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

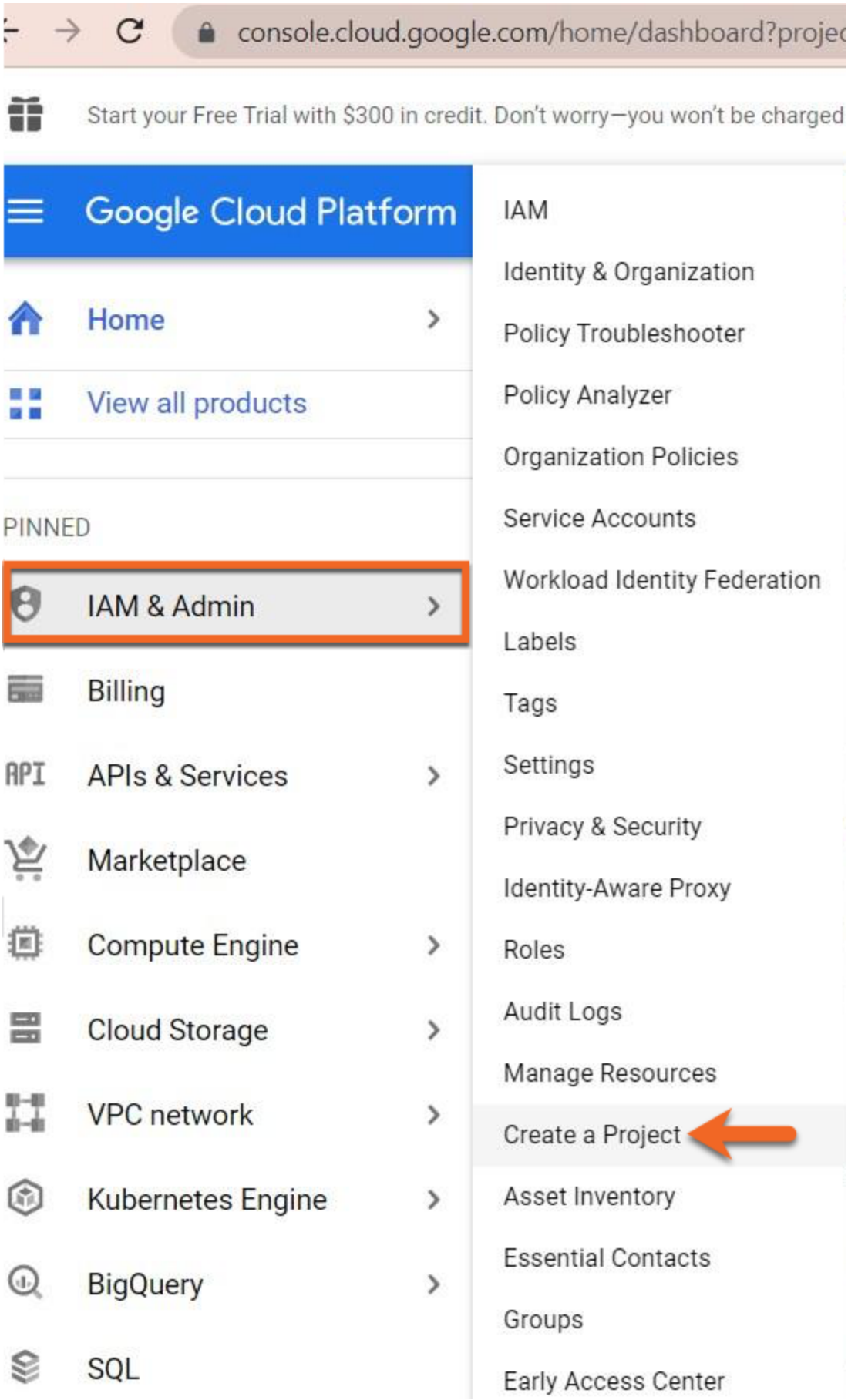
Before you can set up the SecurityCoach integration in your KMSAT console, you will need to set up the integration in your Google Cloud platform by creating a project and a service account. You will also need to enable APIs for your project and obtain a JSON file and unique ID from your service account.

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

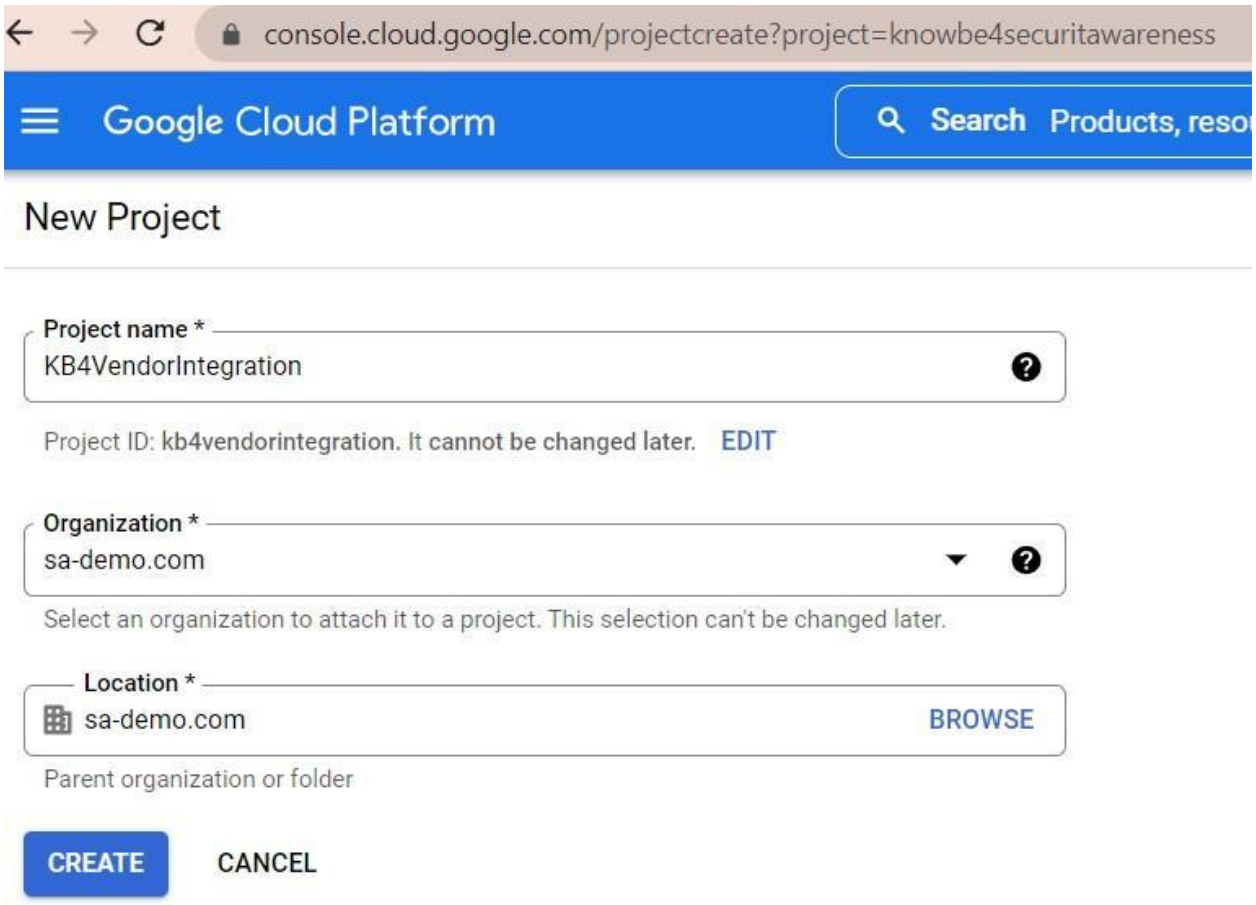
Create a Project

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**.


console.cloud.google.com/home/dashboard?projec
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**.

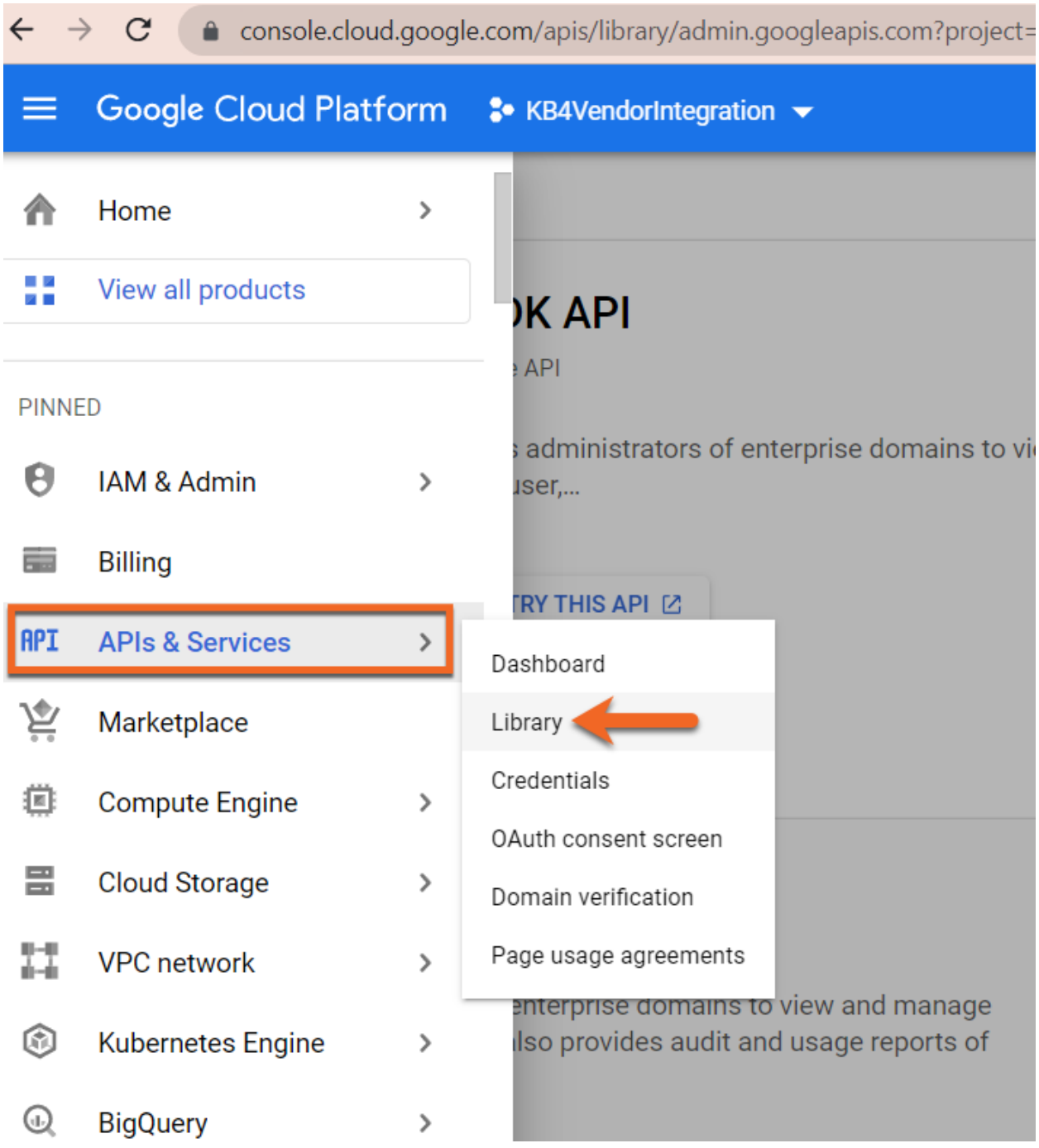


Back to top

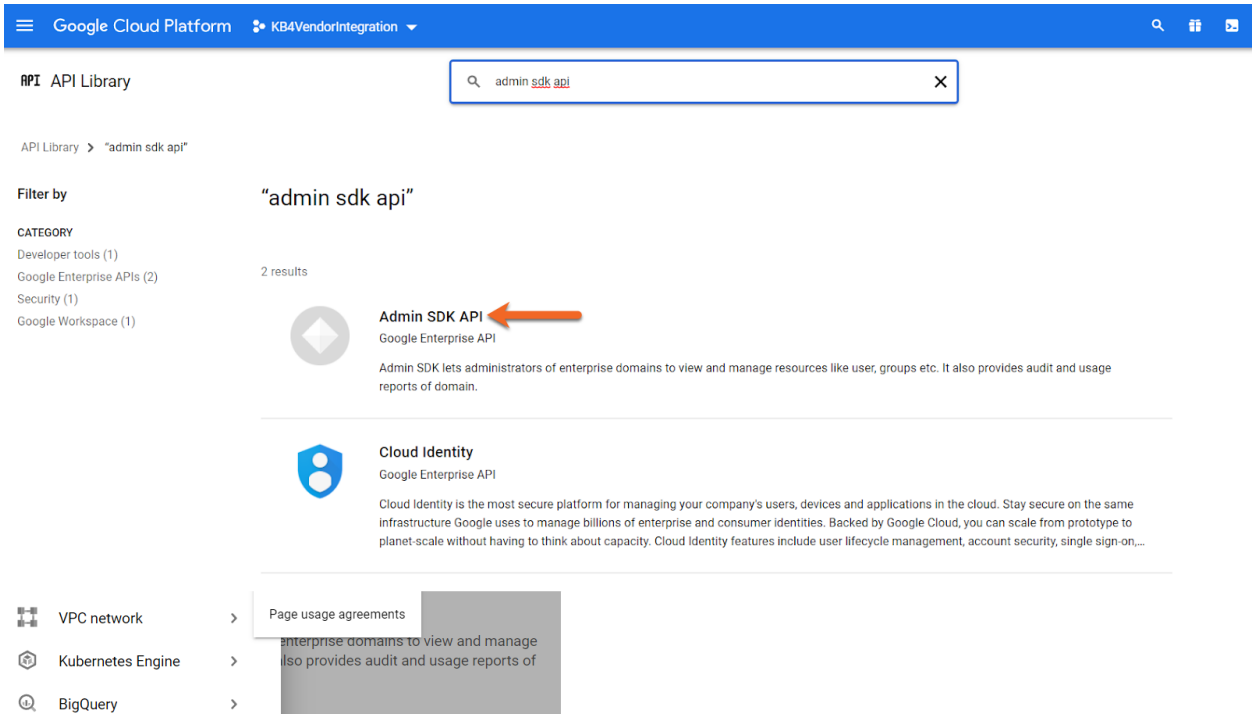
Enable APIs for Your Project

To enable APIs for the project you created in the Create a Project section above, follow the steps below:

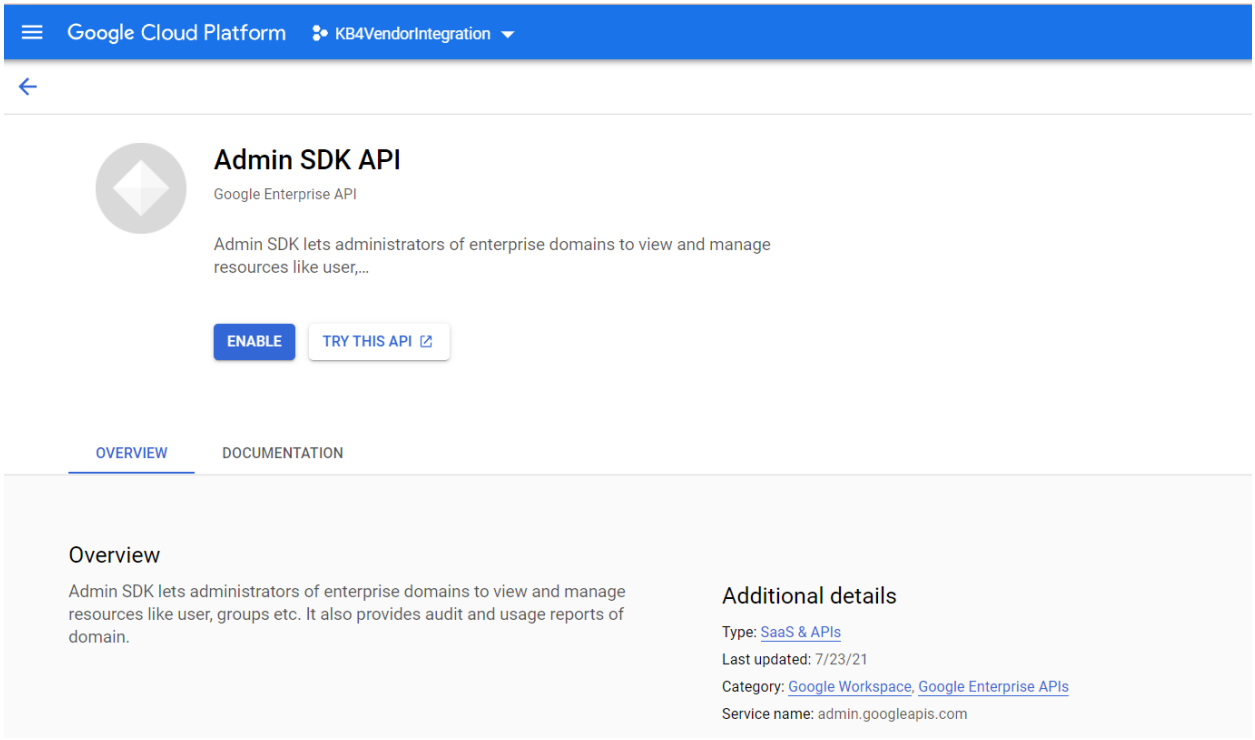
1. At the top of your Google Cloud platform, click the drop-down arrow and select **KB4VendorIntegration** as the current project.
2. Navigate to **APIs & Services** > **Library**.



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**.



5. Click **ENABLE**.

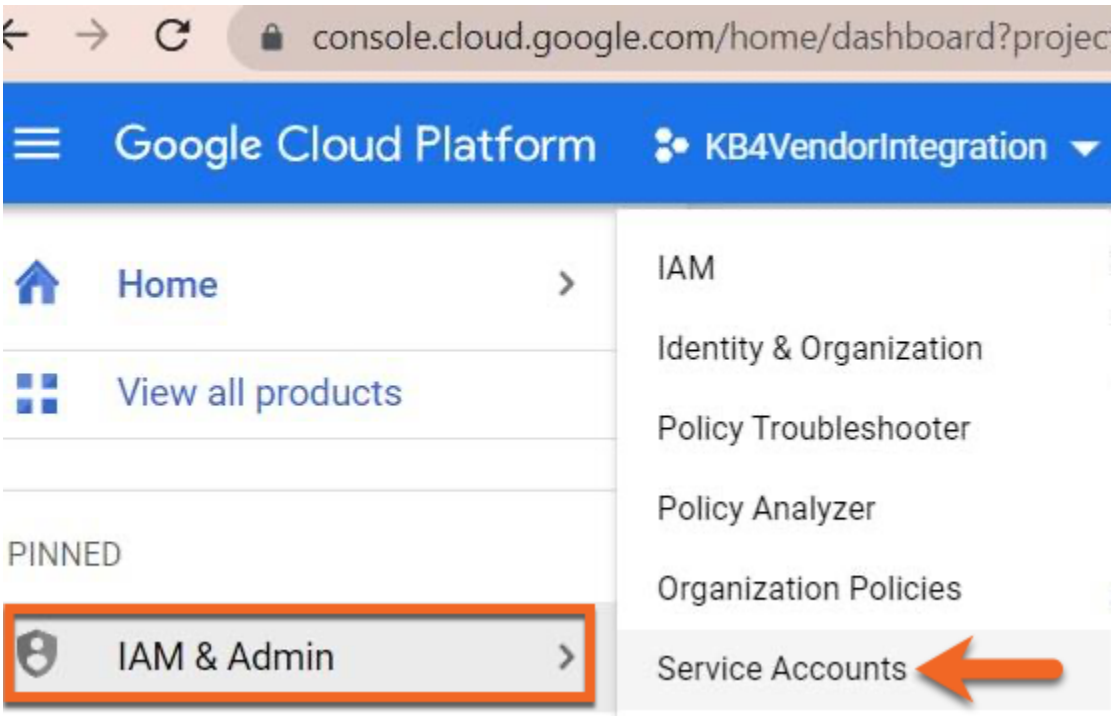


Back to top

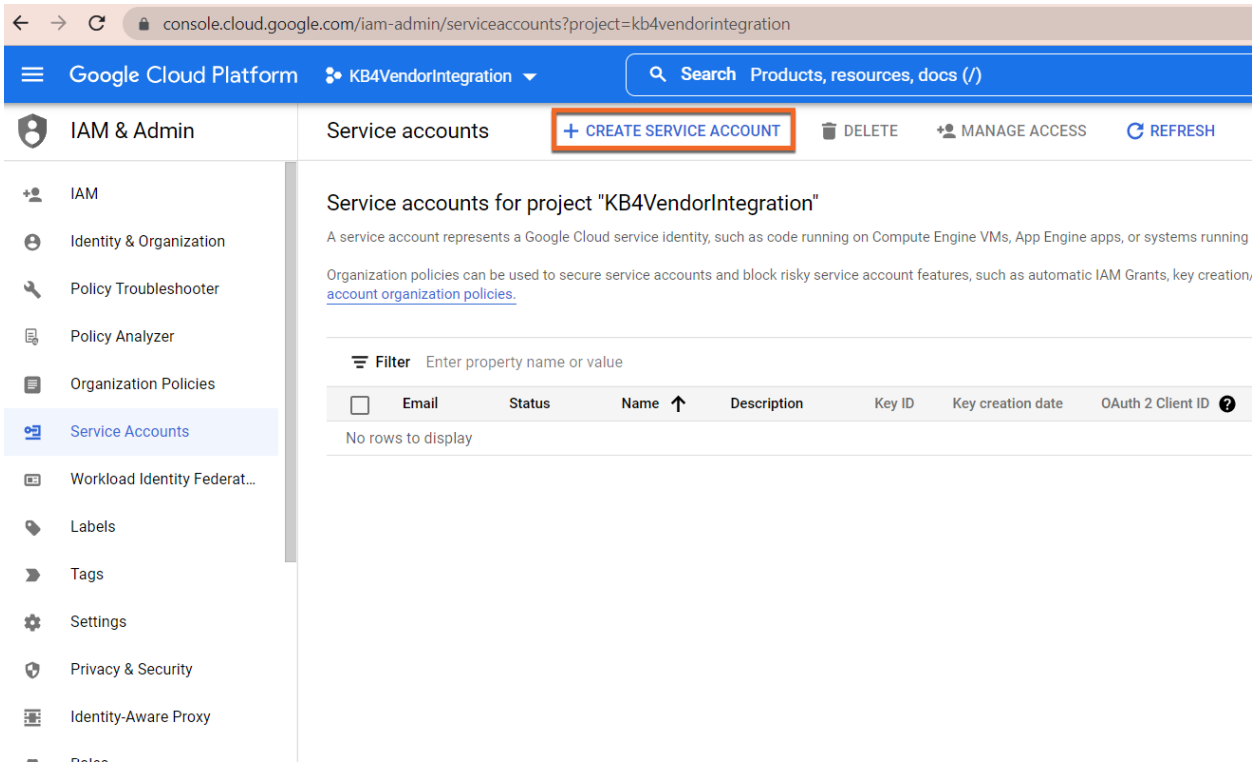
Create a Service Account

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

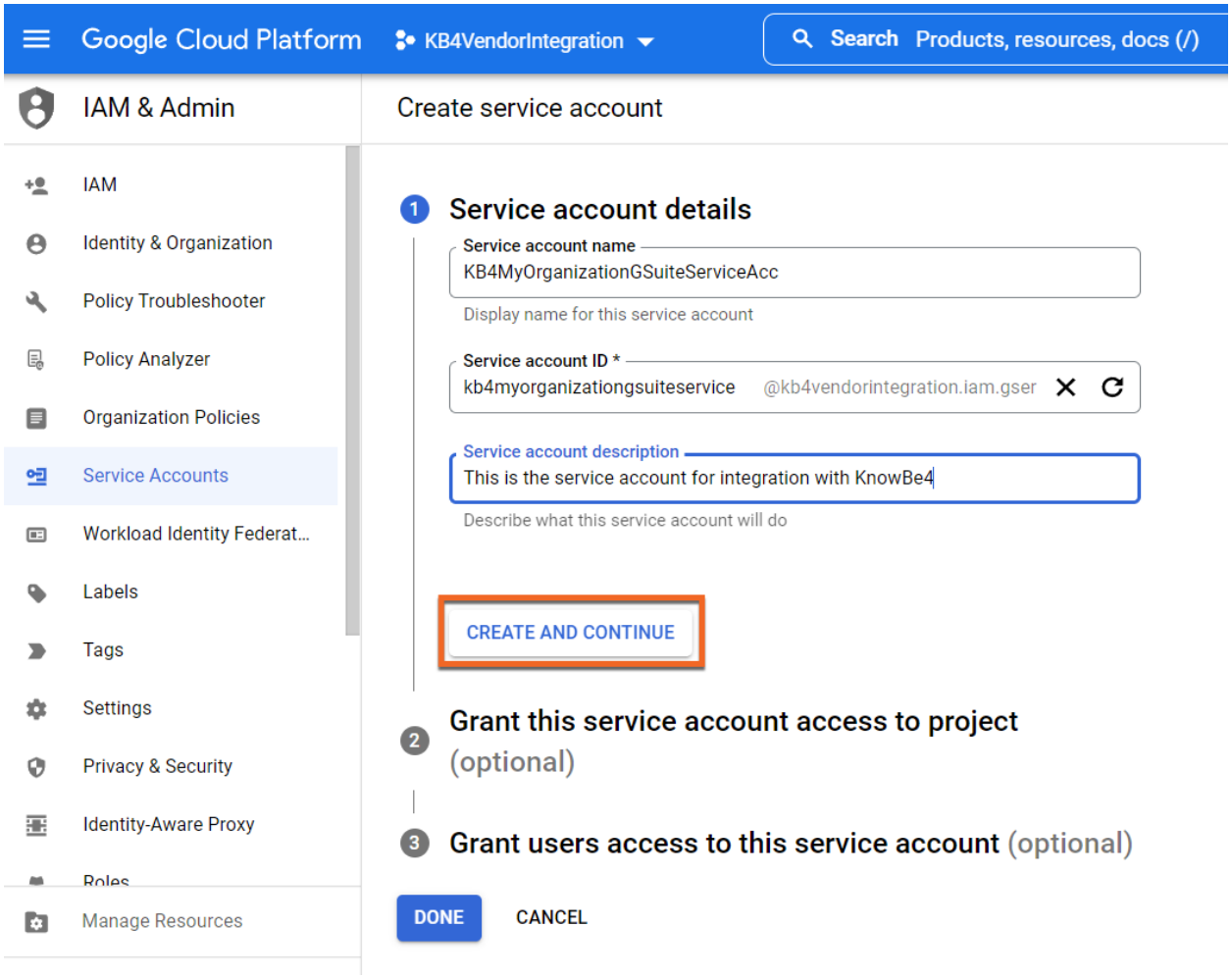
1. At the top of your Google Cloud platform, click the drop-down arrow and select **KB4VendorIntegration** as the current project.
2. Navigate to **IAM & Admin** > **Service Accounts**.



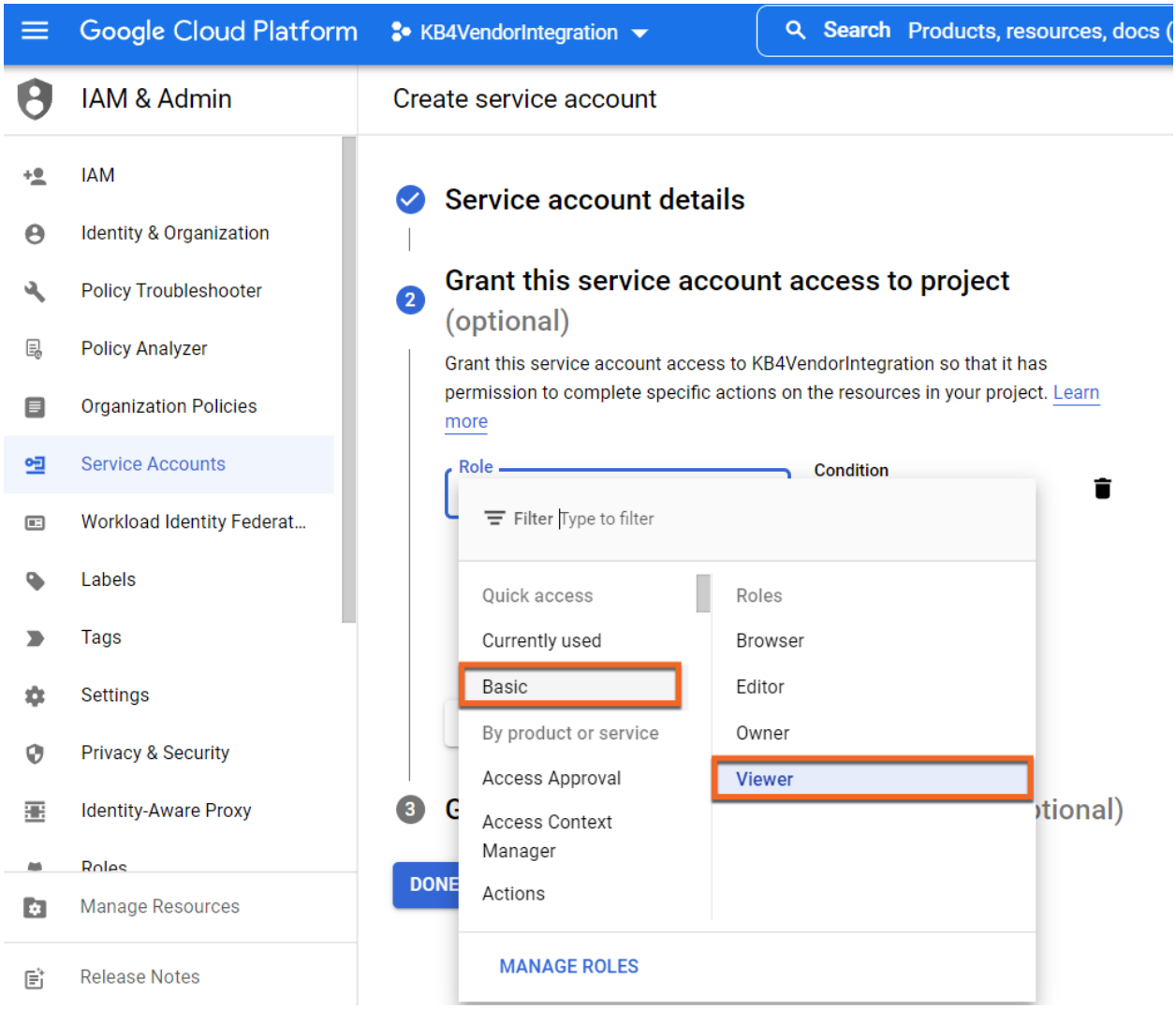
3. In the menu bar at the top of the page, click **+ CREATE SERVICE ACCOUNT**.



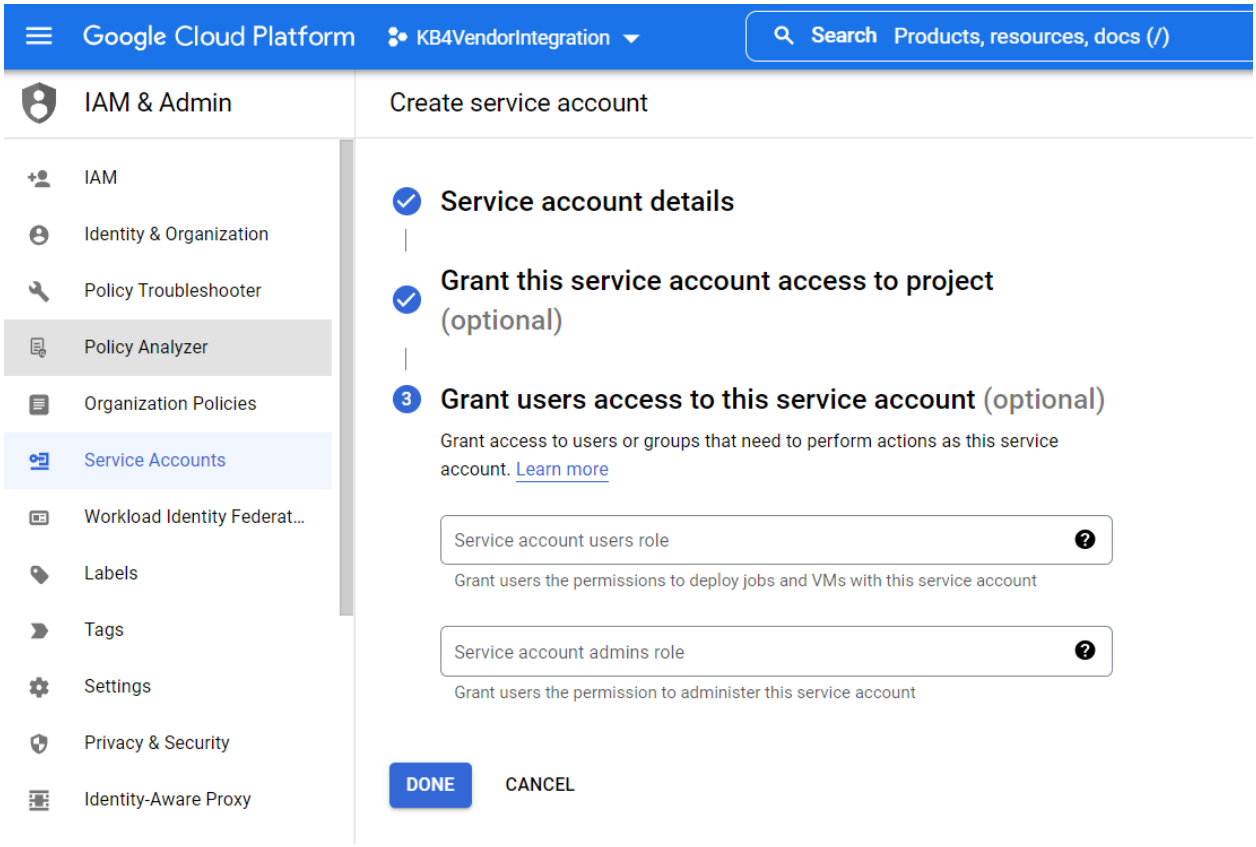
4. Enter a name for your new service account. We recommend "KB4MyOrganizationGSuiteServiceAcc", with "MyOrganization" being your organization's name.
5. For the **Service account description**, enter "This is the service account for integration with KnowBe4".
6. Click **CREATE AND CONTINUE**.



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



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



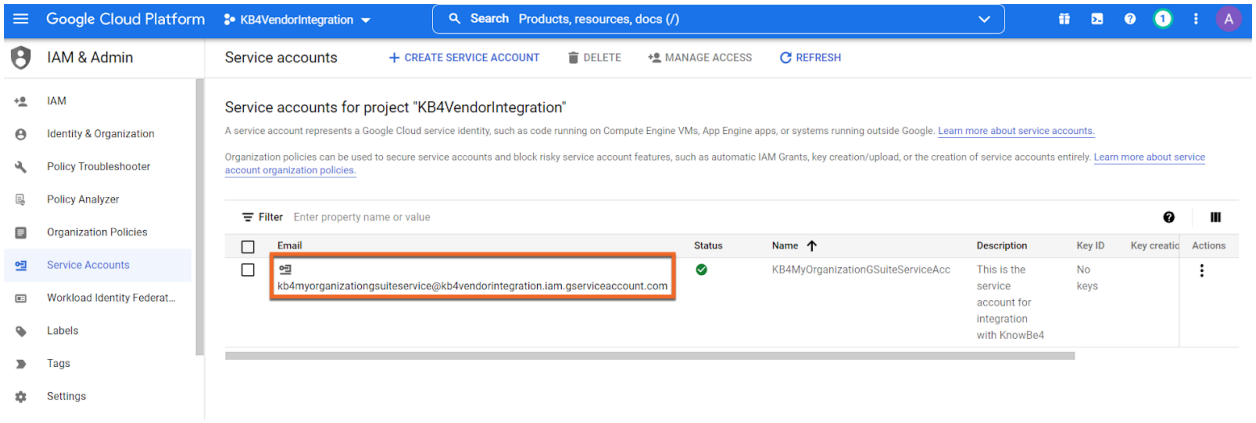
Back to top

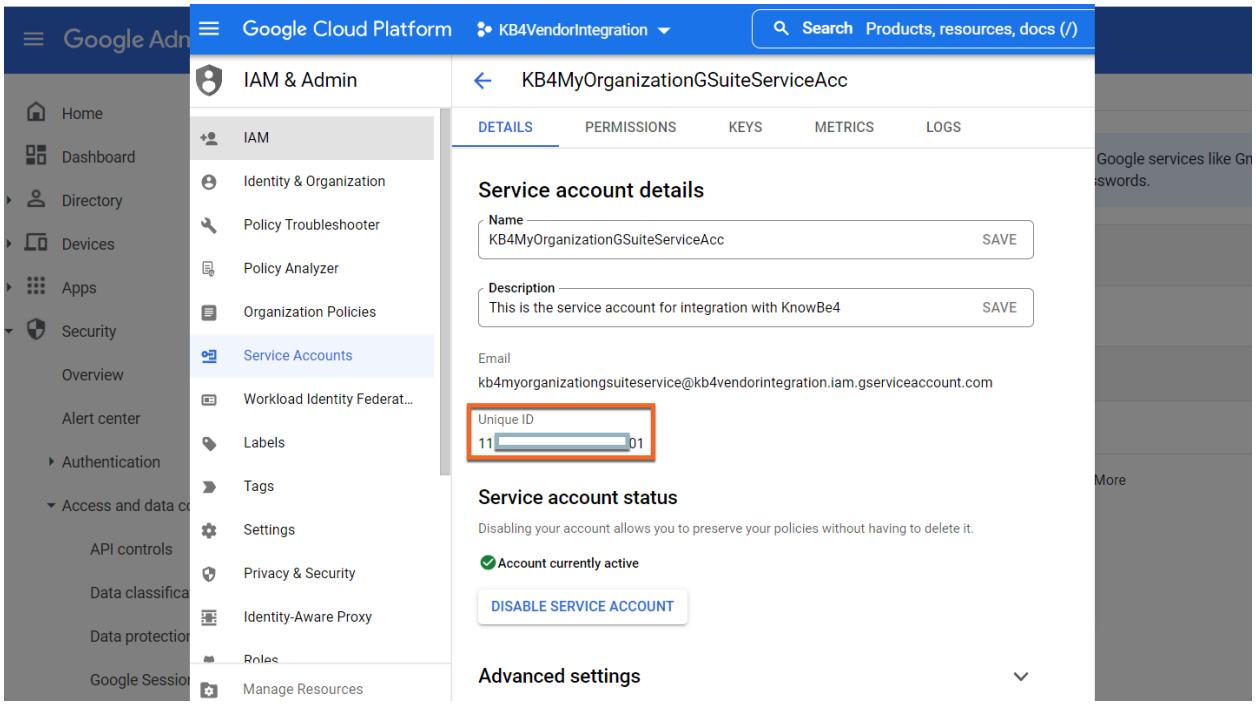
Obtain Your Service Account JSON File and Unique ID

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.

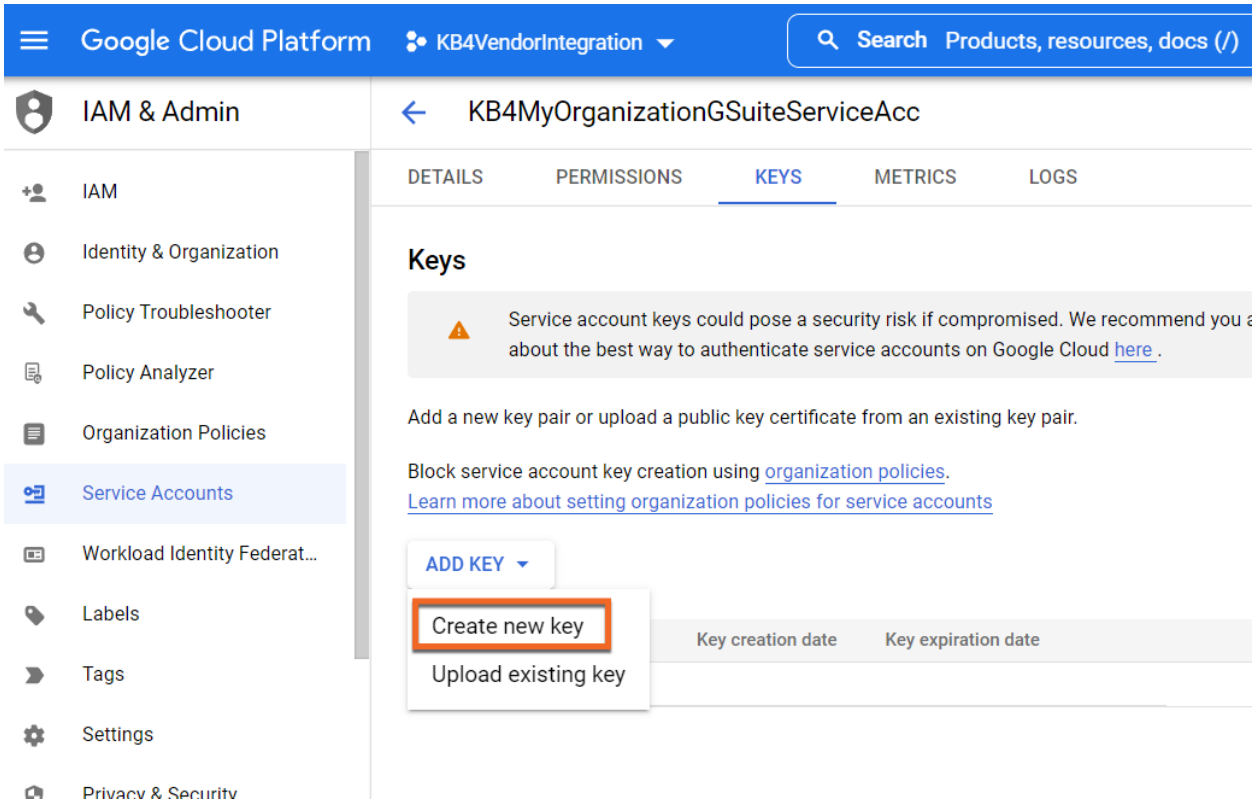
To obtain your JSON file and unique ID, follow the steps below:

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**.

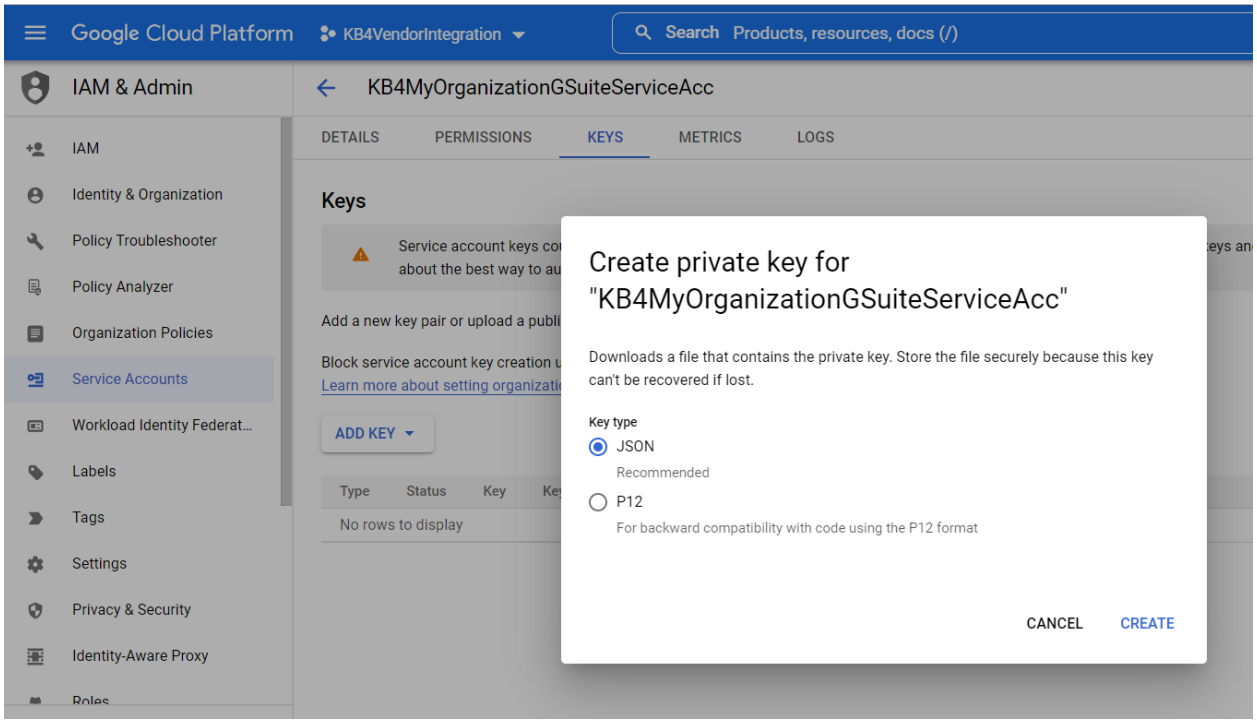




4. Copy the **Unique ID** and save it to a place that you can easily access later. You will need it to complete the steps in the Assign Domain-Wide Delegation and Scopes section of this article.
5. To obtain the JSON file, click **KEYS** in the top menu bar.
6. Click the **ADD KEY** drop-down menu and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



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.



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.

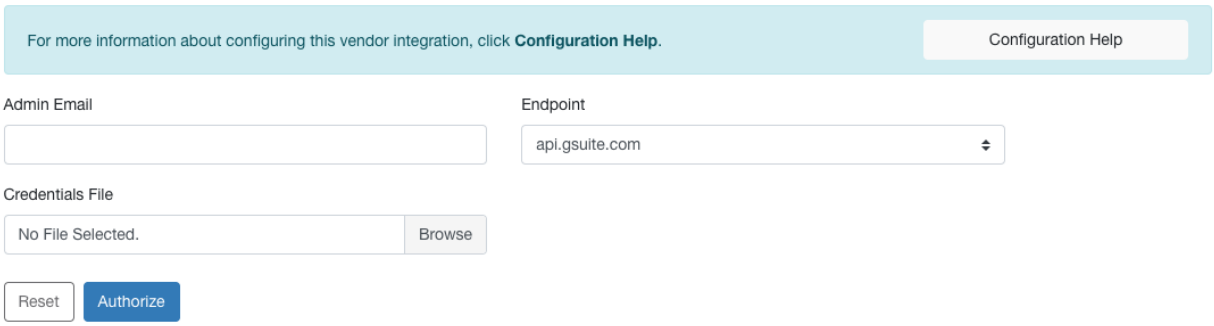
Back to top

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.



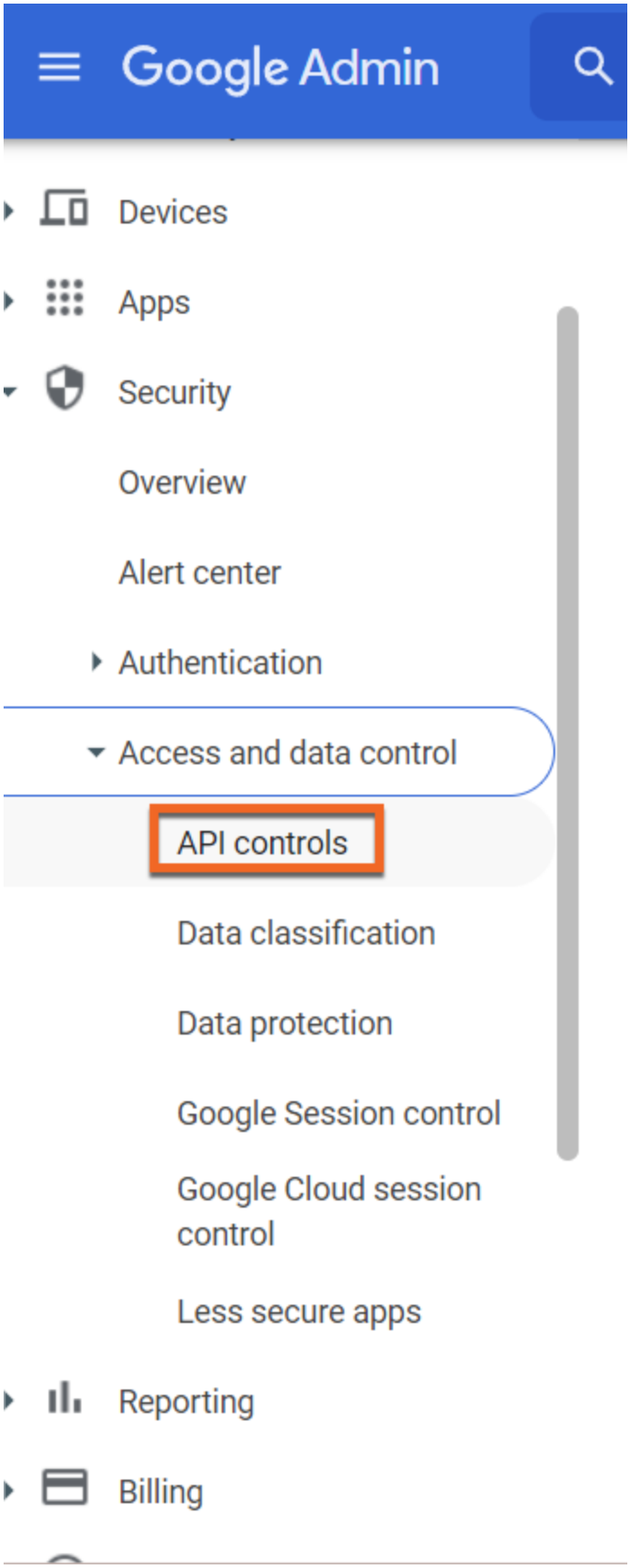
7. Click **Authorize**.

Back to top

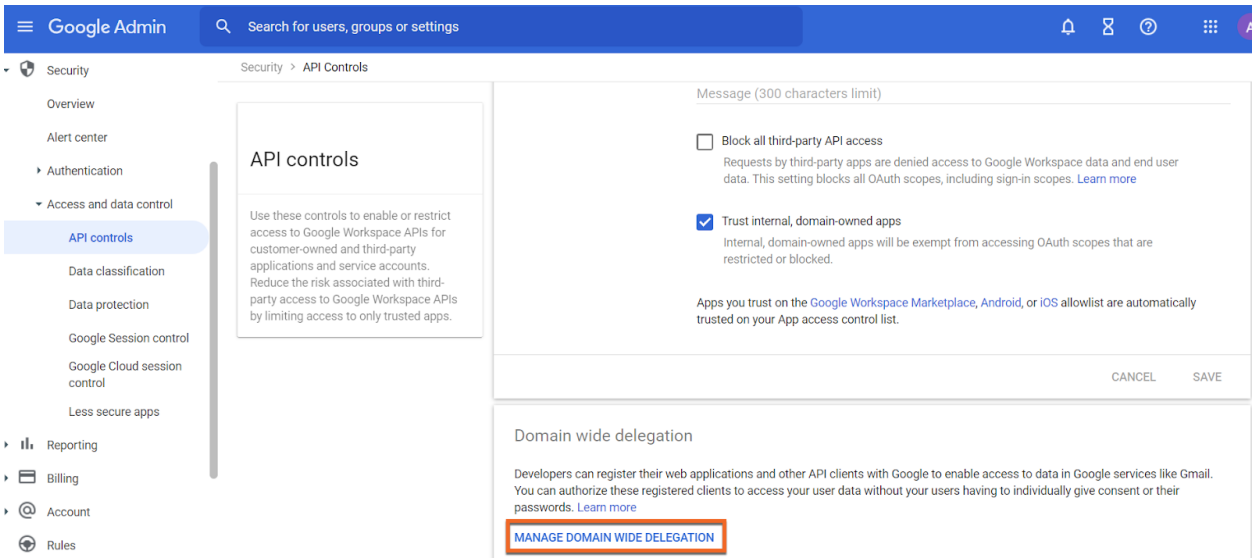
Assign Domain-Wide Delegation and Scopes

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:

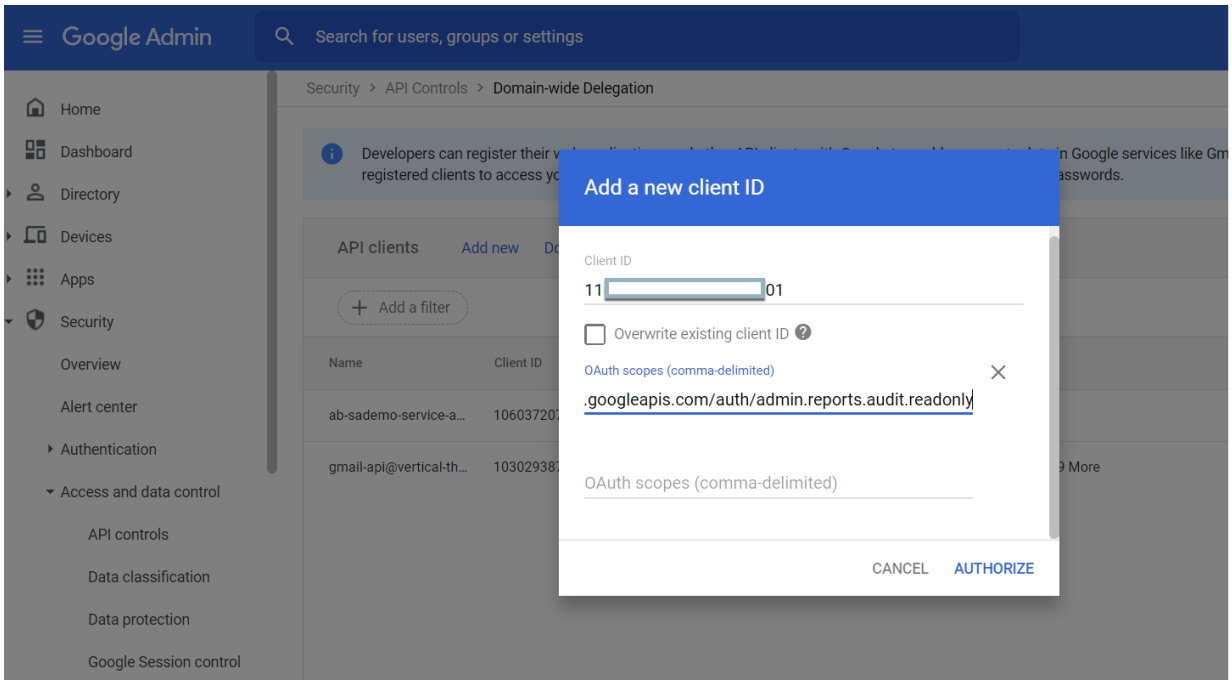
1. Navigate to admin.google.com and enter your administrator login credentials.
2. From the sidebar on the left side of the page, navigate to **Security** > **Access and data control** > **API controls**.


Google Admin
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".
7. Once you have entered your service account ID and scope, click **AUTHORIZE**.


Google Admin
Search for users, groups or settings
Home
Dashboard
Directory
Devices
Apps
Security
Overview
Alert center
Authentication
Access and data control
API controls
Data classification
Data protection
Google Session control
Security > API Controls > Domain-wide Delegation
API clients
Add new
Add a filter
Name
Client ID
Add a new client ID
Client ID
Overwrite existing client ID
OAuth scopes (comma-delimited)
.googleapis.com/auth/admin.reports.audit.readonly
OAuth scopes (comma-delimited)
CANCEL
AUTHORIZE

Back to top