Google Cloud Provisioning Configuration Guide

Last modified on October 19, 2022

This guide explains how to configure Google Cloud as an identity provider (IdP) for user and group provisioning purposes. This guide describes how to create a Google Cloud service account and how to set up the StrongDM Admin UI for provisioning.

Prerequisites

- You must have a Google super administrator account to complete the service account configuration.
- You must be familiar with Google group creation.

Create a Service Account

Follow the steps in this section to create a service account. The service account is used to connect to StrongDM. See additional steps in Google documentation.

Create a project

In the Google Cloud console, create a new project. After the project is created, make sure to select your project from the **Select from** dropdown list on the Dashboard page.

Activate Admin SDK API access

1. In the Google Cloud console, go to **Menu > APIs and Services > Library**.
2. Search the API library for and select the **Admin SDK API**.
3. Enable the API for your project.

Create a new service account

1. In the Google Cloud console, go to **Menu > APIs and Services > OAuth consent screen**.
2. Select the **Internal** user type and click **Create**.
3. Configure the remaining OAuth consent screen information, fill out all mandatory fields, and return to the dashboard.
4. From the **APIs and Services menu**, select **Credentials**.
5. Click **Create credentials** and select **Service account**.
6. Fill out the service account details
7. Select the service account's email address to configure the service account details. The user you are logged in as is the owner of the service account.
8. From the **Keys** tab, add and then create a new JSON key; the key downloads to your computer. You may rename the key for easier identification.
9. From the **Details** tab, copy the **Unique ID**; you use this in the following step.

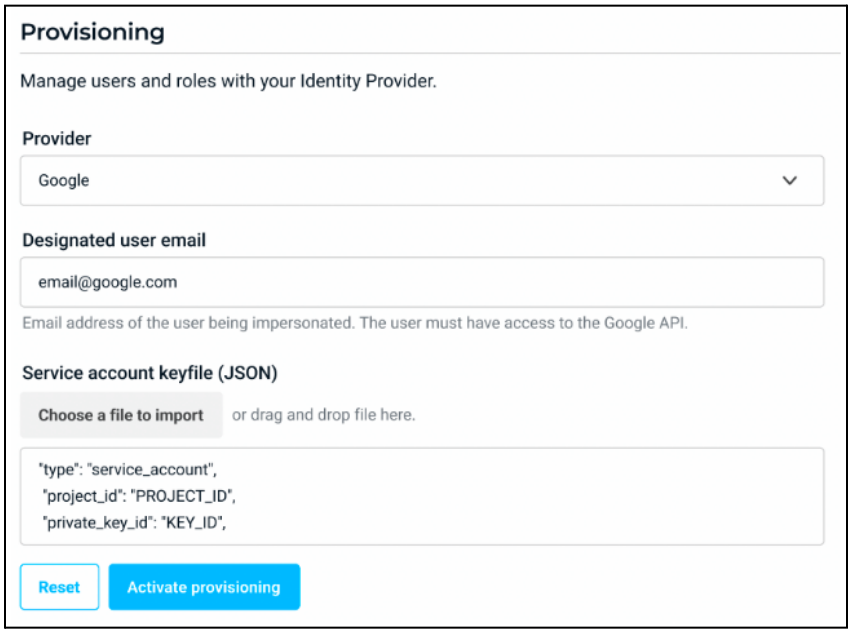
Enable domain delegation

1. Navigate to admin.google.com.
2. Go to **Menu > Security > Access and data control > API Controls**.
3. Select **Manage Domain Wide Delegation**.
4. Click **Add new** and paste the **Unique ID** in the **Client ID** field.
5. In the **OAuth Scopes** fields, enter and authorize the following scopes:

   https://www.googleapis.com/auth/admin.directory.user.readonly
   https://www.googleapis.com/auth/admin.directory.group.readonly
   https://www.googleapis.com/auth/admin.directory.group.member.readonly

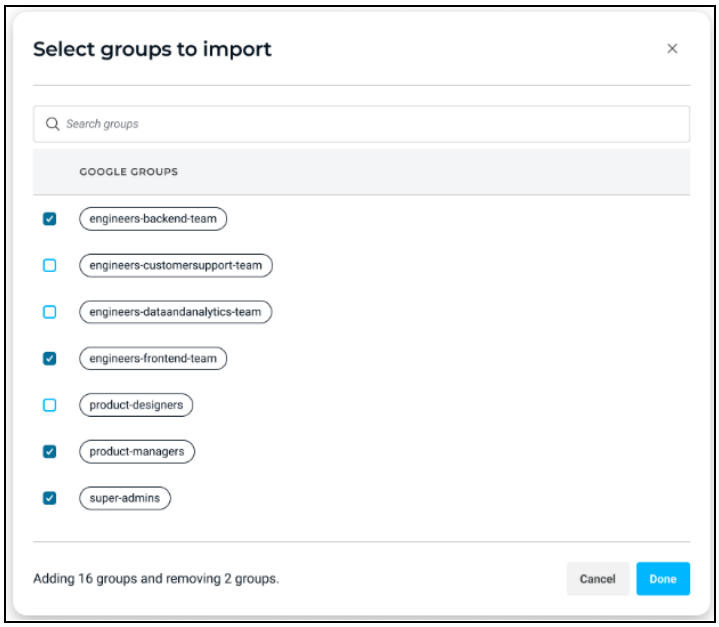
Configure Provisioning in the Admin UI

1. Log in to the StrongDM Admin UI.
2. Go to **Settings > User Management**.
3. Under Provisioning, select **Google** from the **Provider** dropdown.
4. Enter the **Designated user email**. This email address must have appropriate API resource access.
5. Import or manually enter the **Service account keyfile (JSON)**; this is the service account JSON file that downloaded.
6. Click **Activate** provisioning.



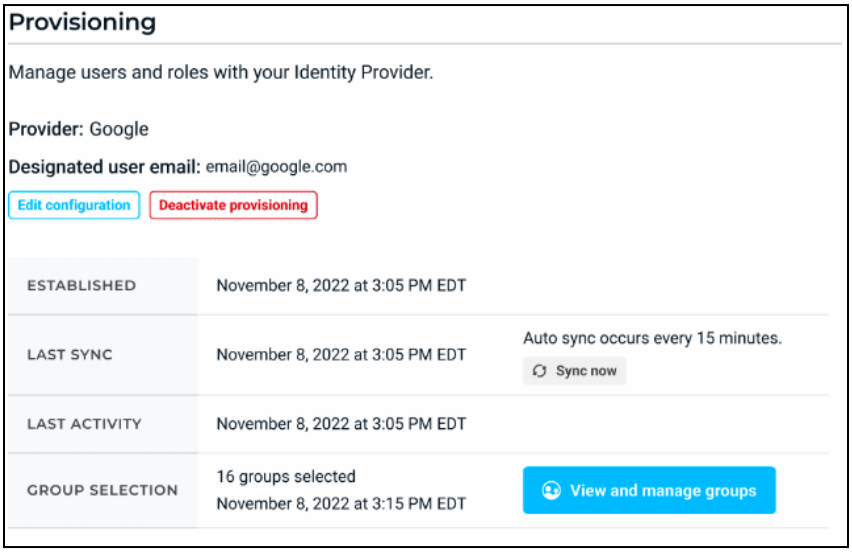
Google Group Provisioning

7. Select groups to import. Information about group creation and management is available in Google documentation.



Select Groups for Google Cloud Provisioning

8. When you are finished, you may view, manage, and sync groups. Note the following properties:
    - **Established**: When provisioning was activated
    - **Last Sync**: Last time the sync ran to check for changes in Google Cloud
    - **Last Activity**: Last time changes were found in Google Cloud and applied in StrongDM
    - **Group Selection**: Number of groups currently selected and the last time groups were selected



Sync Groups for Google Cloud Provisioning as Needed

If you deactivate Google Cloud provisioning and later reactivate it, groups must be reselected.

Troubleshooting and Tips

Due to the nature of how Google user and group provisioning works, there are a few limitations and usage tips to be aware of.

Sync errors and solutions

The following errors may be experienced when **Sync now** is selected; they are expected behaviors.

- A user email that is set up for Google provisioning exists in a separate StrongDM organization.
    - Recommended solution: A user email that exists in one StrongDM organization may not be provisioned into another StrongDM organization. If you do not have access to the incorrect organization, you must contact support@strongdm.com to remove the email address from it. We recommend using different Google workspaces to provision multiple organizations within StrongDM.
- A Google user email is changed to match an existing StrongDM user email.
    - Recommended solution: Keep each user email unique between StrongDM and Google. If you want to provision a new user from Google that already exists in StrongDM, the Google user takes ownership of the existing StrongDM user (that is, manages it and adds additional Google-specific information).
- A Google user group is updated to match an existing role in StrongDM.
    - Recommended solution: Keep each group/role name unique between StrongDM and Google. If you want to provision a new group/role from Google that already exists in StrongDM, the Google group takes ownership of the existing StrongDM role (that is, manages it and adds additional Google-specific information).

If you have any issues with your implementation, please contact support@strongdm.com.