

## Integrating Google Workspace

<https://campus.barracuda.com/doc/96767898/>

Integrating Google Workspace involves performing the following procedures:

- To set up the Google Workspace Project
- To set up Barracuda XDR Dashboard

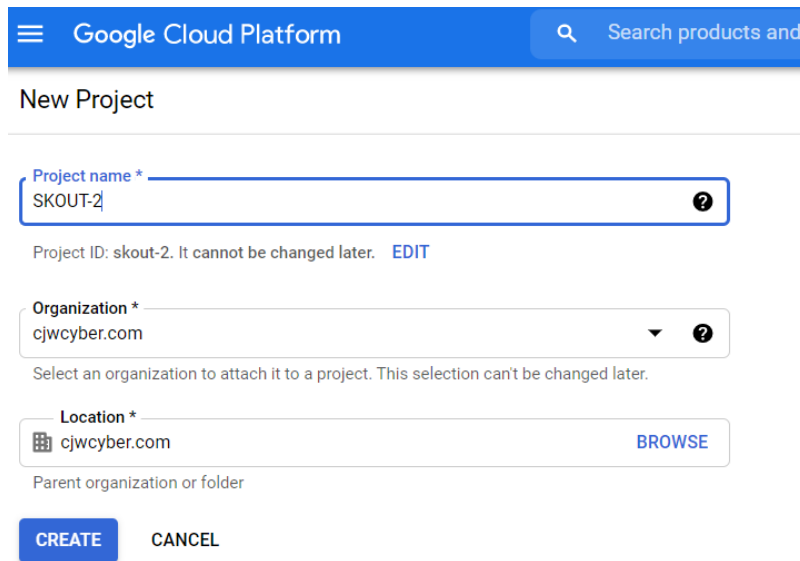
### Setting up the Google Workspace Project

When integrating Google Workspace, you must add a user to a role that has the privileges in the table below, or use **Super Admin** :

Administrator Console Privileges	• <b>Reports</b>
Admin API Privileges	• <b>Organizational Units: Read</b> • <b>Users: Read</b> • <b>Groups: Read</b> • <b>Schema Management: Schema Read</b> • <b>License Management: License read</b> • <b>Billing Management: Billing Read</b> • <b>Domain Allow List Management: Domain Allow List Read</b>

#### To set up the Google Workspace Project

1. Log in to [Google Admin Console](#).
2. Click **Add a User** and populate the user information.  
Take note of the email address. You will need to share it with Barracuda XDR later.
3. Add that new user to either **Super Admin** or create a **Custom Role** that has Access to the Admin API Privileges as outlined in the table above.  
This account cannot have two-factor authentication enforced on it
4. Create a new [Google Workspace Project](#).
5. Enter a **Project Name** and select the **Parent Organization**.



Google Cloud Platform

Search products and

### New Project

Project name \* SKOUT-2 ?

Project ID: skout-2. It cannot be changed later. [EDIT](#)

Organization \* cjwcyber.com ?

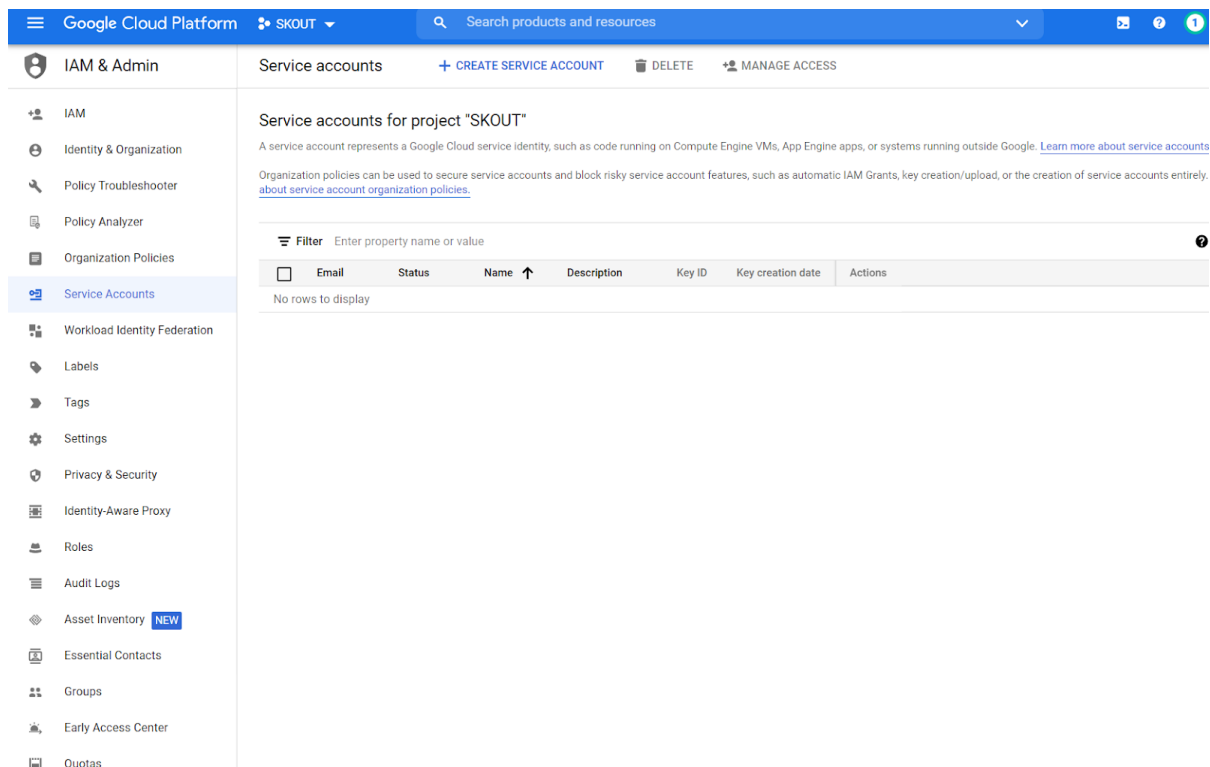
Select an organization to attach it to a project. This selection can't be changed later.

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

Parent organization or folder

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

6. Navigate to [Google Cloud Platform](#) and click **Go to Project Settings**.
7. On the Left Navigation, click **IAM & Admin > Service Accounts**.
8. At the top of the screen, click **Create Service Account**.



Google Cloud Platform SKOUT

Search products and resources

**IAM & Admin**

Service accounts [+ CREATE SERVICE ACCOUNT](#) [DELETE](#) [MANAGE ACCESS](#)

### Service accounts for project "SKOUT"

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 about service accounts](#)

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

**Filter** Enter property name or value ?

<input type="checkbox"/>	Email	Status	Name ↑	Description	Key ID	Key creation date	Actions
No rows to display							

9. Enter the **Service account name** and **Description**. The **Service account id** is generated. Click **Create and Continue**.

Google Cloud Platform SKOUT-2 Search products and resources

IAM & Admin Create service account

**1 Service account details**

Service account name  
skt2-gcp-svc

Display name for this service account

Service account ID  
skt2-gcp-svc @skout-2.iam.gserviceaccount.com

Service account description  
SKOUT Service Account

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

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

Asset Inventory NEW

Essential Contacts

Groups

Early Access Center

Quotas

10. Click **Continue**.

11. In **Service Account Users Role**, enter the user account you created in Step 1, then click **Done**.

Google Cloud Platform SKOUT

Search products and resources

IAM & Admin

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

Asset Inventory NEW

Essential Contacts

Groups

Early Access Center

Quotas

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

gcsdk@cjwcyber.com

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

Service account admins role

gcsdk@cjwcyber.com

Grant users the permission to administer this service account

DONE

CANCEL

You will be brought to the project home page and you will see the service account you created.


12. To create a key, click the three dots under **Action** and click **Manage Keys**.

Service accounts for project "My Project"


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 about service accounts.](#)


Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account organization policies.](#)


Filter Enter property name or value


<input type="checkbox"/>	Email	Status	Name ↑	Description	Key ID	Key creation date	Actions
<input type="checkbox"/>	 file-beats@halogen-basis-314319.iam.gserviceaccount.com	✓	file-beats	This is the file beats service account	No keys		<div>Manage details Manage permissions Manage keys View metrics View logs Disable Delete</div>


13. Click **Add Key > Create new key** .


 IAM & Admin


 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

 Essential Contacts

 Groups


 Early Access Center

 Quotas

← file-beats

DETAILS PERMISSIONS **KEYS** METRICS LOGS

**Keys**

 In many cases you can use Workload Identity Federation instead of service account keys to make your applications more secure. See [documentation](#) .

[GO TO WORKLOAD IDENTITY PAGE](#)

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 creation date	Key expiration date
No rows to display				

14. Select **JSON**.

### Create private key for "file-beats"

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

**Key type**

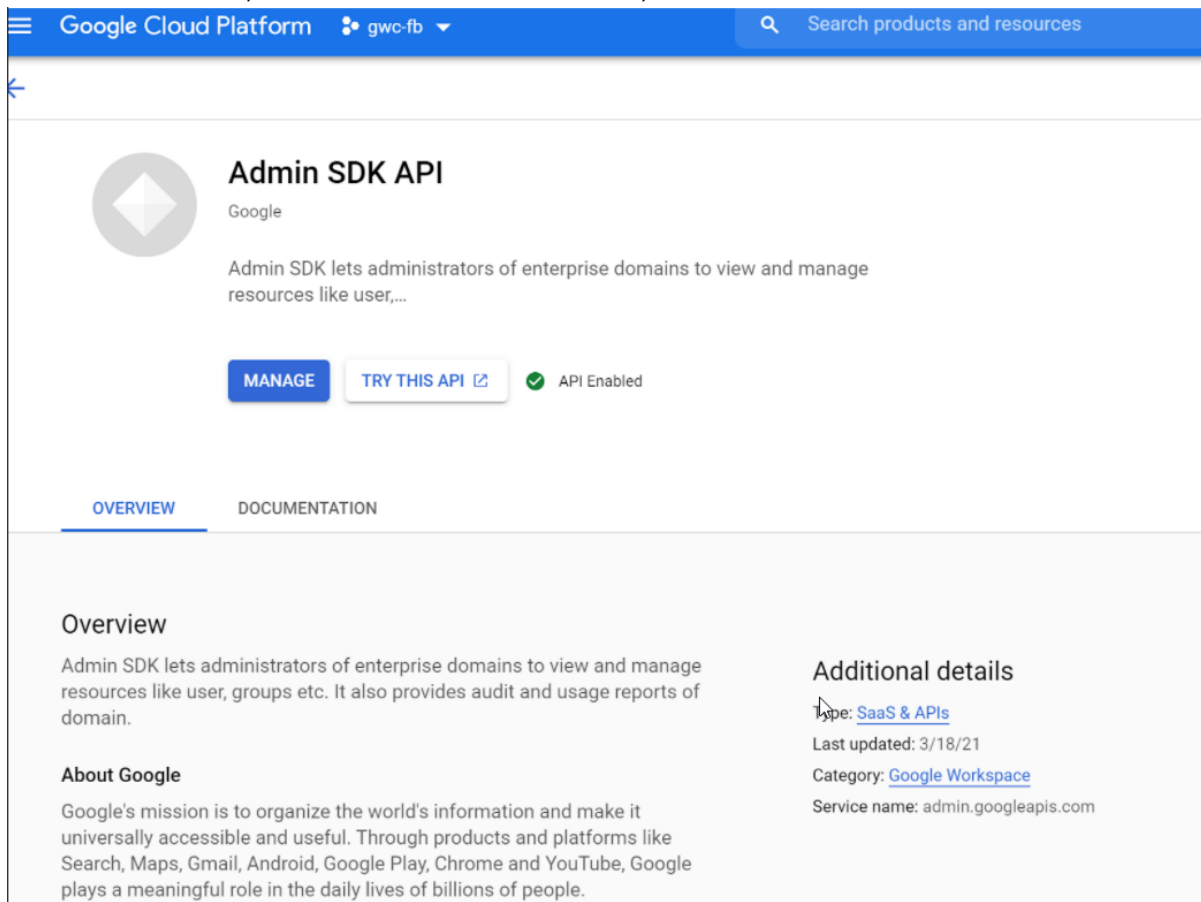
☒ JSON  
Recommended

☐ P12  
For backward compatibility with code using the P12 format

CANCEL CREATE

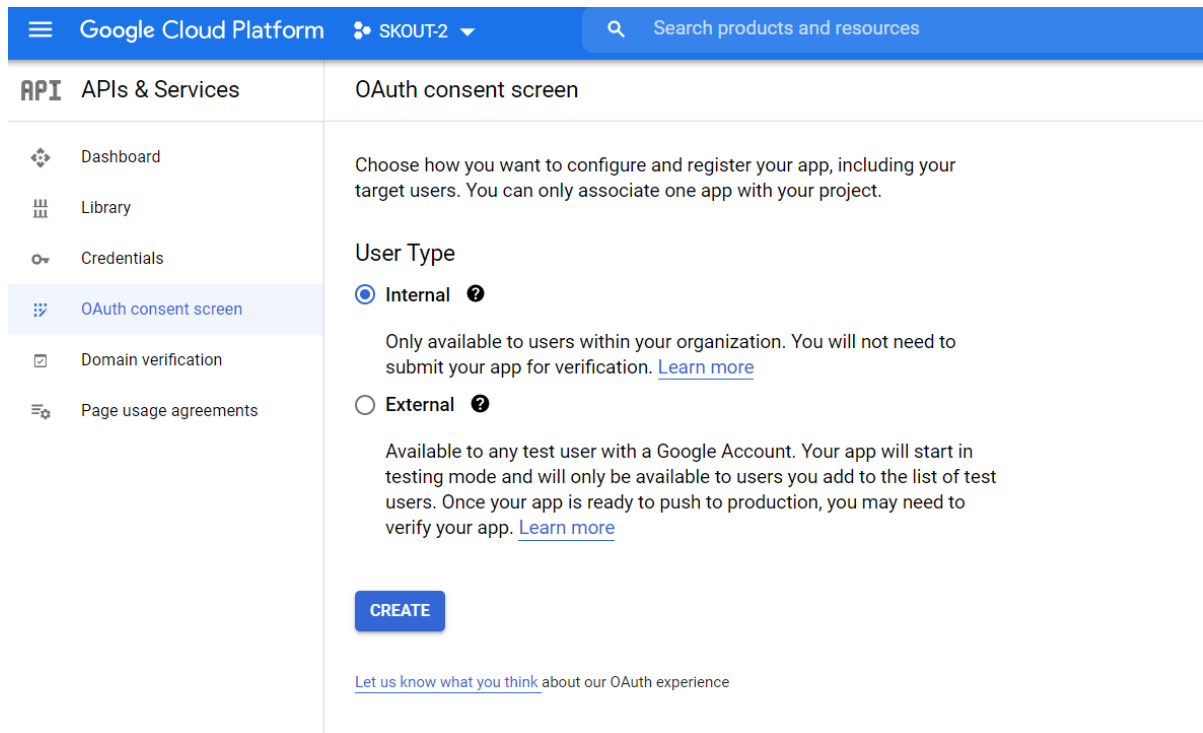
The .JSON file downloads automatically. Save this downloaded file. You must input it on the dashboard.

15. Navigate to <https://console.cloud.google.com/apis/library>. Ensure your project is selected. Search for **Admin SDK API** and click it.
16. If it is not enabled, enable it. When it is enabled, validate it.



The screenshot shows the Google Cloud Platform console interface. At the top is a blue header with the Google Cloud Platform logo, a dropdown menu showing 'gwc-fb', and a search bar. Below the header, the 'Admin SDK API' page is displayed. It features a Google logo icon, the title 'Admin SDK API', and a description: 'Admin SDK lets administrators of enterprise domains to view and manage resources like user,...'. There are two buttons: 'MANAGE' and 'TRY THIS API'. A green checkmark indicates 'API Enabled'. Below this, there are tabs for 'OVERVIEW' and 'DOCUMENTATION'. The 'OVERVIEW' tab is active, showing an 'Overview' section with a description of the Admin SDK and an 'About Google' section. To the right, under 'Additional details', it shows 'Type: SaaS & APIs', 'Last updated: 3/18/21', 'Category: Google Workspace', and 'Service name: admin.googleapis.com'.

17. Navigate to **APIs & Services > OAuth consent screen**. In **User Type**, select **Internal** and click **Create**.



Google Cloud Platform SKOUT-2 Search products and resources

**API** APIs & Services

- Dashboard
- Library
- Credentials
- OAuth consent screen**
- Domain verification
- Page usage agreements

### OAuth consent screen

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

#### User Type

☒ **Internal** ?

Only available to users within your organization. You will not need to submit your app for verification. [Learn more](#)

☐ **External** ?

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more](#)

[CREATE](#)

[Let us know what you think](#) about our OAuth experience

18. Enter an appropriate application name, such as `skt-gcp-monitor` . Enter the **User support email** and, in the **Developer contact information** section, type the **Email address** of any admin user. Slick **Save And Continue**.

Google Cloud Platform

SKOUT-2

Search products and resources

Navigation menu

Services

Dashboard

Library

Credentials

**OAuth consent screen**

Domain verification

Page usage agreements

Edit app registration

1 OAuth consent screen

2 Scopes

3 Summary

App information

This shows in the consent screen, and helps end users know who you are and contact you

App name \*

skt2-gcp-monitor

The name of the app asking for consent

User support email \*

cjw@cjwcyber.com

For users to contact you with questions about their consent

App logo

BROWSE

Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

App domain

To protect you and your users, Google only allows apps using OAuth to use Authorized Domains. The following information will be shown to your users on the consent screen.

Application home page

Provide users a link to your home page

Application privacy policy link

Provide users a link to your public privacy policy

Application terms of service link

Provide users a link to your public terms of service

Authorized domains ?

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the [Google Search Console](#) to check if your domains are authorized. [Learn more](#) about the authorized domain limit.

+ ADD DOMAIN

Developer contact information

Email addresses \*

cjw@cjwcyber.com

These email addresses are for Google to notify you about any changes to your project.

SAVE AND CONTINUE

CANCEL

19. On the **Scopes** page, click **Add or Remove Scopes**. Search for <https://www.googleapis.com/auth/admin.reports.audit.readonly> and add it. Click **Update** > **Save & Continue**.



Google Cloud Platform

SKOUT-2

Search products and resources

APIs & Services

Dashboard

Library

Credentials

OAuth consent screen

Domain verification

Page usage agreements

Edit app registration

OAuth consent screen

Scopes

Summary

Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. [Learn more](#)

ADD OR REMOVE SCOPES

Your non-sensitive scopes

API	Scope	User-facing description
No rows to display		

Your sensitive scopes

Sensitive scopes are scopes that request access to private user data.

API	Scope	User-facing description
Admin	.../auth/admin	View audit reports for your
SDK API	.reports.audit	G Suite domain
	.readonly	

Your restricted scopes

Restricted scopes are scopes that request access to highly sensitive user data.

API	Scope	User-facing description
No rows to display		

SAVE AND CONTINUE

CANCEL

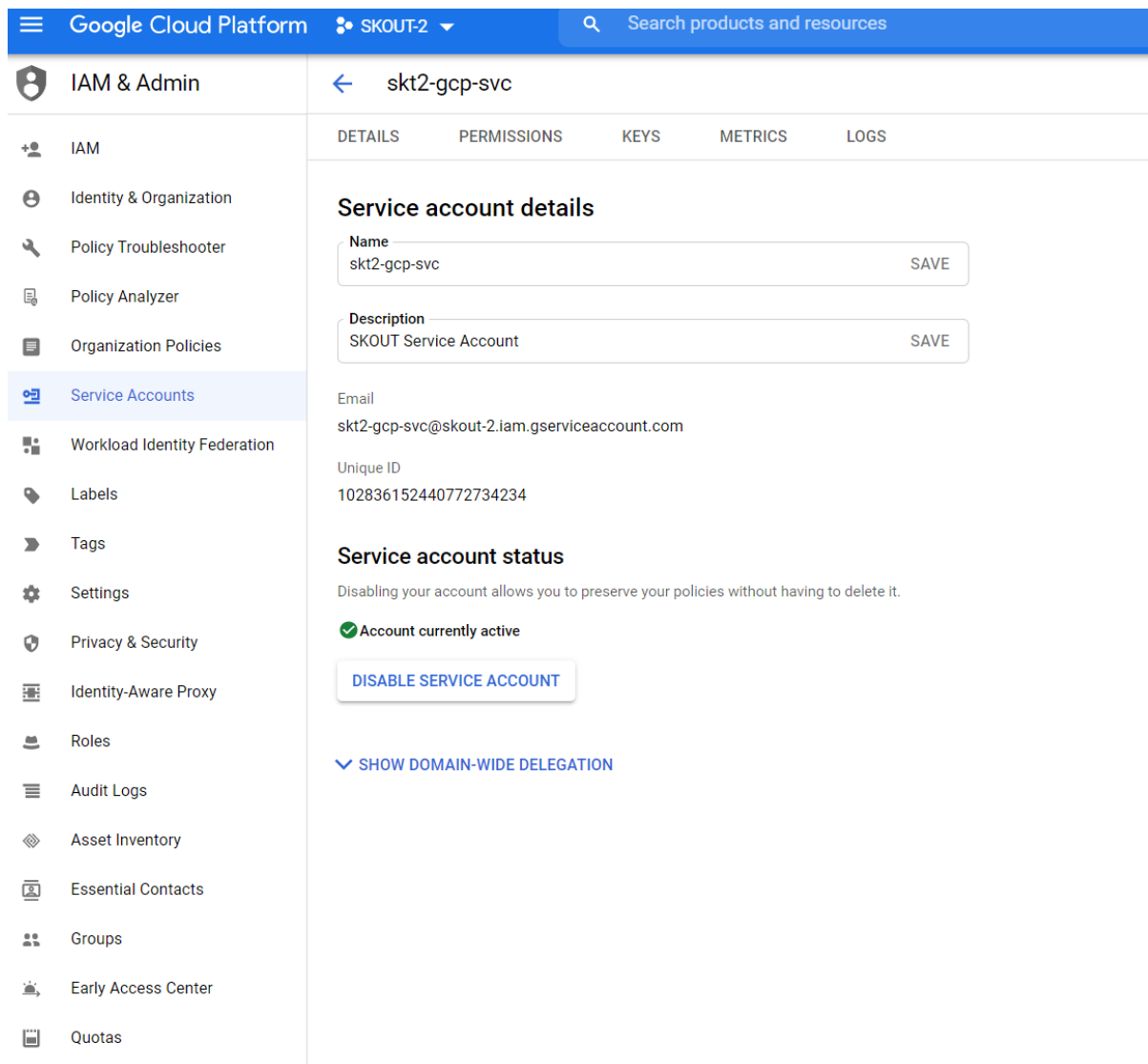
20. On the left navigation bar, click **Credentials**.

21. Click the associated Service account in the **Service Accounts** Table.

22. Click **Show Advanced Settings**.

Integrating Google Workspace

9 / 12

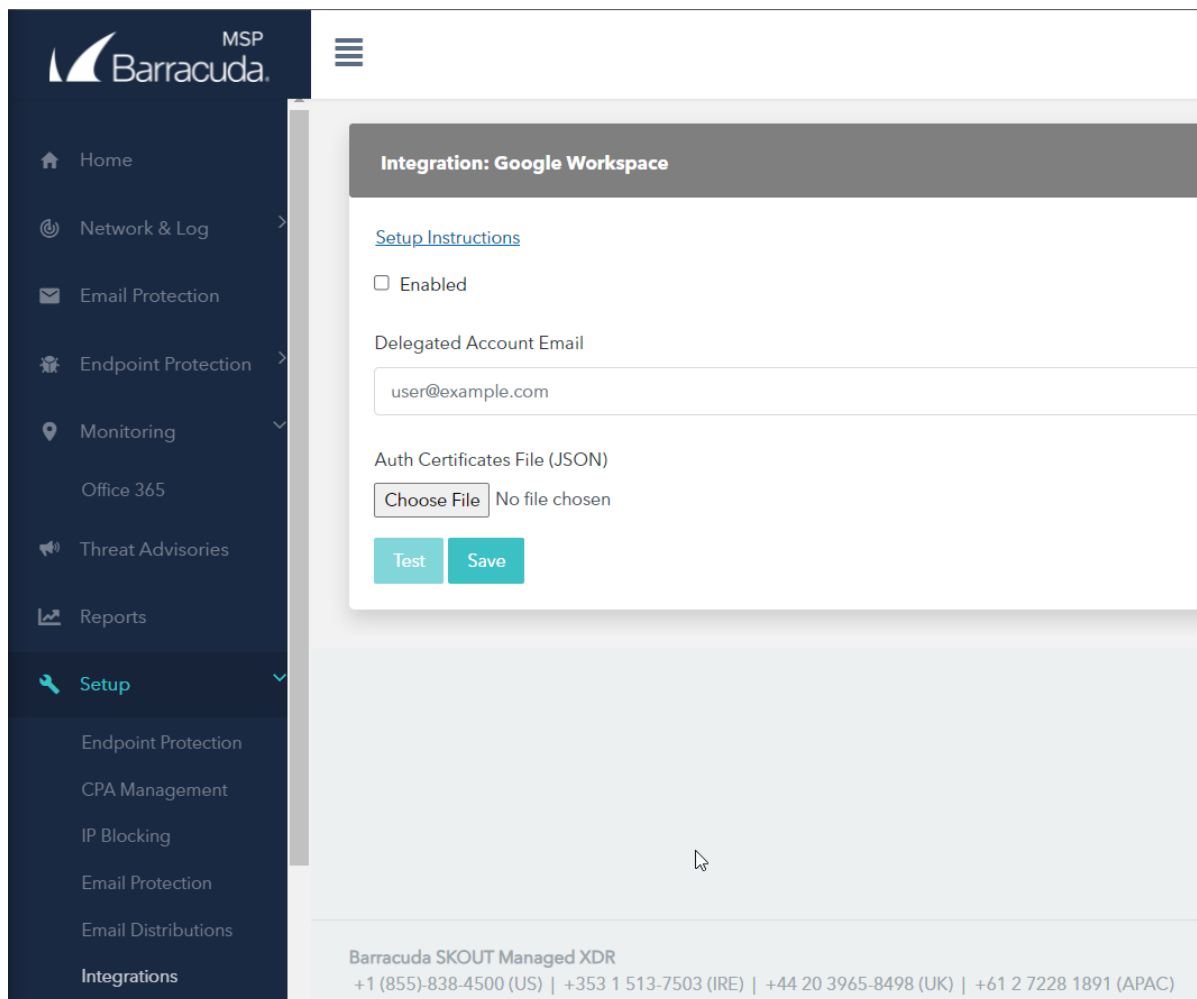


The screenshot shows the Google Cloud Platform IAM & Admin console. The left sidebar lists various IAM & Admin tools, with 'Service Accounts' selected. The main content area shows the details for the 'skt2-gcp-svc' service account. The 'Service account details' section includes fields for 'Name' (skt2-gcp-svc) and 'Description' (SKOUT Service Account), both with 'SAVE' buttons. Below this, the 'Email' is listed as 'skt2-gcp-svc@skout-2.iam.gserviceaccount.com' and the 'Unique ID' is '102836152440772734234'. The 'Service account status' section indicates the account is 'currently active' and provides a 'DISABLE SERVICE ACCOUNT' button. At the bottom, there is a link to 'SHOW DOMAIN-WIDE DELEGATION'.

23. On the **Service Account** page, in the **Domain-wide Delegation** section, copy the **Client ID**.
24. Navigate to [Domain-wide Delegation \(google.com\)](https://domain-wide-delegation.google.com). Click **Add New** and paste the **Client ID** you just copied into its associated field.
25. Add <https://www.googleapis.com/auth/admin.reports.audit.readonly> into **OAuth Scopes** and click **Authorize**.

## To set up Barracuda XDR Dashboard

1. In **Barracuda XDR Dashboard**, click **Administration > Integrations**
2. On the **Google Workspace** card, click **Setup**.
3. Add the Credentials .JSON file that was generated/downloaded earlier, and the email for the user you granted the sufficient privileges.



The screenshot displays the Barracuda XDR MSP dashboard. On the left is a dark blue sidebar with the Barracuda logo and 'MSP' label. The sidebar menu includes: Home, Network & Log, Email Protection, Endpoint Protection, Monitoring, Office 365, Threat Advisories, Reports, Setup (highlighted with a green checkmark), and Integrations. The 'Setup' menu is expanded, showing sub-items: Endpoint Protection, CPA Management, IP Blocking, Email Protection, Email Distributions, and Integrations. The main content area is titled 'Integration: Google Workspace'. It contains a link for 'Setup Instructions', an 'Enabled' checkbox, a 'Delegated Account Email' field with the value 'user@example.com', an 'Auth Certificates File (JSON)' section with a 'Choose File' button and the text 'No file chosen', and two teal buttons labeled 'Test' and 'Save'. At the bottom of the page, there is a footer for 'Barracuda SKOUT Managed XDR' with contact numbers for US, IRE, UK, and APAC regions.

4. Click **Test** and **Save**.

## Figures

1. 1.png
2. 2.png
3. 3.png
4. 5.png
5. 6.png
6. 7.png
7. 8.png
8. 10.png
9. 12.png
10. 13.png
11. 14.png
12. 15.png
13. 16.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.