

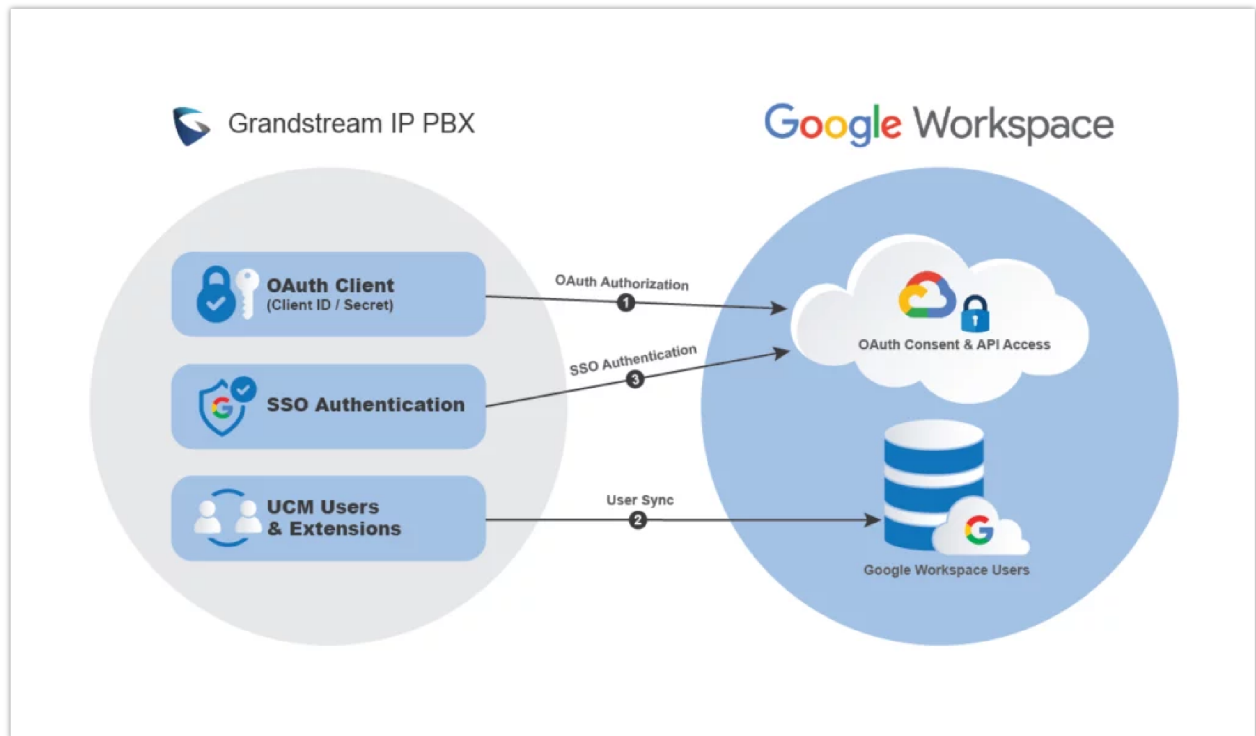
Grandstream Networks, Inc.

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

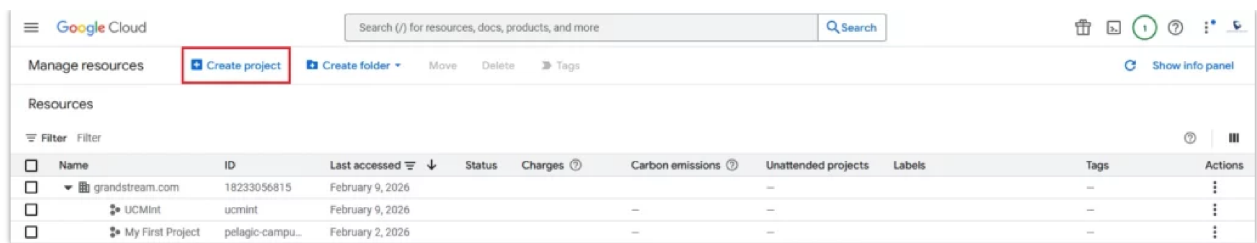
GOOGLE WORKSPACE CONFIGURATION

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.

New Project

You have 9 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)

[Manage Quotas](#)

Project name *

Project ID: ucm-integration-486915. It cannot be changed later. [Edit](#)

Organization *

Select an organization to attach it to a project. This selection can't be changed later.

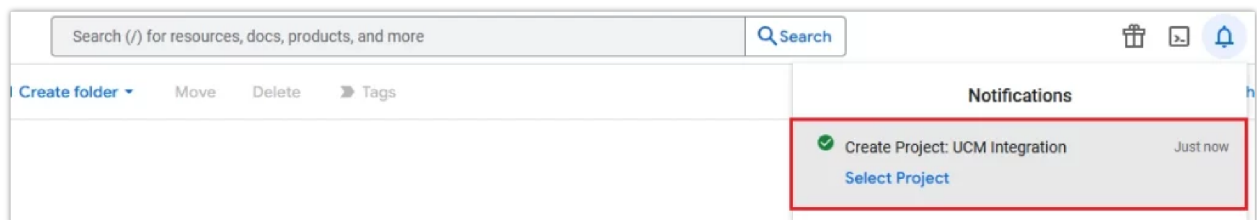
Parent resource * [Browse](#)

Select the organization or folder where this resource will be created

[Create](#) [Cancel](#)

Configuring Project Name and Organization

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

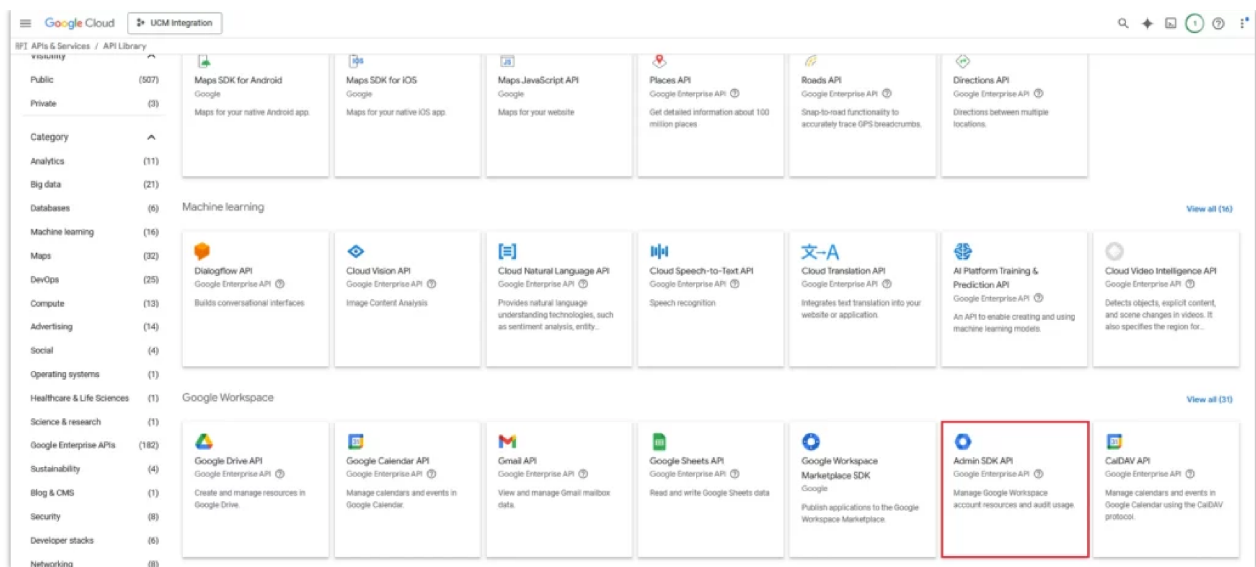


Project Provisioning Confirmation

Enable Google Admin SDK

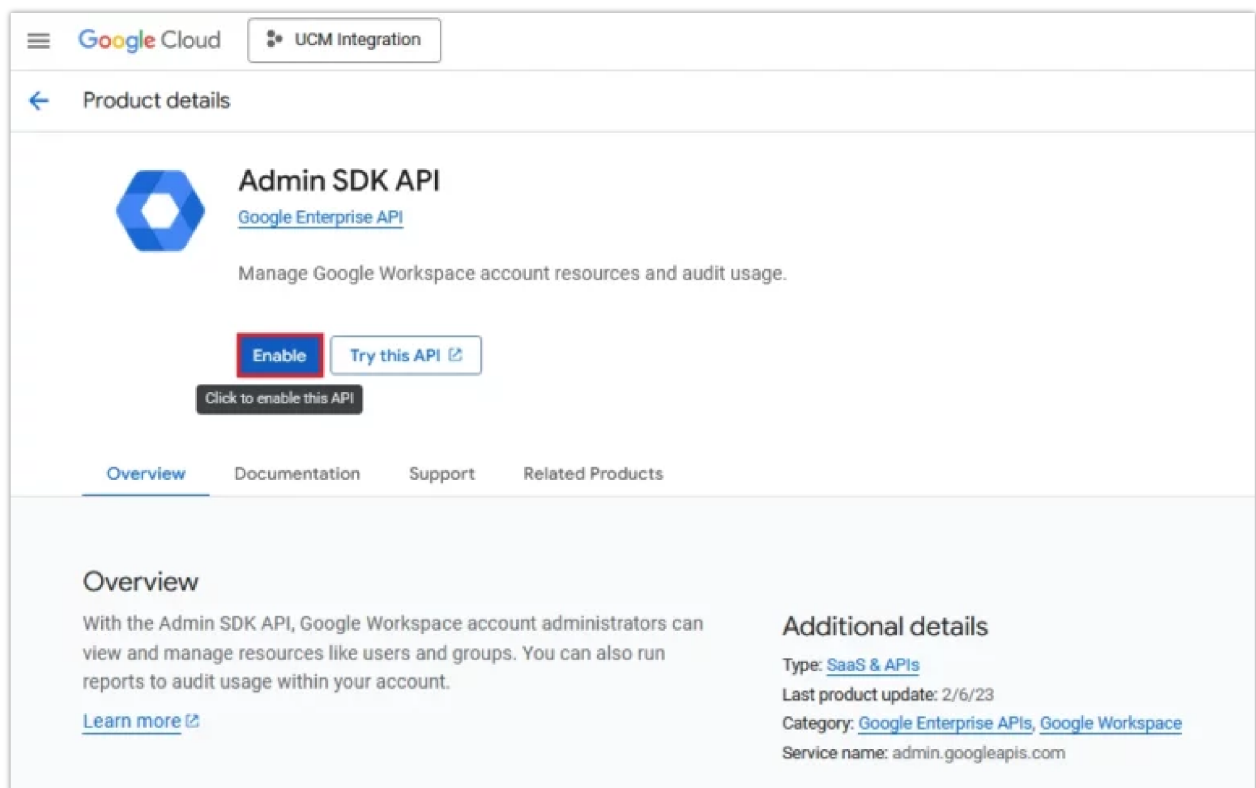
The Google Admin SDK is required for the PBX to retrieve user information from the Google Workspace domain. Without this API enabled, user synchronization and SSO-related user queries will fail even if OAuth authorization succeeds.

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

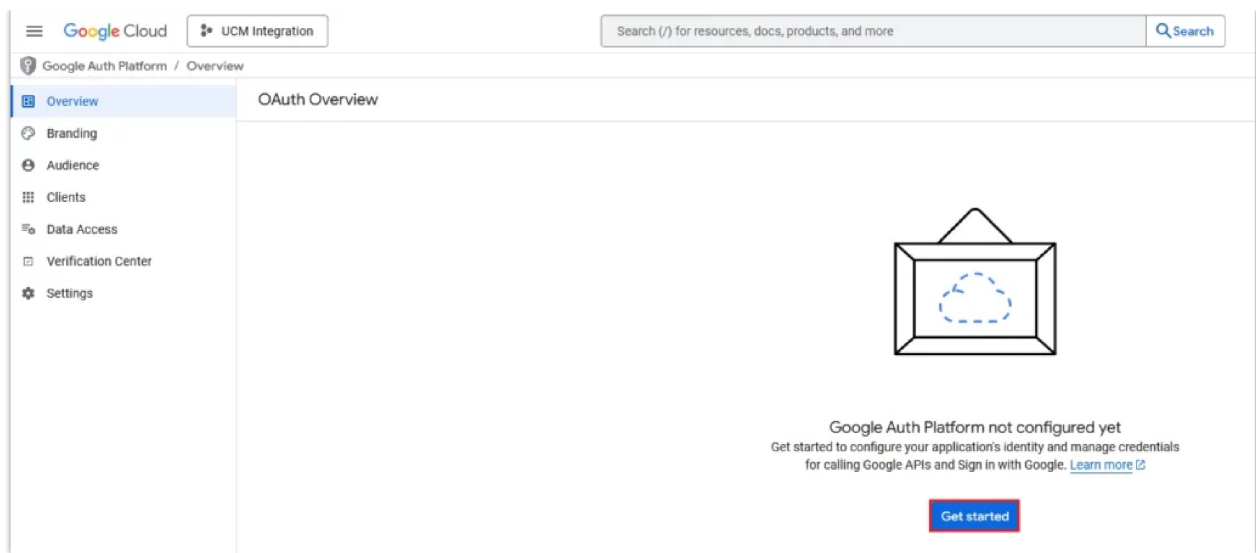
Note:

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).

The screenshot displays the 'Create branding' page within the Google Auth Platform. The breadcrumb trail is 'Google Auth Platform / Overview / Create branding'. The left sidebar menu is identical to the previous screenshot, with 'Overview' selected. The main content area is titled 'Project configuration' and shows a progress indicator with four steps: 1. App Information, 2. Audience, 3. Contact Information, and 4. Finish. The 'App Information' step is active and contains two required fields: 'App name *' with the value 'UCM' and a description 'The name of the app asking for consent', and 'User support email *' with a masked email address and a description 'For users to contact you with questions about their consent. [Learn more](#)'. A 'Next' button is located below these fields. At the bottom of the page, there are 'Create' and 'Cancel' buttons.

Configuring OAuth Consent Screen Details

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

Google Auth Platform / Overview / Create branding

Overview

Branding

Audience

Clients

Data Access

Verification Center

Settings

Project configuration

1 App Information

2 Audience

☒ Internal ?

Only available to users within your organization. You will not need to submit your app for verification. [Learn more about user type](#)

☐ External ?

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)

Next

3 Contact Information

4 Finish

Create Cancel

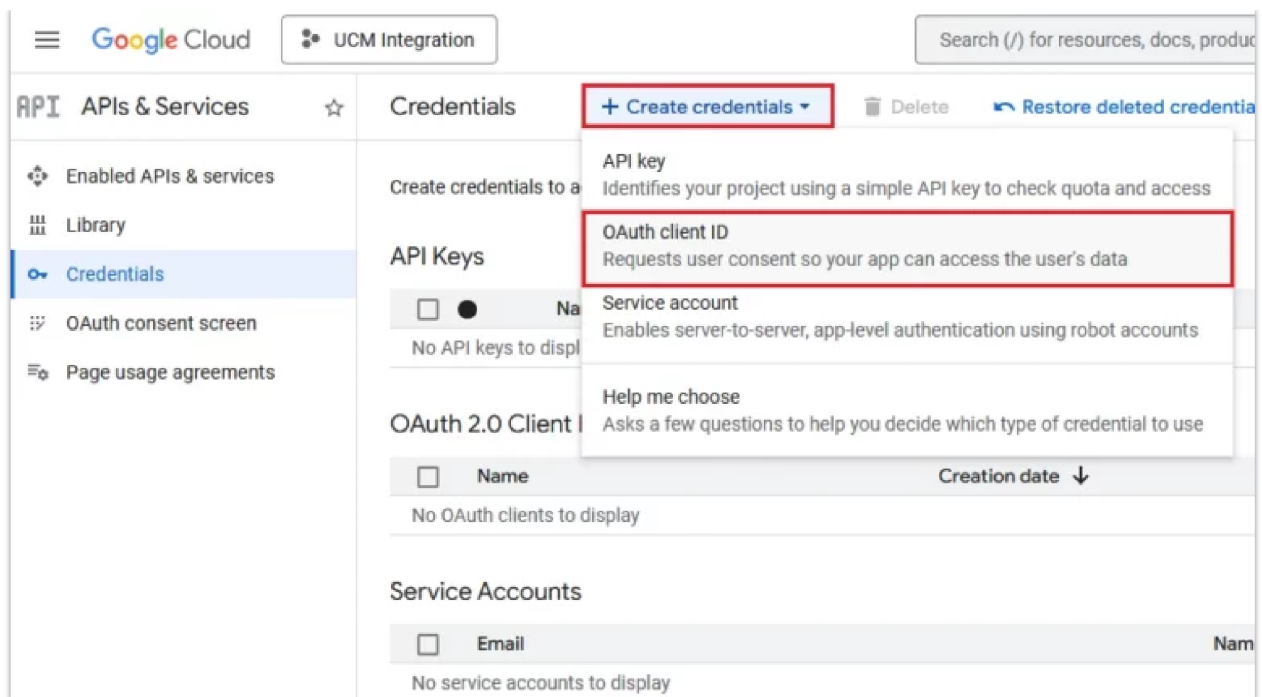
Selecting User Type

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

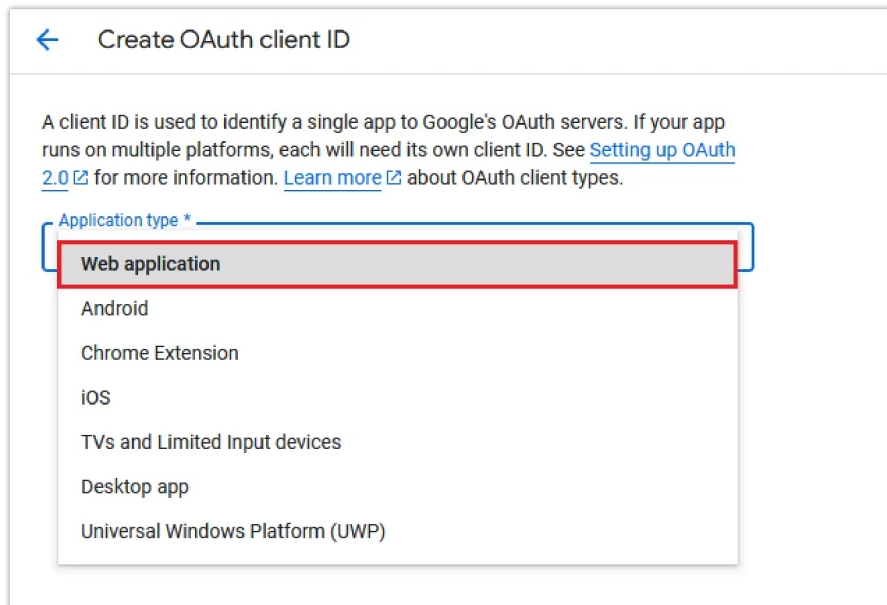
OAuth client credentials allow the PBX to authenticate securely against Google Workspace. These credentials will later be entered on the PBX.

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**.

[←](#) Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *

Web application

Name *

Web client1

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

❗

The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins

?

For use with requests from a browser

+ Add URI

Authorized redirect URIs

?

For use with requests from a web server

URIs 1 *

https://ucm.grandstream.com/googleoauth/

+ Add URI

Note: It may take 5 minutes to a few hours for settings to take effect

Create

Cancel

Configuring Authorized Redirect URI

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

Note:

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.

OAuth client created

The client ID can always be accessed from Clients tab under Google Auth Platform.



OAuth access is restricted to users within your organization unless the [OAuth consent screen](#) is published and verified

Client ID

kgI5lqo94.apps.googleusercontent.com



You will no longer be able to view or download the client secret once you close this dialog. Make sure you have copied or downloaded the information below and securely stored it.

Client secret

qfj5zej11dGx



Creation date

February 10, 2026, 2:47:00 PM GMT+1

Status

✓ Enabled

Download JSON

OK

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**.

Integration of Collaborative Office Platforms > **Google Workspace**

[Basic Settings](#) [User Settings](#) [Single Sign-on \(SSO\)](#)

 **Connected**

For more information about Google Workspace, see [Google Workspace Configuration Manual](#).

Google Workspace Authorization ☒

Enter your Google Workspace app details below.

* Redirect URIs

* Application (Client) ID

* Client Password

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.

 Sign in with Google

Choose an account

to continue to **UCM**

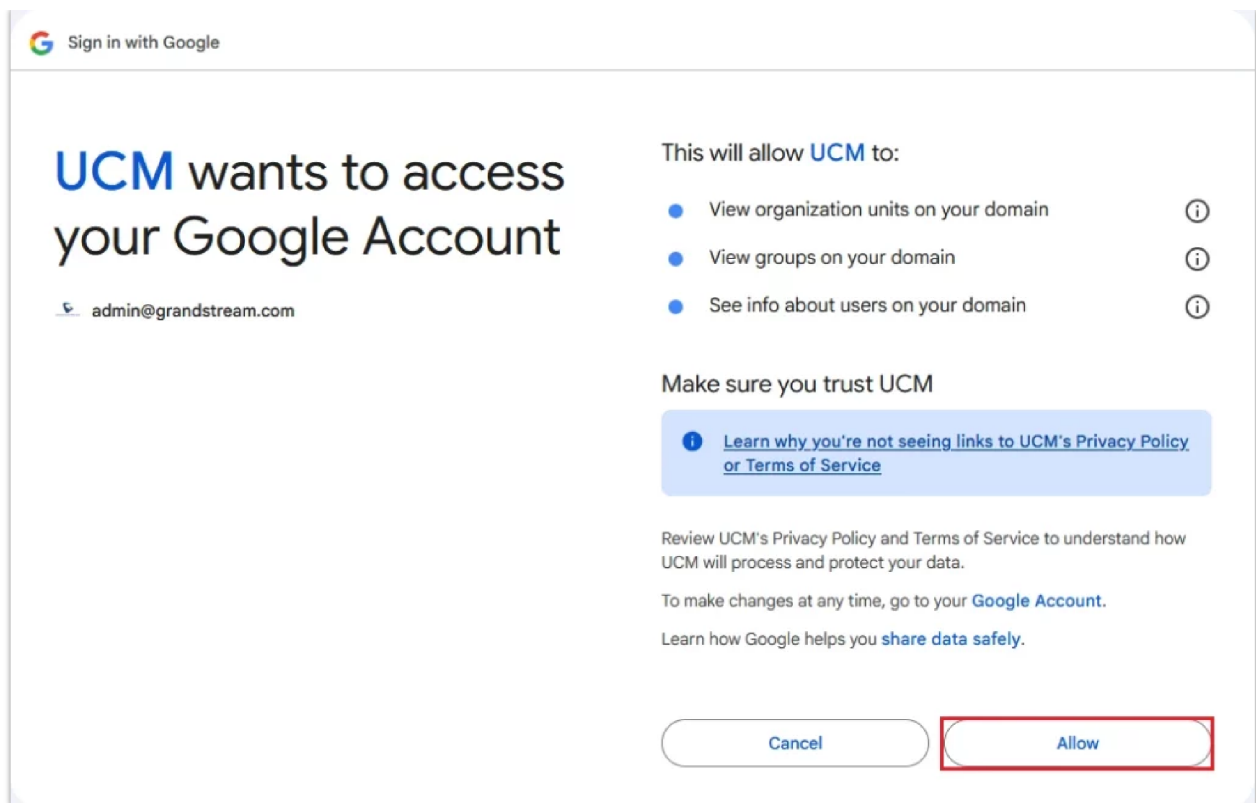
 **UCM Admin**
admin@grandstream.com

 **UCM User**
user@grandstream.com

 **Use another account**

Selecting the Google Workspace Administrator Account

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



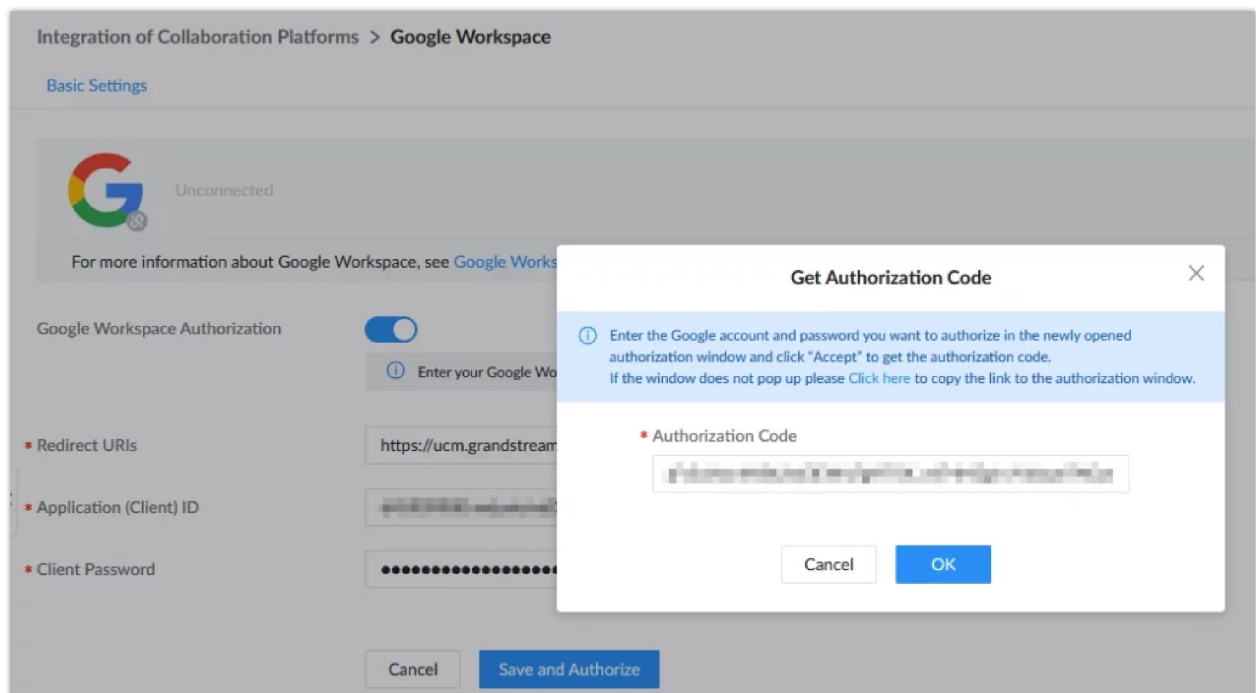
Granting OAuth Consent

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



Google Authorization Code Displayed

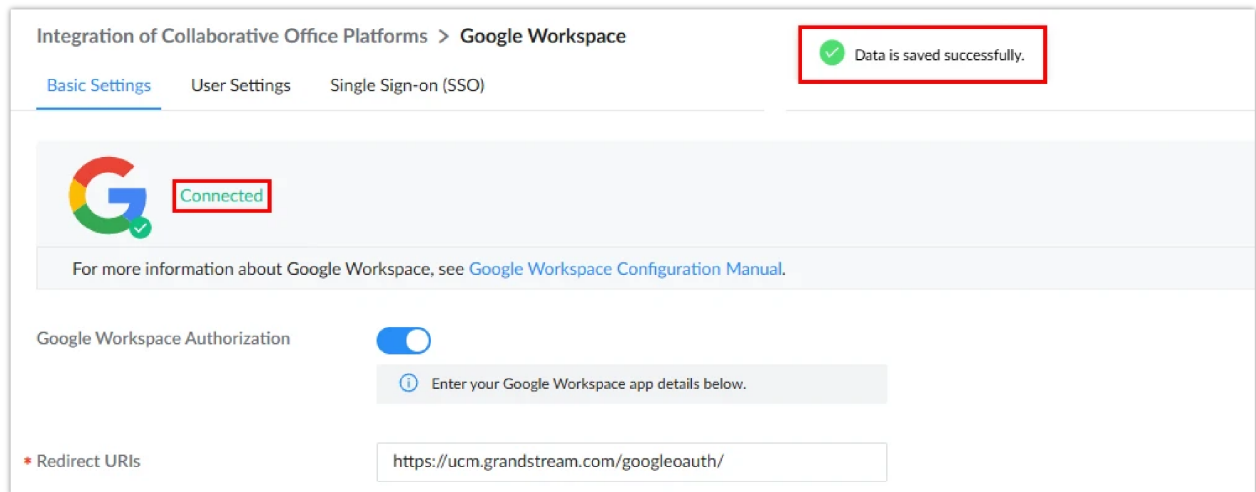
10. Return to the PBX authorization page and paste the copied **Authorization Code** into the required field.



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.



The screenshot shows the 'Integration of Collaborative Office Platforms > Google Workspace' settings page. At the top right, a green checkmark icon and the text 'Data is saved successfully.' are highlighted with a red box. Below this, the 'Basic Settings' tab is active, showing the Google logo with a green checkmark and the word 'Connected' in a red box. A link to the 'Google Workspace Configuration Manual' is provided. Under 'Google Workspace Authorization', a toggle switch is turned on, and a message says 'Enter your Google Workspace app details below.' Below this, the 'Redirect URIs' section shows a text input field containing 'https://ucm.grandstream.com/googleoauth/'.

Successful Google Workspace Authorization on PBX

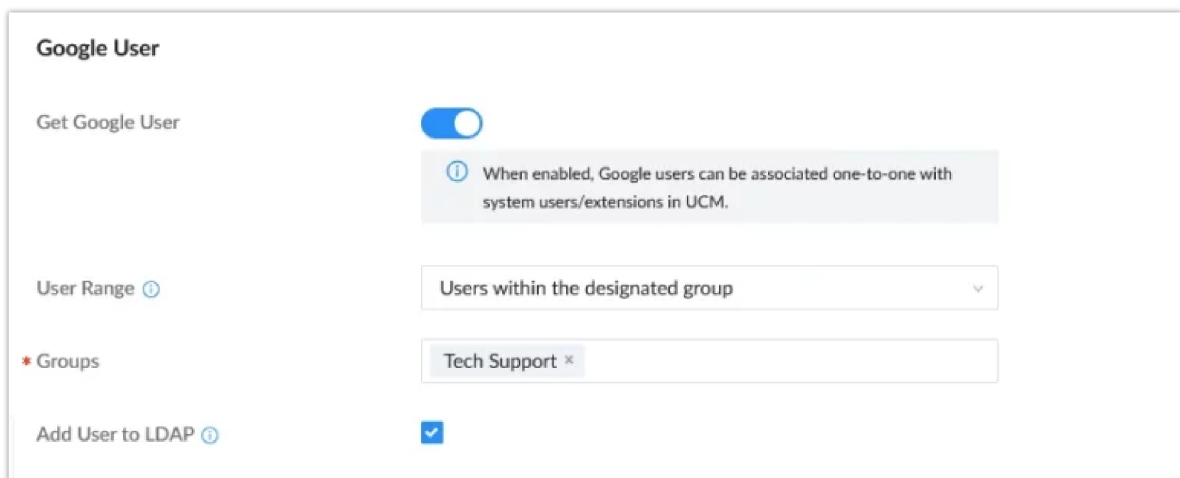
Configure Google User Synchronization

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.

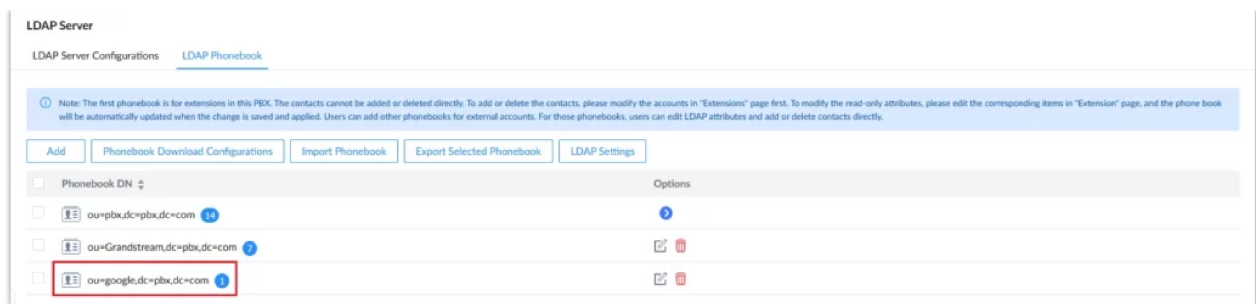
1. Navigate to **User Settings** → **Google User**.
2. Enable **Get Google User**.
3. Select the User Range:
 - **All Users:** retrieves all users from the Google Workspace domain.
 - **Users within the designated organizational unit:** retrieves users from a specified Organizational Unit.
 - **Users within the designated group:** retrieves users belonging to one or more specified Google Workspace groups.
4. If applicable, specify the Organizational Unit or Groups.



The screenshot shows the 'Google User' settings page. The 'Get Google User' toggle switch is turned on. Below it, a message states: 'When enabled, Google users can be associated one-to-one with system users/extensions in UCM.' The 'User Range' dropdown menu is set to 'Users within the designated group'. The 'Groups' section shows a text input field containing 'Tech Support *'. At the bottom, the 'Add User to LDAP' checkbox is checked.

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

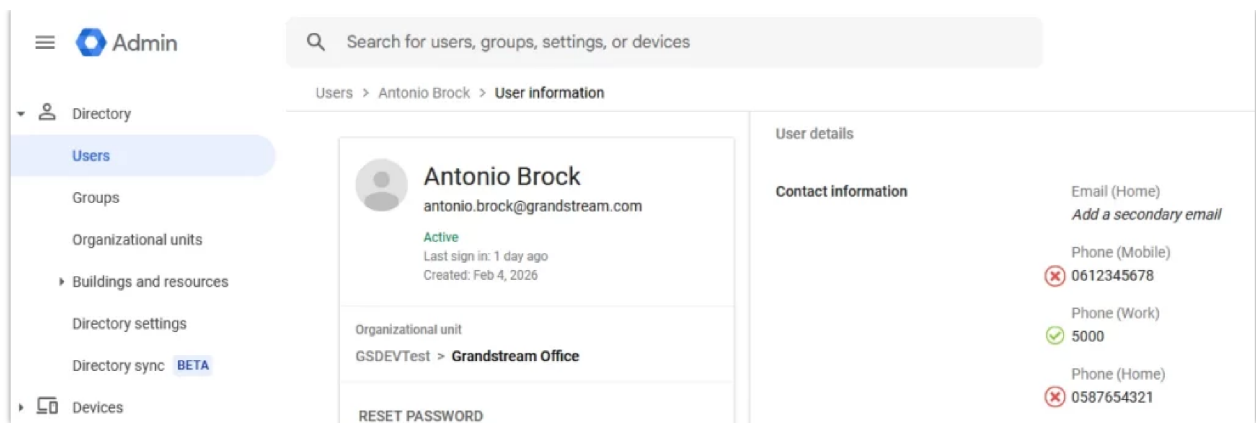
This step defines whether users are linked automatically or manually.

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

Note:

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



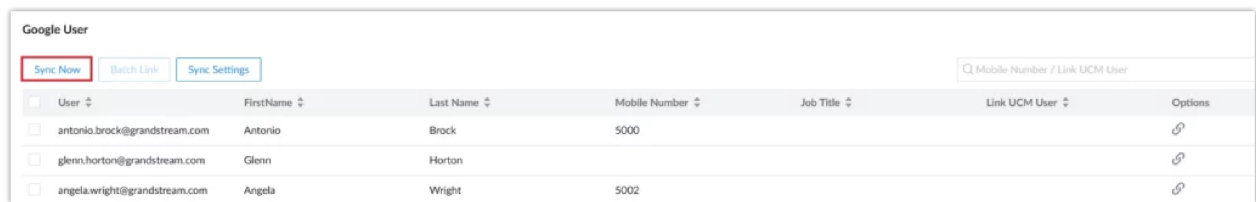
Google User Phone Attributes

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.

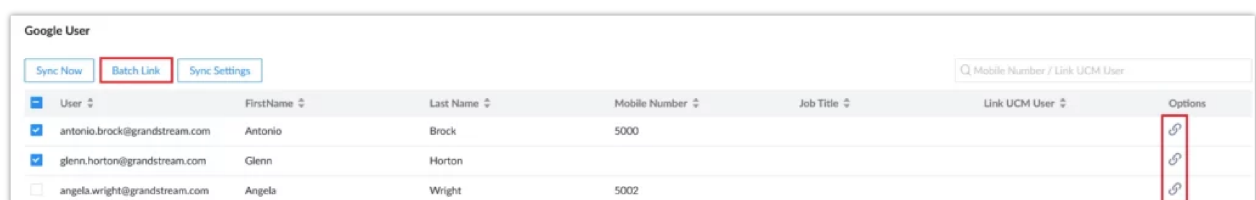
1. Navigate to the **Google User List** section.
2. Click **Sync Now**.
3. Wait for the synchronization process to complete.



Manual Synchronization Sync Now

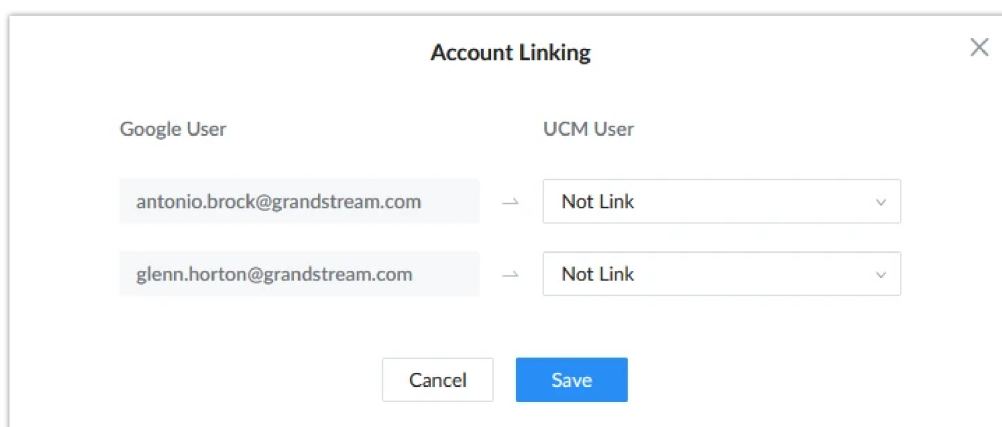
When Manual Link is selected, administrators can explicitly associate Google users with PBX users or extensions.

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 below:

User Management				
System User Information Custom Privilege User Portal/Wave Privileges Extension Login Management User Endpoint Access History				
Add				
Username	Privilege	Last Operation Time		Options
admin	Super Administrator	2026-02-11 08:38:46		
Cindy	Administrator	2026-02-10 14:37:58		
Glen	Administrator	2026-02-10 18:32:12		
Mack	Administrator	2025-12-31 12:07:14		
Antonio	Custom Privilege:Priv1	2025-12-29 14:08:48		

Linked System User Identification

Extensions									
Add Edit Delete Edit All SIP Email Notification More Sync Contact									
☐	Status	Presence Status	Extension	Name	Message	Type	IP and Port	Sync to Contacts	Extension Info No...
☐	Unregistered	Available	5000	Angela Wright	0/0/0	SIP(WebRTC)	--	Synced	
Total: 1 30 / page Goto									

Linked Extension Identification

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:

Integration of Collaborative Office Platforms > Google Workspace

Basic Settings

User Settings

Single Sign-on (SSO)

User Range ⓘ

Users within the designated group

* Groups

Tech Support x

Add User to LDAP ⓘ

☒

Linked User Settings

Linked UCM

☒

ⓘ If enabled, the linked UCM user's information (first name, last name, email, mobile number, job title) will be overwritten by the Google user's information.

Linking Method ⓘ

☐ Automatic Link

☒ Manual Link

ⓘ After saving, edit the link on the right side of the Google users table below.

Cancel

Save

Google User

Sync Now

Batch Link

Sync Settings

☐ User

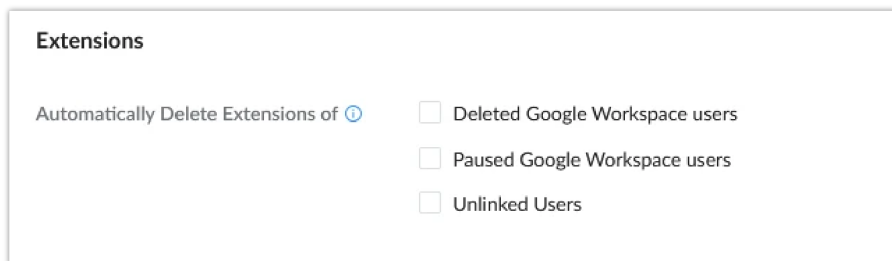
FirstName

Last Name

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.



The screenshot shows a configuration panel titled "Extensions". Below the title, there is a label "Automatically Delete Extensions of" followed by a help icon. To the right of this label are three unchecked checkboxes: "Deleted Google Workspace users", "Paused Google Workspace users", and "Unlinked Users".

Extensions Sync Settings

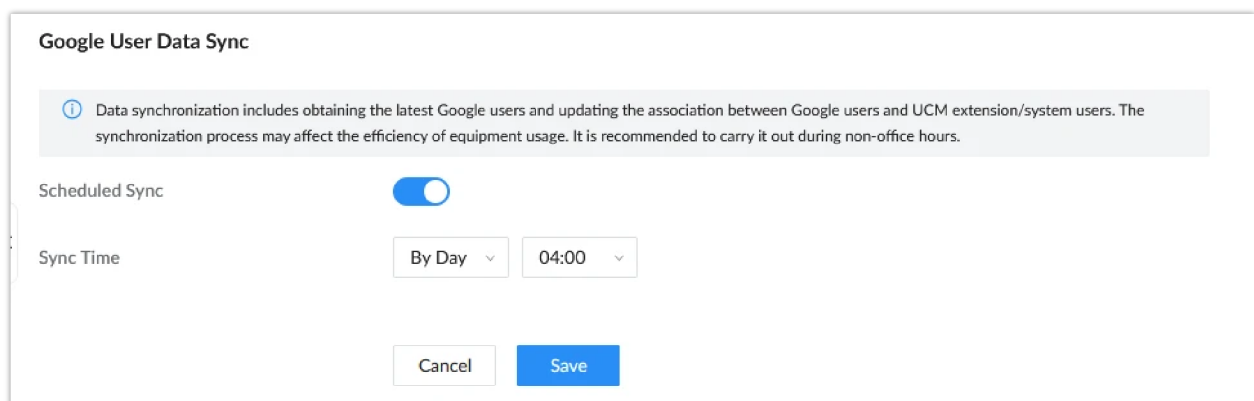
Configure Scheduled Synchronization

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.

Note:

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



The screenshot shows a configuration panel titled "Google User Data Sync". Below the title, there is a help icon and a text box stating: "Data synchronization includes obtaining the latest Google users and updating the association between Google users and UCM extension/system users. The synchronization process may affect the efficiency of equipment usage. It is recommended to carry it out during non-office hours." Below this, there is a "Scheduled Sync" section with a toggle switch that is turned on. Underneath, there is a "Sync Time" section with two dropdown menus: "By Day" and "04:00". At the bottom, there are two buttons: "Cancel" and "Save".

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.

Example:

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

Google Auth Platform / Branding

Overview

Branding

Audience

Clients

Data Access

Verification Center

Settings

Branding

Authorized domains: The following information will be shown to your users on the consent screen.

Application home page

Provide users a link to your home page

Application privacy policy link

Provide users a link to your public privacy policy

Application terms of service link

Provide users a link to your public terms of service

Authorized domains [?]

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the [Google Search Console](#) to check if your domains are authorized. [Learn more](#) about the authorized domain limit.

Authorized domain 1 *

grandstream.com

Authorized domain 2 *

example.com

[+ Add domain](#)

Developer contact information

Email addresses *

admin@grandstream.com

These email addresses are for Google to notify you about any changes to your project.

[Save](#) [Discard changes](#)

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.

Important:

- 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.

Google Auth Platform / Clients / Client: [redacted].apps.googleusercontent.com

Overview
Branding
Audience
Clients
Data Access
Verification Center
Settings

Client ID for Web application [Delete](#)

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins ⓘ
For use with requests from a browser

[+ Add URI](#)

Authorized redirect URIs ⓘ
For use with requests from a web server

URIs 1 *
<https://ucm.grandstream.com/googleoauth/>

URIs 2 *
<https://pbx.example.com/login>

[+ Add URI](#)

Note: It may take 5 minutes to a few hours for settings to take effect

[Save](#) [Cancel](#)

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.

Integration of Collaborative Office Platforms > Google Workspace

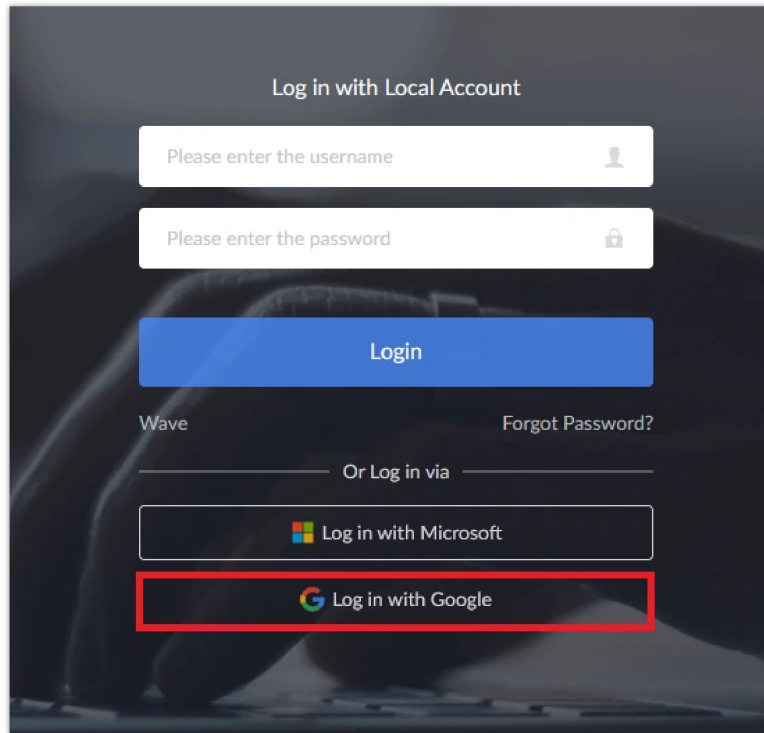
Basic Settings User Settings **Single Sign-on (SSO)**

Single Sign-on (SSO) ☒

ⓘ If enabled, users will be able to log into the webUI and Wave with their linked Google account.

[Cancel](#) [Save](#)

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.

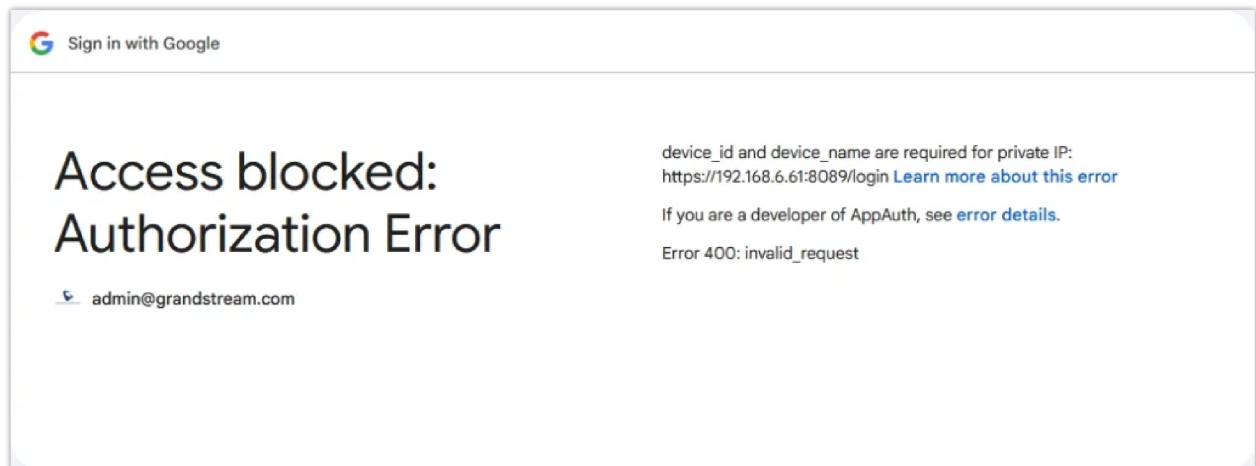


Log in with Google Option

Verify SSO Login

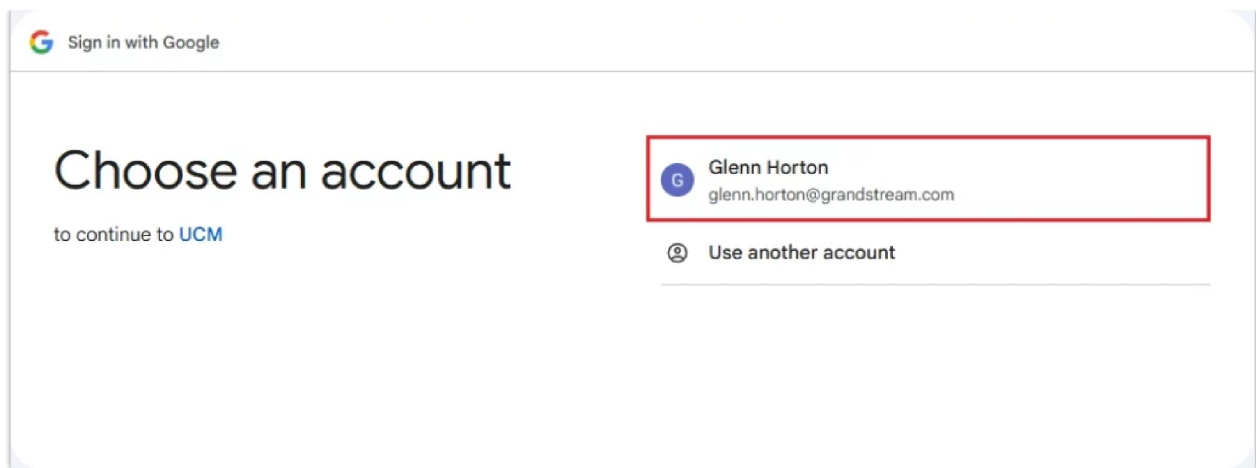
To validate SSO functionality, please refer to the steps below:

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.



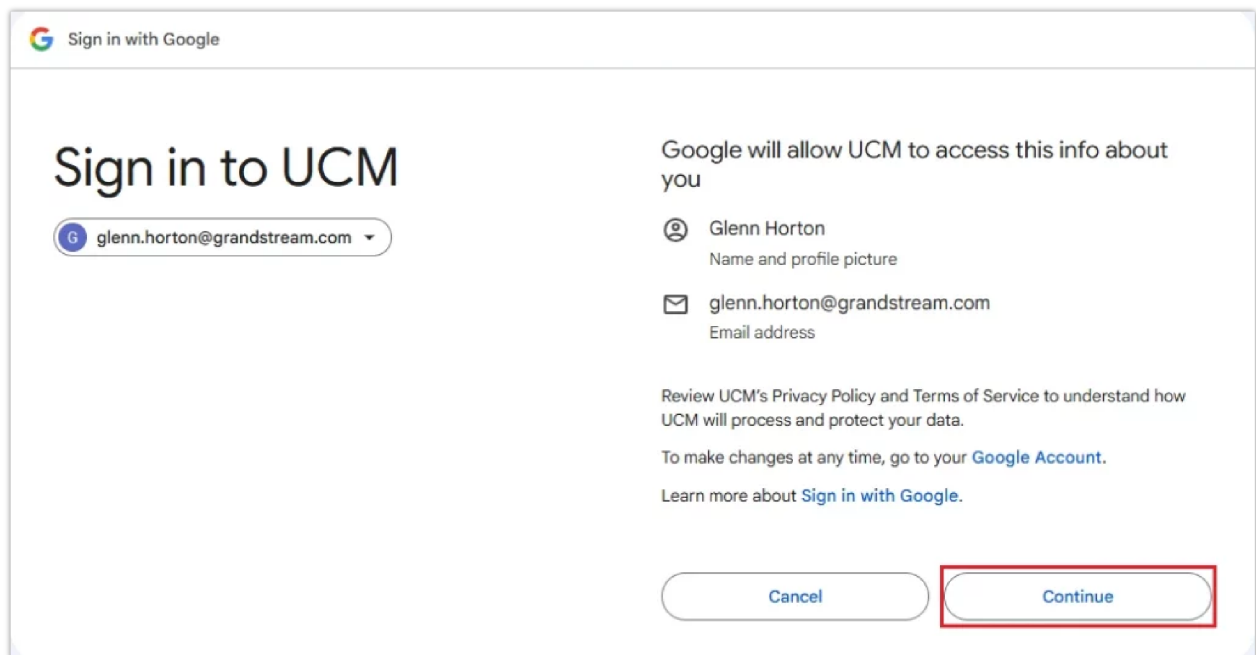
SSO Private IP Access Error

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.

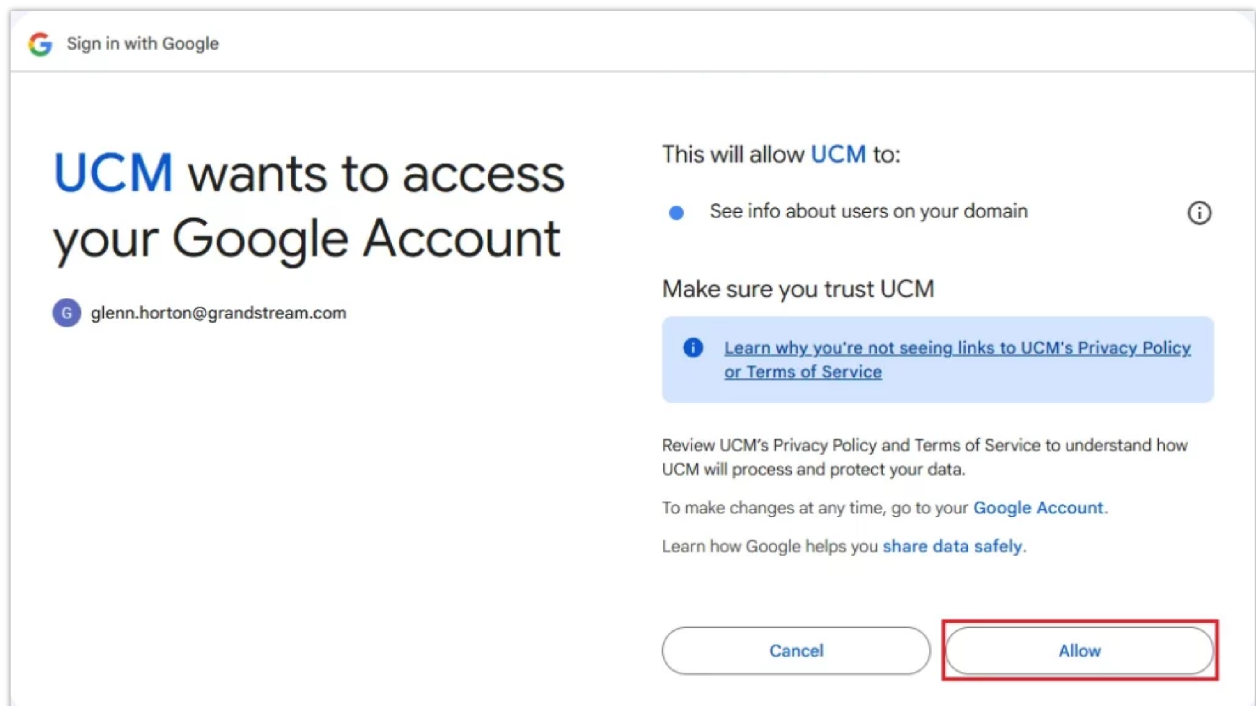


SSO Login Google Account Selection

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.

SUPPORTED MODELS

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

Models	Firmware Required
UCM630x Series	1.0.33.7+
UCM630xA Series	1.0.33.7+
SoftwareUCM	1.0.33.7+
CloudUCM	1.0.33.10+