Directory Password Synchronization with G Suite Configuration Guide

Introduction

Use this guide to enable directory (AD, SQL, Oracle, etc.) to G Suite (formerly Google Apps) password synchronization via SecureAuth IdP.

This enables users' passwords to change in both the directory and G Suite once modified in one location.

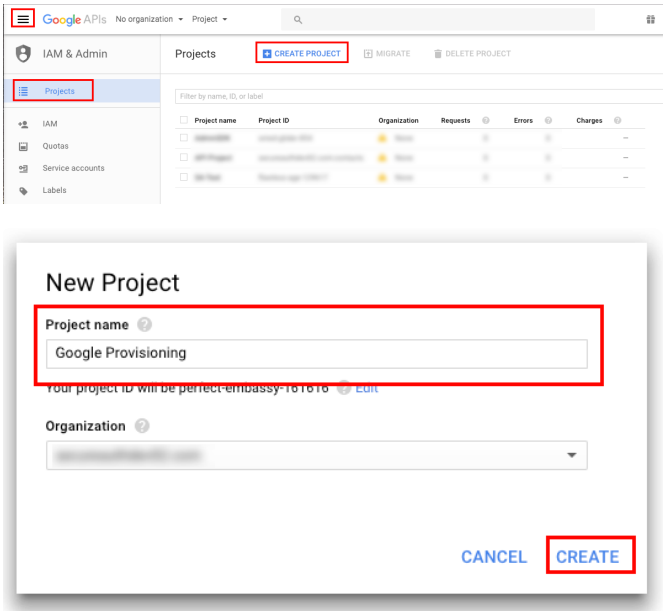
Prerequisites

1. Create a **Service Account** with G Suite
2. Delegate **domain-wide authority** to the G Suite Service Account
3. Have a directory **Service Account** with **read and write** access for SecureAuth IdP
4. Have an Active Directory field to which SecureAuth IdP can map a **Profile Property**

    For other data stores, the field mapping will need to be configured through the directory

G Suite API Configuration Steps

Create Project

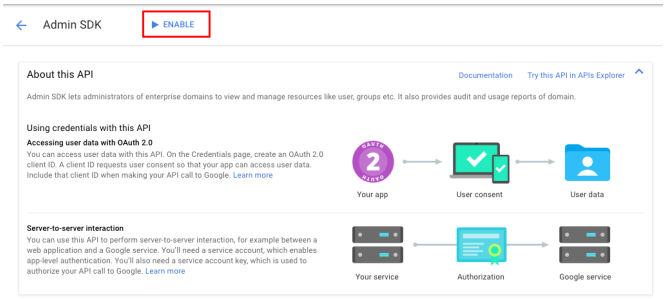


1. Log into the **Google Developers' Console** , and navigate to **IAM & Admin > Projects** from the three bars menu
2. Select **Create Project**

    These steps can also be completed by opening the **Projects** dropdown menu at the top, and selecting **Create project**

3. Provide a **Project Name**, and select an **Organization** if the project is not already being created within one
4. Click **Create**

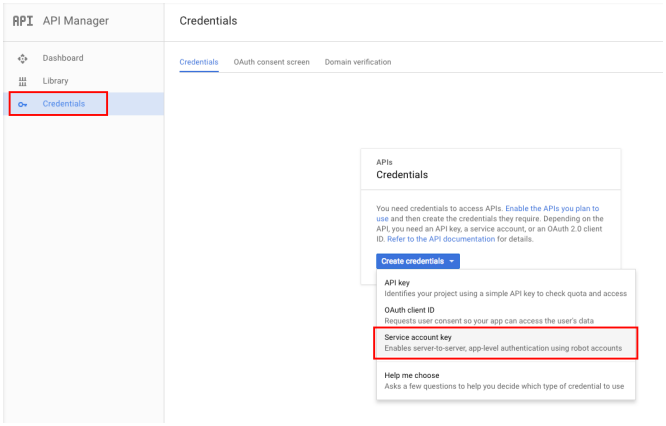
Enable Admin SDK



5. In the **Libraries** section, search for **Admin SDK**, and select the option

6. On the **Admin SDK** page, click **Enable**

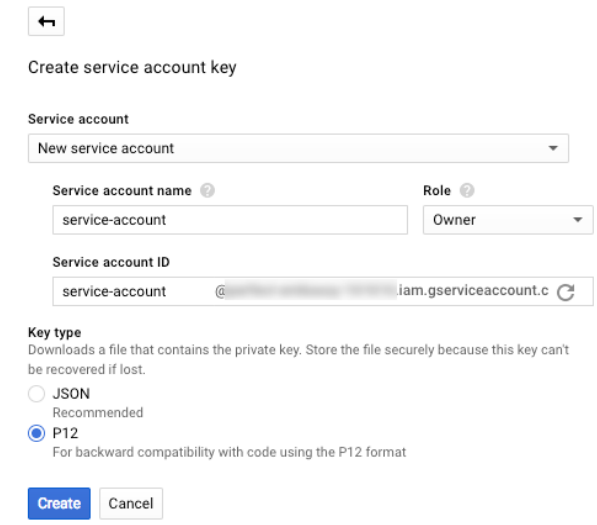
Create Service Account



7. On the **API Manager** page (accessible via the three bars menu), navigate to the **Credentials** section, and click **Create Credentials**

8. Select **Service Account Key**

Create Service Account Key

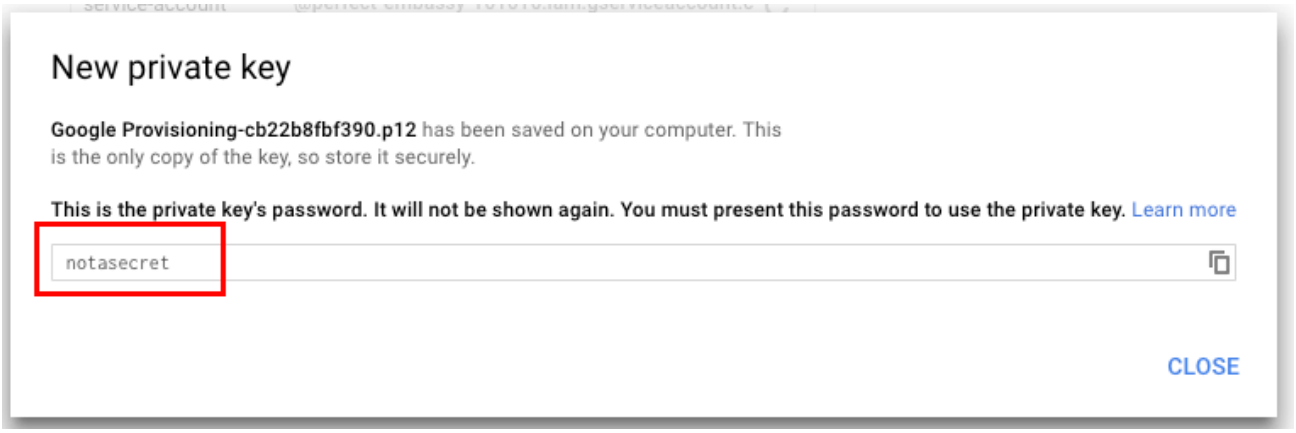


9. Select **New service account** from the **Service Account** dropdown, and provide a **Service Account Name**

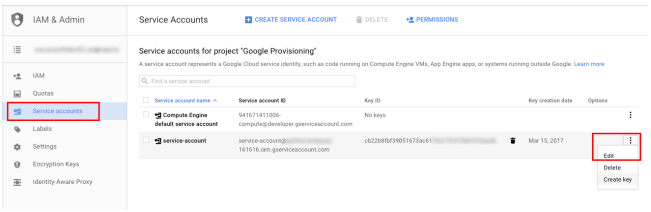
10. Select **Project > Owner** from the **Role** dropdown

11. Select **P12**, and click **Create**

12. Save the p12 file that downloads, which is uploaded to the SecureAuth appliance (see steps below), note the **Private Key Password**, and click **Close**



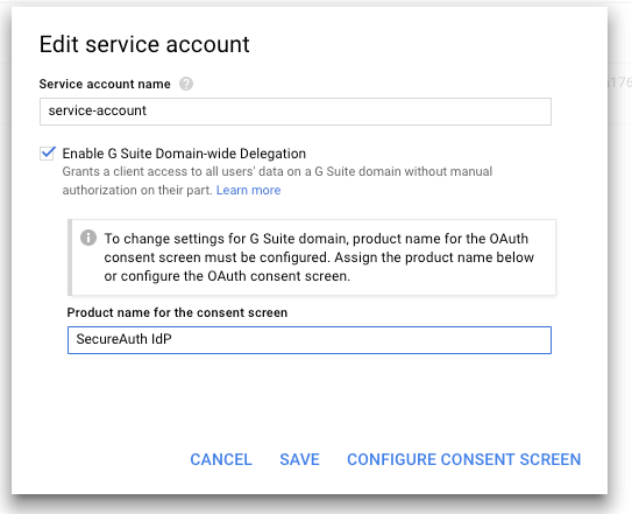
Manage Service Account



13. On the **Credentials** page, click **Manage Service Accounts**

14. Click the three dots on the newly-created service account, and select **Edit**

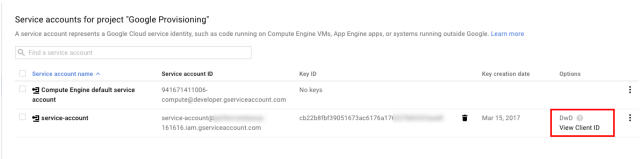
Edit Service Account



15. Check **Enable G Suite Domain-wide Delegation** and provide a **Product name for the consent screen**

16. Click **Save**

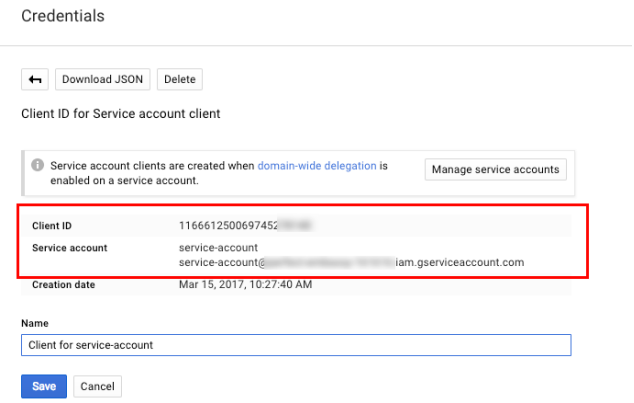
Click **Configure Consent Screen** to set additional (optional) preferences for the consent page; or access the configuration at **API Manager > Credentials > OAuth Consent Screen**



Back on the **Service Accounts** page, a new **DwD** section appears for the service account

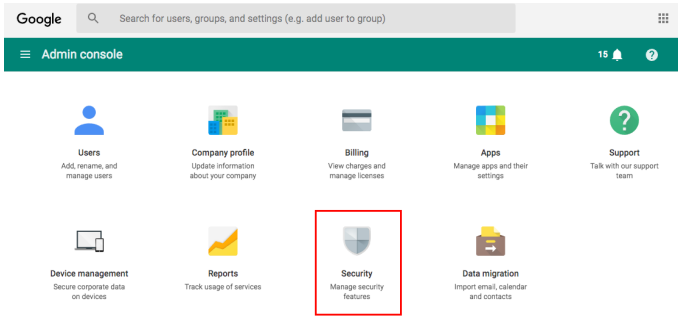
17. Click **View Client ID**

Credentials



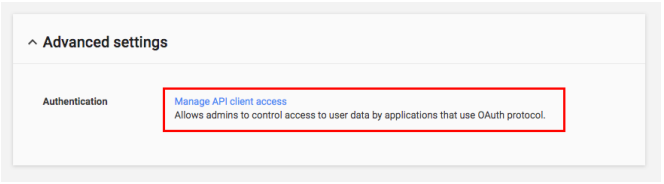
18. Note the **Client ID**, which is used in the G Suite Administrative Configuration Steps (below), and the **Service Account** email address, which is used in the SecureAuth IdP Configuration Steps (below)

G Suite Administration Configuration Steps



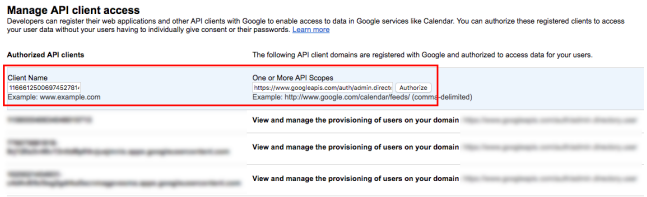
19. Log into the **G Suite Administrative Console** and select **Security**

Security - Advanced Settings



20. Under **Advanced Settings**, select **Manage API Client Access**

Manage API Client Access

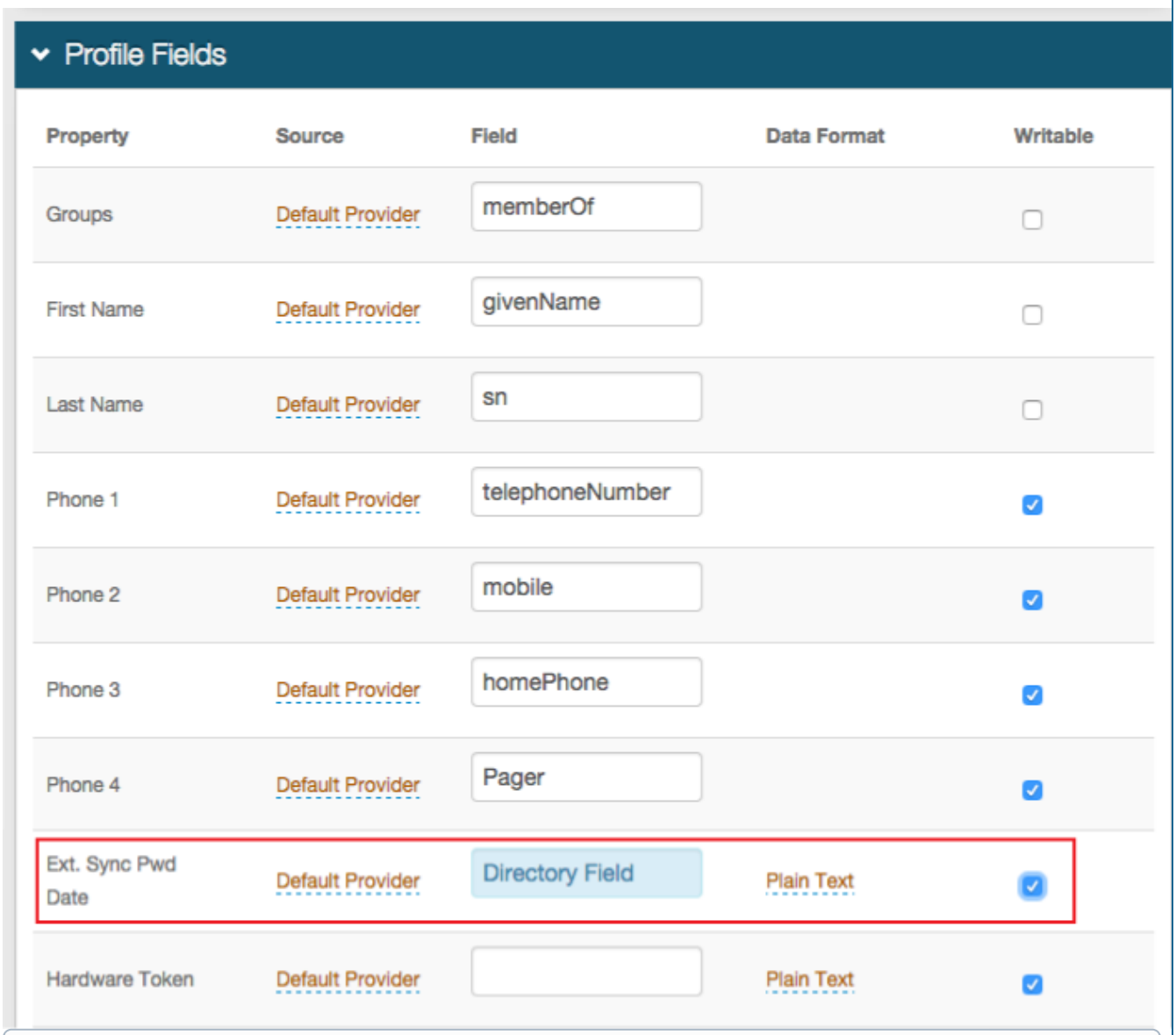


21. Set the **Client Name** to the **Client ID** obtained in the G Suite API Configuration Steps (step 18)

22. Set the **One or More API Scopes** to **https://www.googleapis.com/auth/admin.directory.user** and click **Authorize**

SecureAuth IdP Configuration Steps

Data



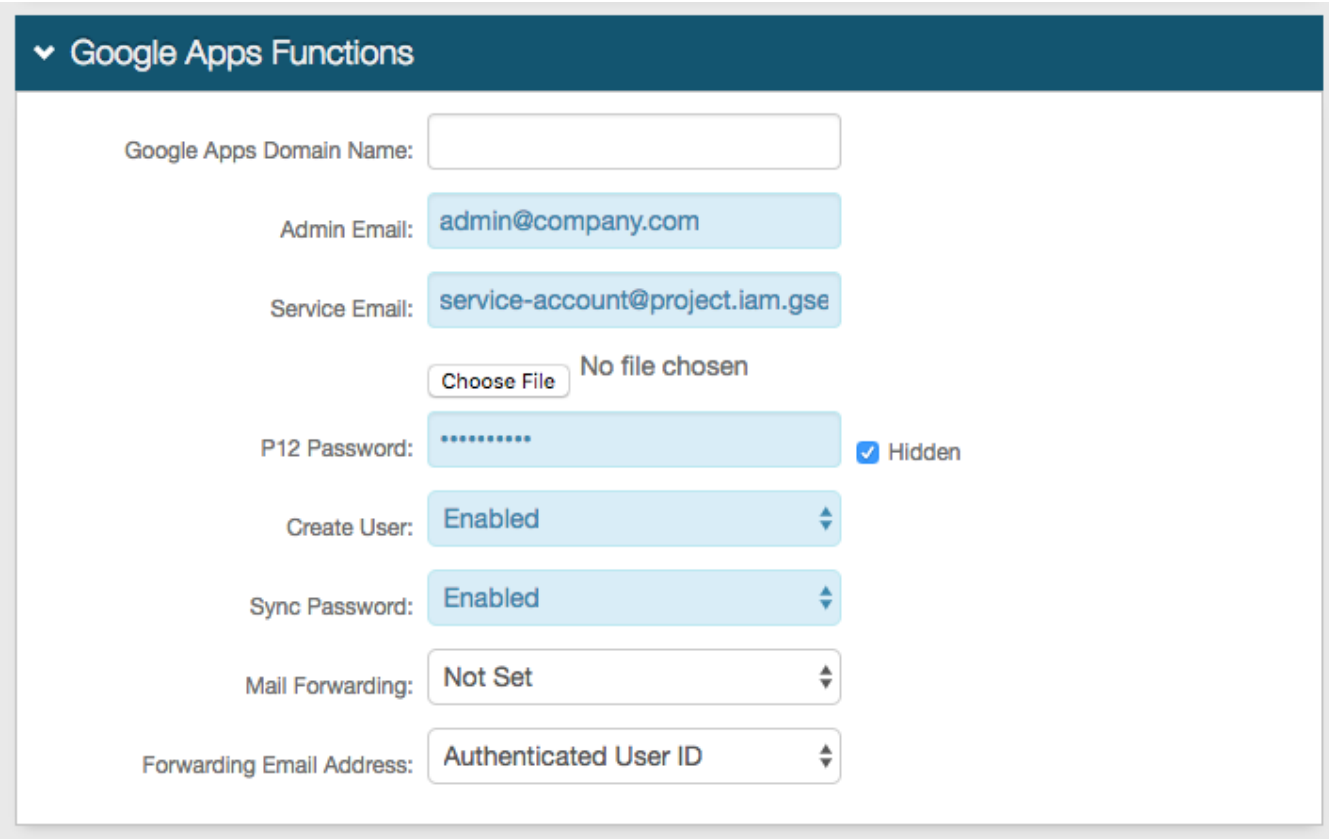
This step is for Active Directory data stores only

1. In the **Profile Fields** section, map a directory field to **Ext. Sync Pwd Date Profile Property**, and check **Writable**

   This is to contain the date on which the G Suite password was last synchronized with AD

Click **Save** once the configurations have been completed and before leaving the **Data** page to avoid losing changes

Post Authentication



2. Leave the **Google Apps Domain Name** field blank

3. Set the **Admin Email** to the G Suite Administrative email account

4. Set the **Service Email** to the **Service Account** email address obtained from the G Suite Steps above (step 18)

5. Click **Choose File** and select the **p12 File** obtained in the G Suite Steps above (step 12)

6. Set the **P12 Password** to the **Private Key Password** obtained in the G Suite Steps above (step 12)

7. Select **Enabled** from the **Create User** dropdown if SecureAuth IdP is to automatically create the G Suite user account (if it does not already exist)

8. Select **Enabled** from the **Sync Password** dropdown if SecureAuth IdP is to conduct a one-way synchronization of the user's directory password to G Suite

    To synchronize on specific dates versus every time the password changes, map a directory field to the **Ext. Sync Pwd Date** property in the **Data** tab

    If no field is mapped, then the password synchronizes every time

G Suite requires passwords with a minimum of 8 characters

9. Select **Enabled** from the **Mail Forwarding** dropdown if another email address will receive messages; select **Disabled** to disable the feature; or select **Not Set** if SecureAuth IdP is to not be included in this feature

10. Select the **Profile Field** that contains the user's **Forwarding Email Address**

Click **Save** once the configurations have been completed and before leaving the **Post Authentication** page to avoid losing changes