorIntegration

Search Products, resources, docs (/)

IAM & Admin

IAM

Identity & Organization

Policy Troubleshooter

Policy Analyzer

Organization Policies

Service Accounts

Workload Identity Federat...

Labels

Tags

Settings

Privacy & Security

Identity-Aware Proxy

Roles

Manage Resources

Create service account

1

Service account details

Service account name

KB4MyOrganizationGSuiteServiceAcc

Display name for this service account

Service account ID *

kb4myorganizationssuiteservice @kb4vendorintegration.iam.gser

X ↺

Service account description

This is the service account for integration with KnowBe4

Describe what this service account will do

CREATE AND CONTINUE

2

Grant this service account access to project (optional)

3

Grant users access to this service account (optional)

DONE

CANCEL

7. Click the **Select a role** drop-down menu and select **Basic > Viewer**.

Google Cloud Platform KB4VendorIntegration Search Products, resources, docs

IAM & Admin Create service account

1 Service account details

2 Grant this service account access to project (optional)

Grant this service account access to KB4VendorIntegration so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Role Condition

Filter |Type to filter

Quick access

Currently used

Basic

By product or service

Access Approval

Access Context Manager

Actions

Roles

Browser

Editor

Owner

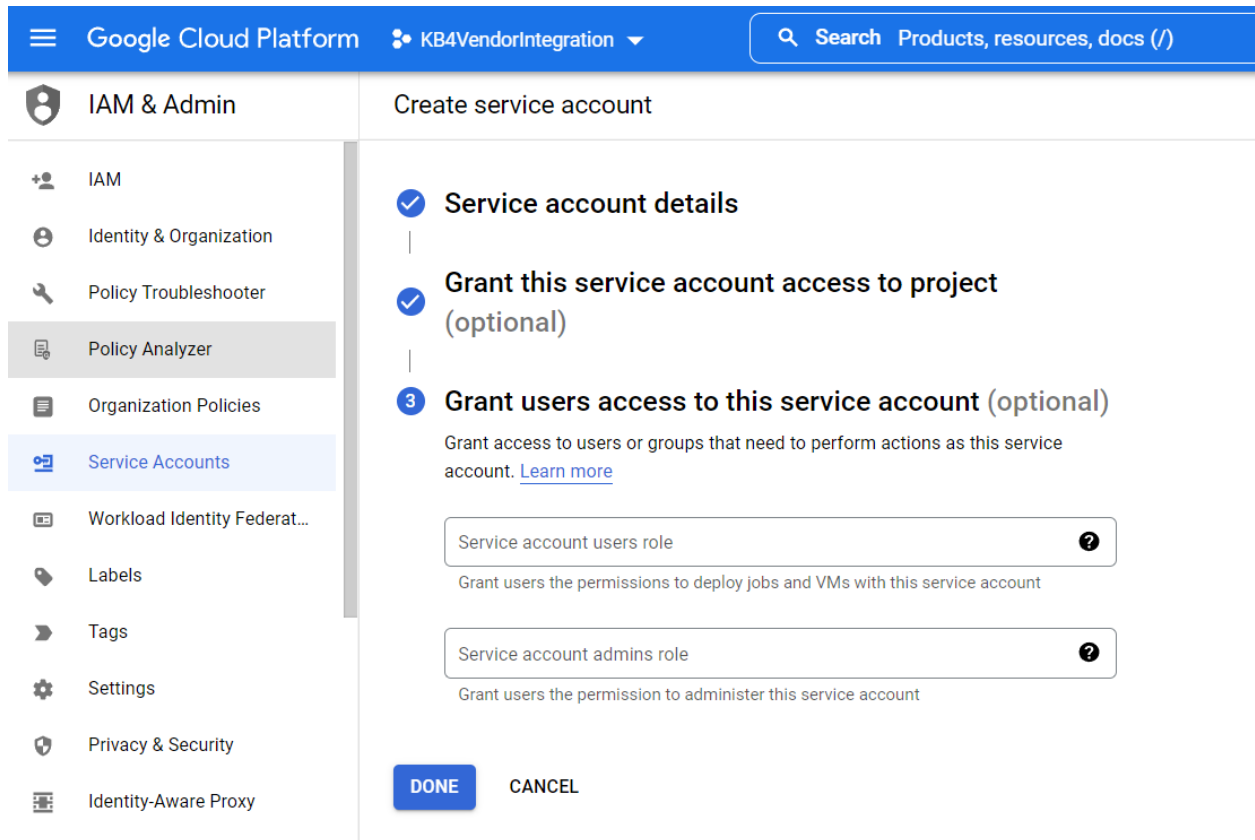
Viewer

MANAGE ROLES

3

DONE

8. Click the white **Continue** button.
9. Skip the **Grant users access to this service account** step and click the blue **DONE** button.



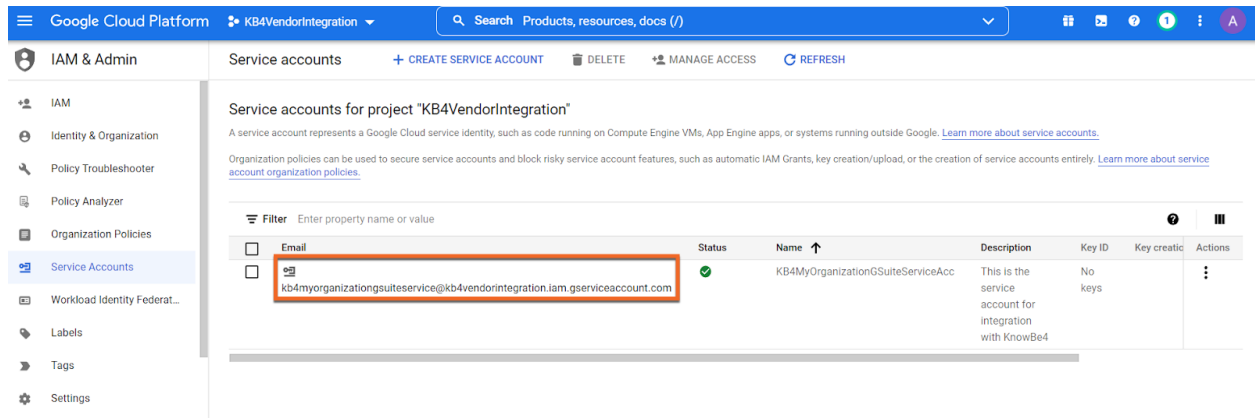
[Back to top](#)

Obtain Your Service Account JSON File and Unique ID

After you have created your service account, you will need to obtain your service account JSON file and unique ID. You will need both of these items later in the integration setup process.

To obtain your JSON file and unique ID, follow the steps below:

1. At the top of your Google Cloud platform, click the drop-down arrow and select **KB4VendorIntegration** as the current project.
2. From the sidebar on the left side of the page, select the **Service Accounts** tab.
3. Click on the service account's name in the **Email** column. When you click, the service account's **DETAILS** page will open. This page lists the **Unique ID**.



4. Copy the **Unique ID** and save it to a place that you can easily access later. You will need it to complete the steps in the [Assign Domain-Wide Delegation and Scopes](#) section of this article.
5. To obtain the JSON file, click **KEYS** in the top menu bar.
6. Click the **ADD KEY** drop-down menu and select **Create new key**.

Google Cloud Platform KB4VendorIntegration

Search Products, resources, docs (/)

IAM & Admin

KB4MyOrganizationGSuiteServiceAcc

DETAILS PERMISSIONS **KEYS** METRICS LOGS

Keys

Service account keys could pose a security risk if compromised. We recommend you read 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

7. In the pop-up window that opens, select **JSON** for the **Key type** and then click **CREATE**. The JSON file will automatically download to your device and the private key will save in the service account's **KEYS** tab.

Google Cloud Platform KB4VendorIntegration

Search Products, resources, docs (/)

IAM & Admin

KB4MyOrganizationGSuiteServiceAcc

DETAILS PERMISSIONS **KEYS** METRICS LOGS

Keys

Service account keys could pose a security risk if compromised. We recommend you read 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 ▾

Type Status Key Key

No rows to display

Create private key for "KB4MyOrganizationGSuiteServiceAcc"

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

Note: You will need this JSON file when you complete the integration setup process in the [Set Up the Integration in Your KMSAT Console](#) section below.

[Back to top](#)

Set Up the Integration in Your KMSAT Console

Once you've set up the integration in your Google Cloud platform, you can set up the integration in your KMSAT console. To set up the integration in your KMSAT console, follow the steps below:

1. Log in to your KMSAT console.
2. Navigate to **SecurityCoach > Setup**.
3. In the **Available Integrations** section, locate the card for the Google integration you want to set up.
4. At the bottom of the card, click **Configure**.



5. In the **Admin Email** field, enter the admin email address.
6. In the **Credentials File** field, click **Browse** and select the JSON file you downloaded in the [Obtain Your Service Account JSON File and Unique ID](#) section of this article.

For more information about configuring this vendor integration, click [Configuration Help](#).

Configuration Help

Admin Email

Endpoint

api.gsuite.com

Credentials File

No File Selected.

Browse

Reset

Authorize

7. Click **Authorize**.

[Back to top](#)

Assign Domain-Wide Delegation and Scopes

After you have set up the integration in your Google Cloud Platform and your KMSAT console, you can assign domain-wide delegation and scopes. To assign domain-wide delegation and scopes, follow the steps below:

1. Navigate to admin.google.com and enter your administrator login credentials.
2. From the sidebar on the left side of the page, navigate to **Security > Access and data control > API controls**.



▸  Devices

▸  Apps

▾  Security

Overview

Alert center

▸ Authentication

▾ Access and data control

API controls

Data classification

Data protection

Google Session control

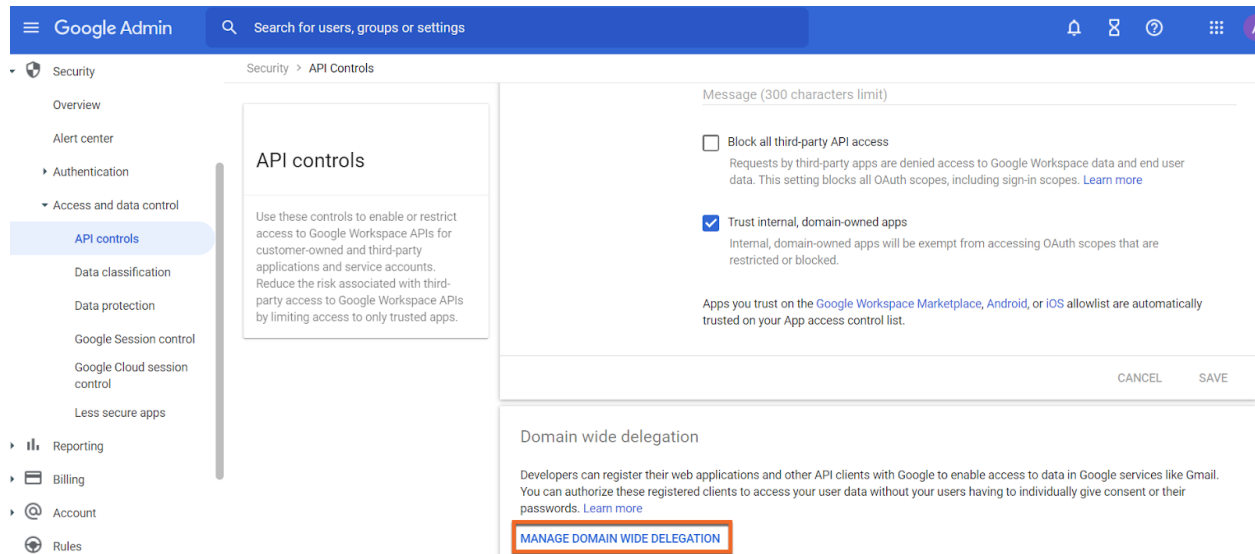
Google Cloud session
control

Less secure apps

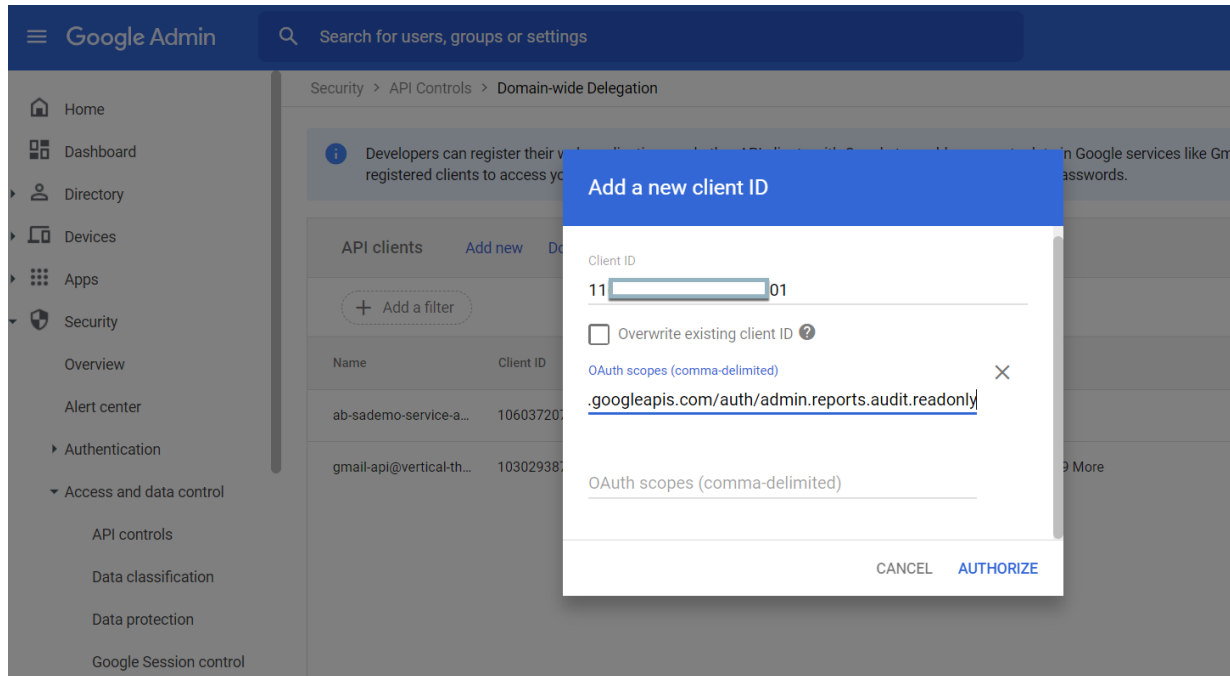
▸  Reporting

▸  Billing

3. Scroll down in the sidebar on the right side of the page until you see the **Domain wide delegation** section. In this section, click **MANAGE DOMAIN WIDE DELEGATION**.



4. Click **Add new**. When you click this button, the **Add a new client** window will open.
5. In the **Client ID** field, enter your service account ID. This is the ID that was from Step 3 in the [Obtain Your Service Account JSON File and Unique ID](#) section of this article.
6. In the **OAuth scopes (comma-delimited)** field, enter ["https://www.googleapis.com/auth/admin.reports.audit.readonly"](https://www.googleapis.com/auth/admin.reports.audit.readonly).
7. Once you have entered your service account ID and scope, click **AUTHORIZE**.



Back to top