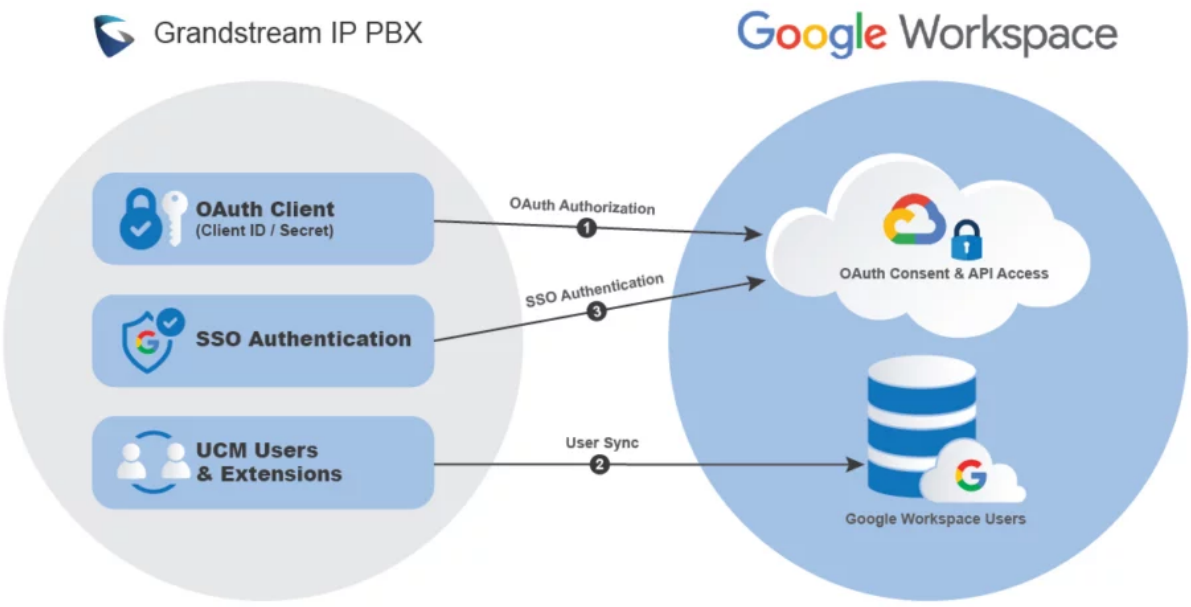
Grandstream Networks, Inc.

Google Workspace Integration

Google Workspace Integration

INTRODUCTION

This guide provides step-by-step instructions for configuring Google Workspace integration with the Grandstream IP PBX, which includes both the Google Workspace application setup and the configuration on the PBX. The goal is to enable secure Google user synchronization and optional Single Sign-On for web access. This guide is intended for administrators performing the initial deployment or validation of the integration.



Google Workspace Integration Architecture

PREREQUISITES

Before proceeding, ensure that all the following prerequisites are met:

- Google Workspace domain with **Super Admin** access
- PBX running supported firmware (Please refer to the Supported Models table)
- A **public FQDN** resolving to the PBX (directly or via reverse proxy)
- HTTPS access to the PBX using the same FQDN

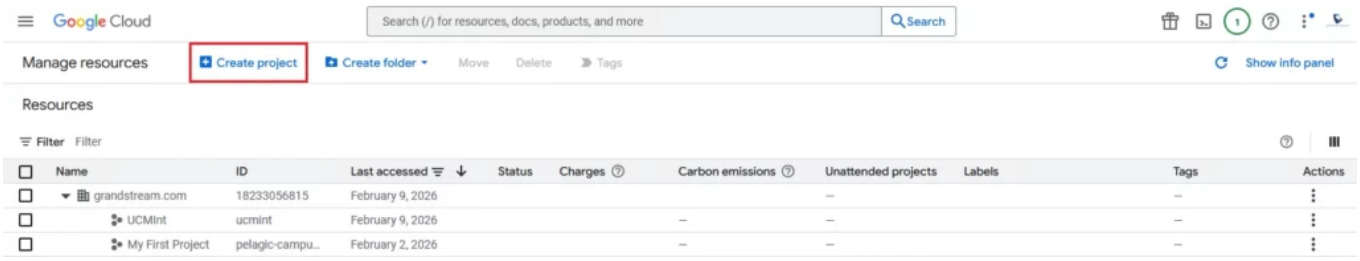
GOOGLE WORKSPACE CONFIGURATION

This section describes how to create and configure the Google OAuth application used by the PBX to communicate with Google Workspace. This application establishes the trust relationship required for user synchronization and SSO. All settings in this section must be completed before proceeding with the PBX-side configuration.

Create a Google Cloud Project

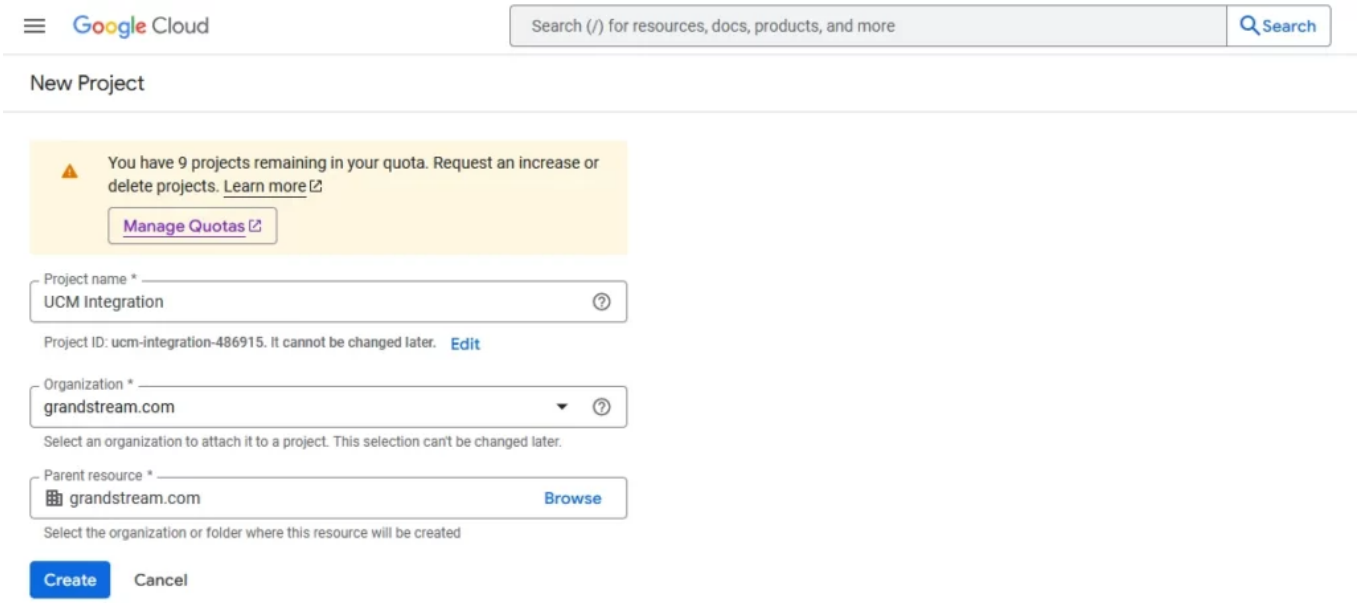
A dedicated Google Cloud project is required to host the OAuth application and manage API access for Google Workspace integration.

1. Log in to the **Google Cloud Console** with a super admin account.
2. Navigate to **IAM & Admin->Manage resources**.
3. Click **Create Project**.



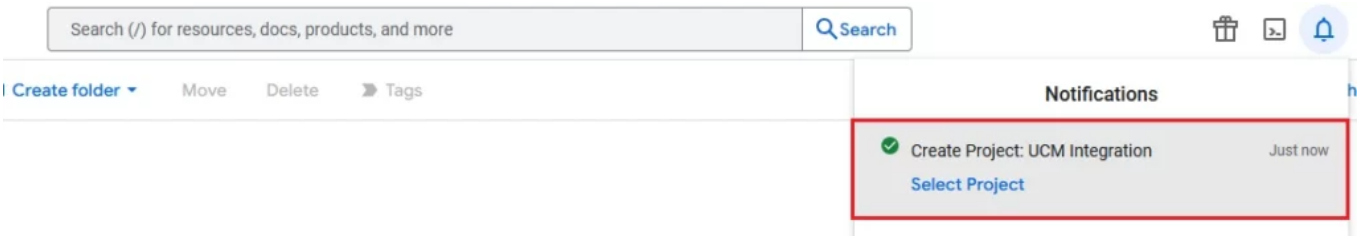
Creating a New Google Cloud Project

4. Enter a project name and select the appropriate organization.



Configuring Project Name and Organization

5. Click **Create** and wait for the project to be provisioned.



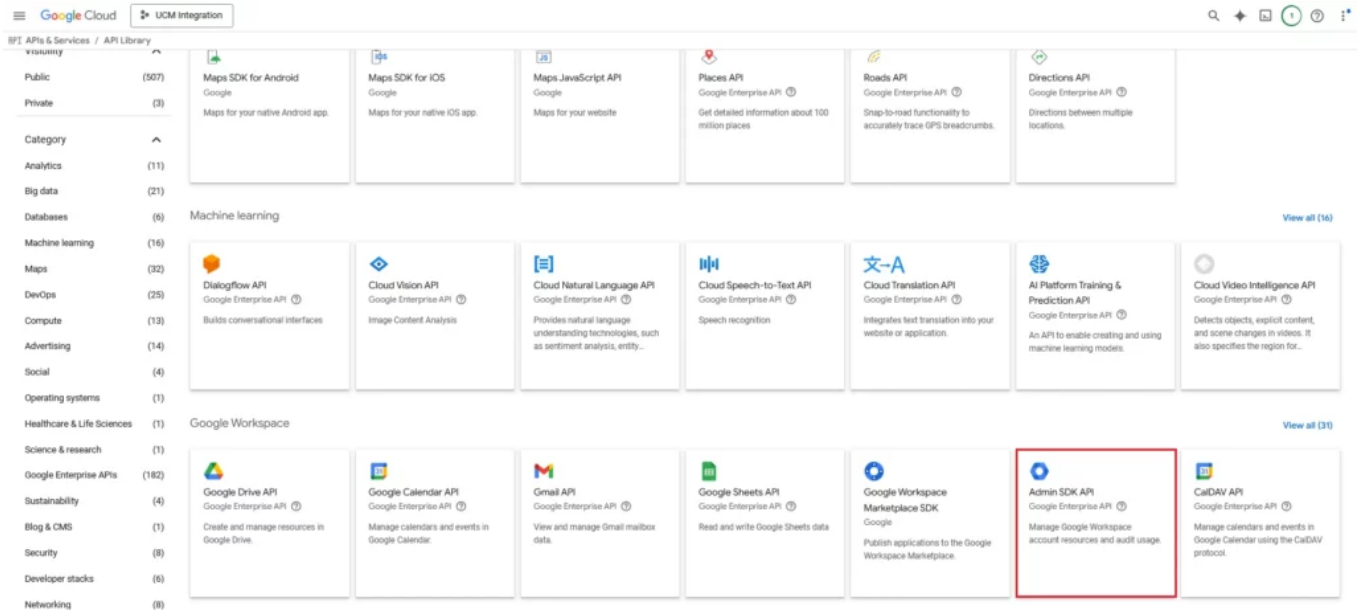
Project Provisioning Confirmation

Enable Google Admin SDK

The Google Admin SDK is required for the PBX to retrieve user information from the Google Workspace domain. Without this API enabled, user synchronization and SSO-related user queries will fail even if OAuth authorization succeeds.

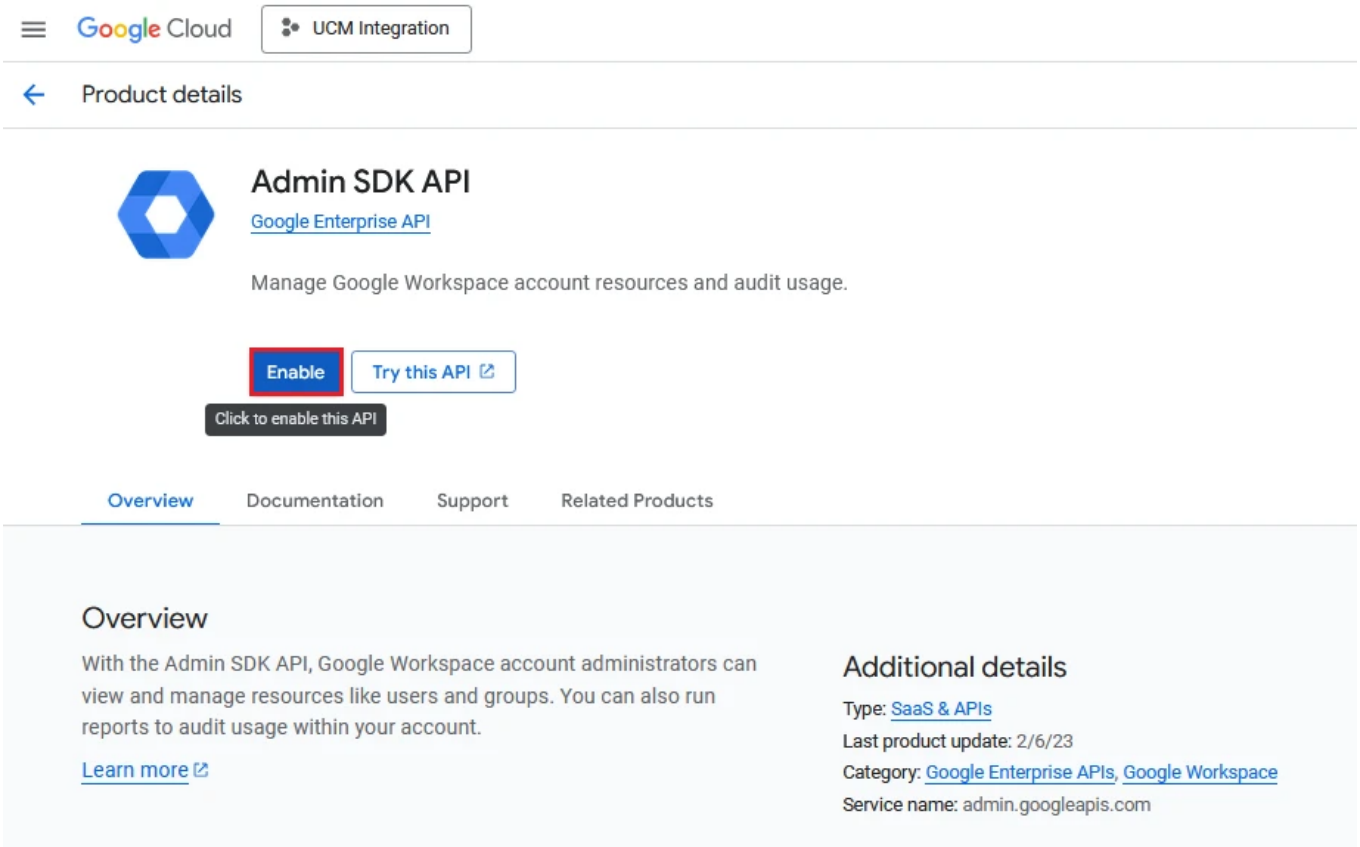
1. In **Google Cloud Console**, select the project created for the PBX integration.

2. Navigate to **APIs & Services->Library**.
3. Search for **Admin SDK API**.



Locating the Admin SDK API

4. Click **Enable**.



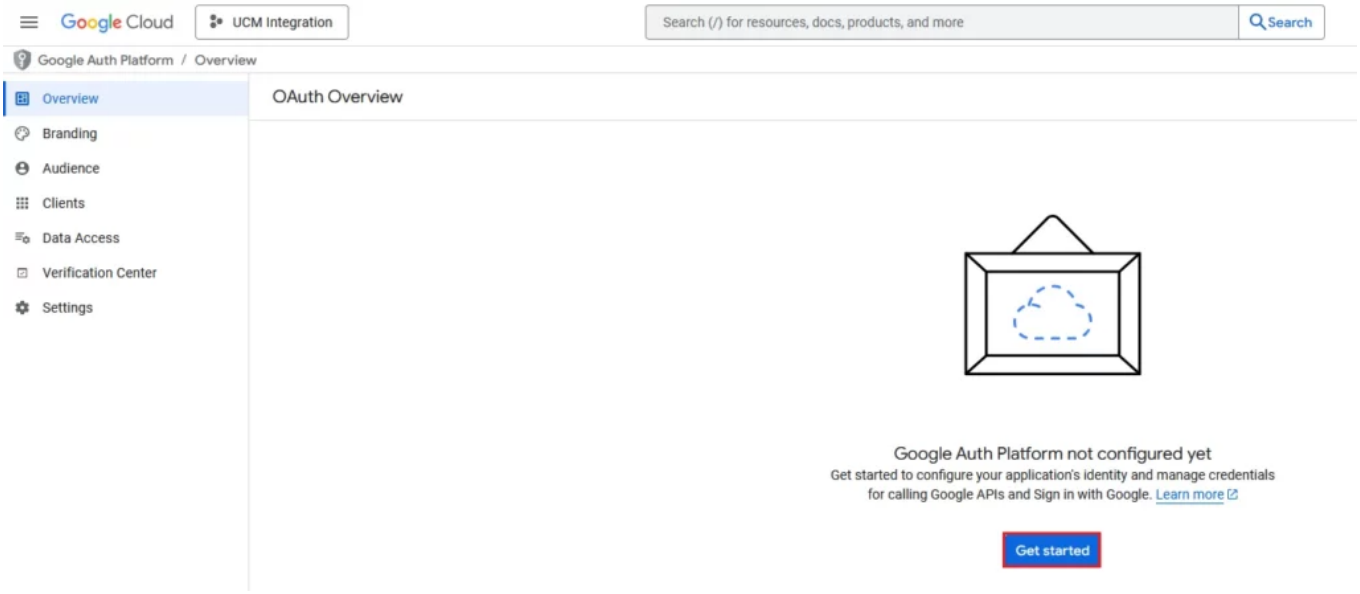
Enabling the Admin SDK API

Enabling the Admin SDK is mandatory for Google user retrieval and synchronization. If this API is not enabled, the PBX will not be able to list or link Google Workspace users.

Configure OAuth Consent Screen

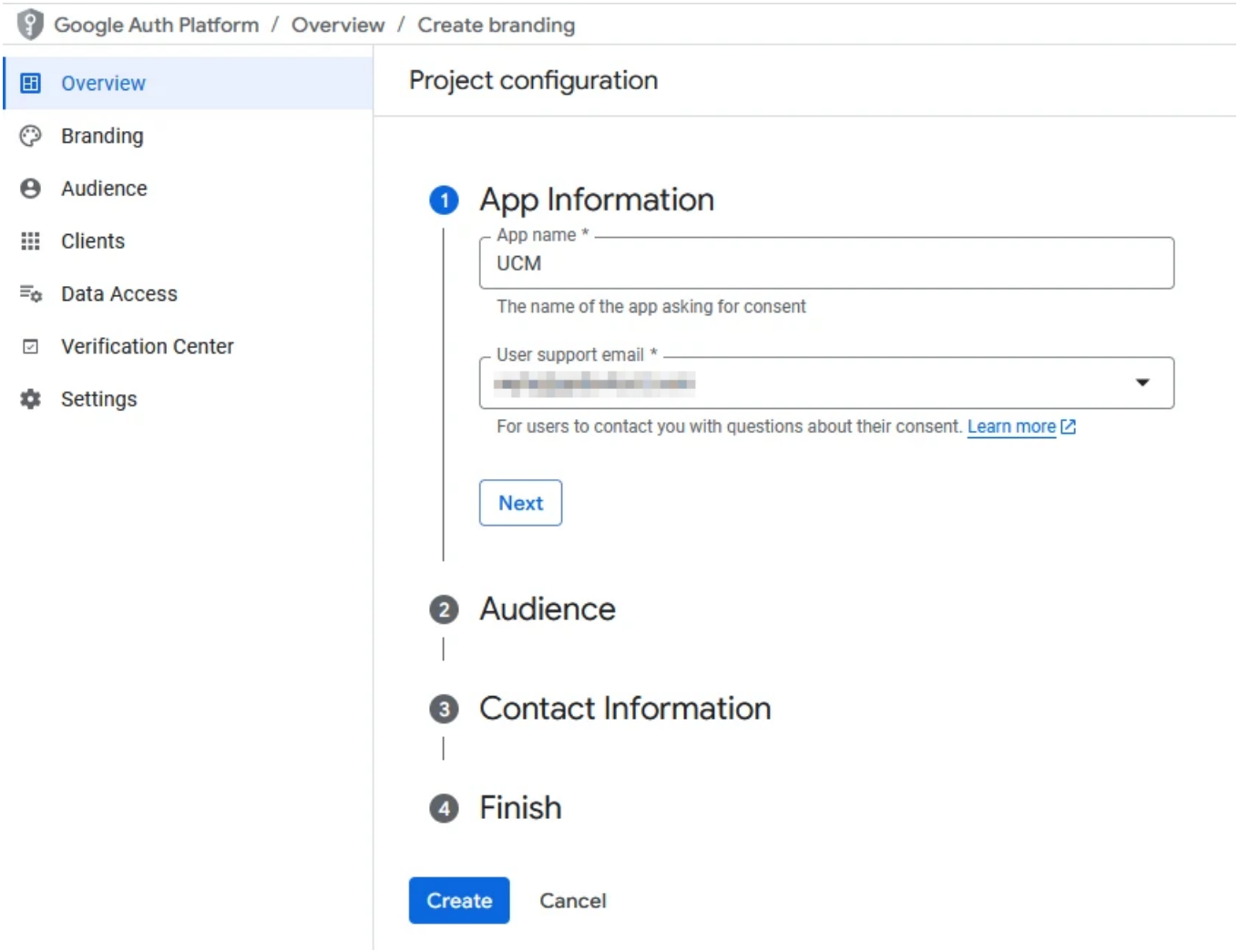
The OAuth consent screen defines how the PBX application is presented to Google Workspace users during authorization. This configuration is mandatory even if the application is used internally only.

1. Navigate to **APIs & Services -> OAuth consent screen**.
2. Make sure the correct new project is selected and click "**Get Started**".



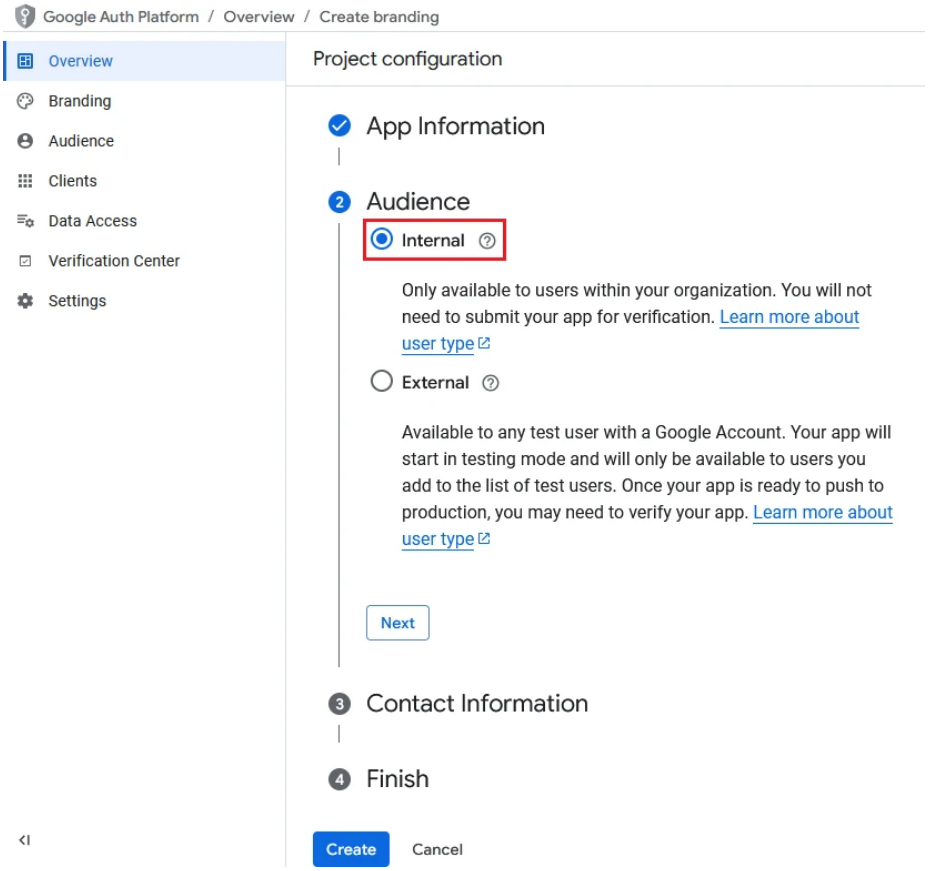
Accessing the OAuth Consent Screen

3. Configure the required application information (Application name, support email).



Configuring OAuth Consent Screen Details

4. Select **Internal** as the user type.



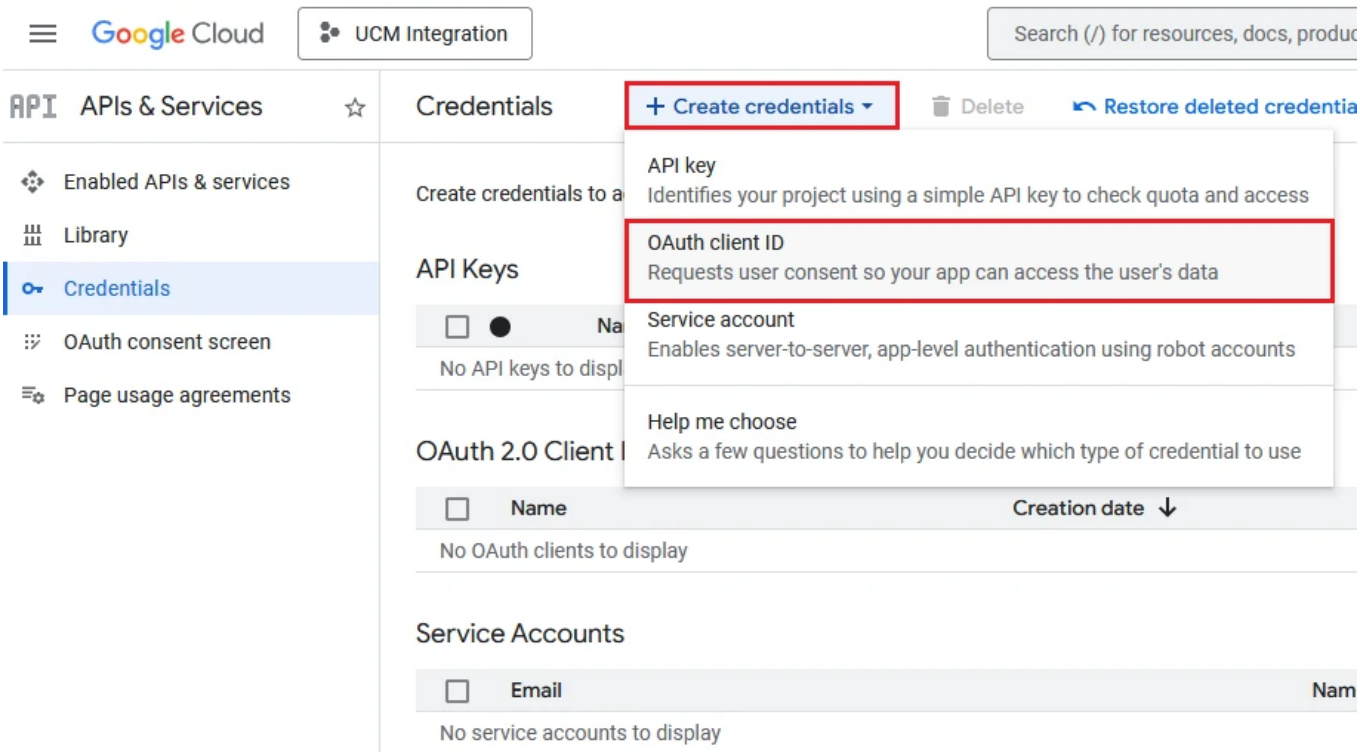
Selecting User Type

5. Enter a valid email address to receive project-related change notifications, agree to the Google API Services: User Data Policy, then click **Create**.

Create OAuth Client Credentials

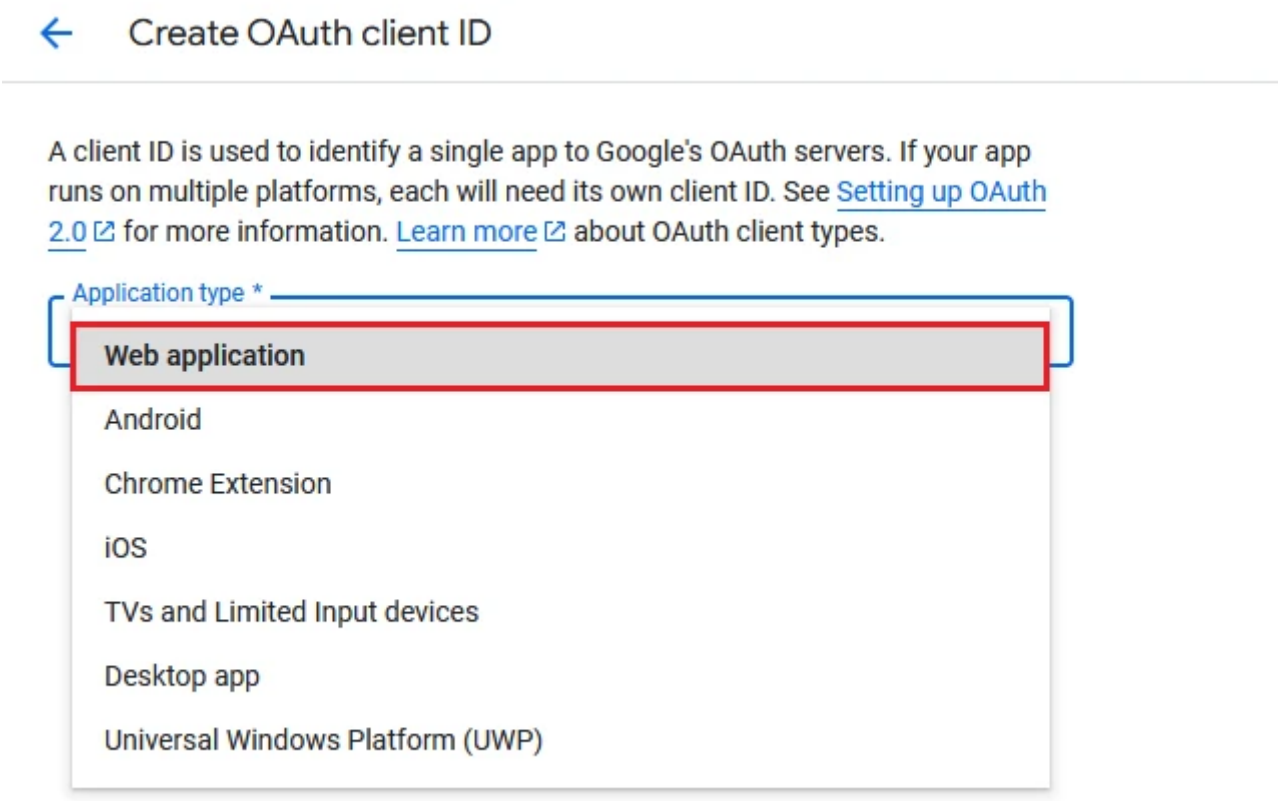
OAuth client credentials allow the PBX to authenticate securely against Google Workspace. These credentials will later be entered on the PBX.

1. Navigate to **APIs & Services -> Credentials**.
2. Click **Create Credentials -> OAuth client ID**.



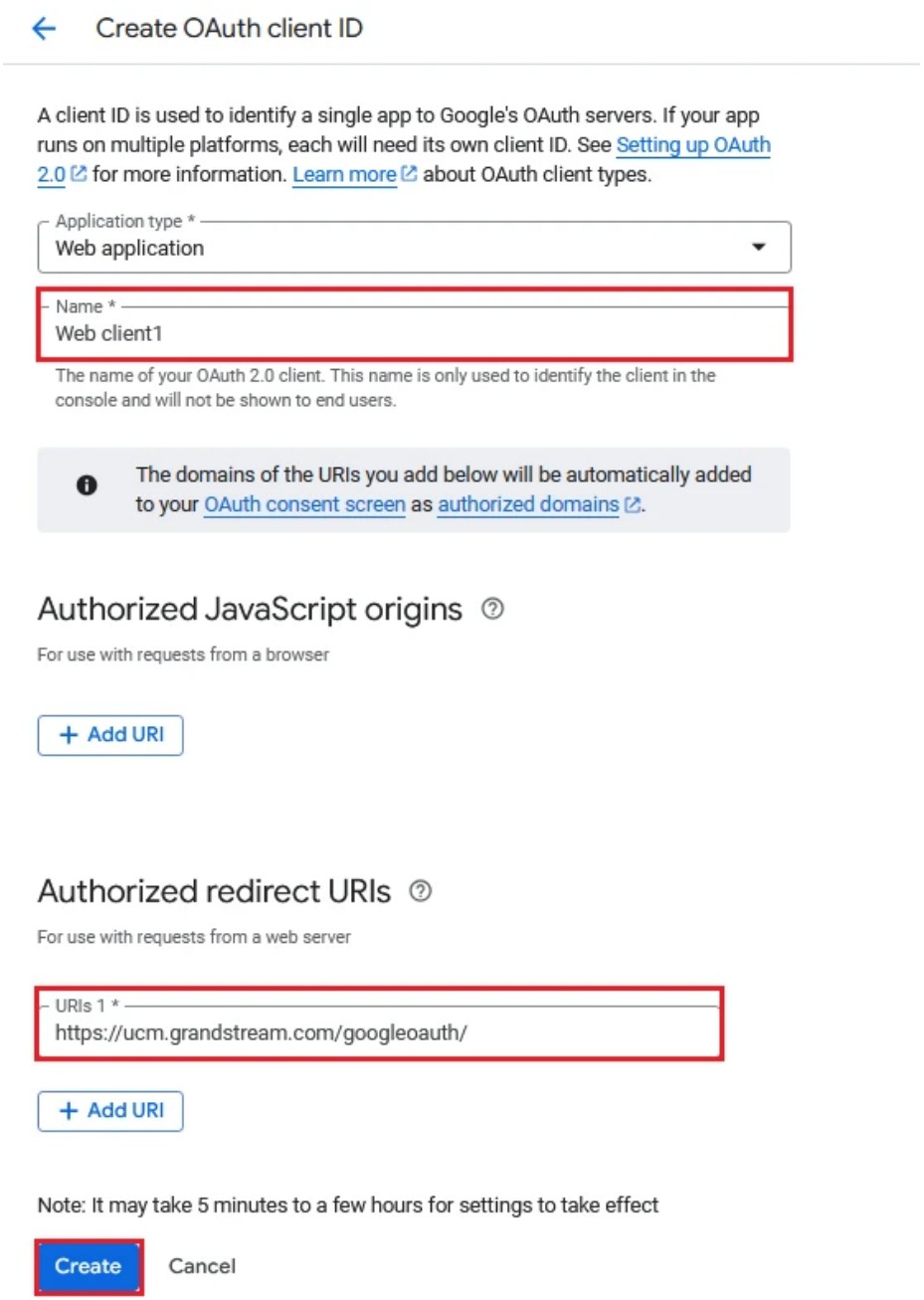
Creating OAuth Client ID - Credentials Page

3. Select **Web application** as the application type.



Selecting Application Type - Web Application

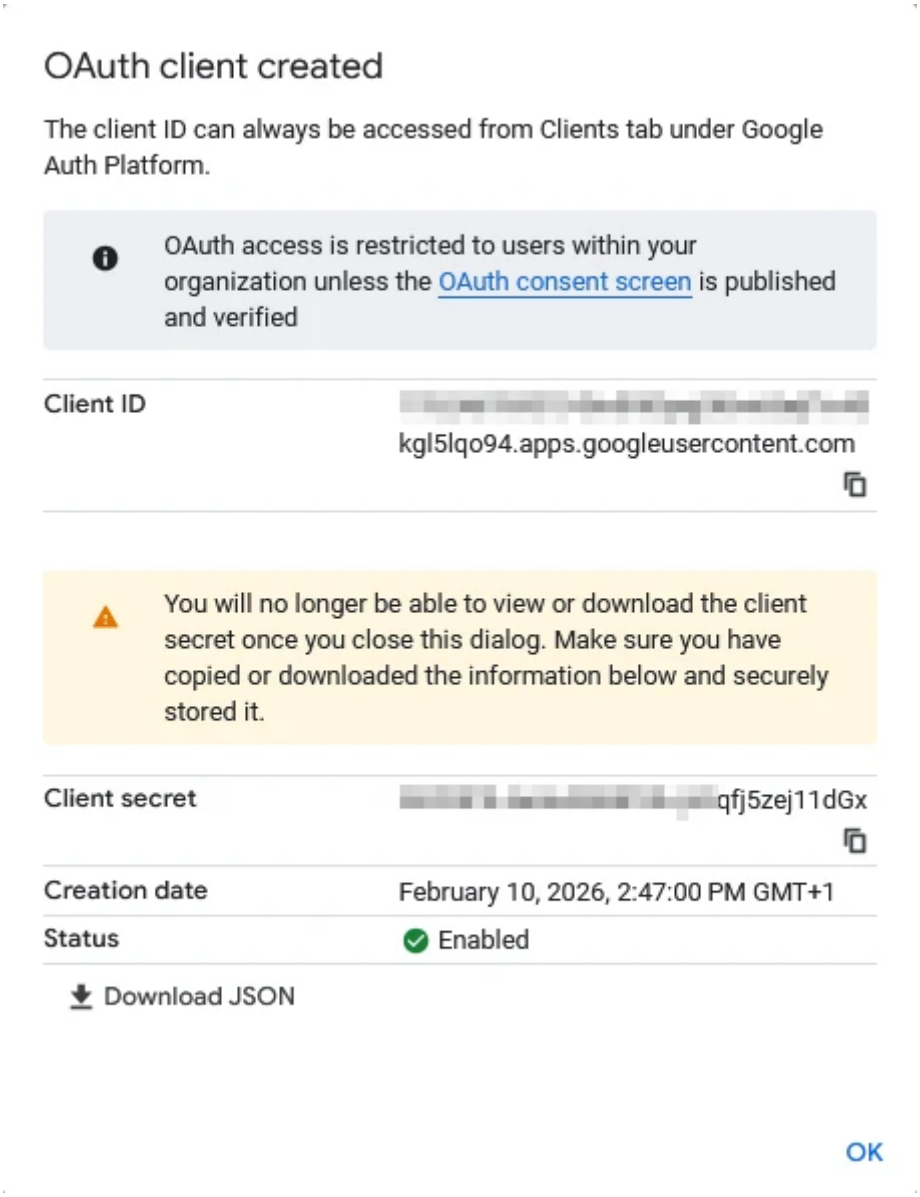
4. Enter a name for the client.
5. Under **Authorized redirect URIs**, add the redirect URI provided by the PBX (HTTPS only).
6. Click **Create**.



Configuring Authorized Redirect URI

7. Record the **Client ID** and **Client Secret** for later use.

The Client Secret **is displayed only once** at the time of creation. Make sure to download the OAuth credentials or securely record the Client ID and Client Secret immediately. If the Client Secret is lost, it must be regenerated in Google Cloud Console and updated on the PBX to restore authorization.



Recording Client ID and Client Secret

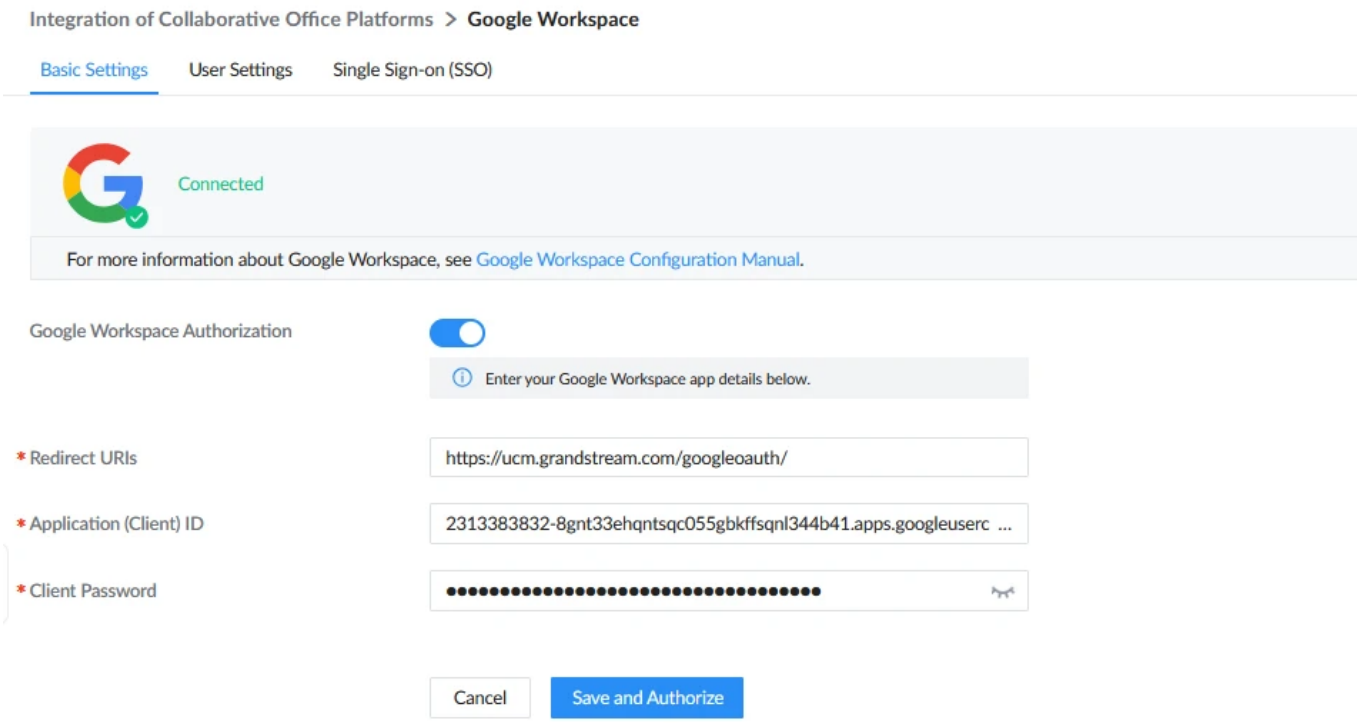
PBX CONFIGURATION

This section describes how to configure the Google Workspace integration on the PBX after the Google Workspace application has been created. OAuth authorization must be completed successfully before Google users can be retrieved, synchronized, or used for SSO.

Configure Google Workspace Authorization

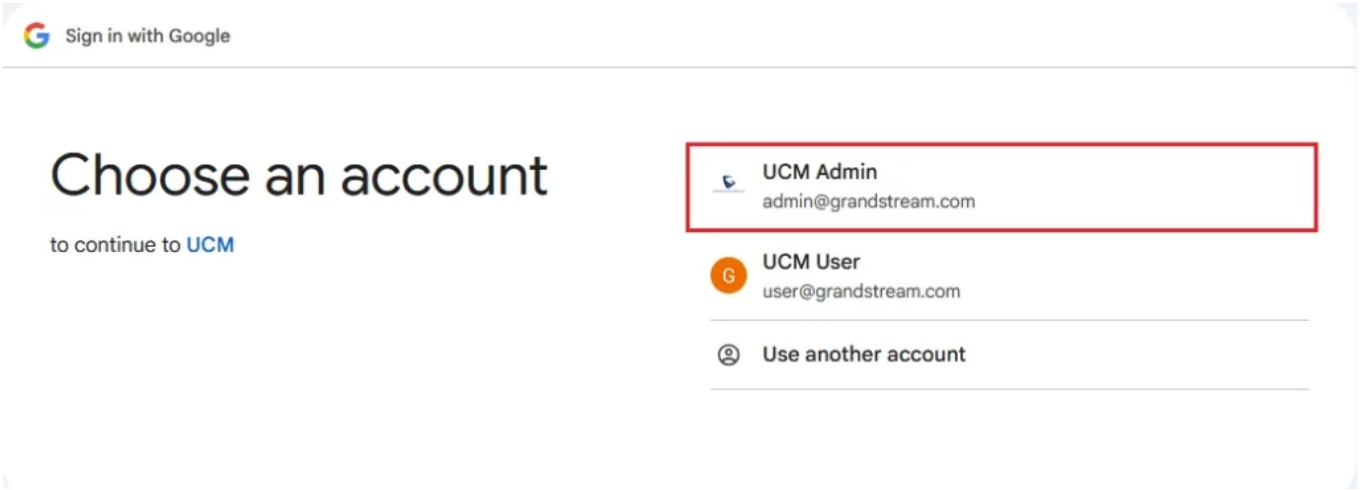
This step establishes the OAuth trust between the PBX and Google Workspace using the Client ID and Client Secret created earlier.

1. Log in to the PBX web interface as an administrator.
2. Navigate to **Integrations -> Integration of Collaborative Office Platforms -> Google Workspace -> Basic Settings**.



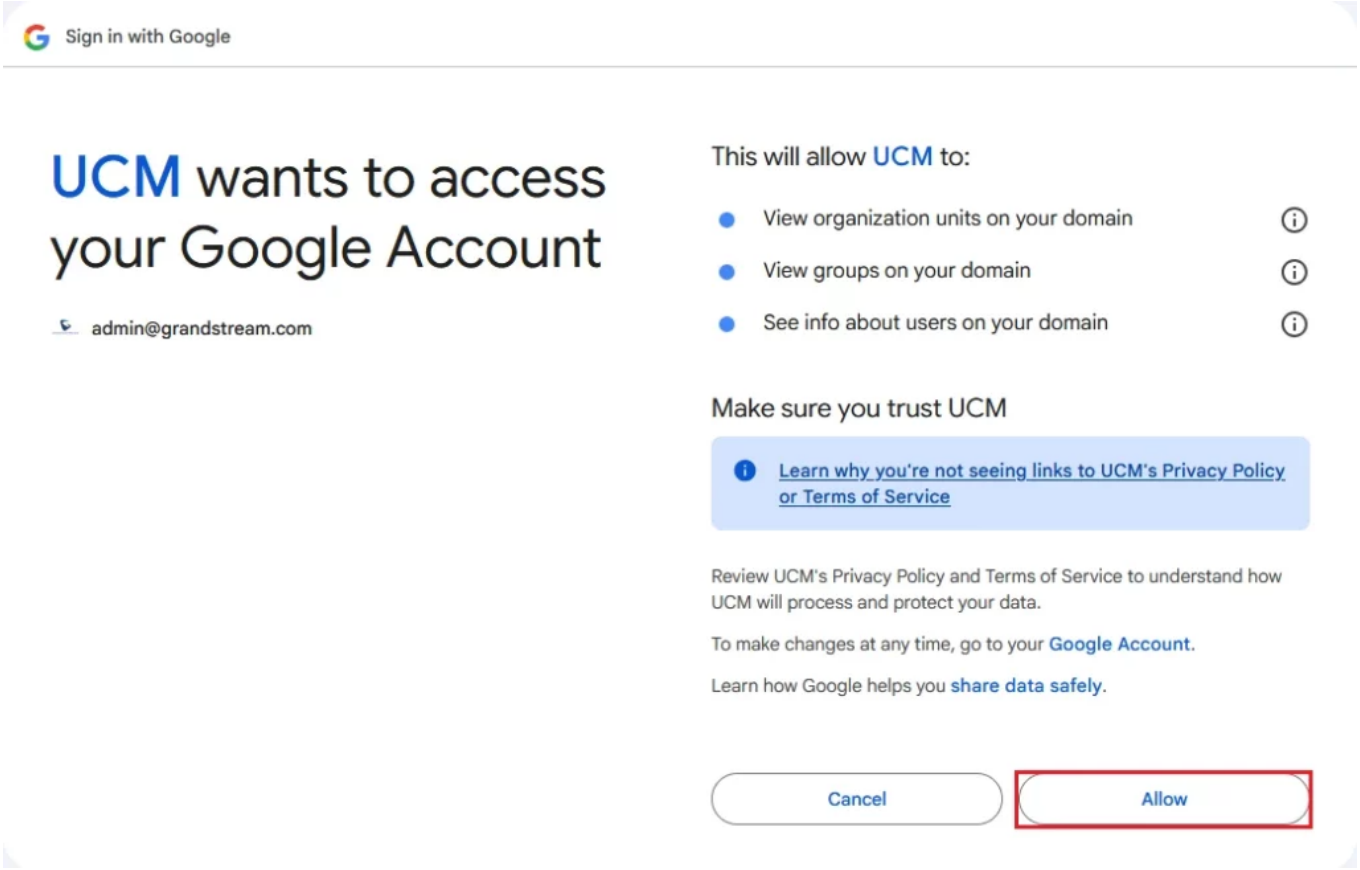
Google Workspace Basic Settings Tab

3. Enable **Google Workspace Authorization**.
4. Enter the **Redirect URI** configured in Google Workspace.
5. Enter the **Application (Client) ID** and **Client Password (Client Secret)** obtained from Google Cloud Console.
6. Click **Save and Authorize**.
7. When redirected, sign in using a Google Workspace administrator account.



Selecting the Google Workspace Administrator Account

8. Review the requested permissions and click **Allow** to grant consent.



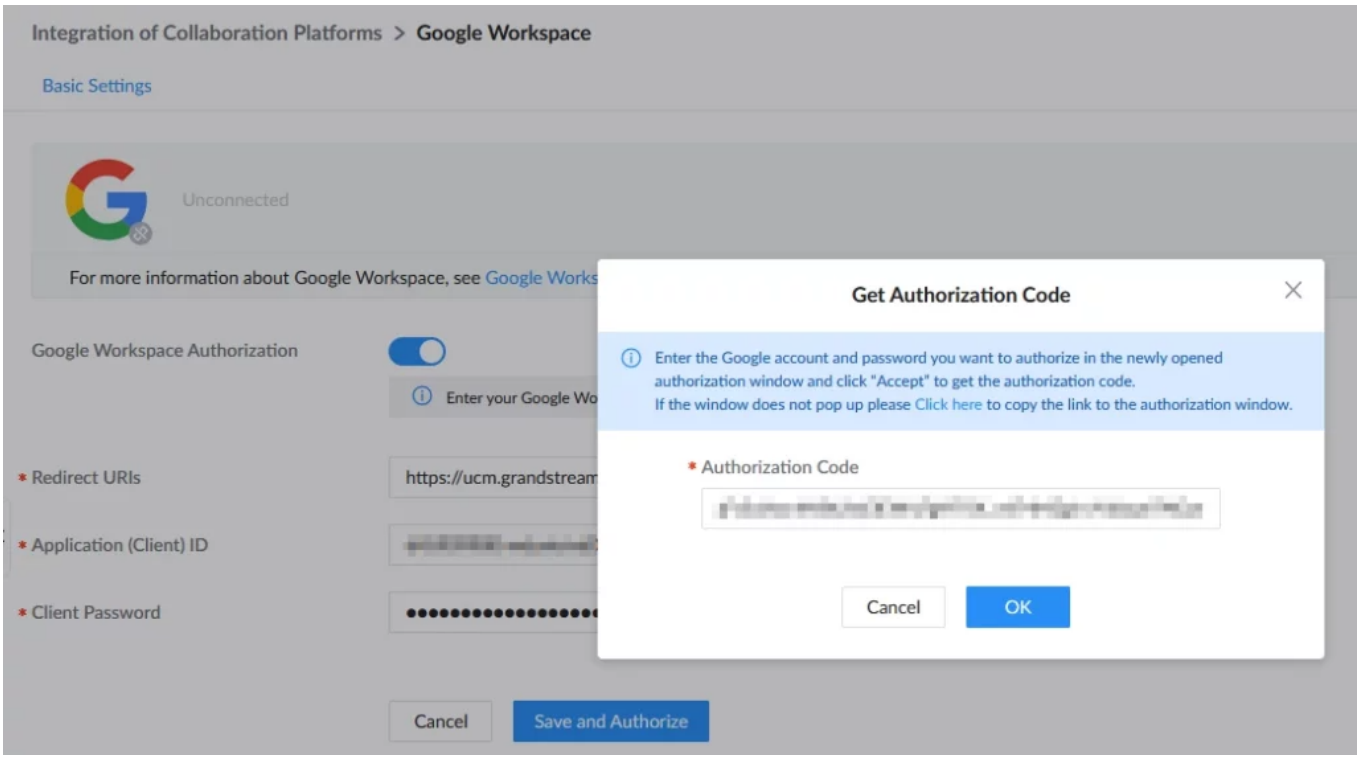
Granting OAuth Consent

9. After consent is granted, Google redirects to a page displaying an **Authorization Code**.



Google Authorization Code Displayed

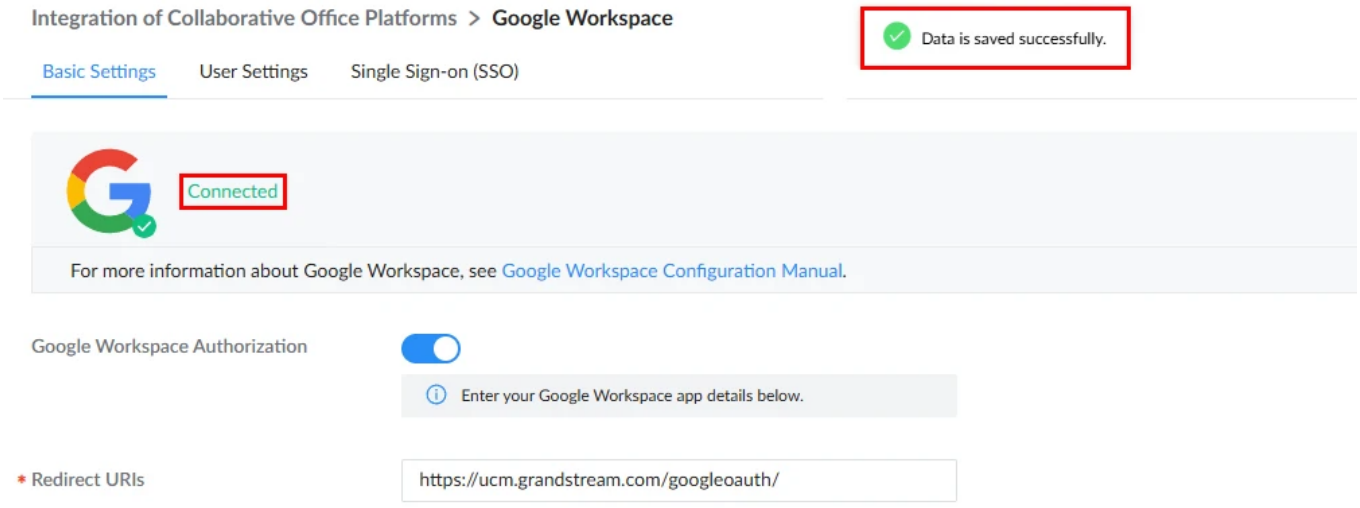
10. Return to the PBX authorization page and paste the copied **Authorization Code** into the required field.



Entering the Authorization Code on PBX

11. Click **Confirm** to complete authorization.

A confirmation prompt is displayed on the PBX indicating that the Google Workspace authorization was successful. Google Workspace-related configuration tabs become available.



Successful Google Workspace Authorization on PBX

Configure Google User Synchronization

After Google Workspace authorization is completed, the PBX can retrieve users from the connected Google Workspace domain. This section explains how to define the user scope and enable synchronization.

Enable Google Workspace User Retrieval

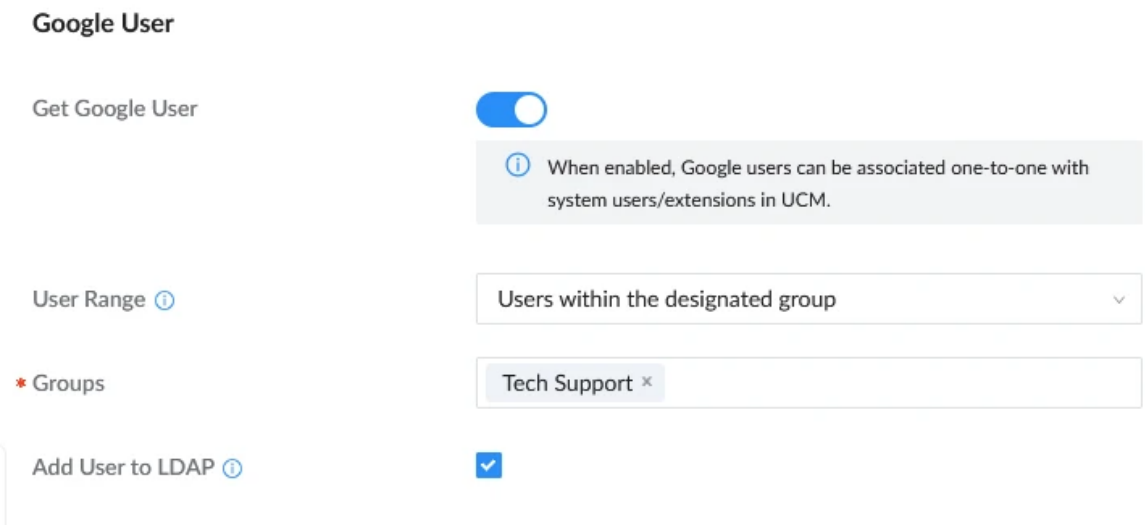
This step determines which Google Workspace users are retrieved and whether they are synchronized into the PBX system.

1. Navigate to **User Settings -> Google User**.
2. Enable **Get Google User**.

3. Select the User Range:

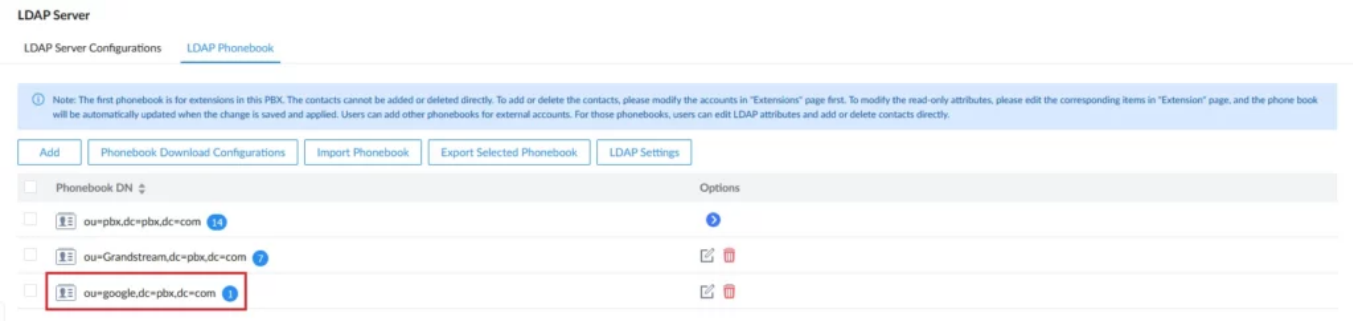
   - **All Users:** retrieves all users from the Google Workspace domain.
   - **Users within the designated organizational unit:** retrieves users from a specified Organizational Unit.
   - **Users within the designated group:** retrieves users belonging to one or more specified Google Workspace groups.

4. If applicable, specify the Organizational Unit or Groups.



User Settings - Google User

5. (Optional) Enable **Add User to LDAP** to synchronize retrieved Google users into the PBX LDAP directory.



Google Workspace PBX LDAP Phonebook

Link Google Workspace Users

Linking associates Google Workspace users with PBX system users or extensions. This association is required for Single Sign-On and optional for user synchronization.

Configure Linking Method

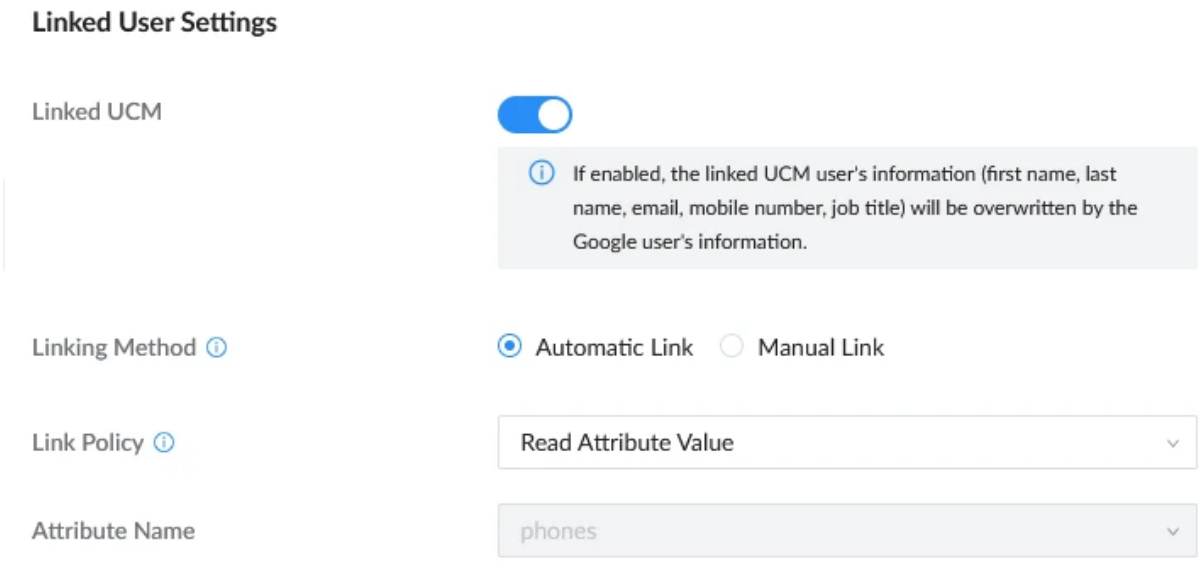
This step defines whether users are linked automatically or manually.

1. Navigate to **User Settings->Linked User Settings**.
2. Enable **Linked PBX*** (*The PBX field in this parameter varies based on the model).
3. Select a Linking Method:

- **Automatic Link:** the PBX automatically links Google users to PBX users or extensions.
- **Manual Link:** administrators manually link users from the Google User List.

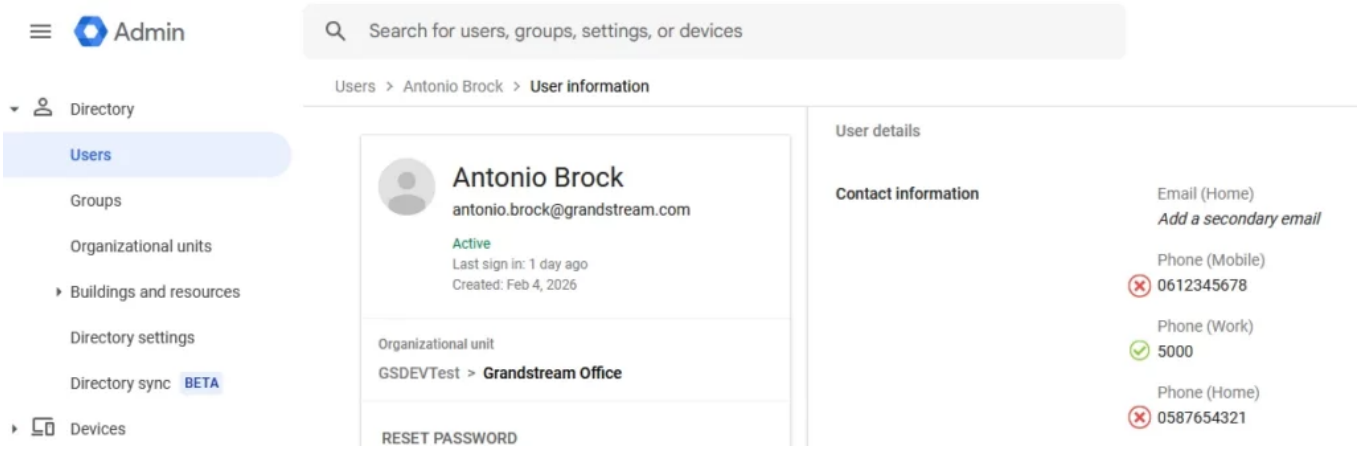
4. When Automatic Link is selected, the PBX determines how Google users are matched to PBX users or extensions. Under **Link Policy**, select one of the following:

- **Automatic Allocation**: the PBX creates or assigns an extension starting from a specified initial extension number.
- **Read Attribute Value**: the PBX reads the Google user phone attribute to create/match a PBX extension.



User Settings - Linked User Settings

When Read Attribute Value is used, the PBX evaluates the Google **Work Number** attribute only. Mobile and Home numbers are ignored.



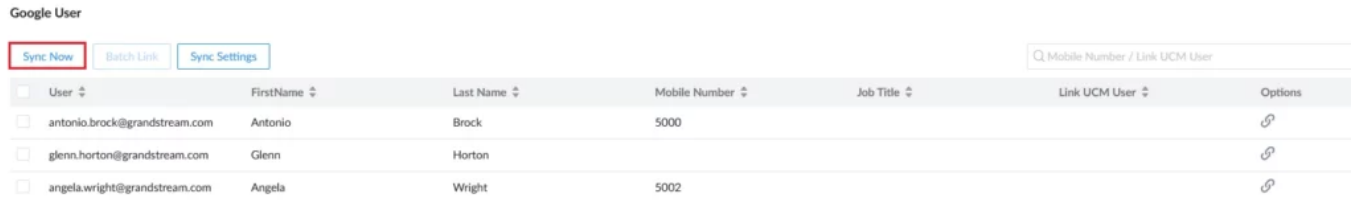
Google User Phone Attributes

Google User List And Manual Operations

After users are retrieved, they are displayed in the Google User List. This section explains how to manually synchronize and link users.

This list allows administrators to retrieve the latest user information immediately.

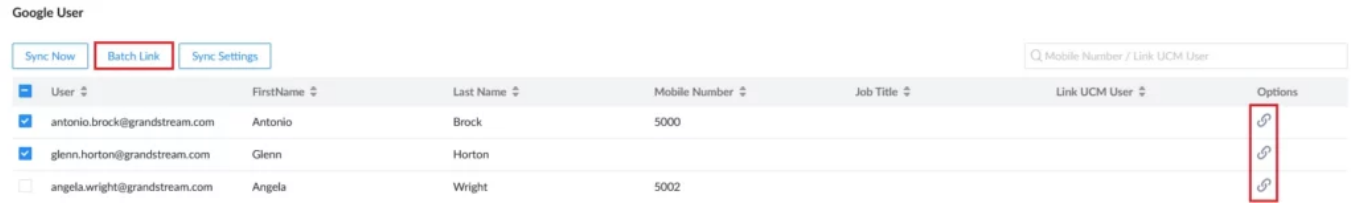
1. Navigate to the **Google User List** section.
2. Click **Sync Now**.
3. Wait for the synchronization process to complete.



Manual Synchronization - Sync Now

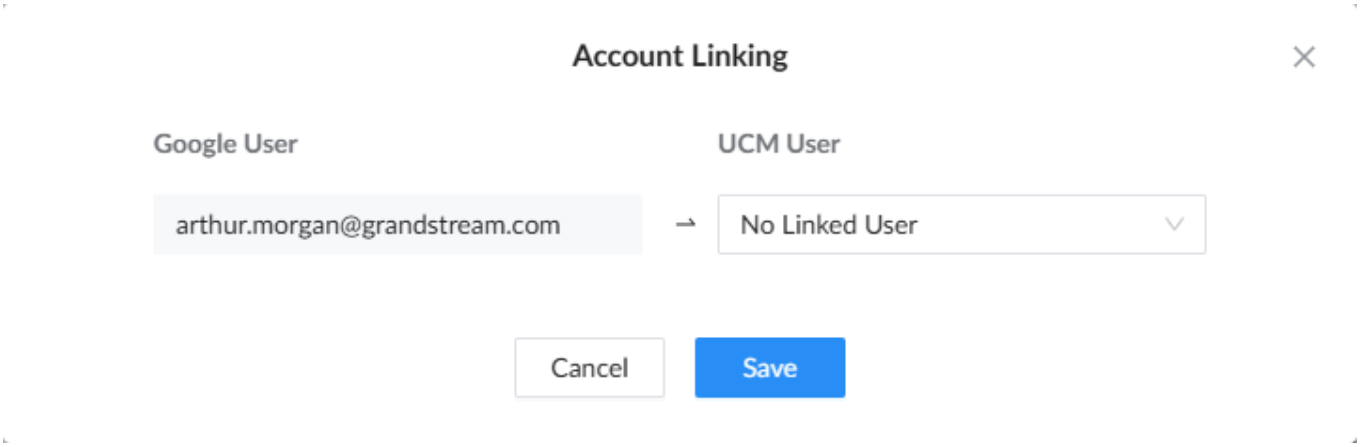
When Manual Link is selected, administrators can explicitly associate Google users with PBX users or extensions.

1. In the **Google User List**, select one or more Google users.
2. Click **Batch Link** or use the **Options** column for individual users.

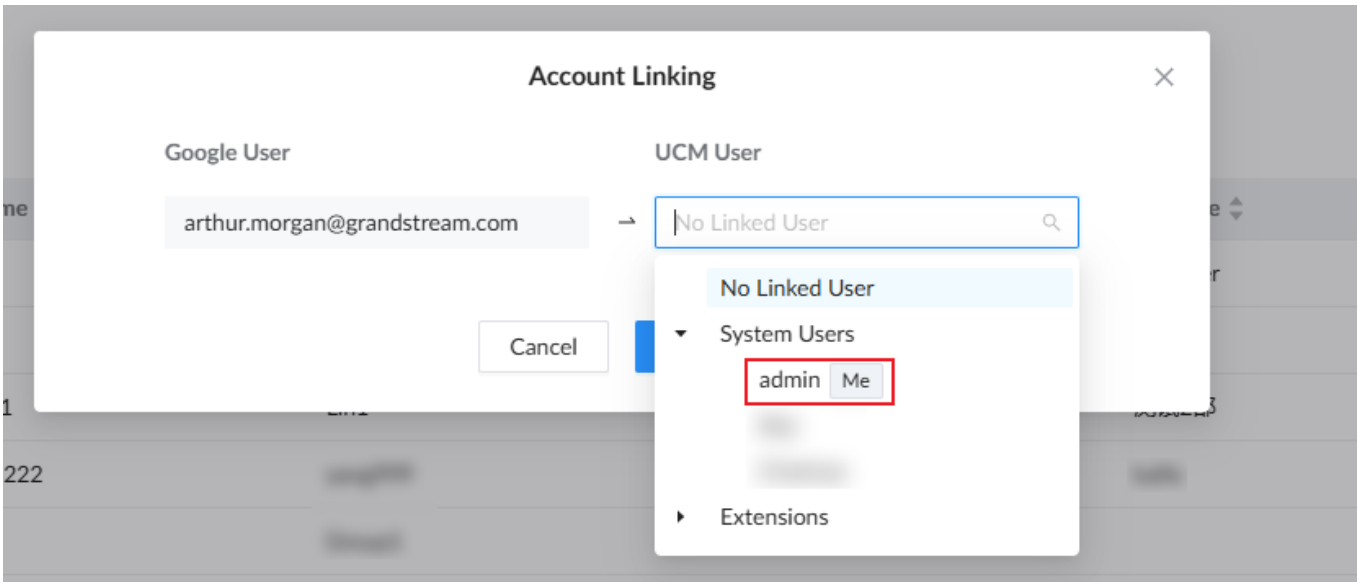


Manual Linking - Batch Link and Options

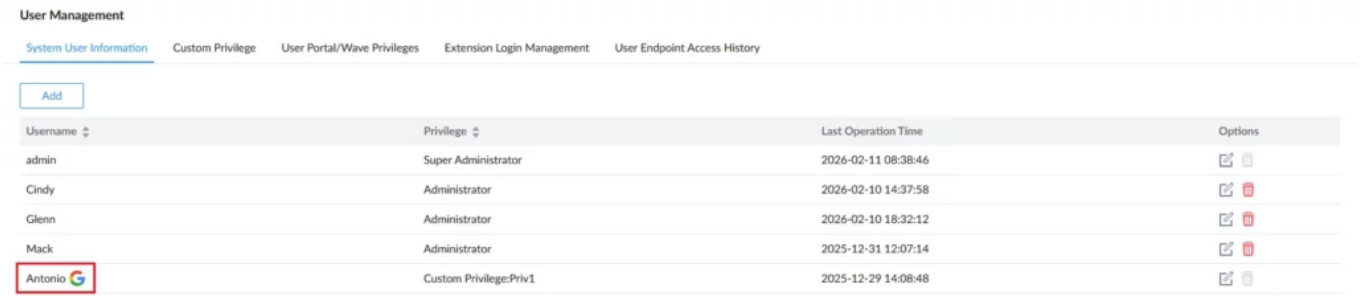
3. Select the target PBX user or extension.
4. Confirm the association.



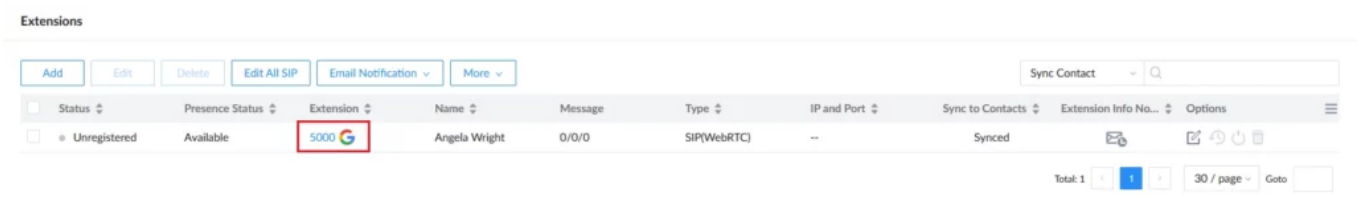
Account Linking Dialog



The linked PBX system users and extensions are identified by a Google icon as shown in the example below.



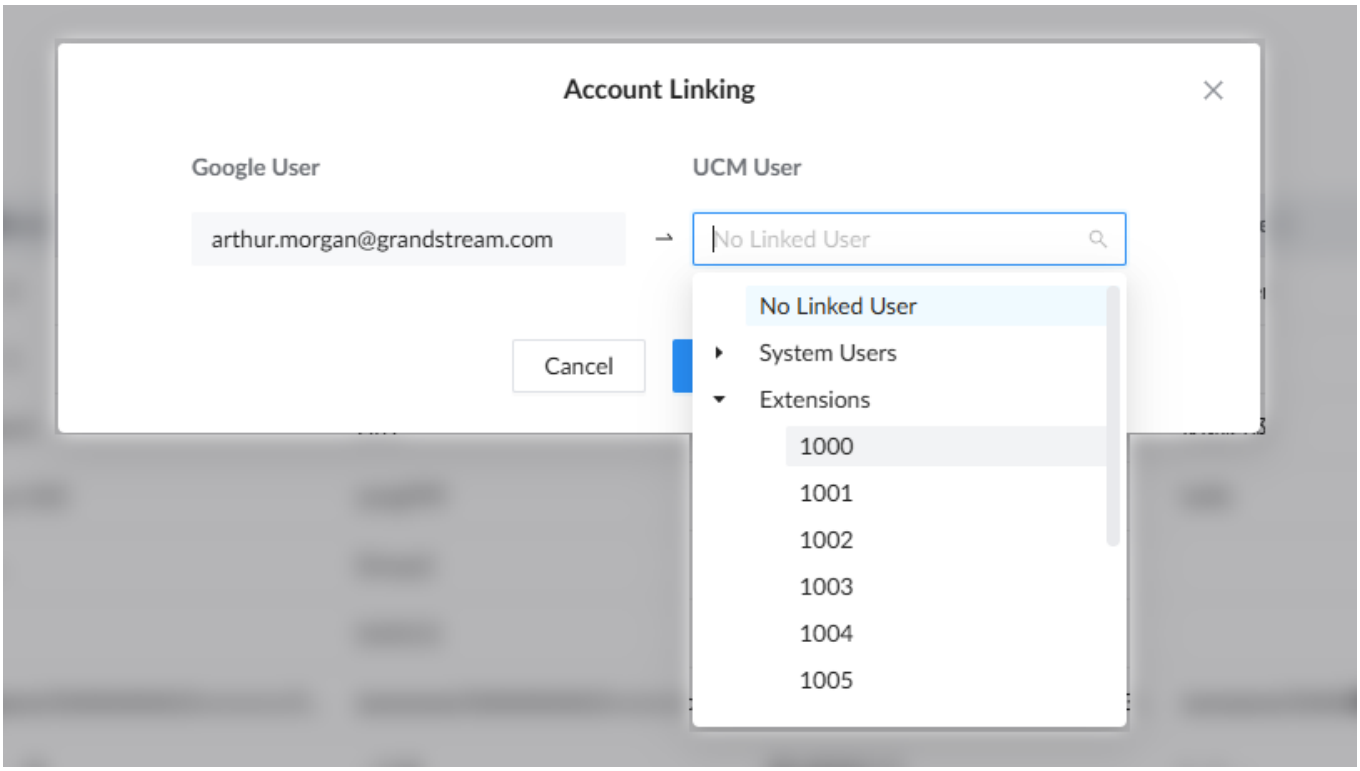
Linked System User Identification



Linked Extension Identification

You can also link a Google Workspace account to an extension, to allow the user to authenticate into Wave using their Google Workspace credentials by linking the Google Workspace account to the extension on the same configuration page.

When linking the account, click on "Extensions" and select an extensions from the list.

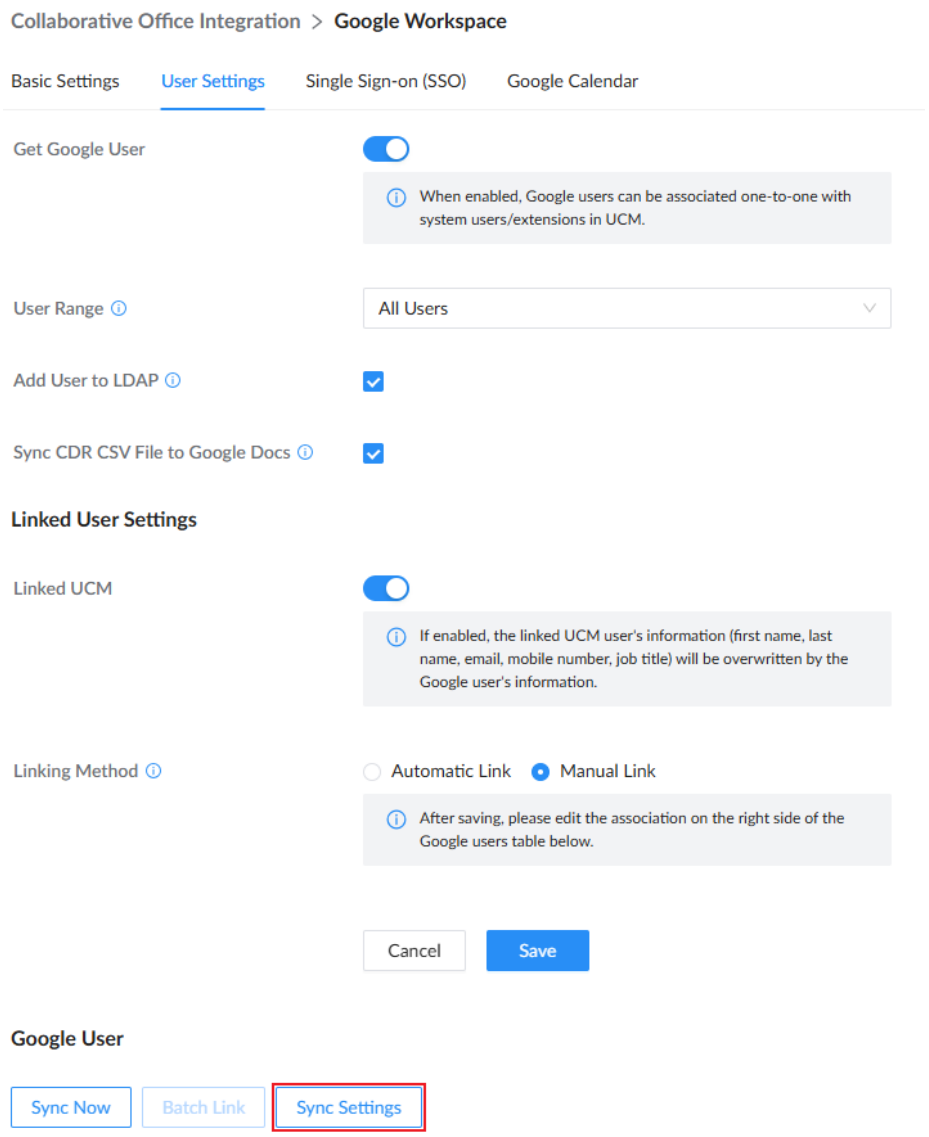


Account Linking

Configure Sync Settings

The Sync Settings page defines how Google Workspace user lifecycle events are handled on the PBX and whether synchronization runs automatically. This section ensures user data consistency between Google Workspace and the PBX.

This Sync Settings page can be accessed from the Google User List as such:



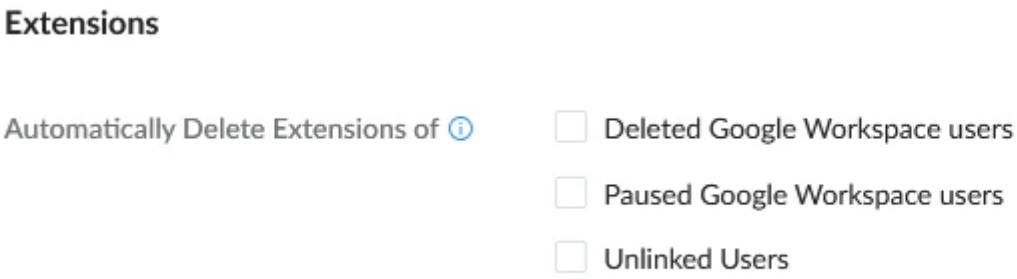
Google Workspace Sync Settings

Configure Extension Cleanup Behavior

This configuration determines how linked PBX extensions are handled when a Google Workspace user is deleted, suspended, or unlinked.

1. Navigate to **Google User List -> Sync Settings**.
2. Under the **Extensions** section, configure the following options as required:

   - **Deleted Google Workspace users:** Automatically deletes the linked PBX extension when the corresponding Google Workspace user is deleted.
   - **Paused Google Workspace users:** Automatically deletes the linked PBX extension when the corresponding Google Workspace user is suspended or paused.
   - **Unlinked Users:** Automatically deletes PBX extensions that are no longer linked to any Google Workspace user.
3. Click Save.



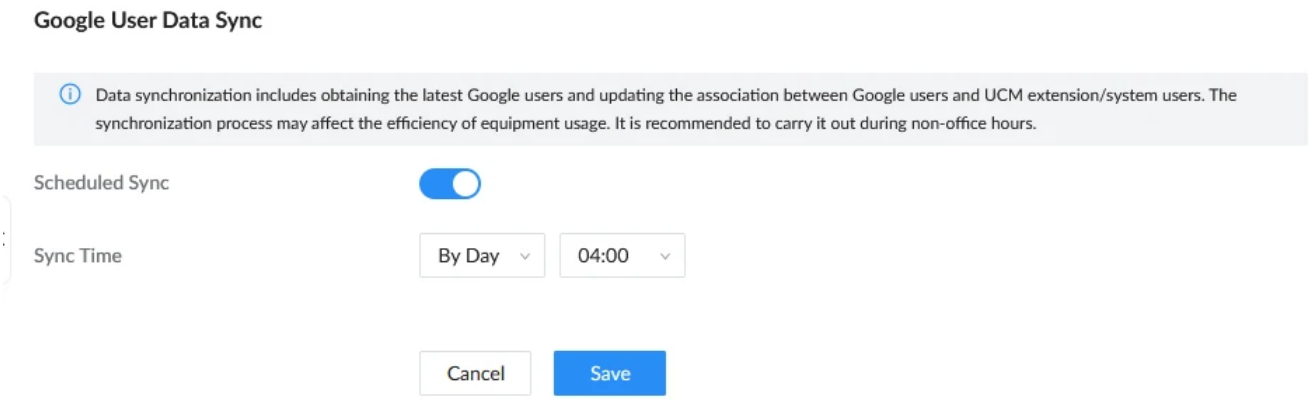
Extensions Sync Settings

Configure Scheduled Synchronization

Scheduled synchronization allows the PBX to periodically retrieve updated Google Workspace user information and maintain link associations automatically.

1. In the **Sync Settings** page, enable **Scheduled Sync**.
2. Configure the desired synchronization schedule.
3. Click Save.

Synchronization may temporarily impact system performance. It is recommended to schedule synchronization outside business hours.



Google User Data Sync Settings

Review Sync History

The Sync History section under Sync Settings provides visibility into previous synchronization attempts and their results. This is useful for validation and troubleshooting.

The following information is displayed:

- **Sync Time:** Date and time when the synchronization was executed.
- **Sync Mode:** Indicates whether the sync was triggered manually or by schedule.
- **Results:** Displays the synchronization result (Success, Partial Success, or Failed).
- **Options:** Provides access to detailed synchronization logs for troubleshooting purposes.


Sync History

Sync Time	Sync Mode	Results	Options
2026-02-09 14:10:04	Manual sync	Success	
2026-02-09 14:09:56	Manual sync	Success	
2026-02-05 16:59:40	Manual sync	Success	
2026-02-05 15:11:11	Manual sync	Success	
2026-02-05 15:10:46	Manual sync	Partial Success	
2026-02-05 15:10:34	Manual sync	Success	
2026-02-05 15:10:30	Manual sync	Failed	
2026-02-05 15:08:56	Manual sync	Failed	

Google Workspace Sync History

Configure Single Sign-On (SSO)

Single Sign-On enables Google account-based authentication for the PBX web interface. When enabled, users can log in using their Google credentials instead of local PBX credentials.

The following conditions must be met for SSO to function correctly:

- **At least one Google Workspace account** must be linked to a PBX user or extension.
- The PBX must be accessed using **a public FQDN over HTTPS**.

Configure Authorized Domain and Redirect URI

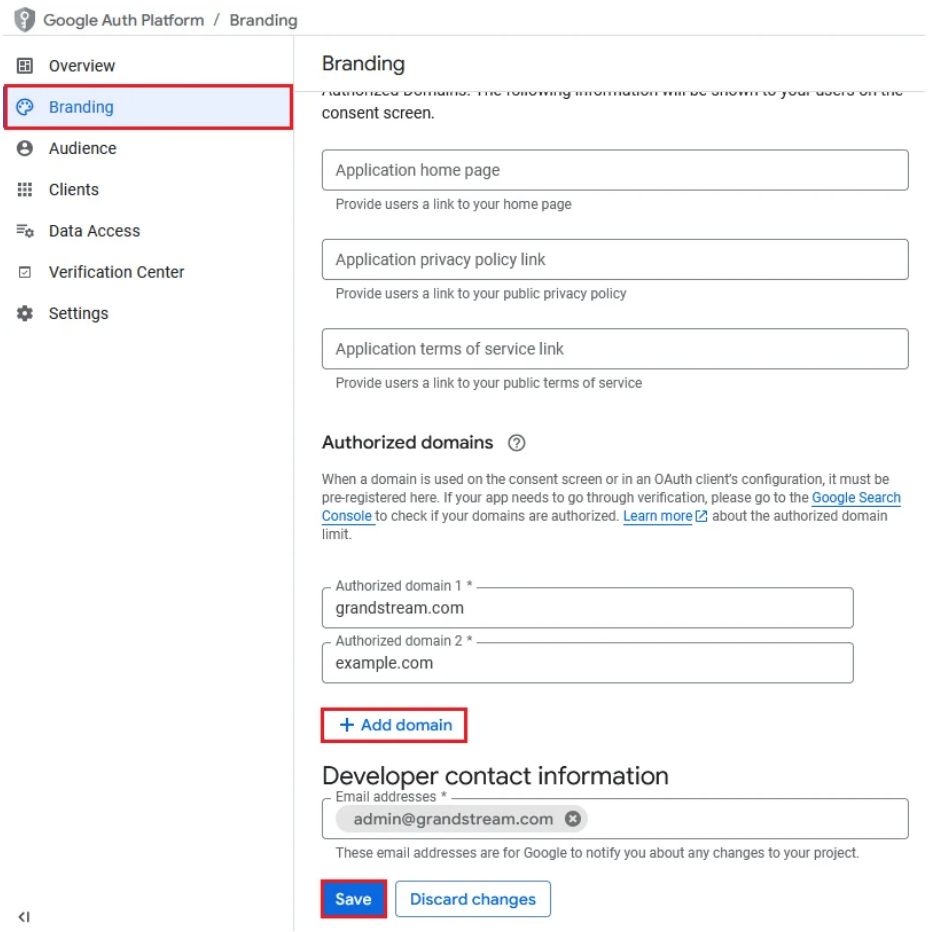
Google requires the domain used to access the PBX to be registered in the OAuth consent screen and the exact login URL to be configured as an authorized redirect URI.

Add Authorized Domain

The domain used to access the PBX must belong to your Google Workspace organization.

1. Log in to **Google Cloud Console**.
2. Select the project created for the PBX integration.
3. Navigate to **APIs & Services->OAuth consent screen**, and access the Branding tab.
4. Under **Authorized domains**, click Add Domain.
5. Enter the root domain of the PBX FQDN (not the full subdomain).
6. Click Save.

If the PBX is accessed via: "https://pbx.example.com", enter: "example.com".



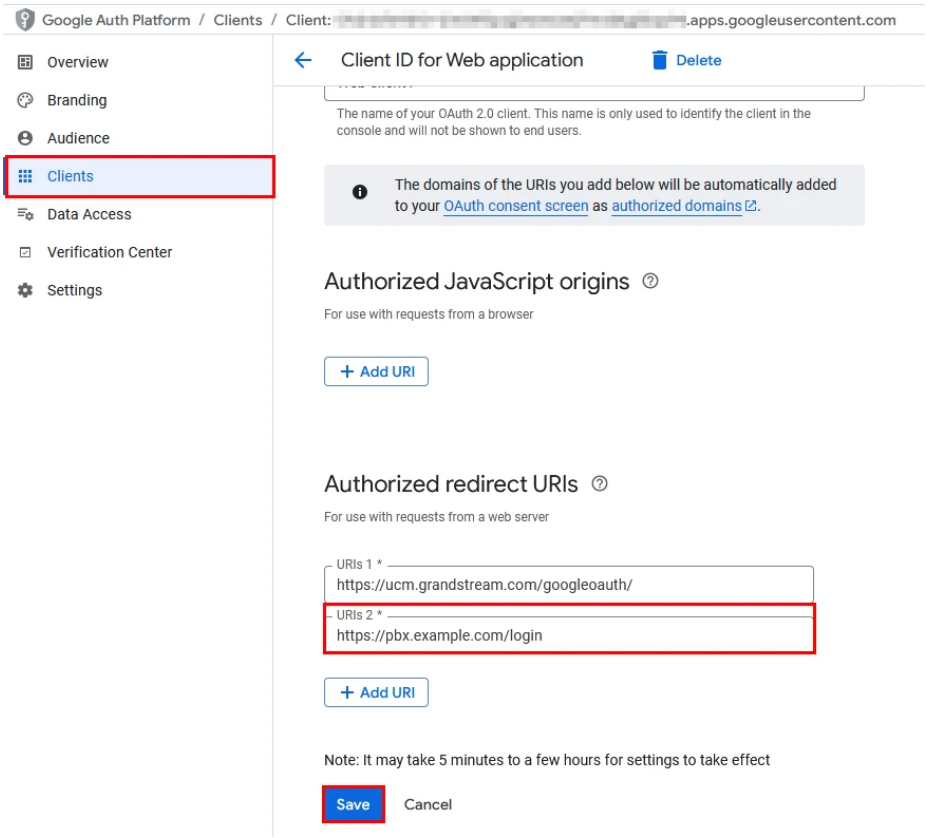
Authorized Domains Configuration

Configure Authorized Redirect URI

After adding the authorized domain, configure the exact redirect URI used by the PBX during OAuth authentication.

1. Navigate to **APIs & Services -> Credentials**.
2. Locate the previously created **OAuth 2.0 Client ID**.
3. Click Edit.
4. Under **Authorized redirect URIs**, click **Add URI**.
5. Enter the exact HTTPS login URL used to access the PBX.
6. Click Save.

- The URI must match exactly (including HTTPS and path).
- Do not omit /login.
- Any mismatch will result in redirect_uri_mismatch or invalid_request errors.



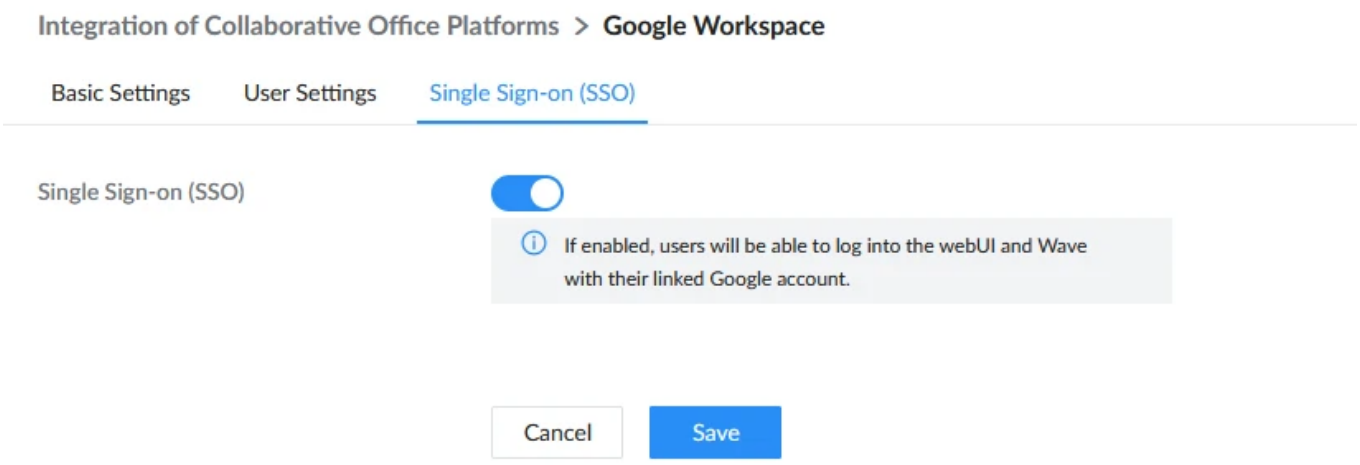
Authorized Redirect URI for SSO

Configure SSO on the PBX

After the Google side configuration is complete and OAuth authorization has already been successfully established under **Basic Settings**, enable SSO on the PBX.

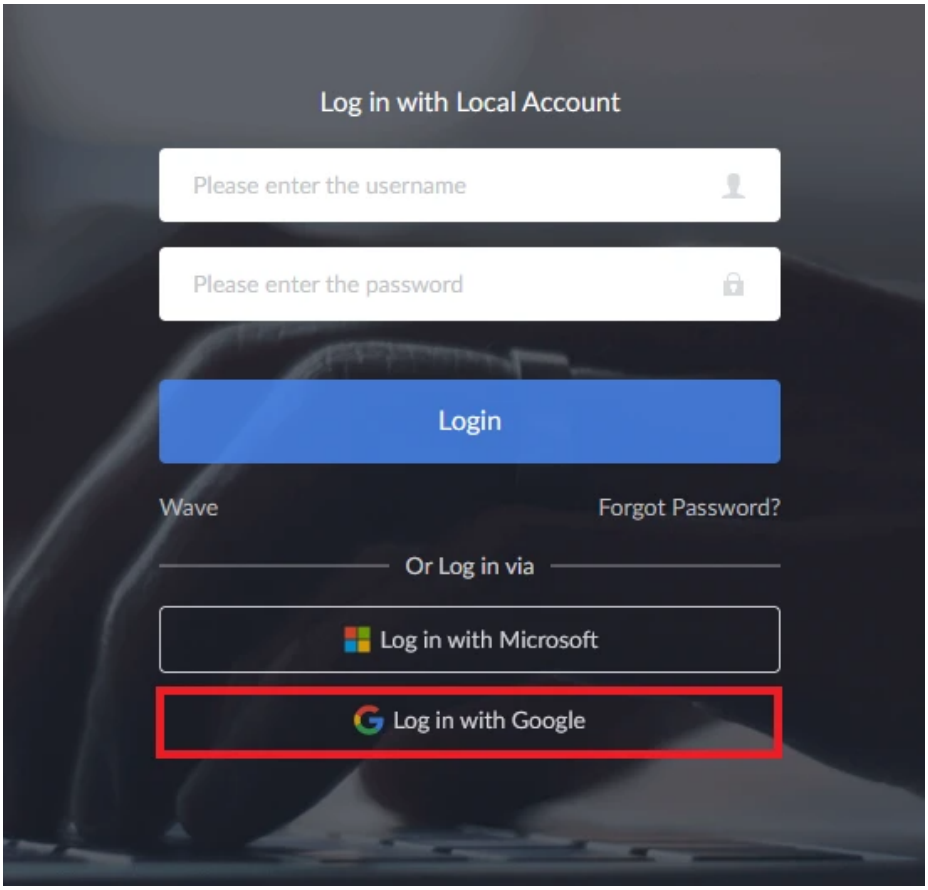
1. Log in to the PBX web interface as an administrator.
2. Navigate to **Integrations->Integration of Collaborative Office Platforms->Google Workspace->Single Sign-On (SSO)**.
3. Enable **Google Workspace SSO**.
4. Save the configuration.

Users will be unable to use the SSO feature if there are no linked PBX users/extensions.



Google Workspace Single Sign-on (SSO) Tab

Once enabled, the PBX will use Google authentication for linked users, and the **Sign in with Google** option will appear on the PBX login page.

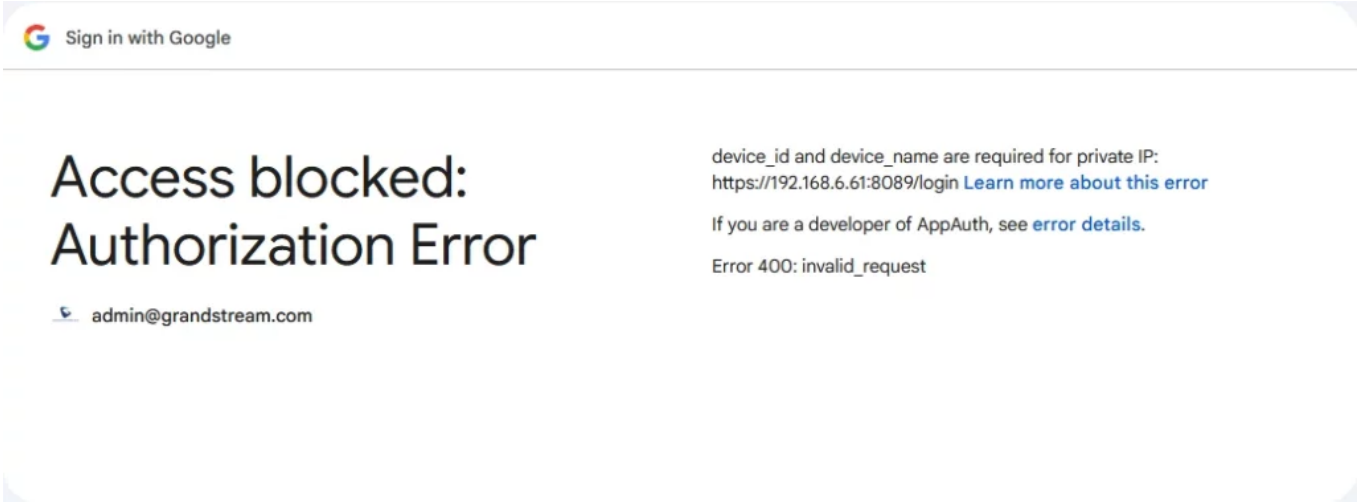


Log in with Google Option

Verify SSO Login

To validate SSO functionality, please refer to the steps below:

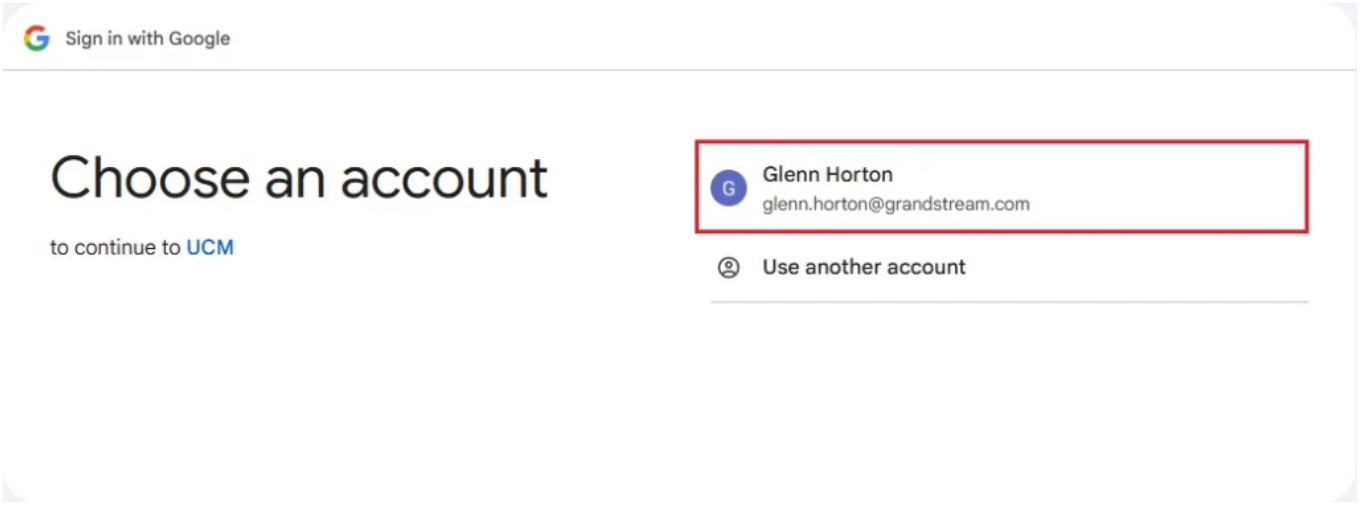
1. Open the PBX login page using the configured **public FQDN** (https://pbx.example.com). If a private IP is used, Google will block the OAuth request and display the following error.



SSO Private IP Access Error

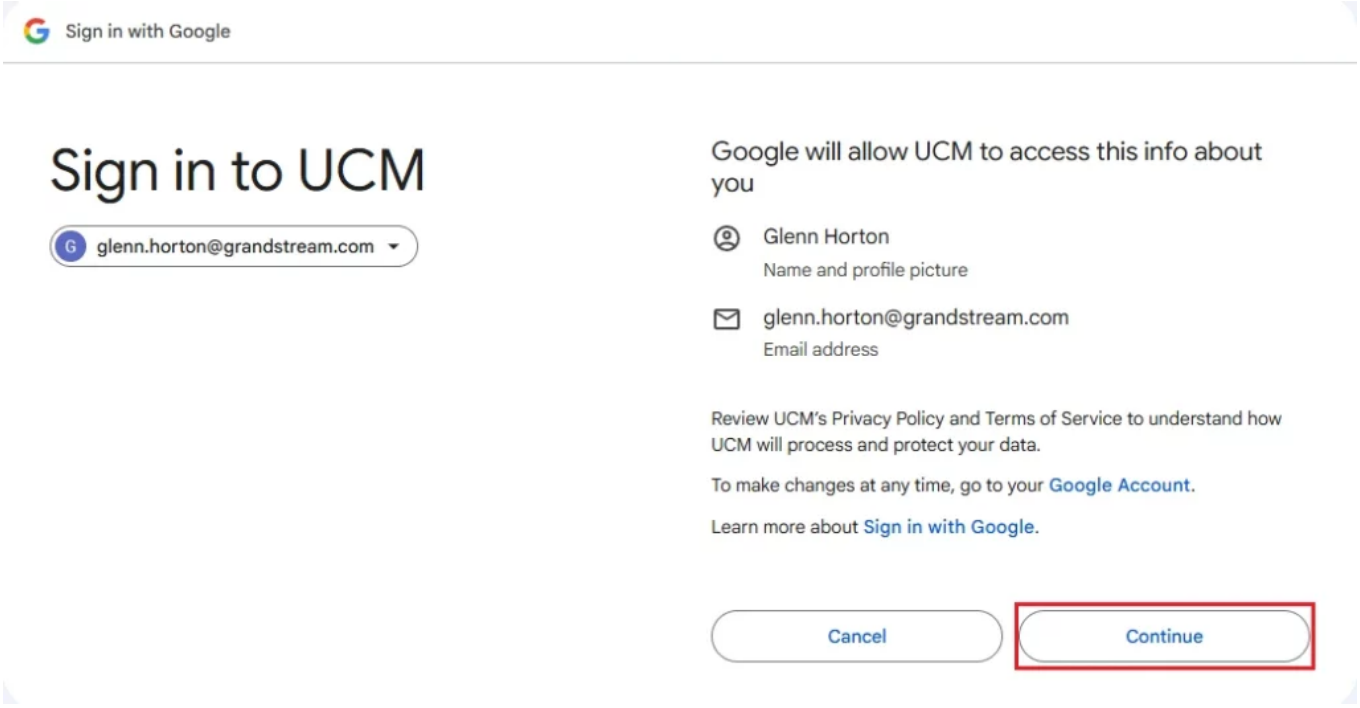
2. Click **Sign in with Google**.
3. Sign in using a Google Workspace account that:

- Exists in the Workspace domain.
- Has been retrieved under User Settings.
- Is linked to a PBX user or extension.

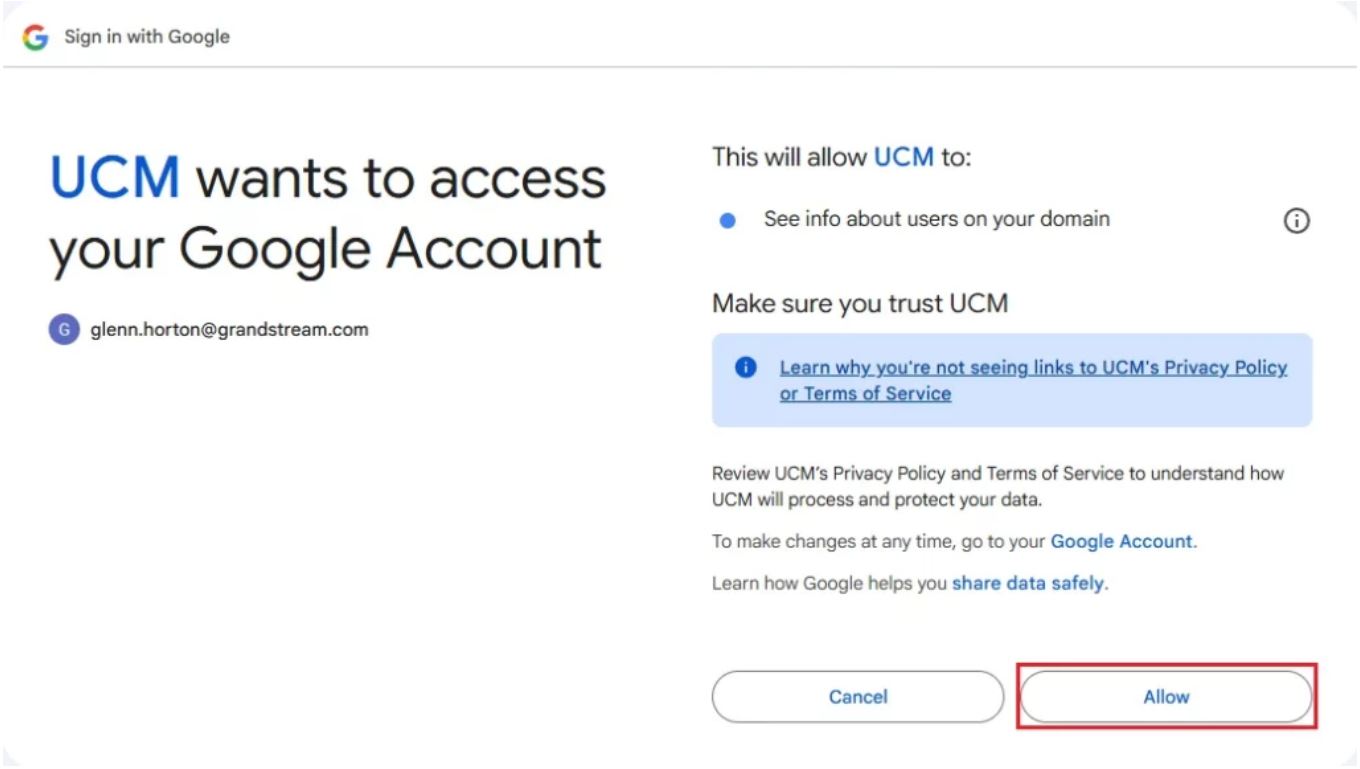


SSO Login - Google Account Selection

4. Grant consent if prompted.



SSO Login - Google Authentication Confirmation



SSO Login - Google Consent Screen

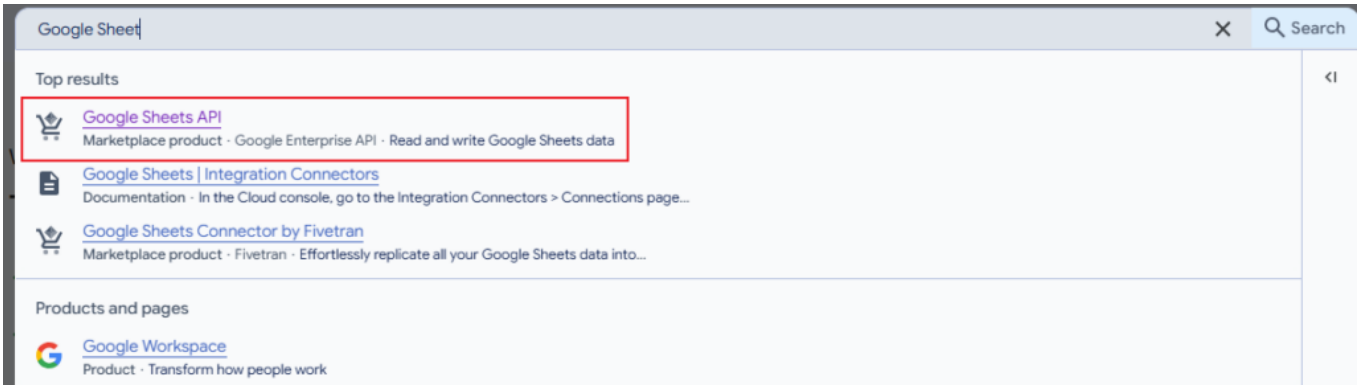
If the configuration is correct, the user is redirected back to the PBX and logged in under the mapped user account.

CDR Synchronization to Google Sheets

Using this integration, the administrator can configure to have the CDR synchronized to Google Sheets. A new spreadsheet will be create everyday to synchronize all the CDR of that day.

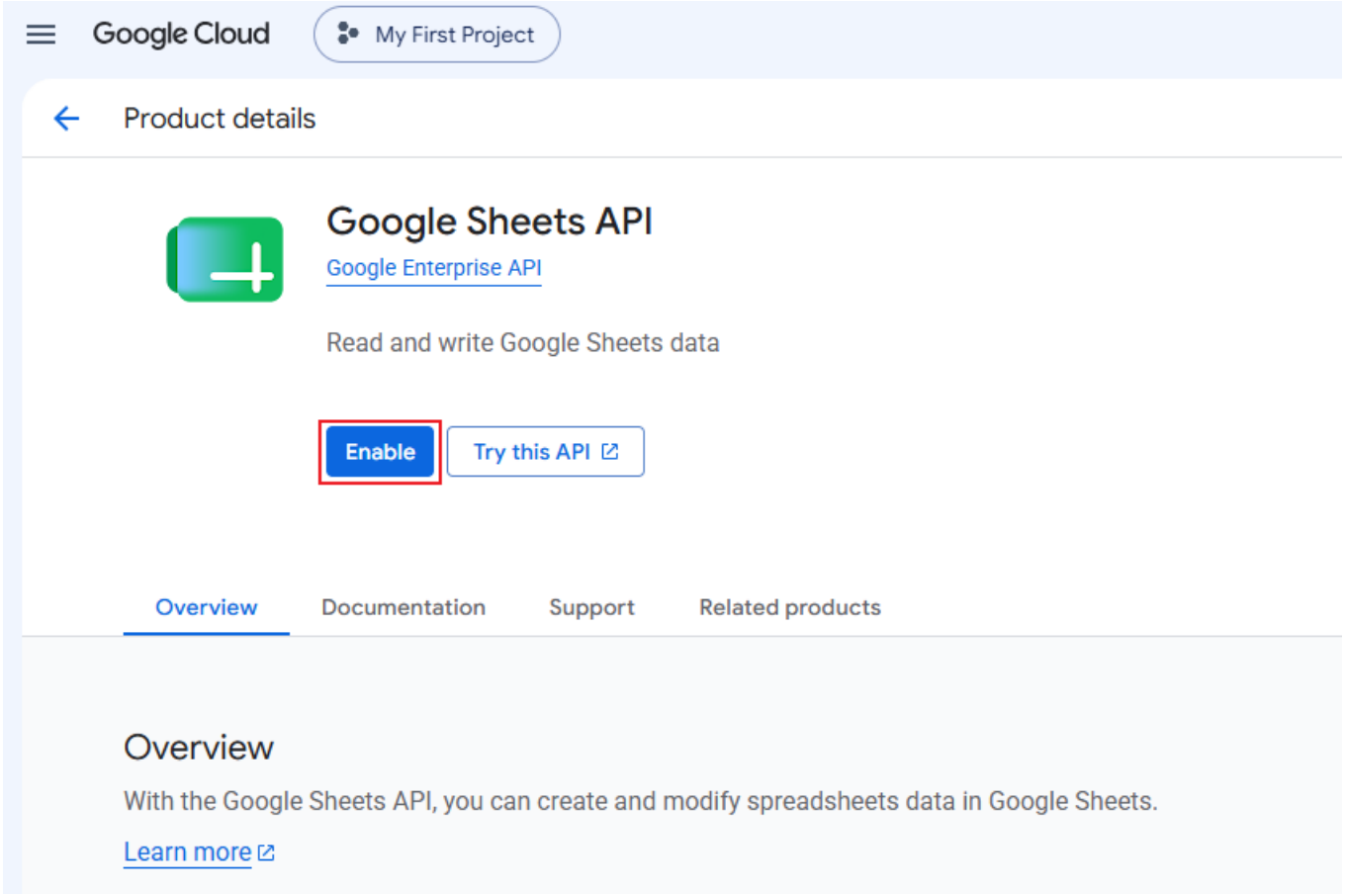
For the configuration of this feature, follow the steps below.

1. On Google Cloud Console, search "Google Sheets API". Click on the market place product.



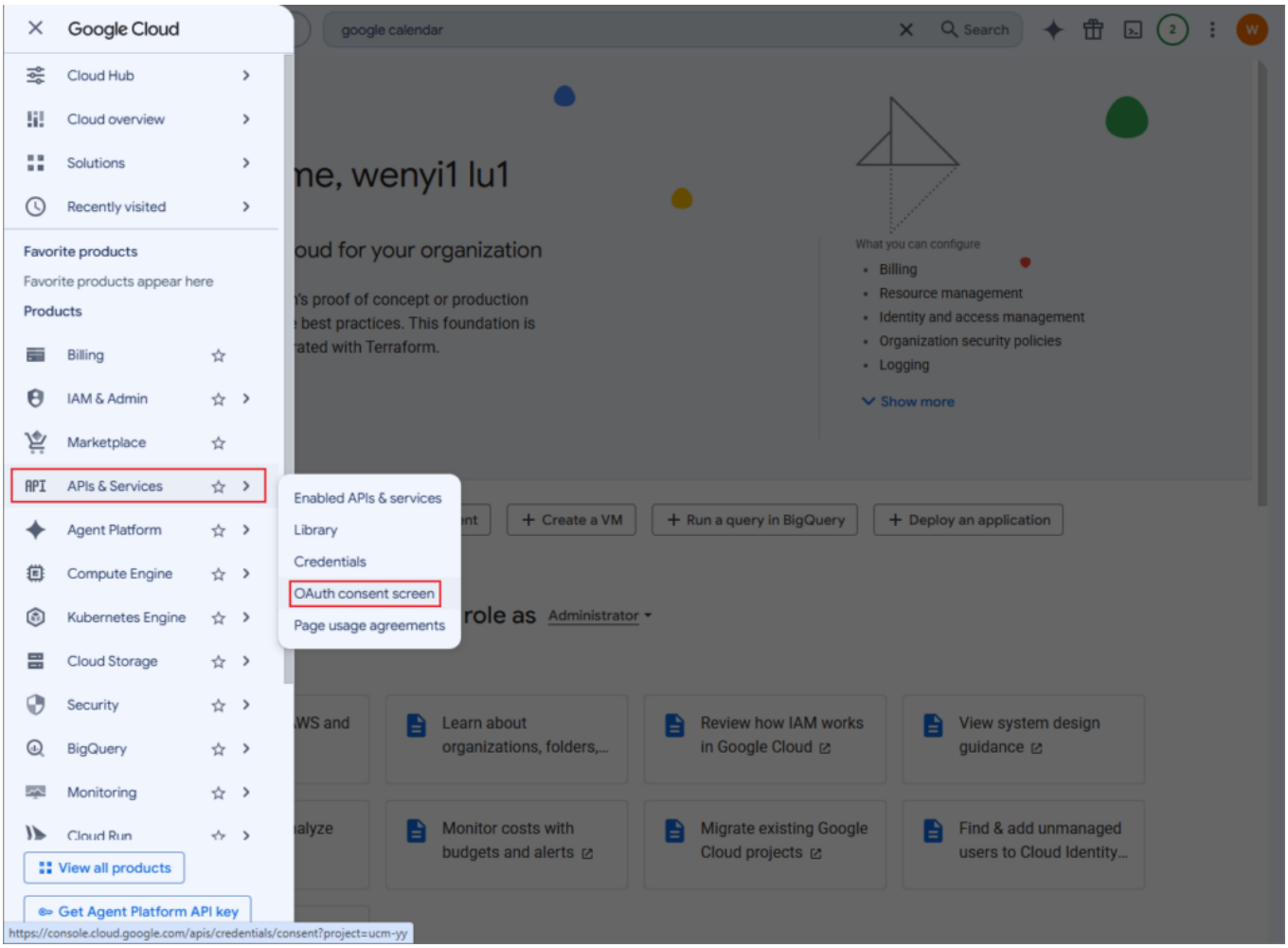
Google Cloud Console Search

2. Click "Enable" to activate Google Sheets API.



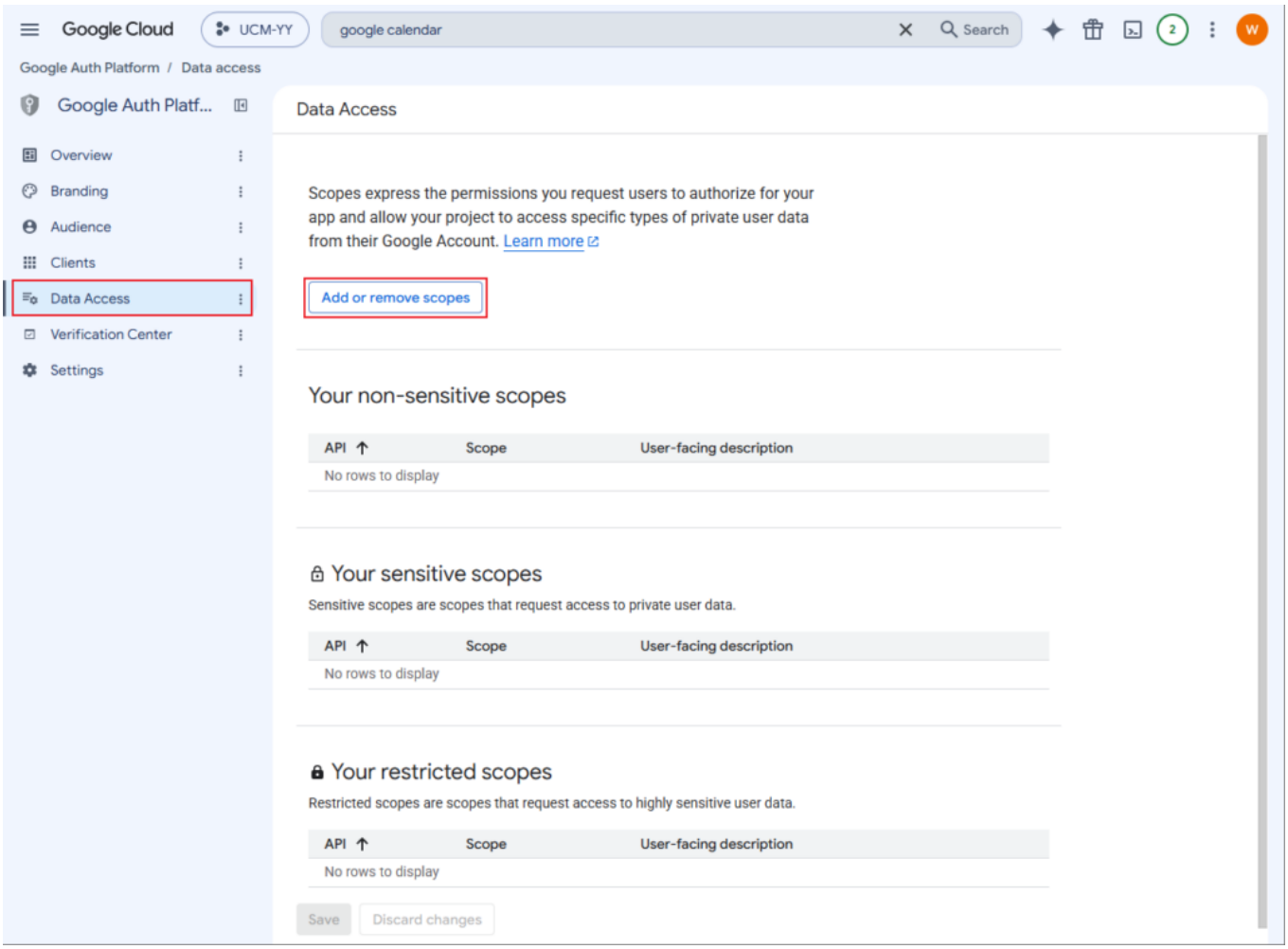
Google Sheets API

3. On the sidebar, hover the mouse cursor on "APIs & Services" then click on"OAuth consent screen".



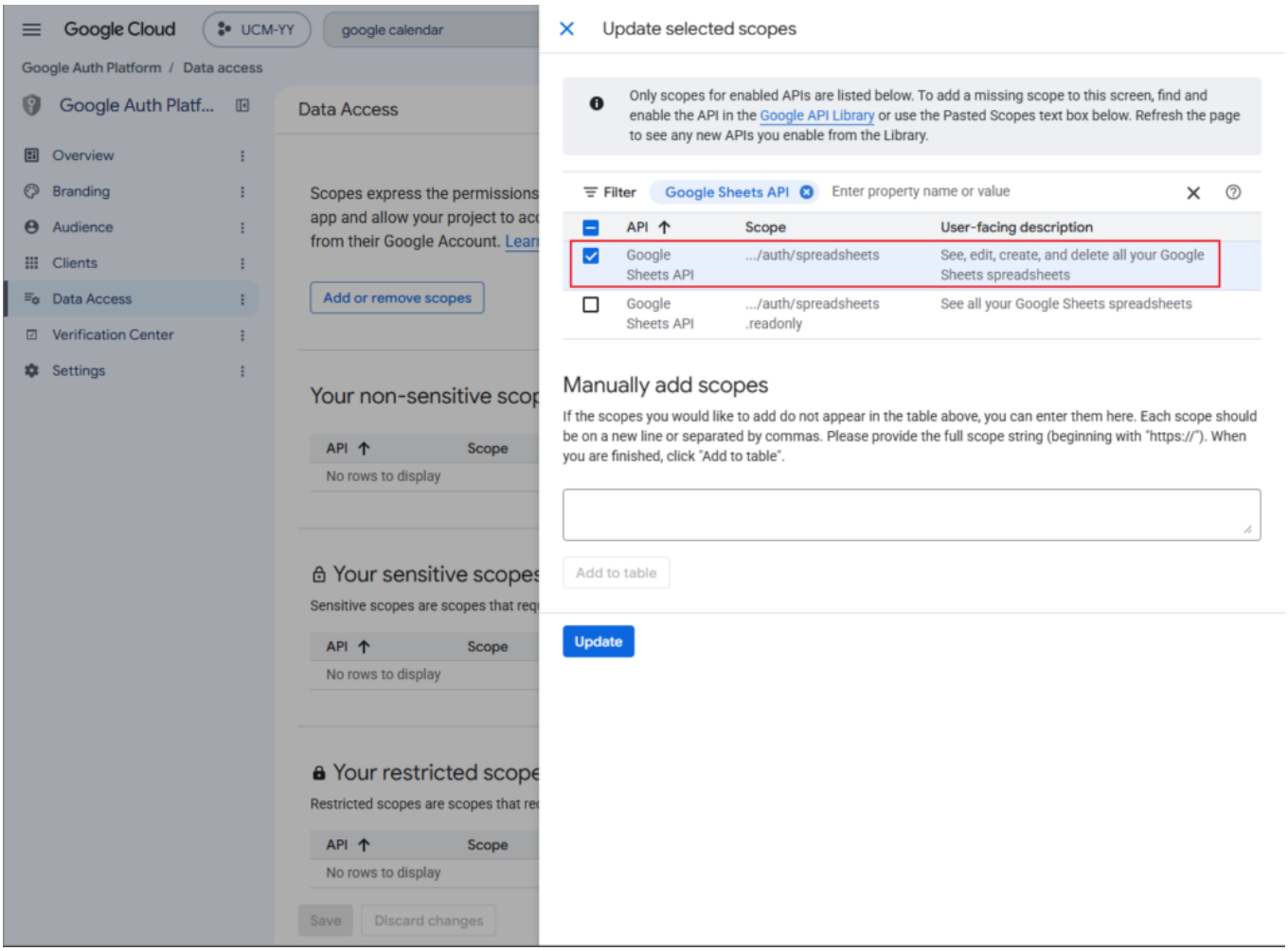
Google Cloud Console

4. Click on "Data Access on the side bar, then click "Add or remove scopes" button.



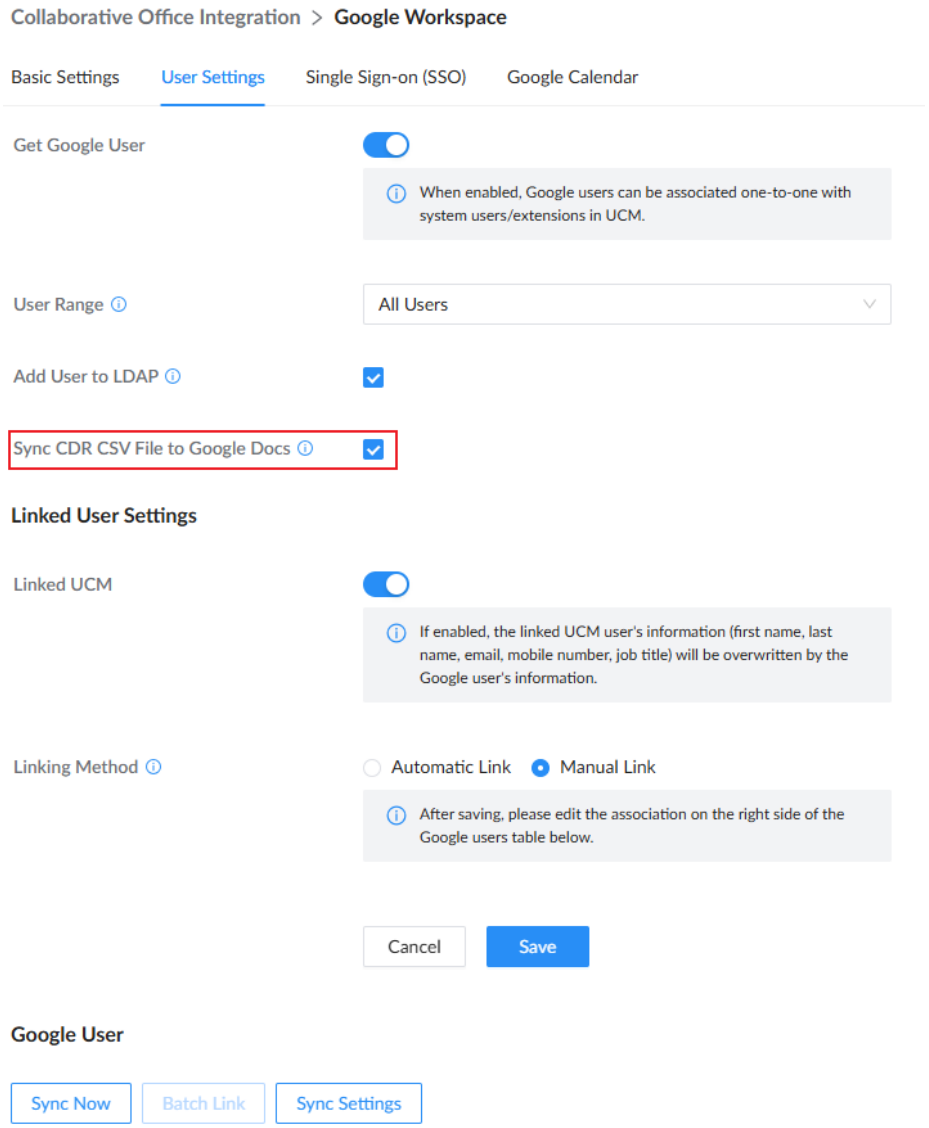
Data Access

5. On the search bar, type "Google Sheets API" and from the results, select the scope highlighted below.



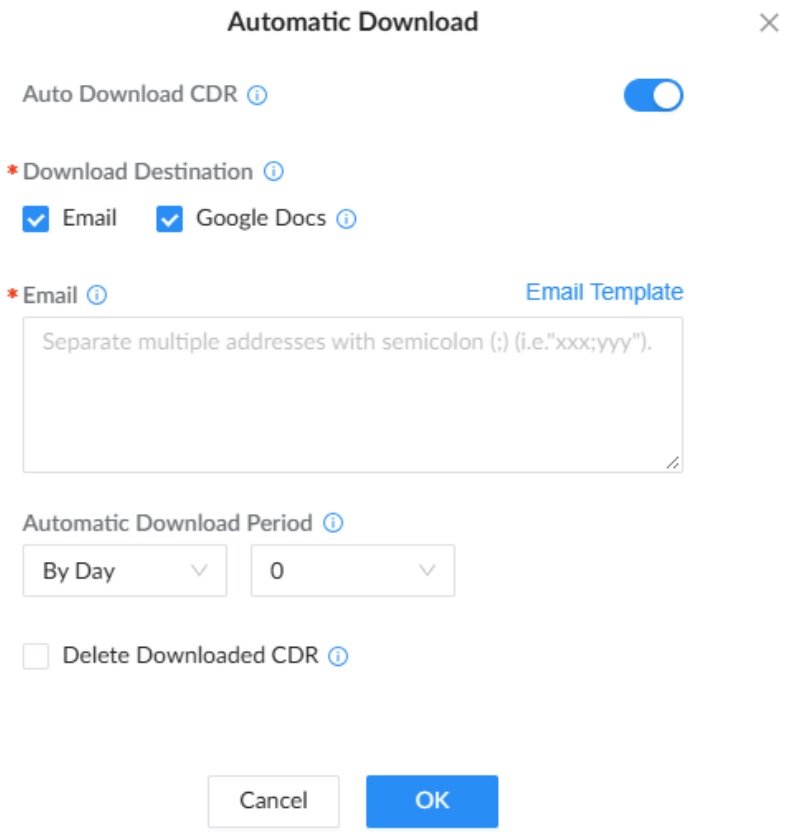
Add Scope

6. On the UCM, Navigate to **Integrations > Google Workspace** then click on the button "Integration", after that navigate to **User Settings** tab and find the option highlighted below and enable it.



Google Workspace - User Settings

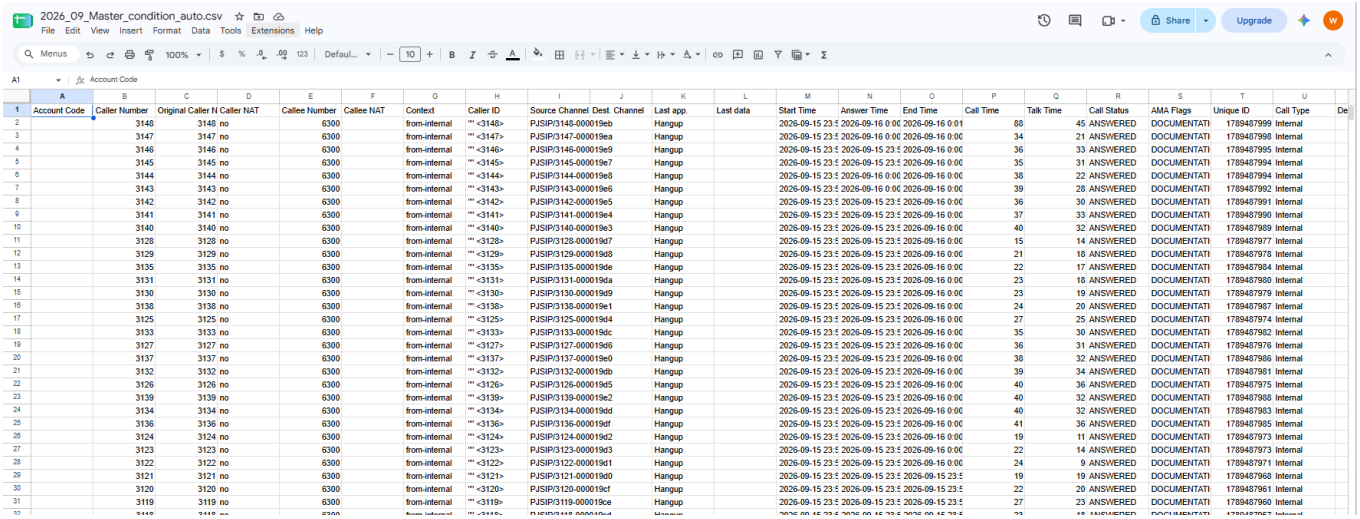
7. Then navigate to **CDR > CDR**, then click on "Automatic Download" and enable "Google Docs" as a download destination.



CDR Automatic Download

The sheets created in each spreadsheet is affected by the option "Automatic Download Period". E.g., If it is set to "Daily" then one new sheet will be created each day.

You can view the CDR spreadsheet by going to your Google Sheets and the record of call details will be logged same as the following figure.



CDR - Google Sheets

GOOGLE-CALENDAR-BASED ROUTING

Overview

The Google Calendar-based call routing feature is an extension of the UCM call routing functionality. In modern hybrid work environments, an employee's work status (e.g., in a meeting, at their desk) directly impacts the calling experience. This section explains how to enable smart routing based on Google Calendar schedules. By automatically synchronizing and analyzing users' Google Calendar events, the UCM can determine when to automatically enable the "Do Not Disturb" presence status for a user, thereby activating the call policy configured for that status. This avoids high-frequency invalid ringing and optimizes the customer waiting experience through automated rules, making communication workflows better aligned with actual business rhythms.

Prerequisites

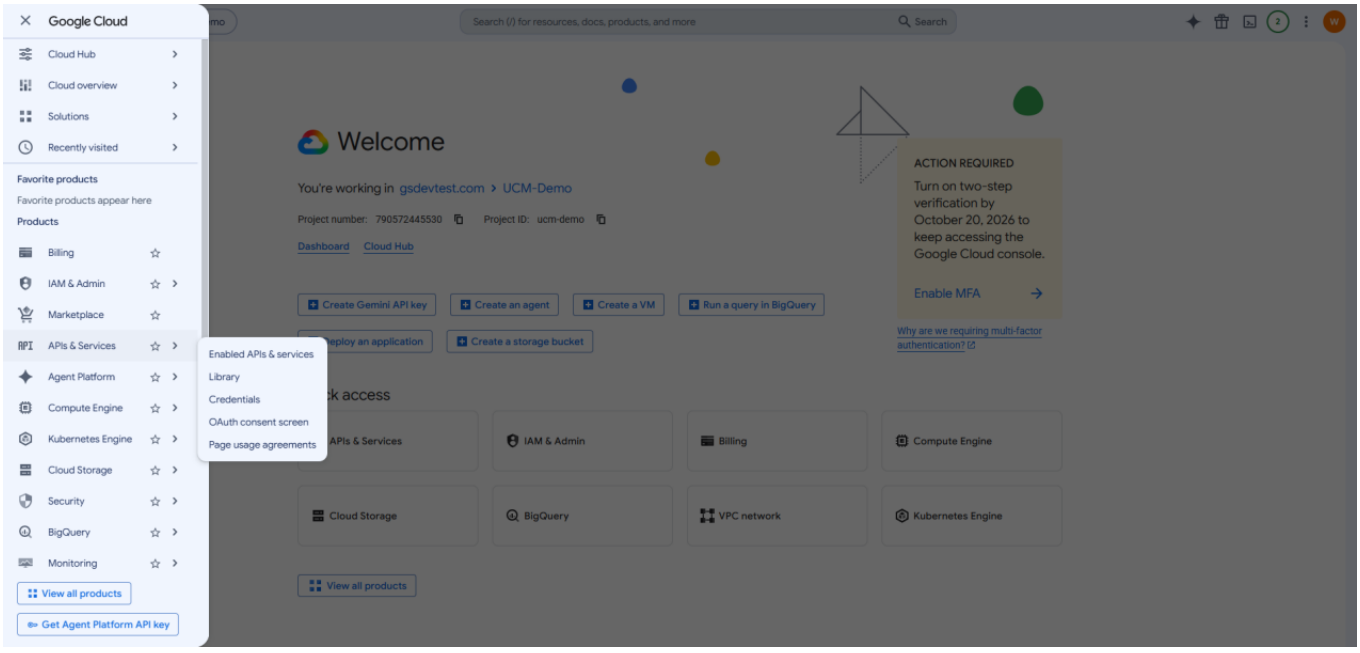
Google Calendar integration serves as an extension of Google Workspace capabilities.

- If your UCM has not yet integrated with Google Workspace, please refer to the section [GOOGLE WORKSPACE INTEGRATION].
- The subsequent features in this section assume that the UCM has successfully integrated with Google Workspace.

Enabling Google Calendar API

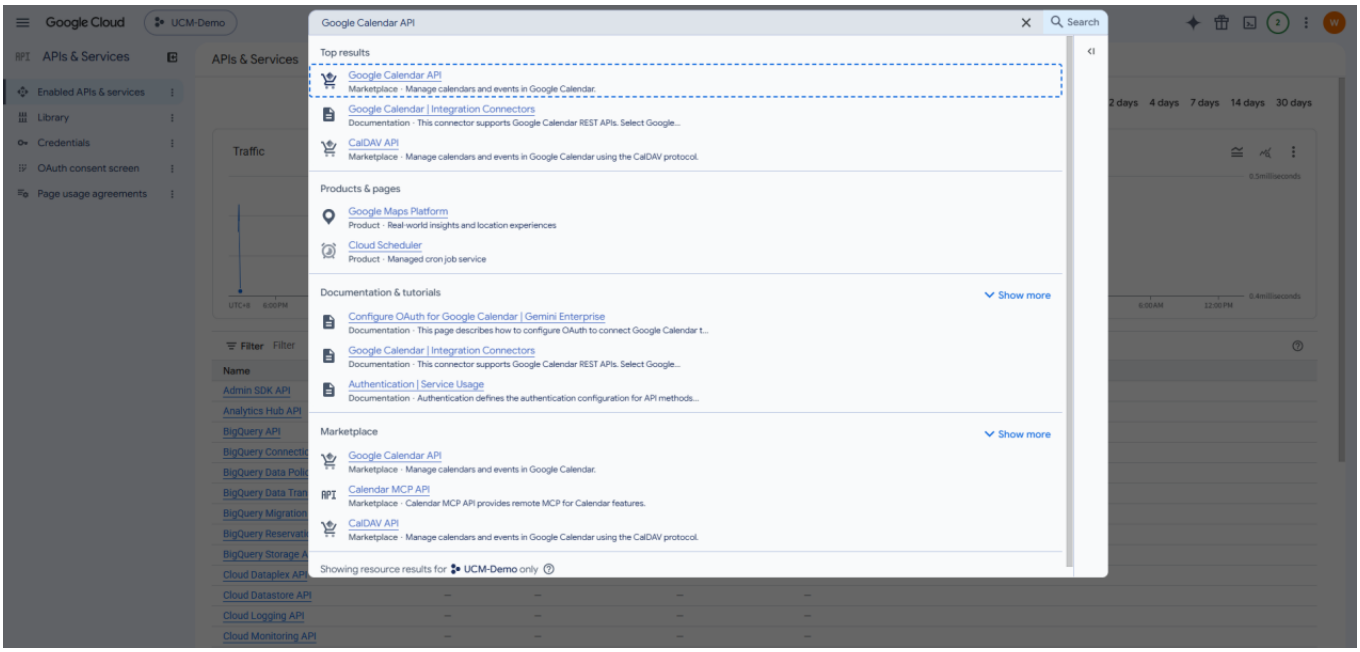
Log into https://console.cloud.google.com using an Admin account, select the project associated with your UCM. Navigate to the API configuration page via the navigation bar and enable the Google Calendar API.

1. From the side bar, click on "APIs & Services" then click on "Enabled APIs & Services".



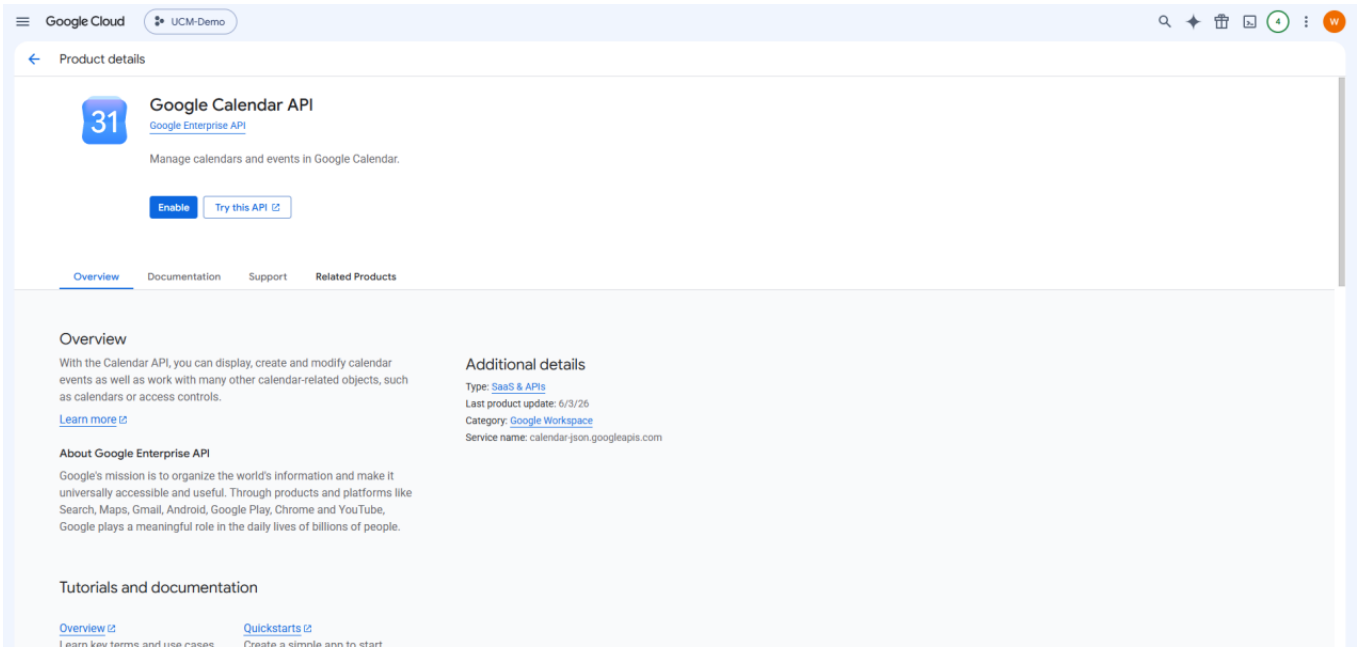
Google Cloud Home Page

2. Click on the search button and look up "Google Calendar API".



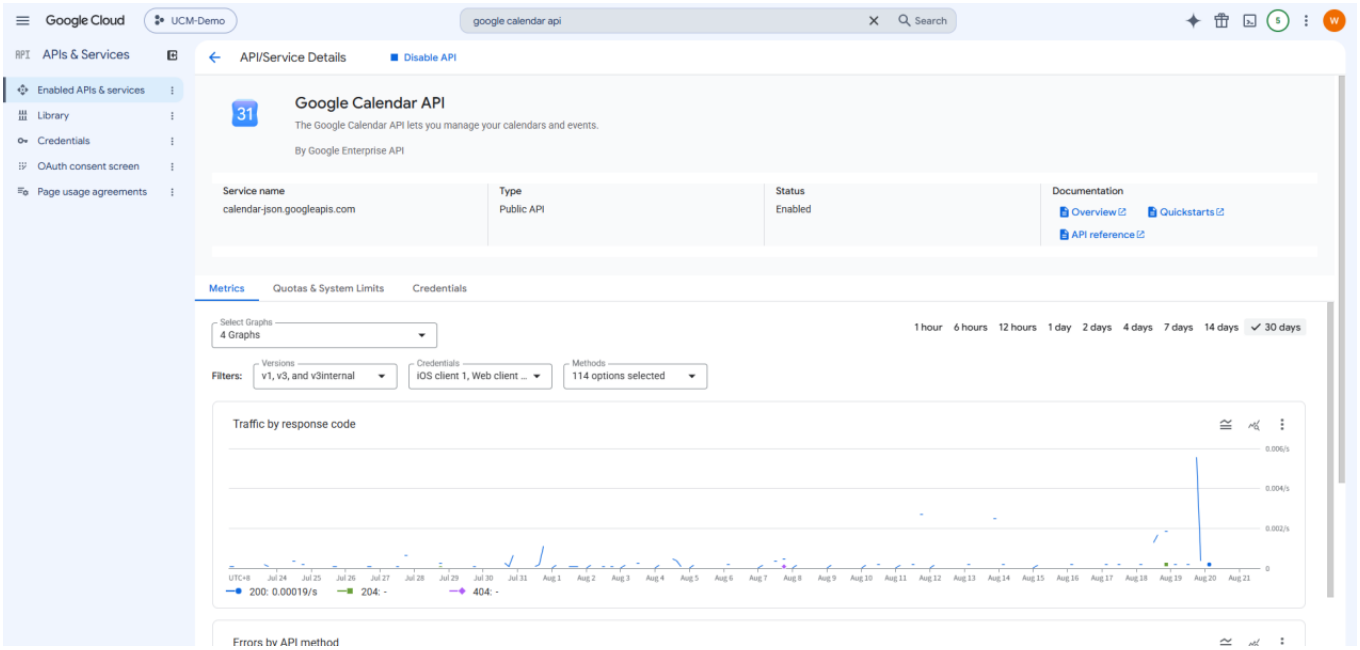
Google Cloud APIs and Services

3. Click on "Enable" after opening the product page.



Enable Google Calendar API

4. Once enabled, the following page will be displayed.

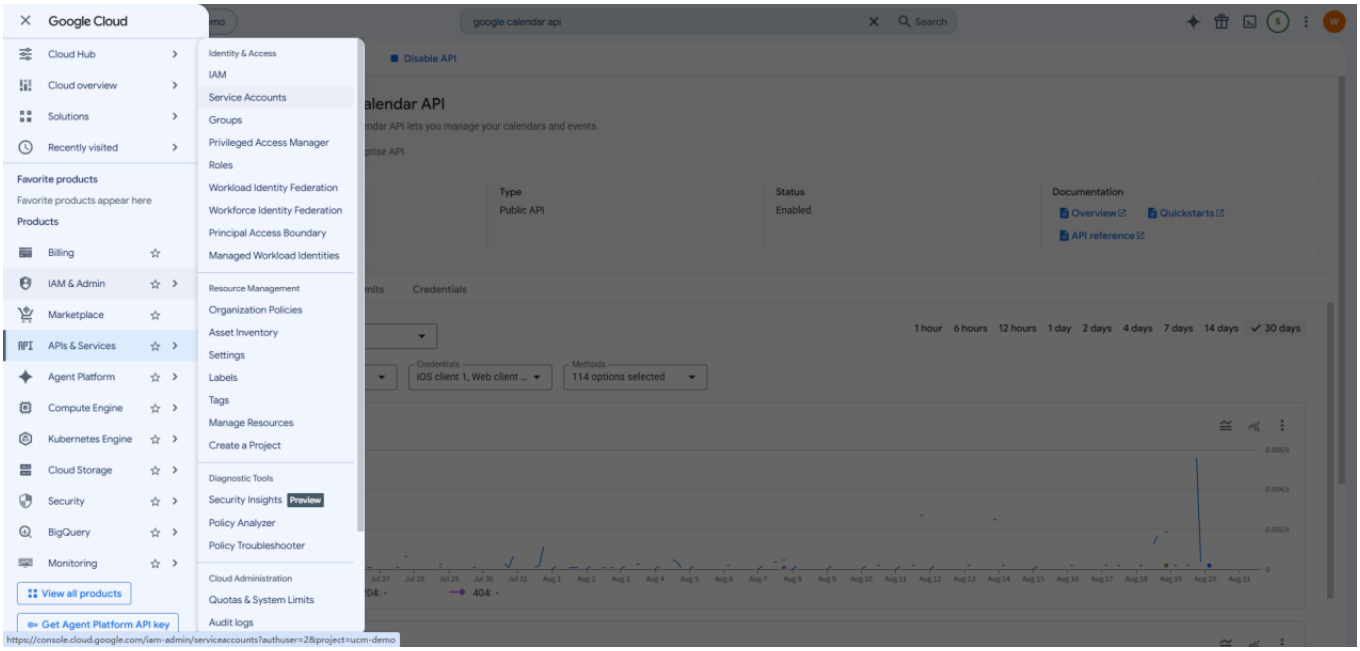


Google Calendar API

Adding Service Account and Key

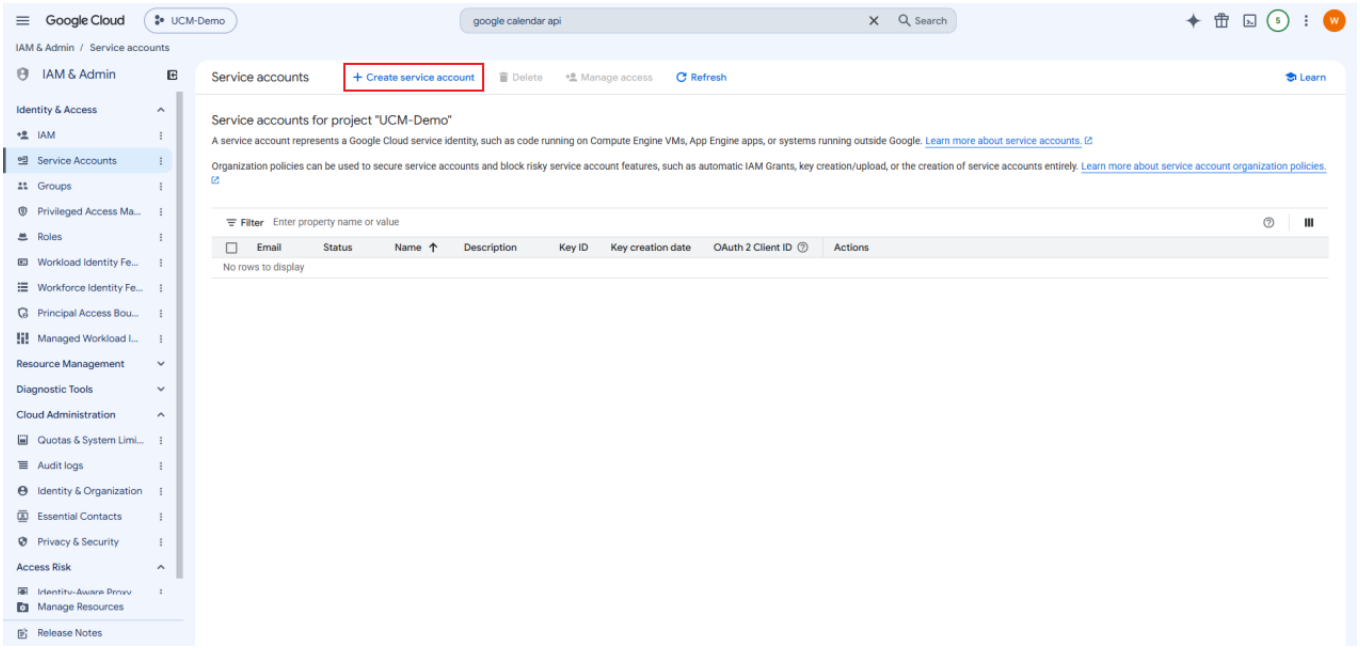
To be able to connect to the API, the administrator should create a service account. The credentials of the services accounts are the information required to authenticate into the server.

1. Open the sidebar then click on "APIs & Services" then click on "Service Accounts".



Service Accounts

2. Click the button "Create service account".

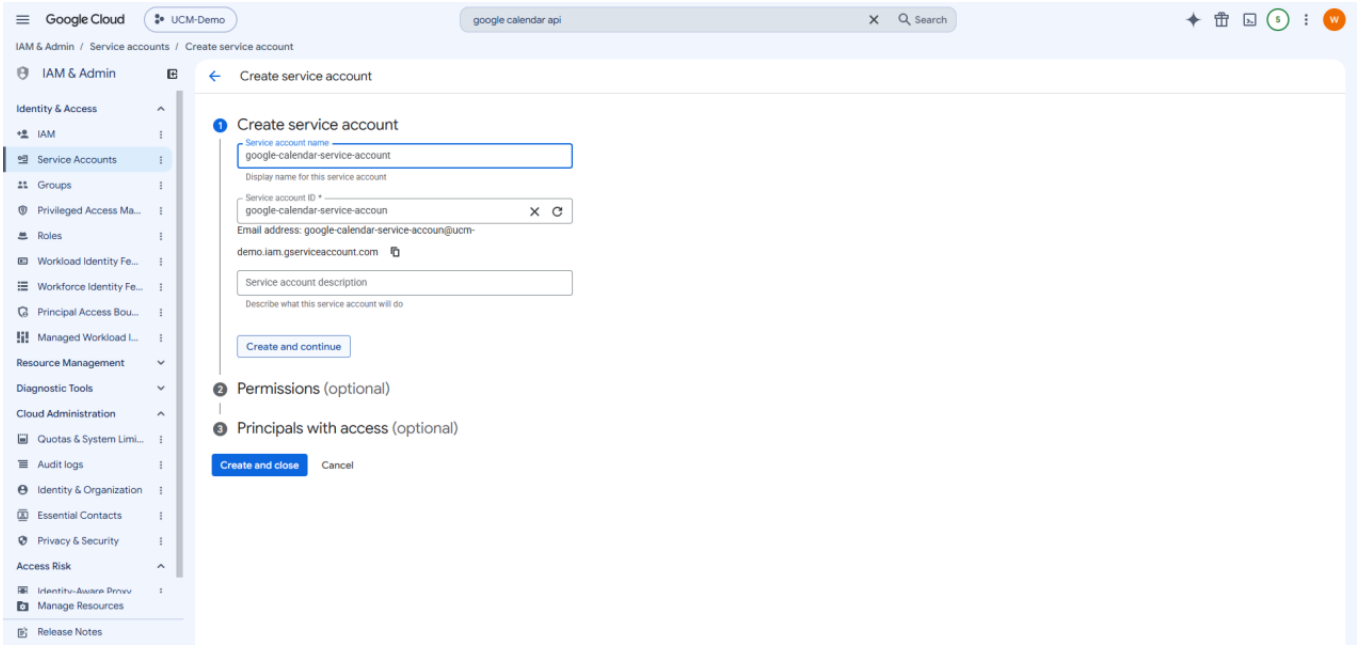


Service Account Creation

3. Enter the following information in the respective fields.

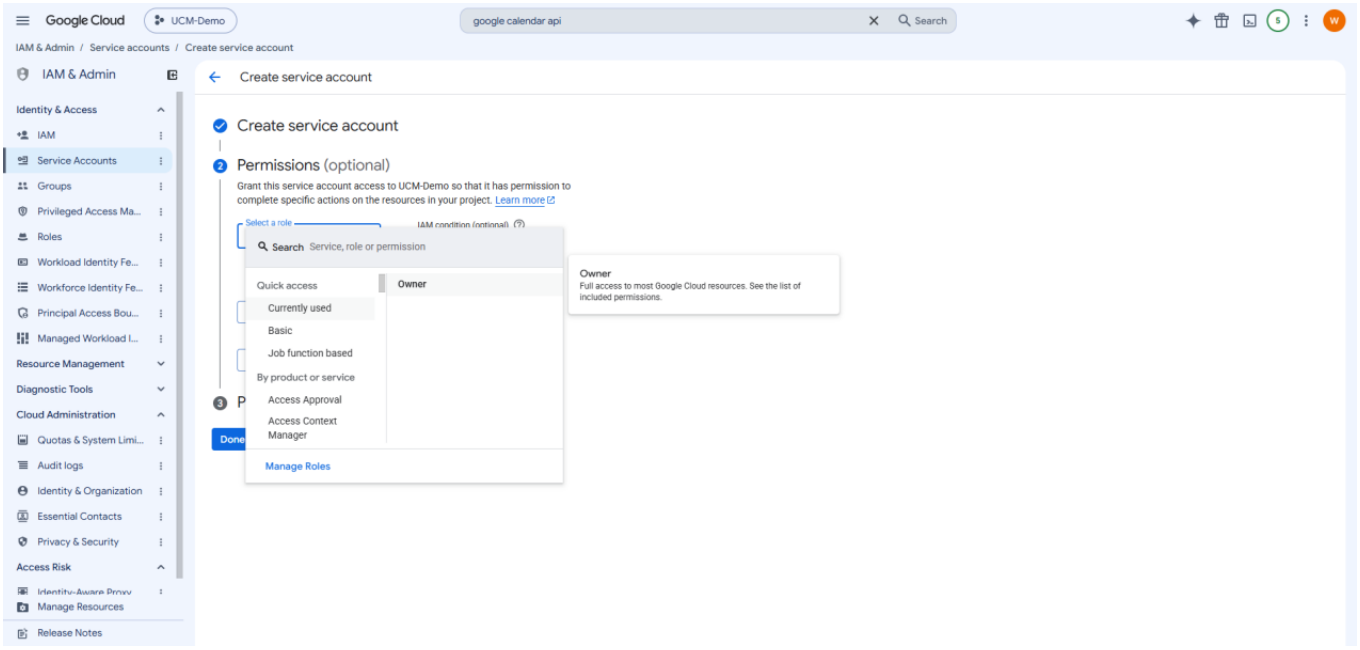
- **Service account name**: Enter a unique name to help easily identify this account.
- **Service account ID**: Enter the ID of the account.
- **Service account description**: Describe the purpose of this account.

4. Once the fields are configured, click on "Create and continue".



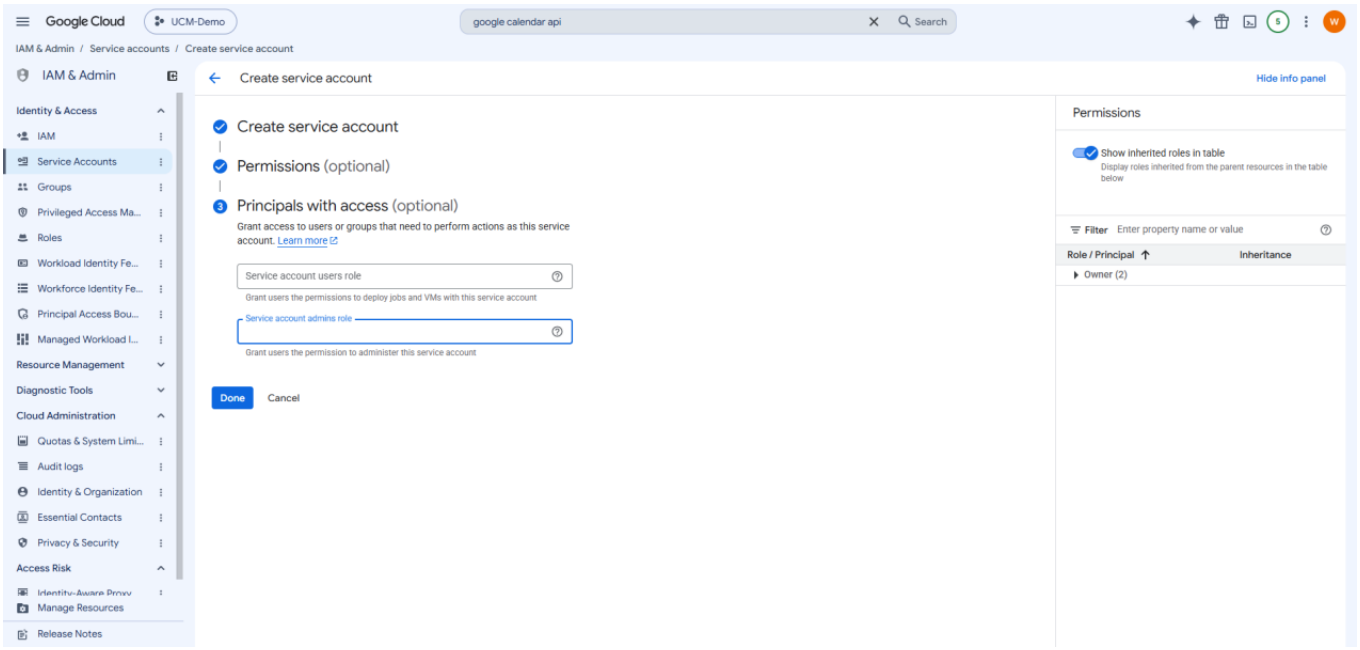
Service Account Configuration

5. In the role field, select "Owner", then click on "Create and continue".



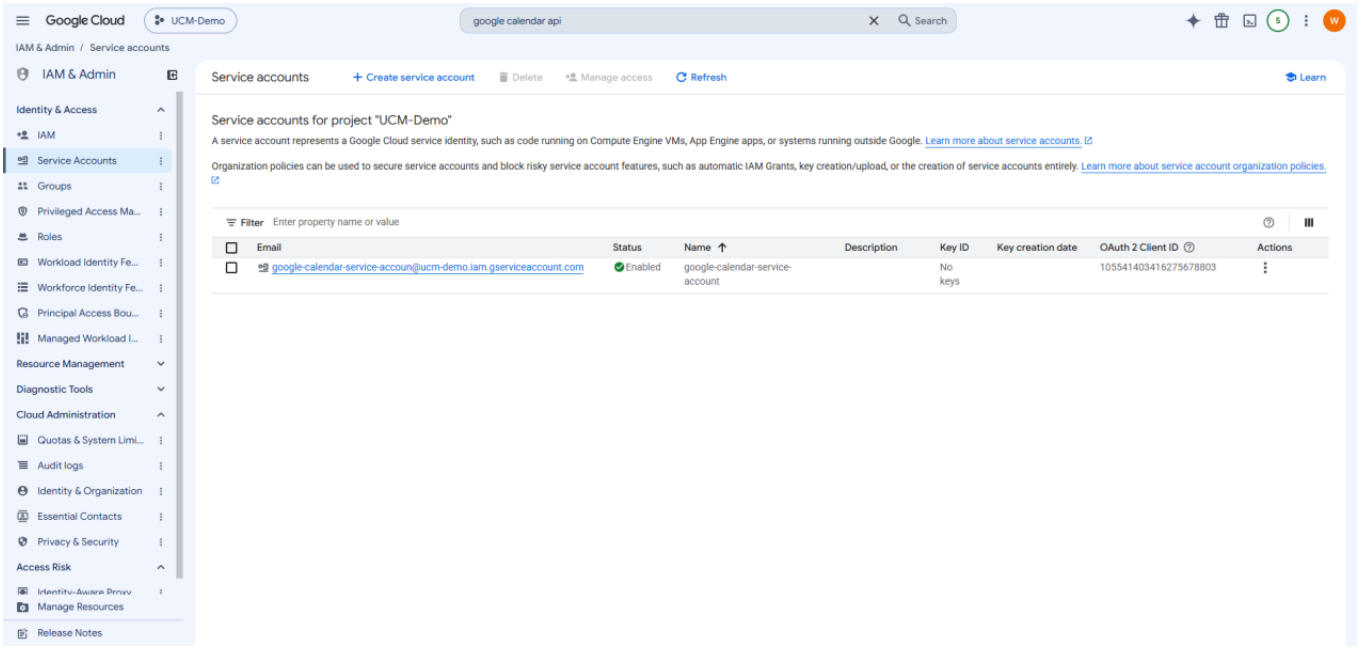
Service Account Permissions

6. Click on "Done".



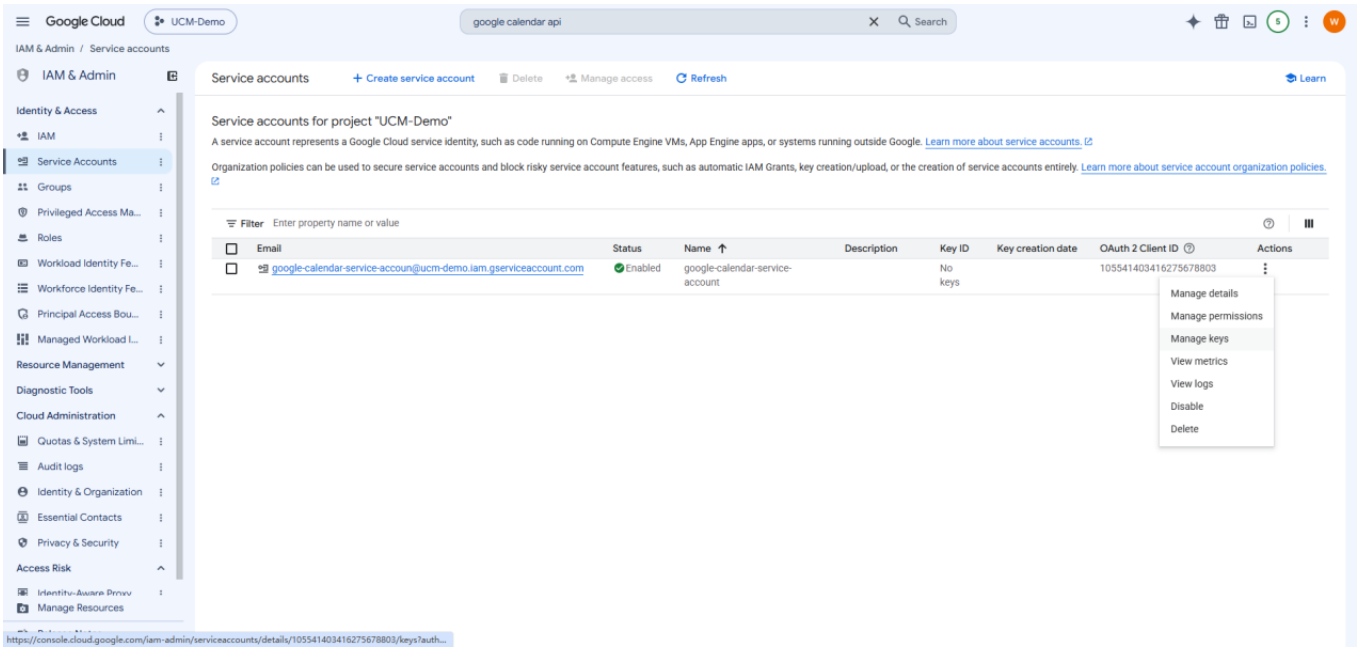
Service Account Principals with Access

The service account will be displayed on the list, as shown in the screenshot below.



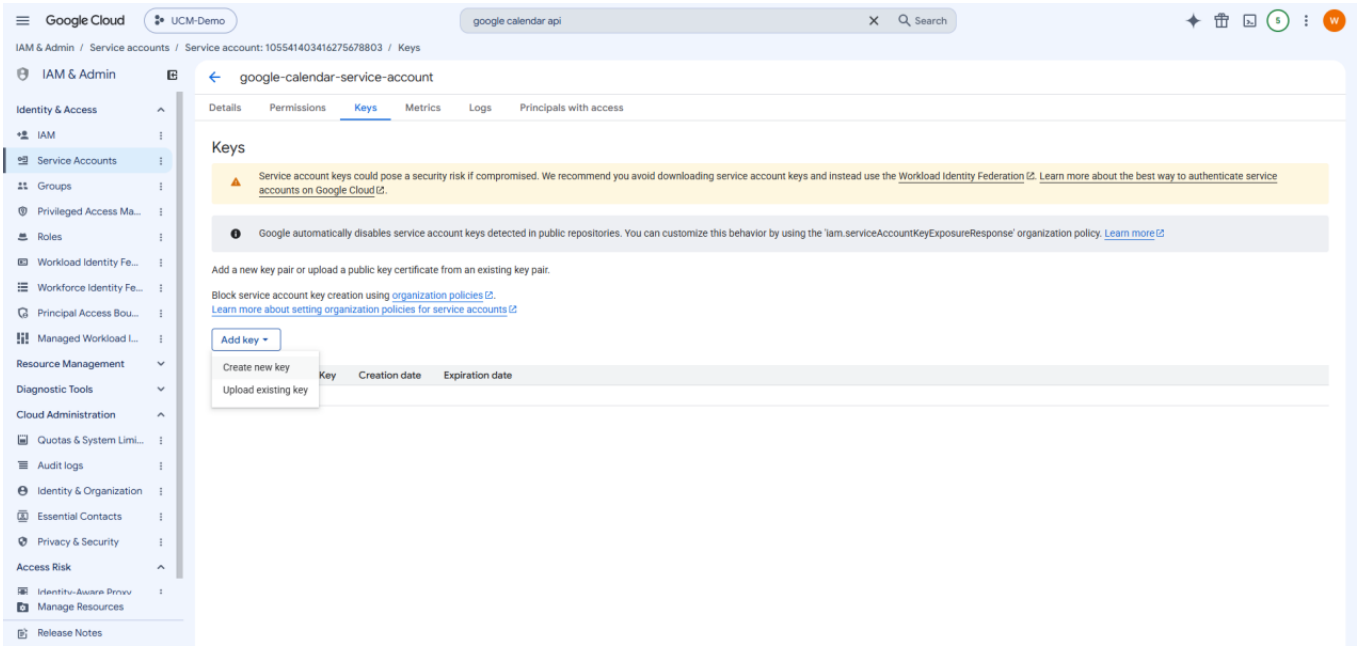
Service Account Created

7. Click on the three-dot button then click on "Manage keys".



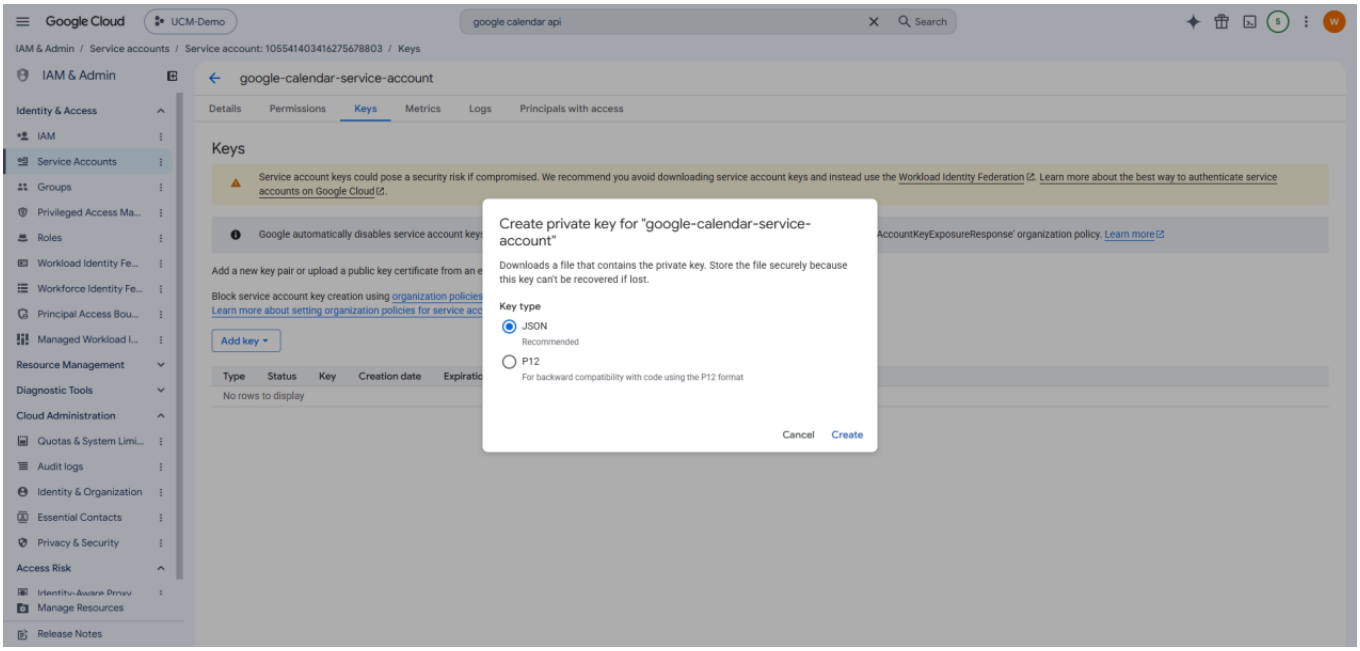
Manage Keys

8. Click on "Add key", then click on "Create new key".



Create New Key

9. Select "JSON", then click Create.

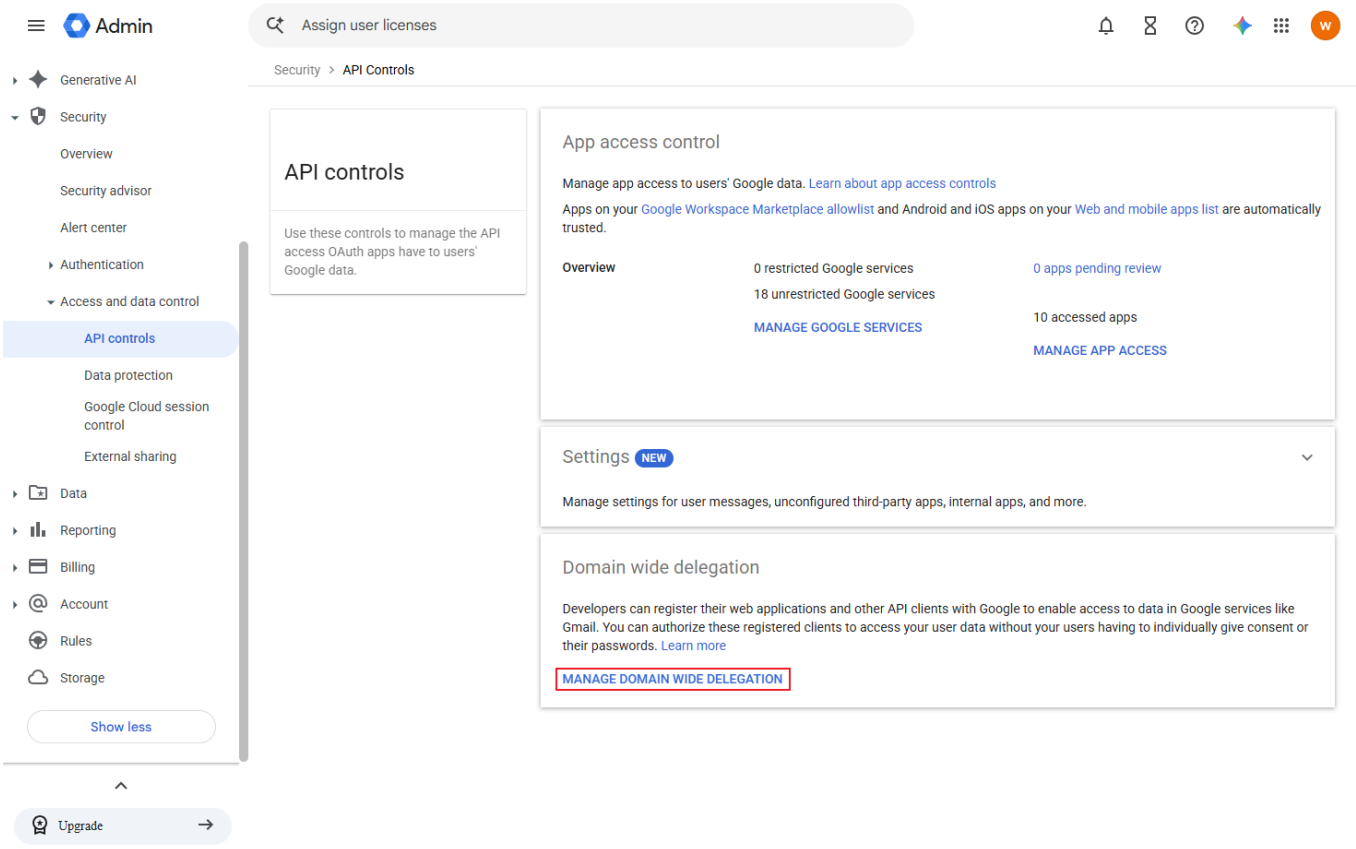


Select Key Type

Once the steps above are completed, a JSON-formatted key file will be created and save locally. Keep this key confidential and store it safely.

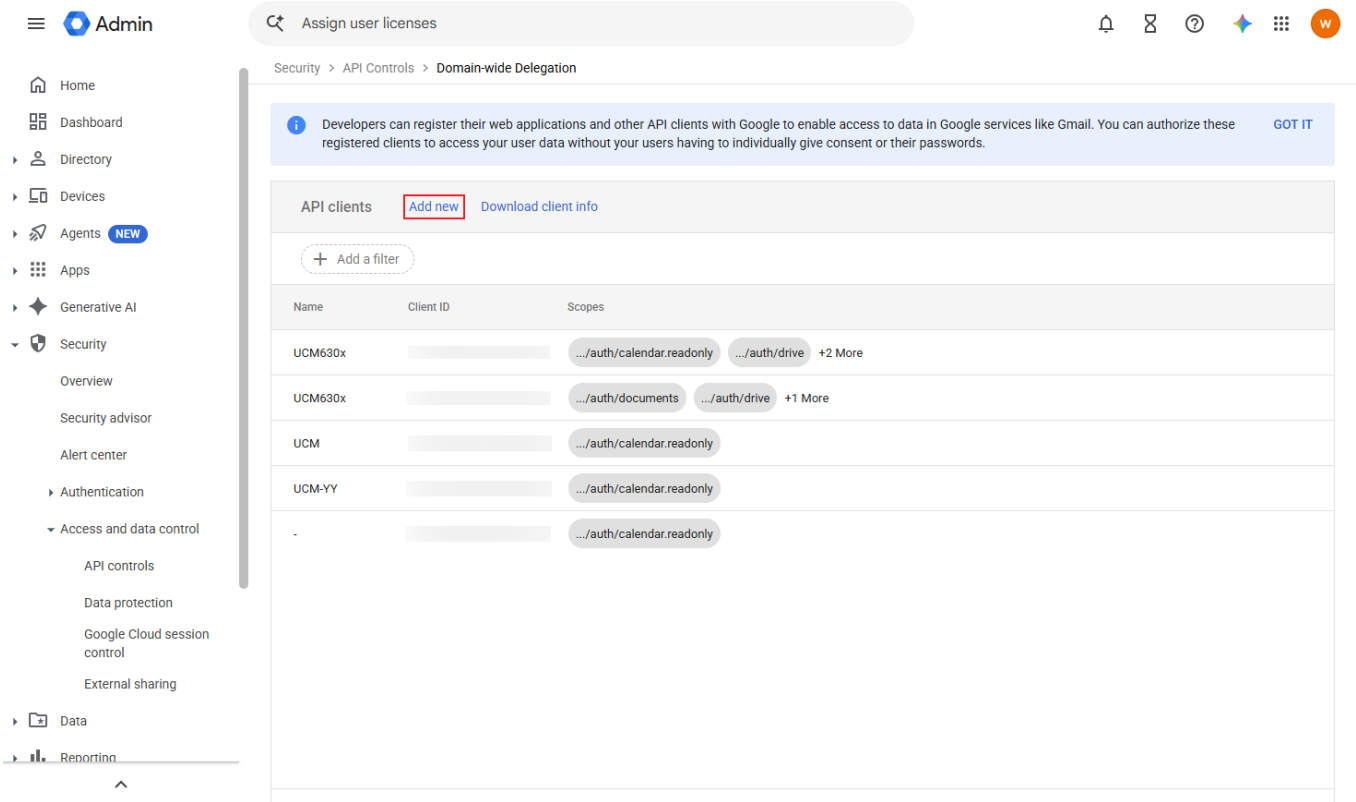
Enable Domain-wide Delegation

1. Log in with your Admin account https://admin.google.com, and use the navigation bar to navigate to **Security > Access and data control > API controls**, then click on "Manage Domain Wide Delegation".

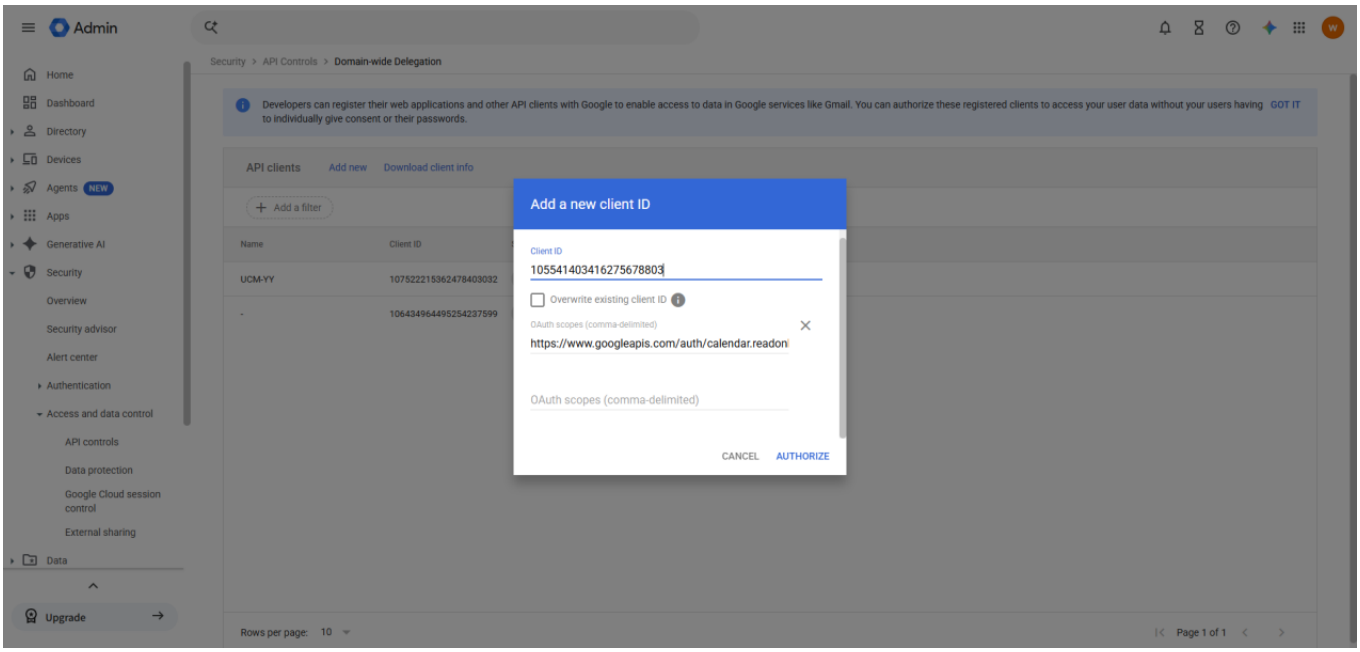


API Controls

2. Click on "Add new" to create a new ID along with its scope.



Add New API Client



Client ID & OAuth Scopes

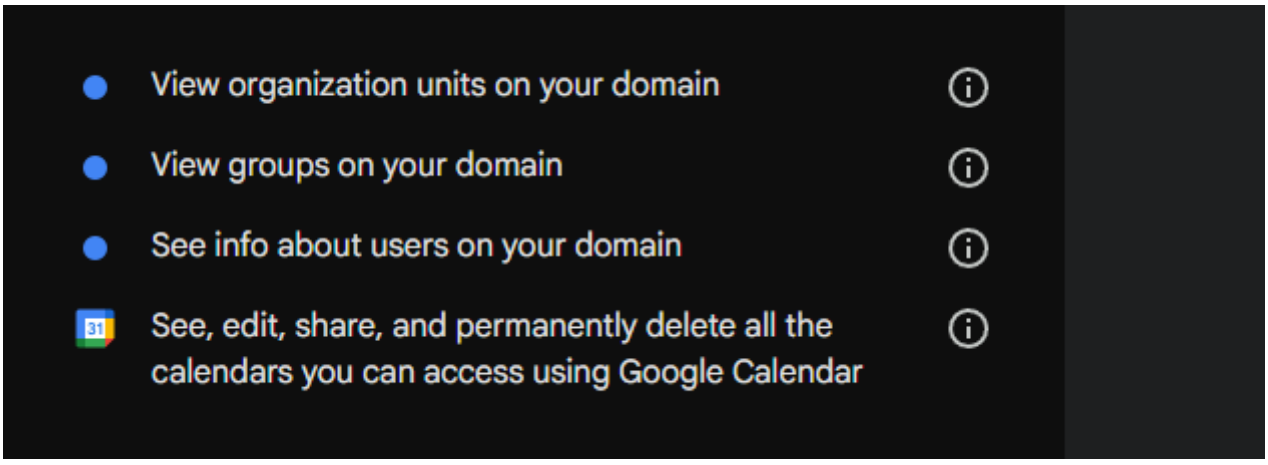
Use the following OAuth scope for reading the calendar events "https://www.googleapis.com/auth/calendar.readonly". Remove the quotation marks when copying the scope.

For more information regarding the scopes of OAuth, please refer to the following link: https://developers.google.com/identity/protocols/oauth2/scopes#calendar

If you want the UCM to promptly detect the events you add/delete/modify in Google Calendar, you need to enable WebHook and complete the following steps in the section below. Use the anchor referenced in the section below to view the steps required to configure a webhook.

Google Workspace OAuth2

If your UCM has already completed integration with Google Workspace, please repeat the OAUTH2 authorization steps to ensure you have Google Calendar permissions:

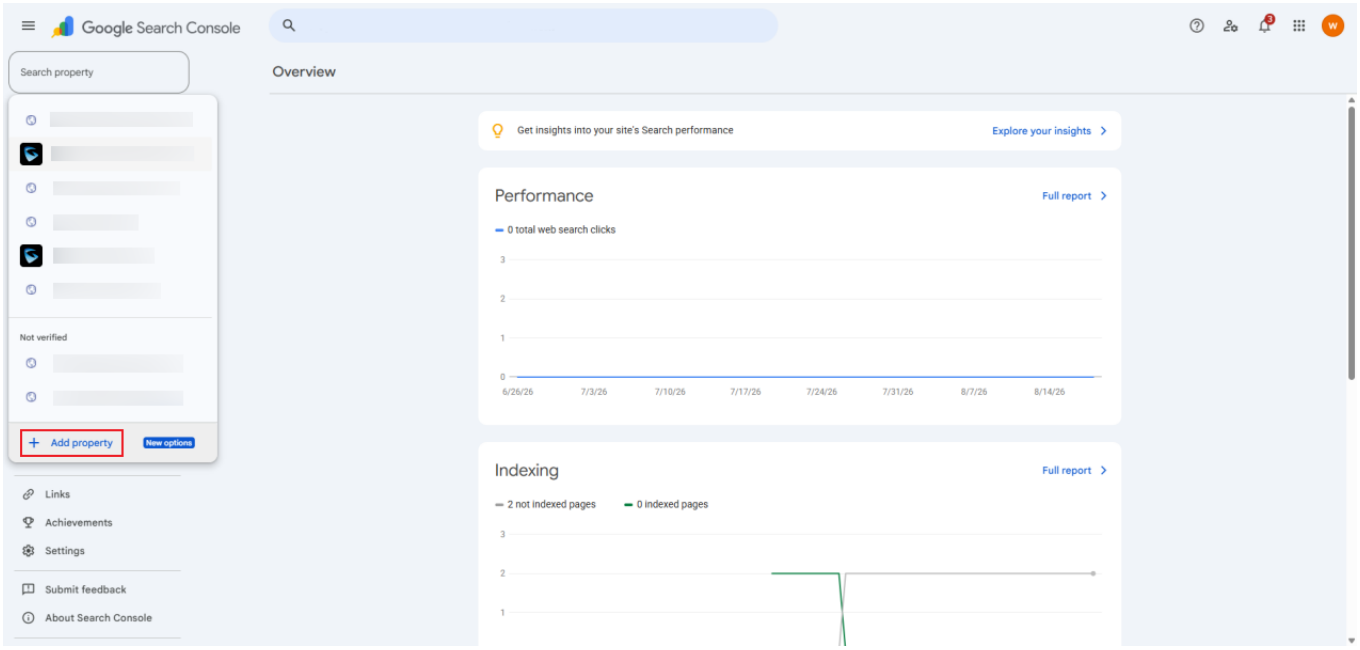


This section [Create OAuth Client Credentials] shows how to create OAuth credentials, please follow the same steps to create OAuth credentials for Google Calendar.

Webhook Domain Name Authentication

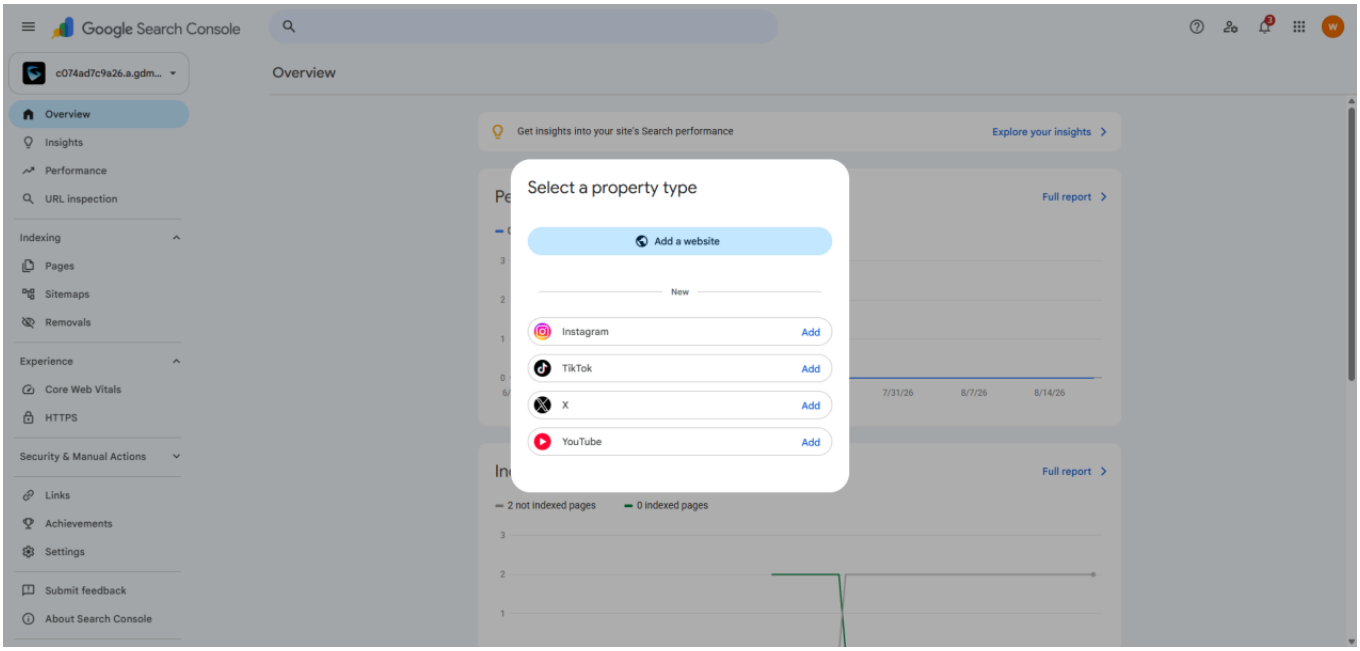
Log in to https://admin.google.com using an Admin account and navigate to the API controls page.

1. On Google Search Console, click on the list of properties (owned domains) on the sidebar, then click on "Add Property".



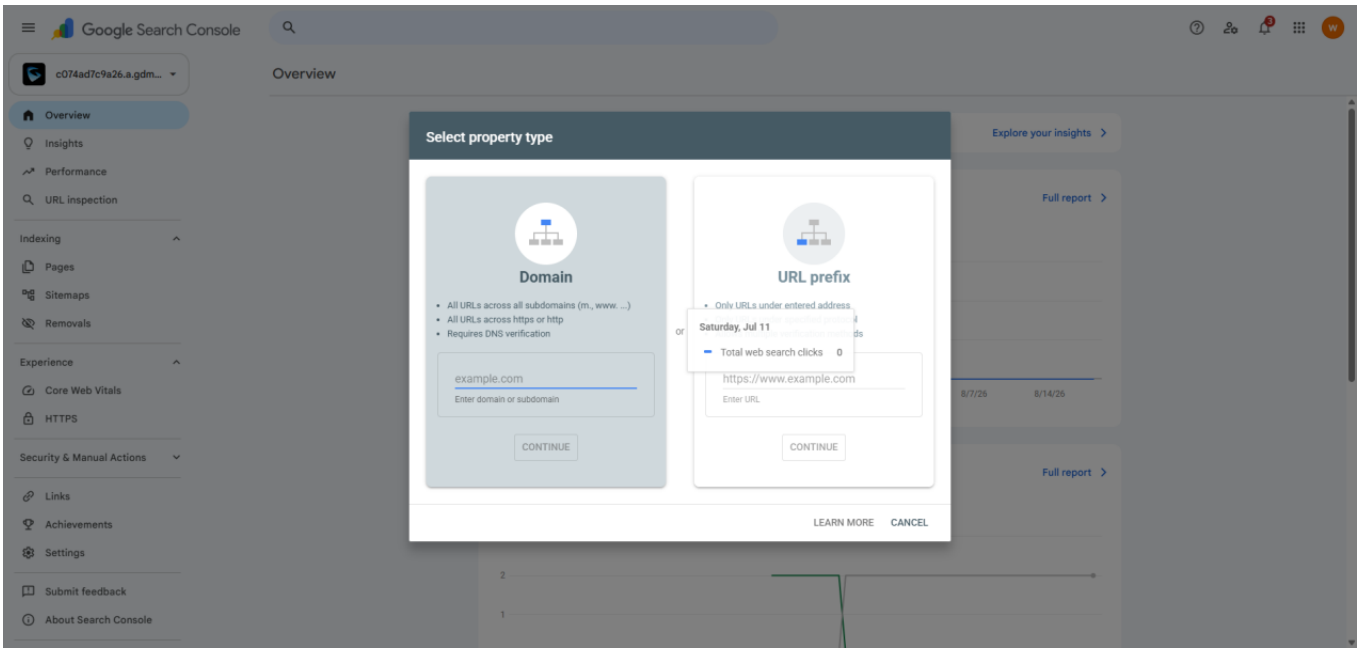
Google Search Console

2. Select "Add a website".



Select a Property Type

3. Enter your domain name in Domain section.



Select a Property Type 2

After authentication is complete, you need to add the Google-generated authentication TXT flag to the domain provider platform. After completion, DNS resolution will return the text as google-site-verification=XXXXXXXXXXXXXXXXXXX.

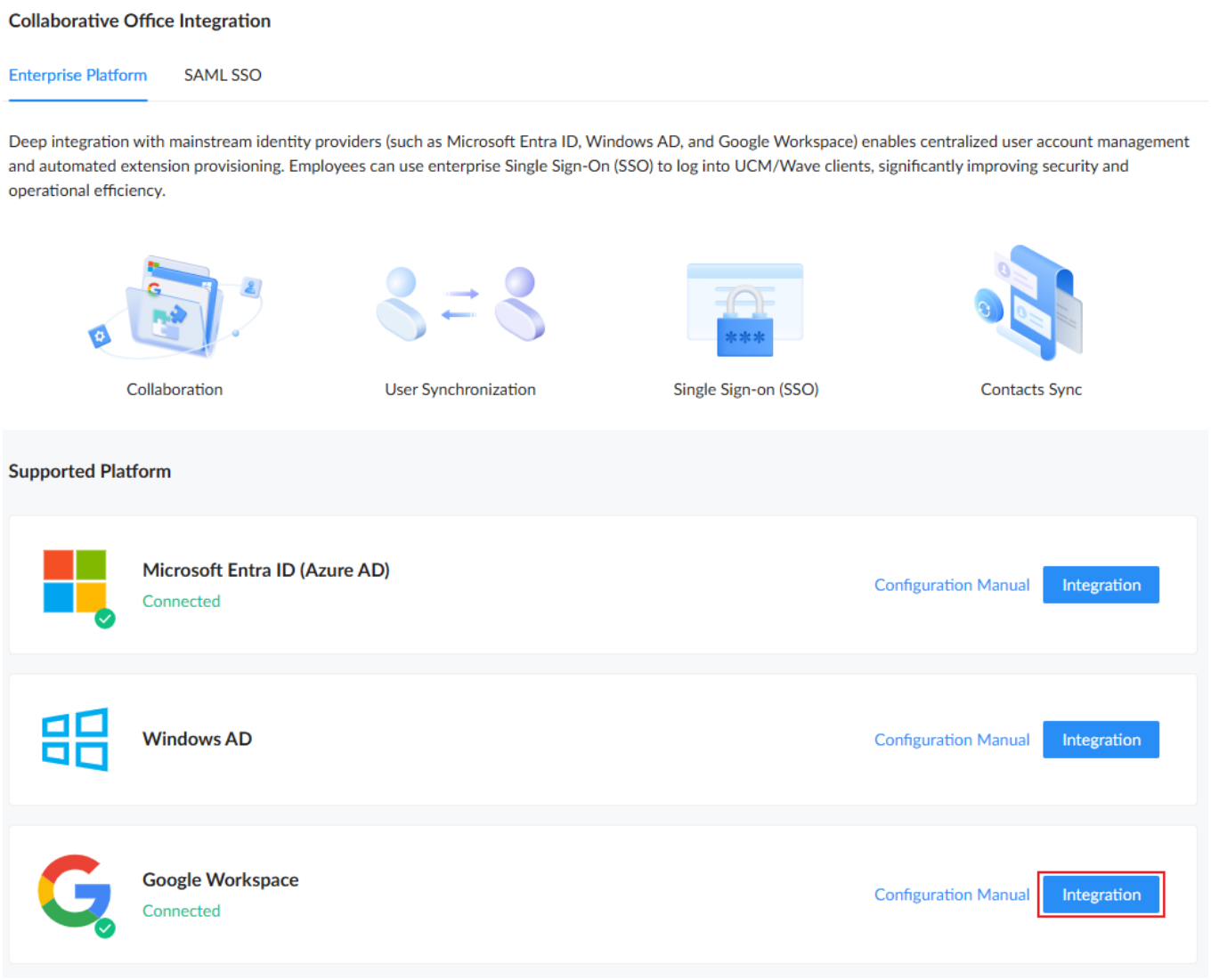
If you are using the URL of the UCM provided by gdms.cloud domain (xxxx.a.gdms.cloud) and you wish to add this URL as a property, please reach out to Grandstream support.

UCM Configuration

After completing the preparations, you may go to the UCM page to enable Google Calendar configuration and enable call routing based on Google Calendar schedules for extensions.

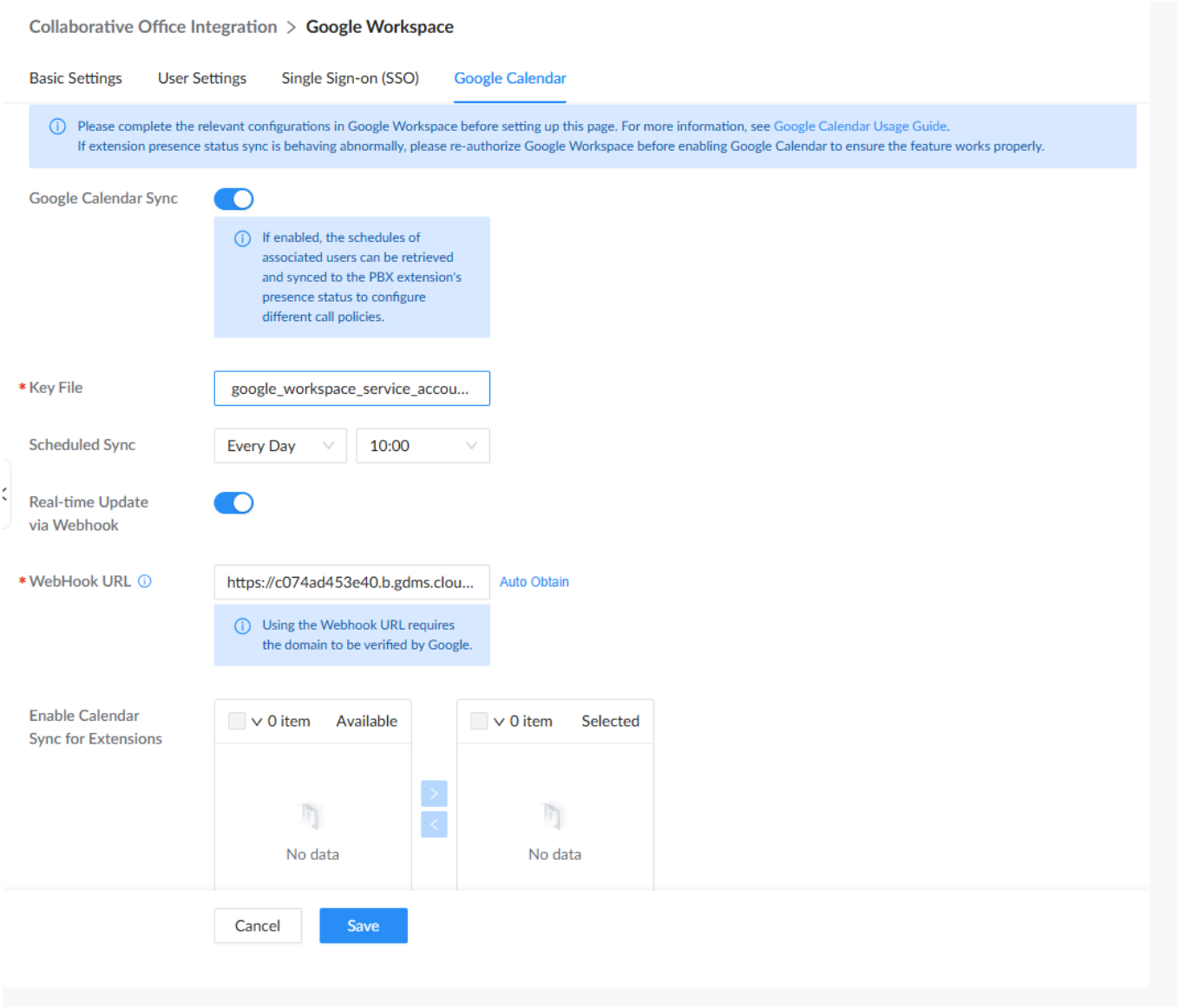
Enabling Google Calendar Configuration

Log into the UCM configuration page with the admin account, then navigate to **Integrations > Collaborative Office Integration** > **Enterprise Platform**, then click on "Integration" button of Google Workspace.



Enterprise Platform Integration

Navigate to "Google Calendar" tab, then configure the required fields.



Google Calendar Configuration

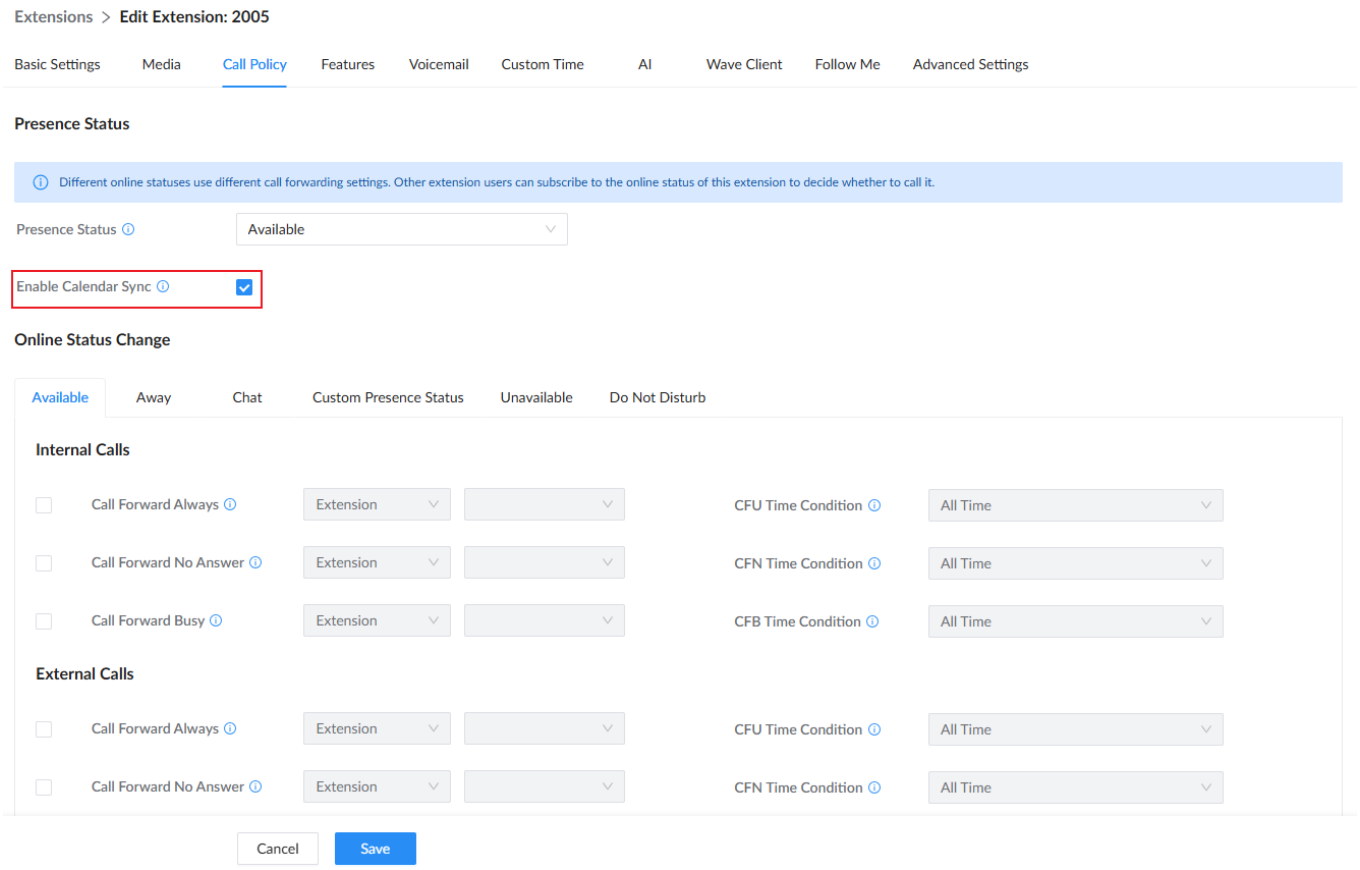
Key File: The key file saved locally during the preparatory steps.

Scheduled Sync: selects the frequency and timing of UCM syncing events from Google Calendar (considering WebHook's real-time nature, it is recommended to sync daily at midnight to synchronize Google Calendar events for the next 24 hours).

WebHook URL: The URL that was successfully authenticated in the prerequisites steps should be in https://XXXXXX/calendar-webhook format.

Enable Google Calendar Routing for Extensions

If you have not selected the extensions in the step above, you can still configure the extensions by navigating to **Extension/Trunk > Extensions**. Select the extension to synchronize, then click on edit settings button Edit button icon (pencil and ruler) for modifying the item, then navigate to "Call Policy". Tick the box next to "Enable Calendar Sync", after that click "Save".



Call Policy

SUPPORTED DEVICES

Google Workspace User Account Sync and Single Sign-on

The table below lists the supported models and firmware support for the Google Workspace integration single sign-on and user account synchronize it.

Devices	Firmware Required
UCM630x Series	1.0.33.7+
UCM630xA Series	1.0.33.7+
SoftwareUCM	1.0.33.7+
CloudUCM	1.0.33.10+
Wave Desktop	1.35.6+
Wave Mobile App	Android: 1.0.35.7+iOS: 1.35.7+
Wave Web	1.0.35.7+

Extension Routing and Google Sheets Sync

The table below lists the supported models and firmware support for the Google Workspace integration for extension call routing.

Models	Firmware Required
UCM630x Series	1.0.35.x or higher
UCM630xA Series	1.0.35.x or higher