

Google

Introduction

Integration with Google services

Service Account credentials: Prerequisites

Step 1. Google Project for Sense integrations

Step 2. Enable the Identity and Access Management (IAM) API

Step 3. Service account

Step 4. Service account Private Key file

Step 5. Enable the IAM Service Account Credentials API

Step 6. Enable APIs, required for the calls from workflows

Step 7. Configure scopes for the service account

References

Related stories:

Introduction

The introduction of the [Service Connections](#) feature within our [Automations](#) Product (aka [workflows](#)) marks a significant advancement in facilitating real-time synchronization between HR events and external services, such as [Google Calendar](#), among others. By bridging this gap, we aim to unlock a wide array of new scenarios for our clients, enhancing the potential of our product.

Integration with Google services

Our initial integration focuses on Google services, including a suite of tools like [Google Calendar](#), [Google Forms](#), and [Google Docs](#). This integration plays a crucial role in enabling seamless communication between our platform and 3rd party services.

The integration with Google APIs operates at a low level, requiring the workflow designer to manually define calls to the Google API using HTTP requests and responses. While this may seem intricate, comprehensive documentation provided by [Google APIs Explorer](#) ([Google APIs Explorer | Google for Developers](#)) serves as a valuable resource for this purpose.

It's essential to note that currently, our platform [does not offer pre-built workflow activities](#) to streamline communication with the Google API. For instance, adding an event to Google Calendar requires an HTTP call to the Google API with the help of [Google / API Request](#) activity (there is no [Google / Calendar API - add event](#) activity). However, we have implemented a mechanism that smoothly handles authentication for these calls, easing the burden on users.

Google supports various authentication methods, one of which is the "Service Account credentials" ([Service account credentials | IAM Documentation | Google Cloud](#)). Service accounts are specialized accounts primarily utilized by applications rather than individual users, offering a secure means of authentication within our integration framework.

Service Account credentials: Prerequisites

Before registering a new Google Service Connection within the system, a series of preliminary actions must be undertaken. These steps are conducted within the client's Google Cloud environment and necessitate an individual with administrative permissions to execute them effectively.

Step 1. Google Project for Sense integrations

Create a project to group resources together within an organization.

Service account that will be created in the next steps have to be created in the context of a project.

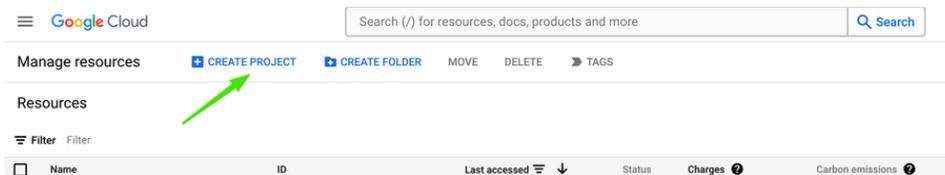
 Project Creator role is required to create a project

 Create a project | [Google Distributed Cloud Hosted](#) | [Google Cloud](#)

Steps

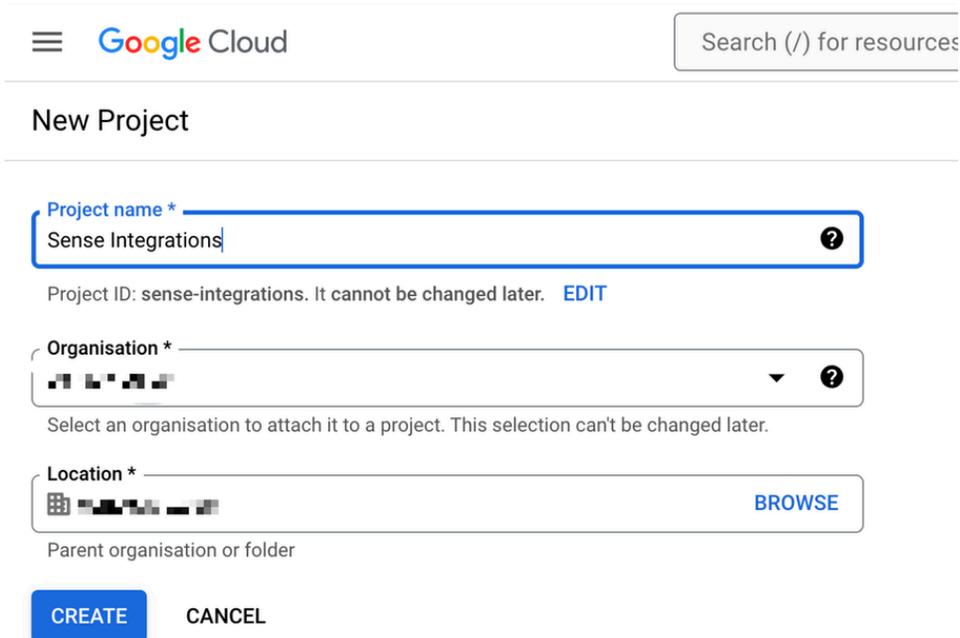
1. Go to Resource Manager

[Manage resources – Google Cloud console](#)



2. Press the `Create Project` button

3. Give it a name, e.g. `Sense integrations`



Step 2. Enable the Identity and Access Management (IAM) API

Manages identity and access control for Google Cloud resources, including the creation of service accounts, which you can use to authenticate to Google and make API calls.

Steps

1. Go to "APIs and Services" page

<https://console.cloud.google.com/apis/dashboard>

1. Check the project

2. Enable API

Name	Requests	Errors (%)	Latency, median (ms)	Latency, 95% (ms)
	1	0	393	511

2. Ensure that the right project (Sense Integrations) is selected.
3. Press the + Enable APIs and services link
4. Find and click on the API called Identity and Access Management (IAM) API

Product details

Identity and Access Management (IAM) API

Google Enterprise API

Manages identity and access control for Google Cloud resources, including the creation of service...

MANAGE TRY THIS API API Enabled

OVERVIEW DOCUMENTATION RELATED PRODUCTS

Overview

Manages identity and access control for Google Cloud resources, including the creation of service accounts, which you can use to authenticate to Google and make API calls. Enabling this API also enables the IAM Service Account Credentials API (iamcredentials.googleapis.com). However, disabling this API doesn't disable the IAM Service Account Credentials API.

Tutorials and documentation

[Learn more](#)

Additional details

Type: [SaaS & APIs](#)
 Last product update: 27/02/2024
 Category: [Google Enterprise APIs](#)
 Service name: iam.googleapis.com

5. Press the Enable button

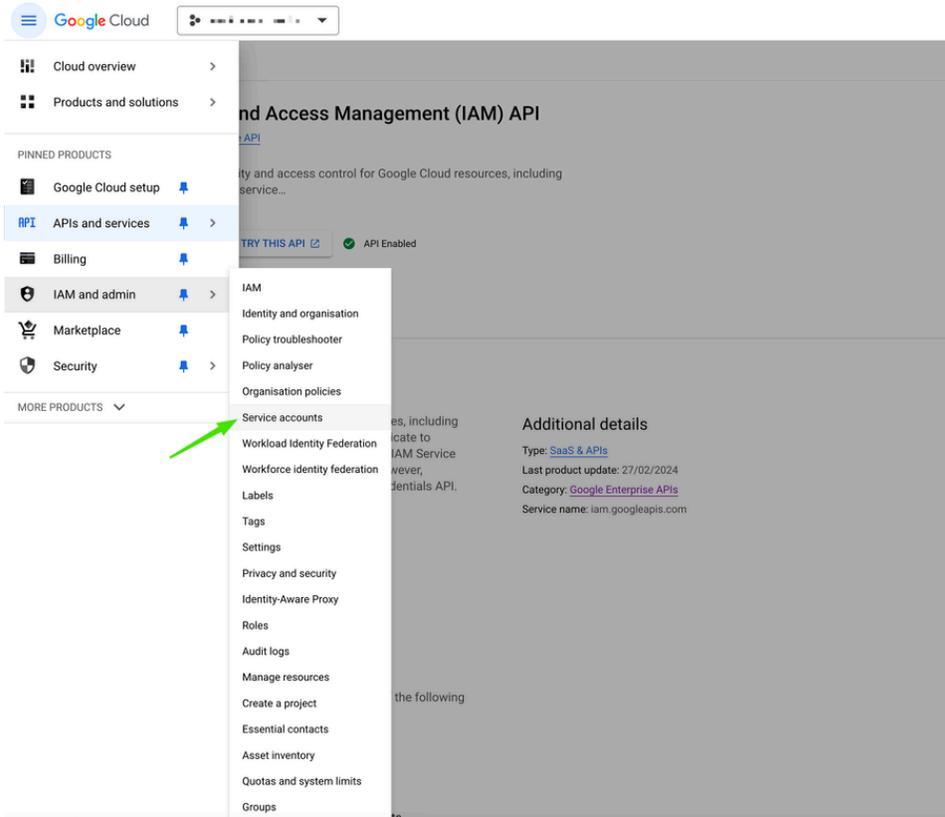
Step 3. Service account

Create a service account.

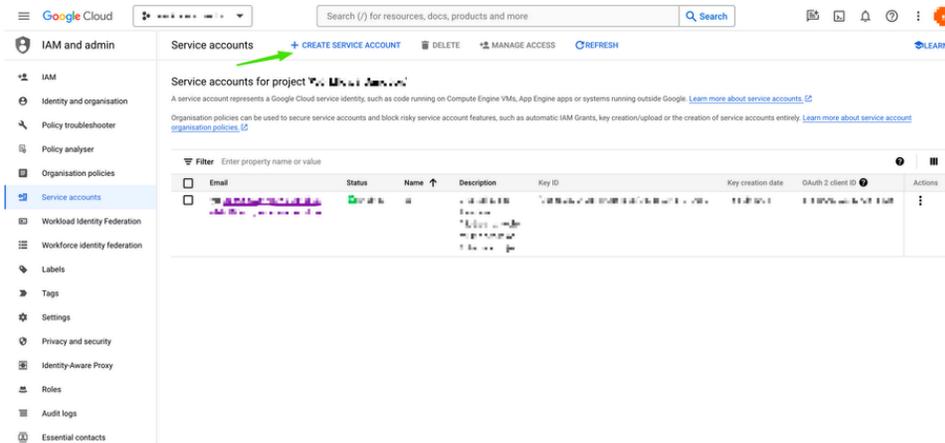
[Create service accounts](#) | [IAM Documentation](#) | [Google Cloud](#).

Steps

1. Go to menu → IAM and admin → Service accounts



2. Press the **+ Create Service Account** button



3. Give it a name, e.g. **Service Account for Sense** , Press **Done**

Google Cloud Search (/) for resources, docs, products and more

IAM and admin

- IAM
- Identity and organisation
- Policy troubleshooter
- Policy analyser
- Organisation policies
- Service accounts**
- Workload Identity Federation
- Workforce identity federation
- Labels
- Tags
- Settings
- Privacy and security
- Identity-Aware Proxy
- Roles
- Audit logs
- Essential contacts

1 Service account details

Service account name
Service Account for Sense

Display name for this service account

Service account ID *
service-account-for-sense

Email address: service-account-for-sense@414210.iam.gserviceaccount.com

Service account description

Describe what this service account will do

CREATE AND CONTINUE

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

3 Grant users access to this service account (optional)

DONE CANCEL

Step 4. Service account Private Key file

Steps

1. Go to the service account → **Keys** tab. Press the **Add key** → **Create new key**

Google Cloud Search (/) for resources, docs, products and more

IAM and admin

- IAM
- Identity and organisation
- Policy troubleshooter
- Policy analyser
- Organisation policies
- Service accounts**
- Workload Identity Federation
- Workforce identity federation
- Labels
- Tags
- Settings

DETAILS PERMISSIONS **KEYS** METRICS LOGS

Keys

Service account keys could pose a security risk if compromised. We recommend that you avoid downloading service account keys and instead use the [Workload Identity Federation](#) 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 [organisation policies](#).

[Learn more about setting organisation policies for service accounts](#)

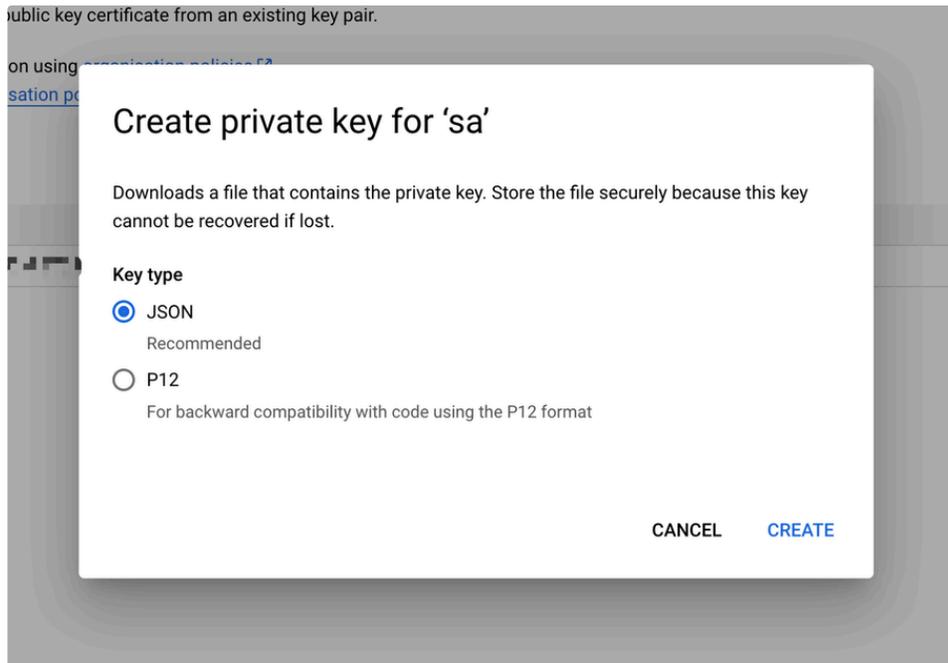
ADD KEY ▾

Create new key

Upload existing key

Key	Key creation date	Key expiry date

2. Choose **JSON** format



⚠ Service account keys are a security risk if not managed correctly. The file have to be deleted immediately after it is uploaded to Sense Automate.

Step 5. Enable the IAM Service Account Credentials API

Creates short-lived credentials for impersonating IAM service accounts.

Steps

1. Go to "APIs and Services" page

<https://console.cloud.google.com/apis/dashboard>

Google Cloud

Search (f) for resources, docs, products and more

APIs and Services

ENABLE APIS AND SERVICES

1. Check the project

2. Enable API

Traffic

Errors

Median latency

Name	Requests	Errors (%)	Latency, median (ms)	Latency, 95% (ms)
	1	0	393	511

2. Ensure that the right project (Sense Integrations) is selected.
3. Press the + Enable APIs and services link
4. Find and click on the API called IAM Service Account Credentials API

Google Cloud

Product details

IAM Service Account Credentials API

Google Enterprise API

MANAGE TRY THIS API API Enabled

OVERVIEW DOCUMENTATION RELATED PRODUCTS

Overview

Service Account Credentials API allows developers to create short-lived, limited-privilege credentials for their service accounts on GCP.

Additional details

Type: [SaaS & APIs](#)
 Last product update: 30/04/2022
 Category: [Google Enterprise APIs](#)
 Service name: iamcredentials.googleapis.com

Tutorials and documentation

[Learn more](#)

Terms of Service

By using this product, you agree to the terms and conditions of the following licence: [Google Cloud Platform](#).

5. Press the **Enable** button

Step 6. Enable APIs, required for the calls from workflows

Steps

1. Go to "APIs and Services" page

<https://console.cloud.google.com/apis/dashboard>

1. Check the project

2. Enable API

Name	Requests	Errors (%)	Latency, median (ms)	Latency, 95% (ms)
	1	0	393	511

2. Ensure that the right project (**Sense Integrations**) is selected.

3. Press the **+ Enable APIs and services** link

4. Find the required API

5. Press the **Enable** button

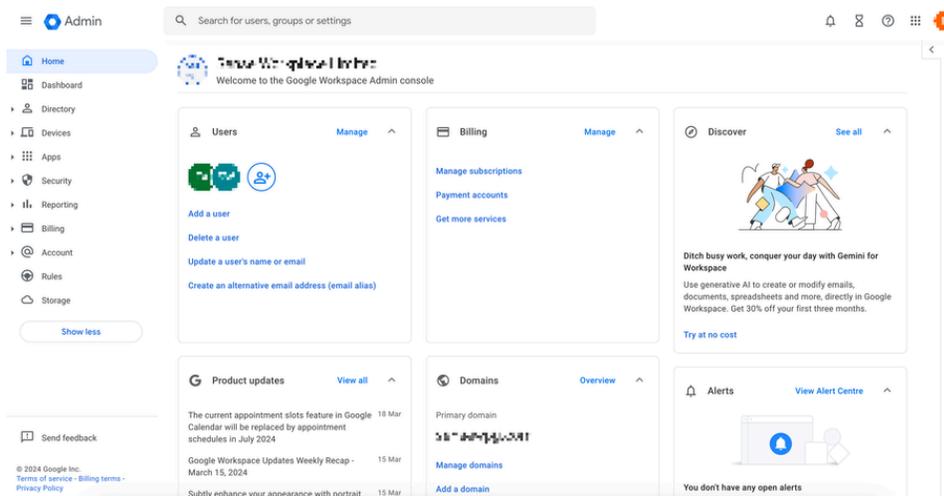
Step 7. Configure scopes for the service account

Workspace administrator of the organization need to authorize the service account to access Workspace user data on behalf of users in the Google Workspace domain.

Steps

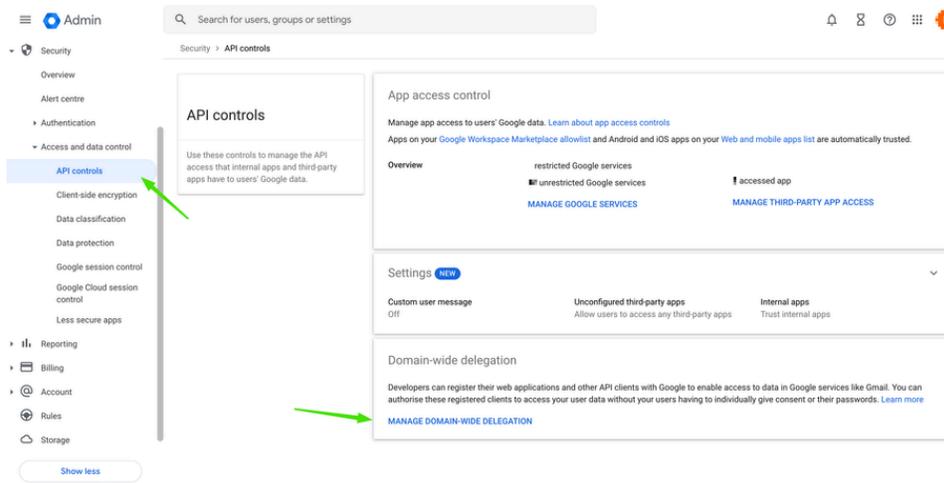
1. Go to Google Workspace domain's Admin console

[Admin console \(google.com\)](https://admin.google.com)



2. Go to Menu > Security → Access and data control → API Controls

3. Select Manage Domain-wide delegation [Domain-wide delegation \(google.com\)](https://admin.google.com)



4. Click Add new

5. In the Client ID field, enter the service account's Client ID. You can find your service account's client ID in the ****Service accounts**** page.

6. In the OAuth scopes (comma-delimited) field, enter the list of scopes that your application should be granted access to. For example, if your application needs domain-wide full access to the Google Drive API and the Google Calendar API, enter: `https://www.googleapis.com/auth/drive, <https://www.googleapis.com/auth/calendar >`

7. Click Authorize

References

- APIs Documentation
 - [Google APIs Explorer | Google for Developers](#)
- About Service accounts
 - [Service account credentials | IAM Documentation | Google Cloud](#)

Related stories:

- [ENG-4627: Ability to capture credentials for Google calendar integration](#) READY FOR QA
- [ENG-4628: Activity to make API calls to Google Calendar](#) READY FOR QA