Automatically fetch user accounts (Google IAM)

STEP 1: Enable APIs

You'll need access to one of the following APIs:

- **Cloud Identity API** (for non-Google Workspace orgs)
- **Admin SDK API** (for Google Workspace)

How to Enable:

1. Go to Google Cloud Console
2. Navigate to: APIs & Services > Library
3. Search for:
   - Cloud Identity AP
   - Admin SDK API
4. Click **Enable**

STEP 2: Set Up a Service Account

1. In the Cloud Console, go to : IAM & Admin > Service Accounts
2. Click **Create Service Account**
3. Name it and click **Create and Continue**
4. Assign roles:
   - For Cloud Identity: Cloud Identity User Read
   - For Admin SDK: Viewer or User Management Admin

STEP 3: Create and Download Credentials

1. Go back to your service account.
2. Under the **Keys** tab, click **Add Key > JSON**
3. Save the .json file securely — this will be used to authenticate API requests.

STEP 4: Grant Domain-Wide Delegation (if using Admin SDK)

This allows your service account to impersonate an admin.

1. In the Service Account settings, enable **“Enable G Suite Domain-wide Delegation”**
2. Go to your Google Admin console
3. Add a new client: Security > API Controls > Domain-wide Delegation
   - **Client ID:** from your service account JSON

STEP 5: Fetch User Accounts Pro-grammatically

Use Python and google-auth + google-api-python-client.

STEP 6: Automate the Process

- Schedule the script to run via:
  - **Cloud Scheduler** (GCP-native)
  - **Cron job** (Linux VM)
  - **Cloud Functions / Cloud Run** (for serverless)

STEP 7: Send or Sync Data

Once you fetch users:

- You can store them in:
  - Elasticsearch

Revision #2
Created 18 June 2025 09:06:01
Updated 18 June 2025 09:23:59