Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Kdo Cy / CEA
CoE Software Engineering

Google Service Account Setup

Version 1.0.0-2-g24d61c2, 16.11.2026

Table of Contents

1. Create the service account in the project **2**
2. Set up domain-wide delegation in the Google Admin Console **2**

The automation in this repository authenticates against the Google Workspace Admin SDK as a service account with domain-wide delegation. This document records how that service account is created and authorized.

1. Create the service account in the project

```
# Login
gcloud auth login

# Get user id
USER_ID="$(gcloud auth list --format 'value(ACCOUNT)')"

# Get organization id
ORGANIZATION_ID="$(gcloud organizations list --format
'value(ID)')"

# Make user policy admin for organization
gcloud organizations \
  add-iam-policy-binding \
  "${ORGANIZATION_ID}" \
  --member="user:${USER_ID}" \
  --role="roles/orgpolicy.policyAdmin"

# Define name of new project
PROJECT_ID="name-of-project"

# Create project and select it
gcloud projects create "${PROJECT_ID}"
gcloud config set project "${PROJECT_ID}"

# Enable service account key creation policy on project
gcloud resource-manager org-policies disable-enforce \
  constraints/iam.disableServiceAccountKeyCreation \
  --project="${PROJECT_ID}"

# Define service account name
SERVICE_ACCOUNT="service-account-for-admin-api"

# Create service account
gcloud iam service-accounts create "${SERVICE_ACCOUNT}" \
  --display-name="${SERVICE_ACCOUNT}"

# Create service account key
gcloud iam service-accounts keys create service-account-key.json \
  --iam
-account=${SERVICE_ACCOUNT}@${PROJECT_ID}.iam.gserviceaccount.com

# print the client ID, will be needed later
gcloud iam service-accounts describe
${SERVICE_ACCOUNT}@${PROJECT_ID}.iam.gserviceaccount.com \
  --format="value(uniqueId, email)"
```

2. Set up domain-wide delegation in the Google Admin Console

1. Enable domain-wide delegation in the Google Admin Console:

   ```
   Security > Access and data control > API controls > Manage
   domain wide delegation > Add new
   ```

   Set the client ID to the unique ID from the previous step and add this scope:

`https://www.googleapis.com/auth/admin.directory.user`

2. Assign the administrative role:

   `Account > Admin roles > User Management Admin (hover) > Assign admin > Assign service accounts`

   Enter the email address from the previous step, then click `Assign role`.