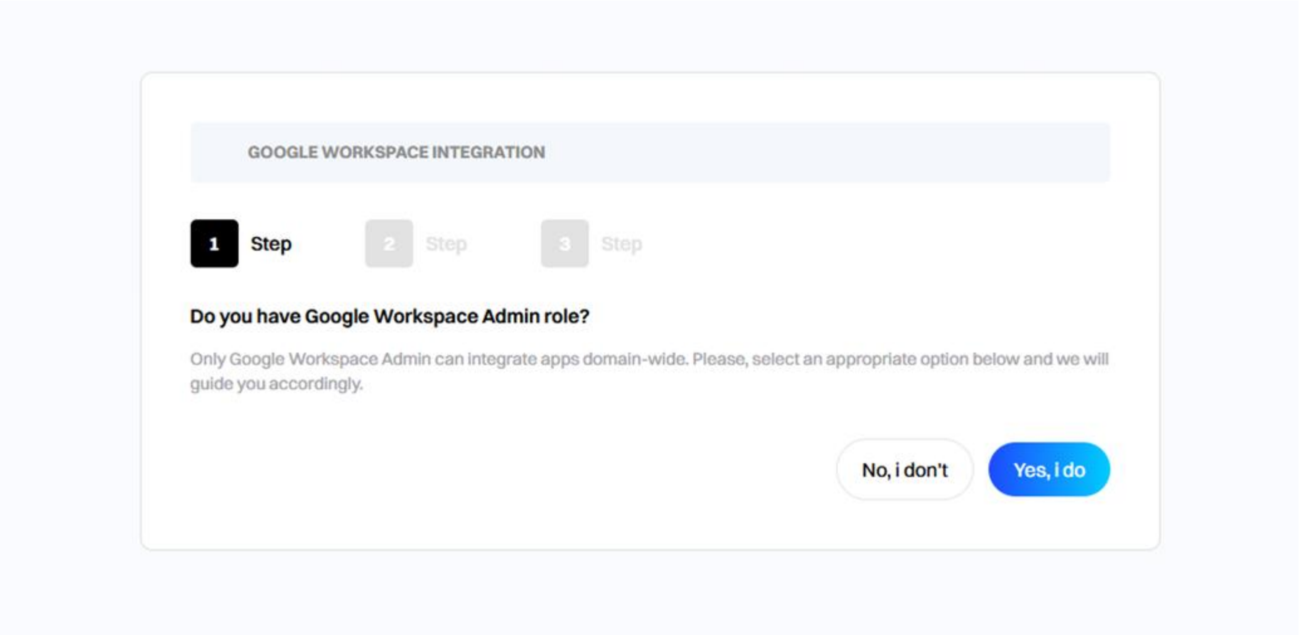
Google Workspace Integration Guide

Overview

This guide explains how to integrate **CustomEsignature** with **Google Workspace** for centralized email signature management. The setup ensures consistent, professional branding across all employee communications. Steps include whitelisting the app, configuring API access, installing the Marketplace app, and connecting CustomEsignature. Admin access is required—non-admins should share this guide with their Workspace administrator.

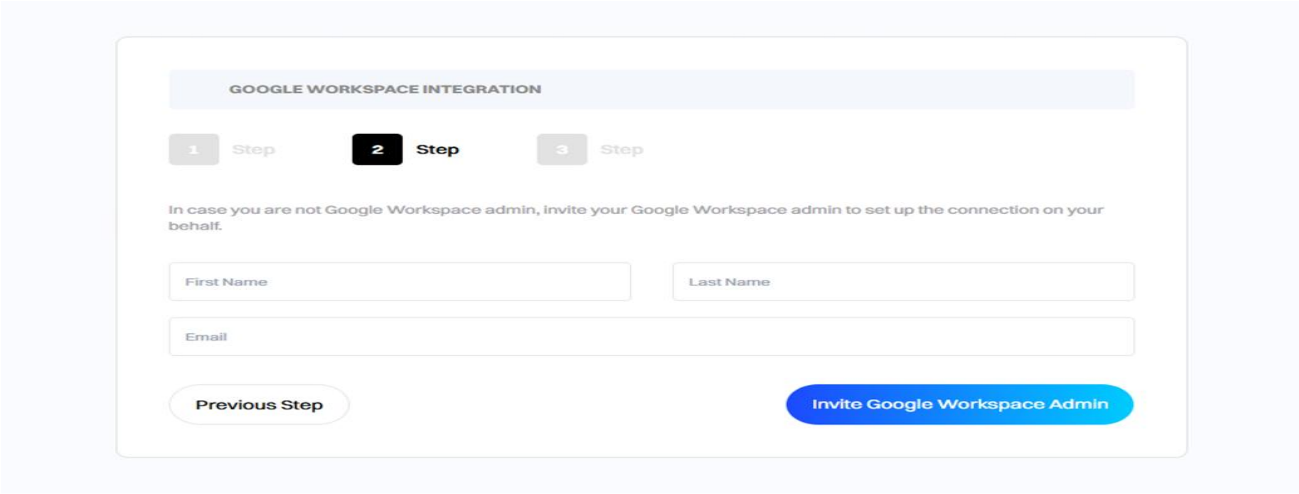


GOOGLE WORKSPACE INTEGRATION

Do you have Google Workspace Admin role?

Only Google Workspace Admin can integrate apps domain-wide. Please, select an appropriate option below and we will guide you accordingly.

Before proceeding, ensure you have the necessary administrative privileges within Google Workspace. If you are not a Google Workspace administrator.



GOOGLE WORKSPACE INTEGRATION

In case you are not Google Workspace admin, invite your Google Workspace admin to set up the connection on your behalf.

First Name

Last Name

Email

Prerequisites

Before initiating the integration process, please ensure the following prerequisites are met:

Google Workspace Administrator Access: You must have administrative privileges for your Google Workspace (formerly G Suite) account to configure the necessary settings and permissions.

Active CustomEsignature Account: An active CustomEsignature account with pre configured signature templates is required. These templates will be deployed to your Google Workspace users.

Access to CustomEsignature Integration Portal: You need access to the CustomEsignature Google Workspace integration portal, typically found at `https://app.customesignature.com/integrations/google/connect`.

Part 1: Organization-Wide Signature Deployment

This section details the steps required to whitelist the CustomEsignature Email Signatures application within your Google Workspace environment, enabling organization-wide signature deployment.

Step 1: Whitelist CustomEsignature Email Signatures Application

1. **Access Google Admin Console:**

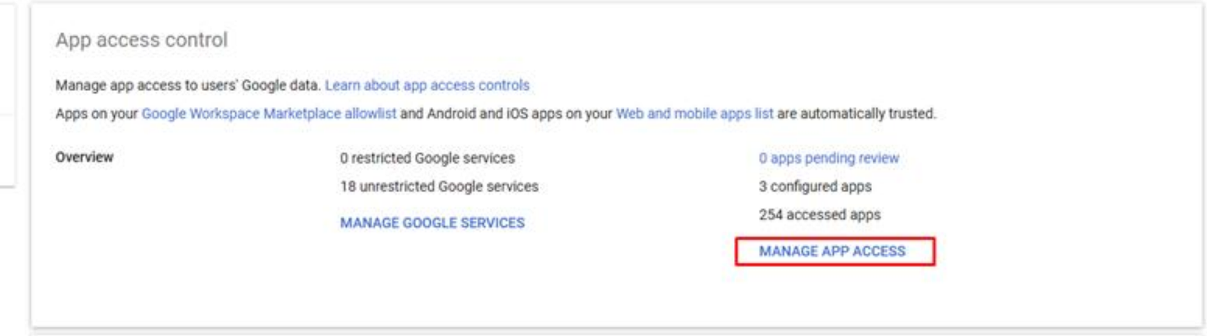
- Go to admin.google.com.
- Sign in using your Google Workspace administrator account credentials.
- Navigate to the Google Admin Console dashboard.
- This dashboard provides access to all Google Workspace administrative functions.

Step 2: Navigate to API Control and Manage App Access

1. **Access Security Settings:**

On the left-hand side navigation menu, locate and click on the **Security** tab. Within the Security section, navigate to **Access and data control**.

Click on **API control**.



App access control

Manage app access to users' Google data. Learn about app access controls

Apps on your Google Workspace Marketplace allowlist and Android and iOS apps on your Web and mobile apps list are automatically trusted.

Overview

0 restricted Google services

18 unrestricted Google services

0 apps pending review

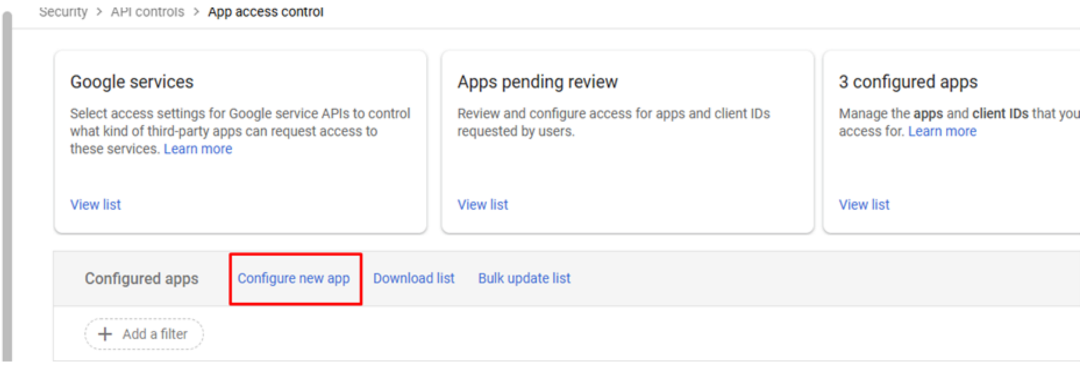
3 configured apps

254 accessed apps

2. **Manage App Access:**

Click on **Manage App Access**.

Subsequently, click on the **Configured new app** text to initiate the process of adding a new application.



Security > API controls > App access control

Google services

Select access settings for Google service APIs to control what kind of third-party apps can request access to these services. Learn more

Apps pending review

Review and configure access for apps and client IDs requested by users.

3 configured apps

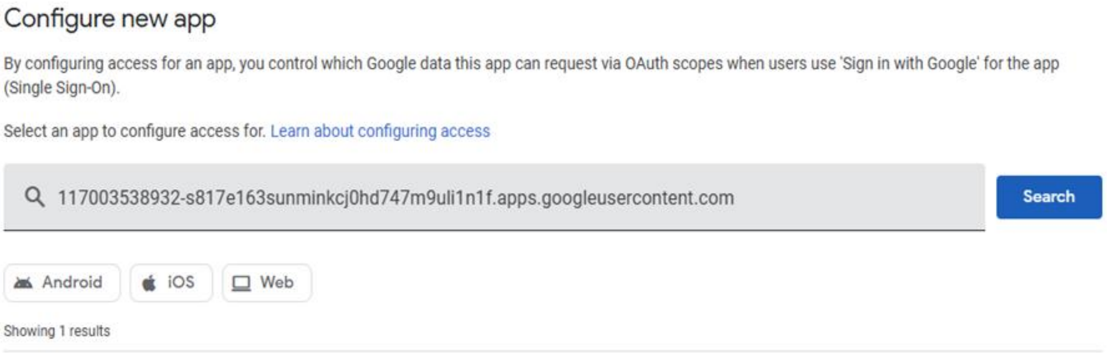
Manage the **apps** and **client IDs** that you access for. Learn more

3. **Add CustomEsignature Application:**

Copy the CustomEsignature Client ID provided below:

117003538932- s817e163sunminkcj0hd747m9uli1n1f.apps.googleusercontent.com

Paste this Client ID into the search bar and click **Search**.



Configure new app

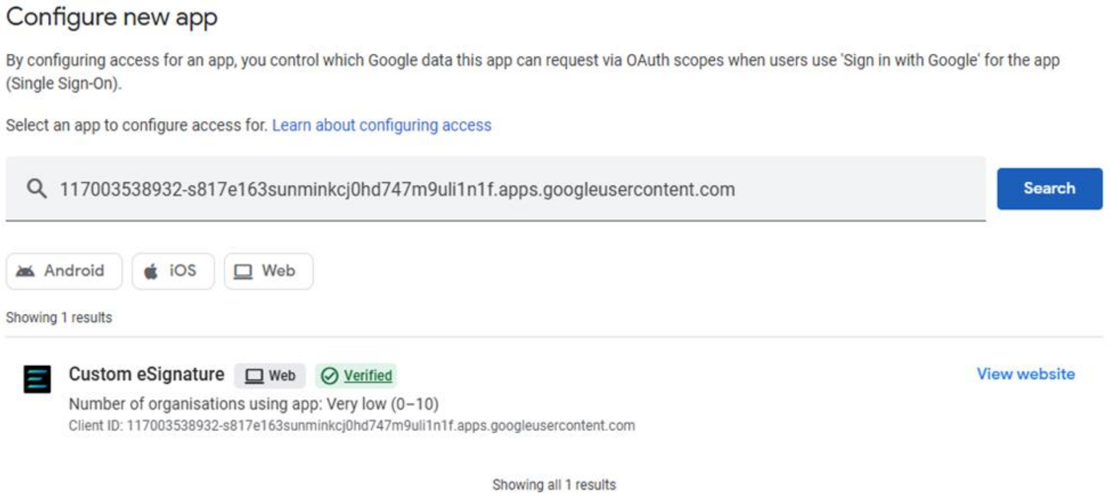
By configuring access for an app, you control which Google data this app can request via OAuth scopes when users use 'Sign in with Google' for the app (Single Sign-On).

Select an app to configure access for. Learn about configuring access

117003538932-s817e163sunminkcj0hd747m9uli1n1f.apps.googleusercontent.com

Showing 1 results

Tap the CustomEsignature app that appears in the search results list to select it.



Configure new app

By configuring access for an app, you control which Google data this app can request via OAuth scopes when users use 'Sign in with Google' for the app (Single Sign-On).

Select an app to configure access for. Learn about configuring access

117003538932-s817e163sunminkcj0hd747m9uli1n1f.apps.googleusercontent.com

Search

Android · iOS · Web

Showing 1 results

Custom eSignature · Web · Verified · View website

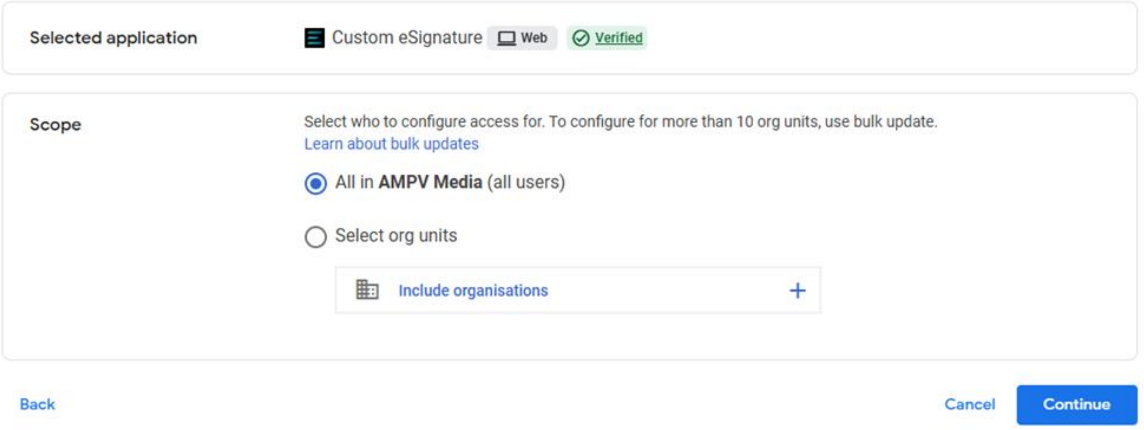
Number of organisations using app: Very low (0–10)

Client ID: 117003538932-s817e163sunminkcj0hd747m9uli1n1f.apps.googleusercontent.com

Showing all 1 results

4. **Configure Access for Users:**

   Select the scope of users for whom you wish to configure access. You can choose **all users** or specific **organizational units** (a segment of users for whom you need to add email signatures).



Selected application: Custom eSignature · Web · Verified

Scope: Select who to configure access for. To configure for more than 10 org units, use bulk update. Learn about bulk updates

● All in **AMPV Media** (all users)

○ Select org units

Include organisations +

Back · Cancel · Continue

Recommendation: It is highly recommended to configure access for all users of your Google Workspace account to ensure the CustomEsignature application and its deployed signatures function correctly for everyone.

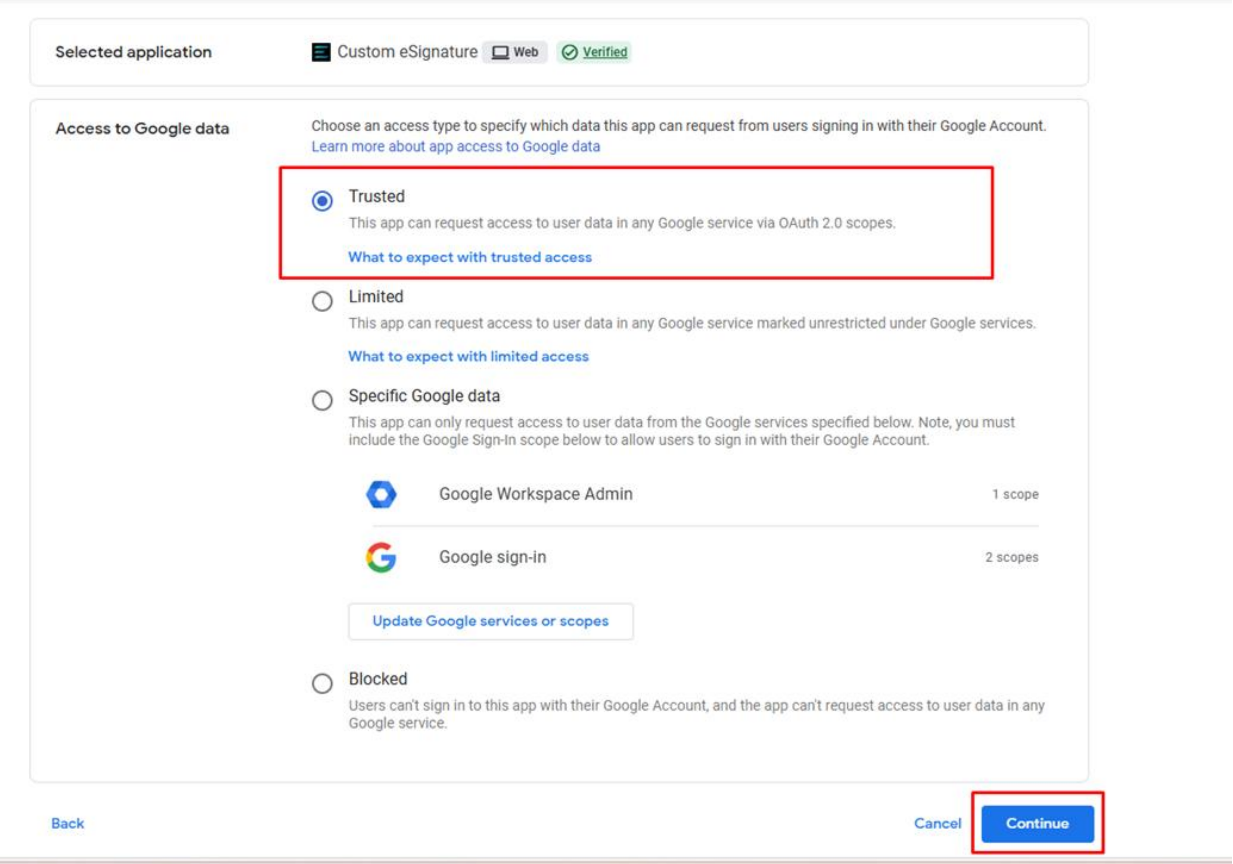
Click **Continue**.

5. **Set Trust Level and Configure:**

Choose **Trusted**.

Select **Allowlist for exemption from API access blocks in context-aware access. Available only for apps added via OAuth client IDs.**

Click **Configure**.



Selected application — Custom eSignature · Web · Verified

Access to Google data

Choose an access type to specify which data this app can request from users signing in with their Google Account.
Learn more about app access to Google data

● Trusted
This app can request access to user data in any Google service via OAuth 2.0 scopes.
What to expect with trusted access

○ Limited
This app can request access to user data in any Google service marked unrestricted under Google services.
What to expect with limited access

○ Specific Google data
This app can only request access to user data from the Google services specified below. Note, you must include the Google Sign-In scope below to allow users to sign in with their Google Account.

Google Workspace Admin	1 scope
Google sign-in	2 scopes

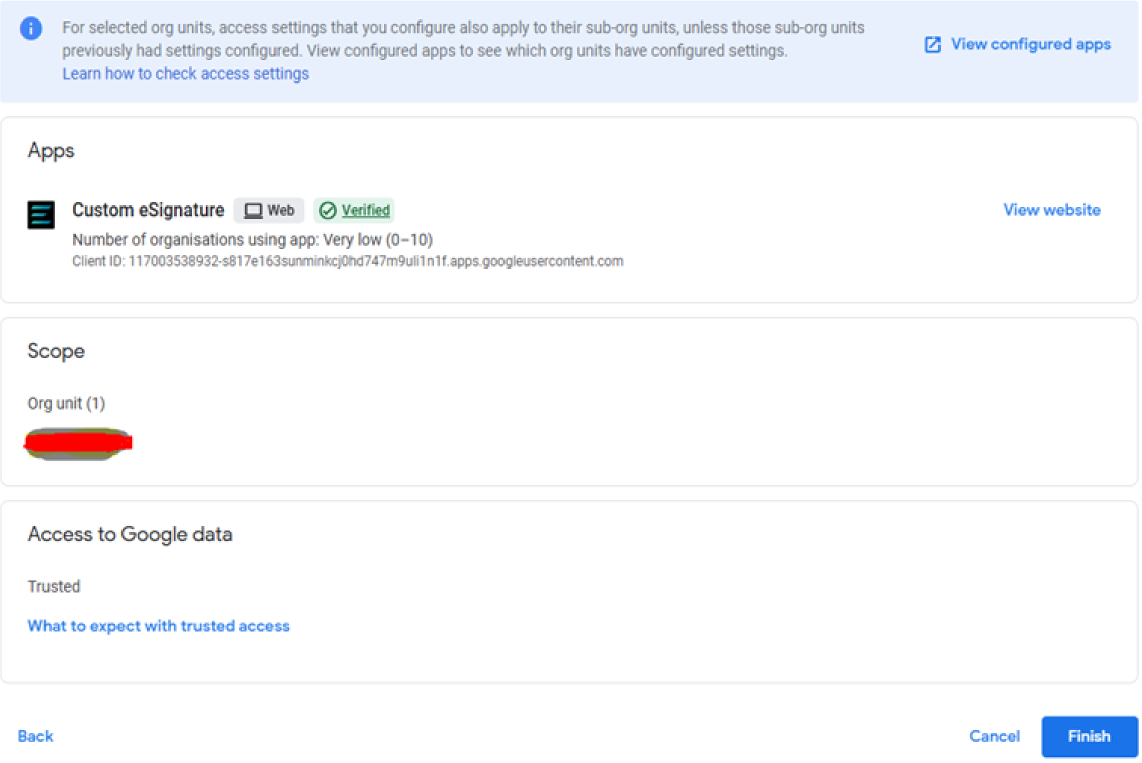
Update Google services or scopes

○ Blocked
Users can't sign in to this app with their Google Account, and the app can't request access to user data in any Google service.

6. **Confirm Information:**

Carefully review and confirm all the displayed information.

Click **Continue**.



For selected org units, access settings that you configure also apply to their sub-org units, unless those sub-org units previously had settings configured. View configured apps to see which org units have configured settings. Learn how to check access settings

Apps

Custom eSignature

Number of organisations using app: Very low (0–10)

Client ID: 117003538932-s817e163sunminkcj0hd747m9uli1n1f.apps.googleusercontent.com

Scope

Org unit (1)

[redacted]

Access to Google data

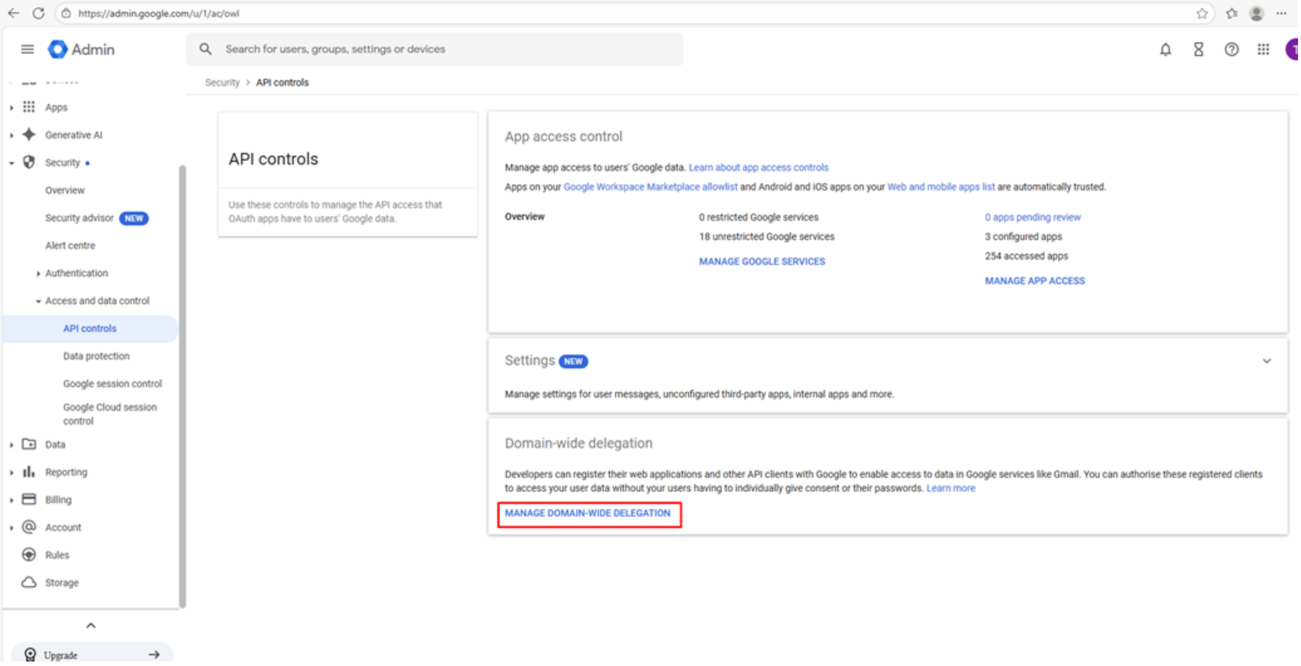
Trusted

What to expect with trusted access

Step 3: Configure Domain-Wide Delegation

1. **Access API Control (Revisit):**

   Click on **Go to the Google Admin "API control"** again.



API controls

Use these controls to manage the API access that OAuth apps have to users' Google data.

App access control

Manage app access to users' Google data. Learn about app access controls

Apps on your Google Workspace Marketplace allowlist and Android and iOS apps on your Web and mobile apps list are automatically trusted.

Overview

0 restricted Google services
18 unrestricted Google services
MANAGE GOOGLE SERVICES

0 apps pending review
3 configured apps
254 accessed apps
MANAGE APP ACCESS

Settings NEW

Manage settings for user messages, unconfigured third-party apps, internal apps and more.

Domain-wide delegation

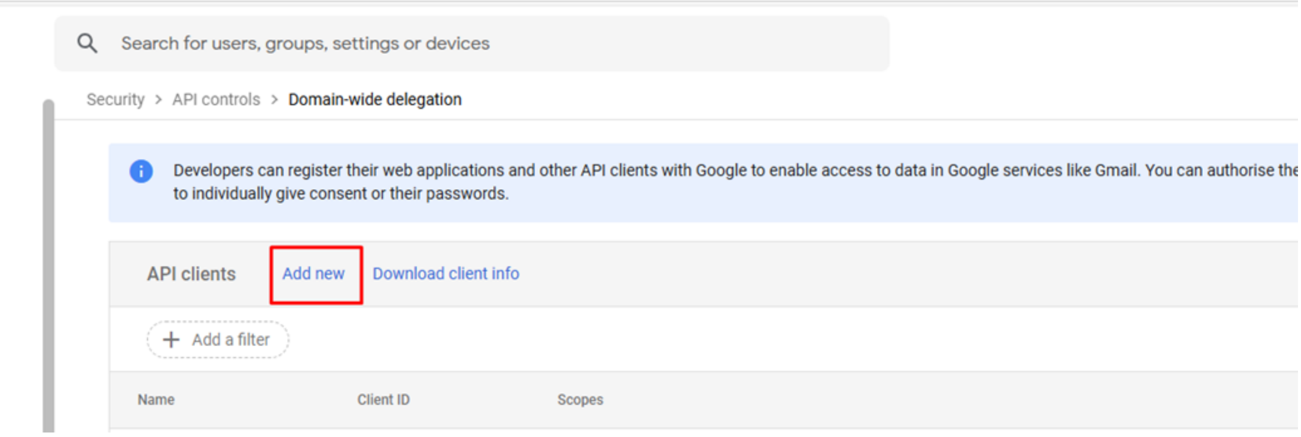
Developers can register their web applications and other API clients with Google to enable access to data in Google services like Gmail. You can authorise these registered clients to access your user data without your users having to individually give consent or their passwords. Learn more

MANAGE DOMAIN-WIDE DELEGATION

2. **Manage Domain-Wide Delegation:**

Click on **Manage Domain Wide Delegation**.

Under **API clients**, click on **Add new**.



Search for users, groups, settings or devices

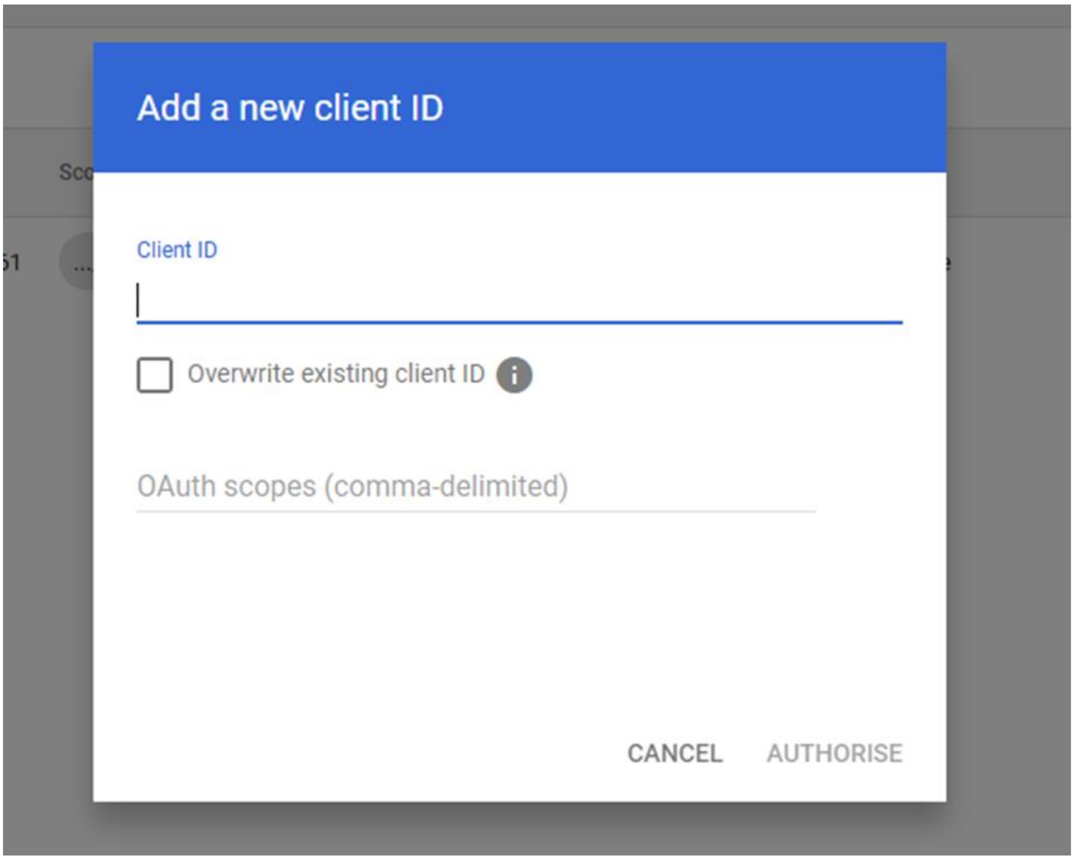
Security > API controls > Domain-wide delegation

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Gmail. You can authorise the to individually give consent or their passwords.

3. **Add Client ID and OAuth Scopes:**

First, add the CustomEsignature Client ID.

Please add this client ID: **104231469178207939061**

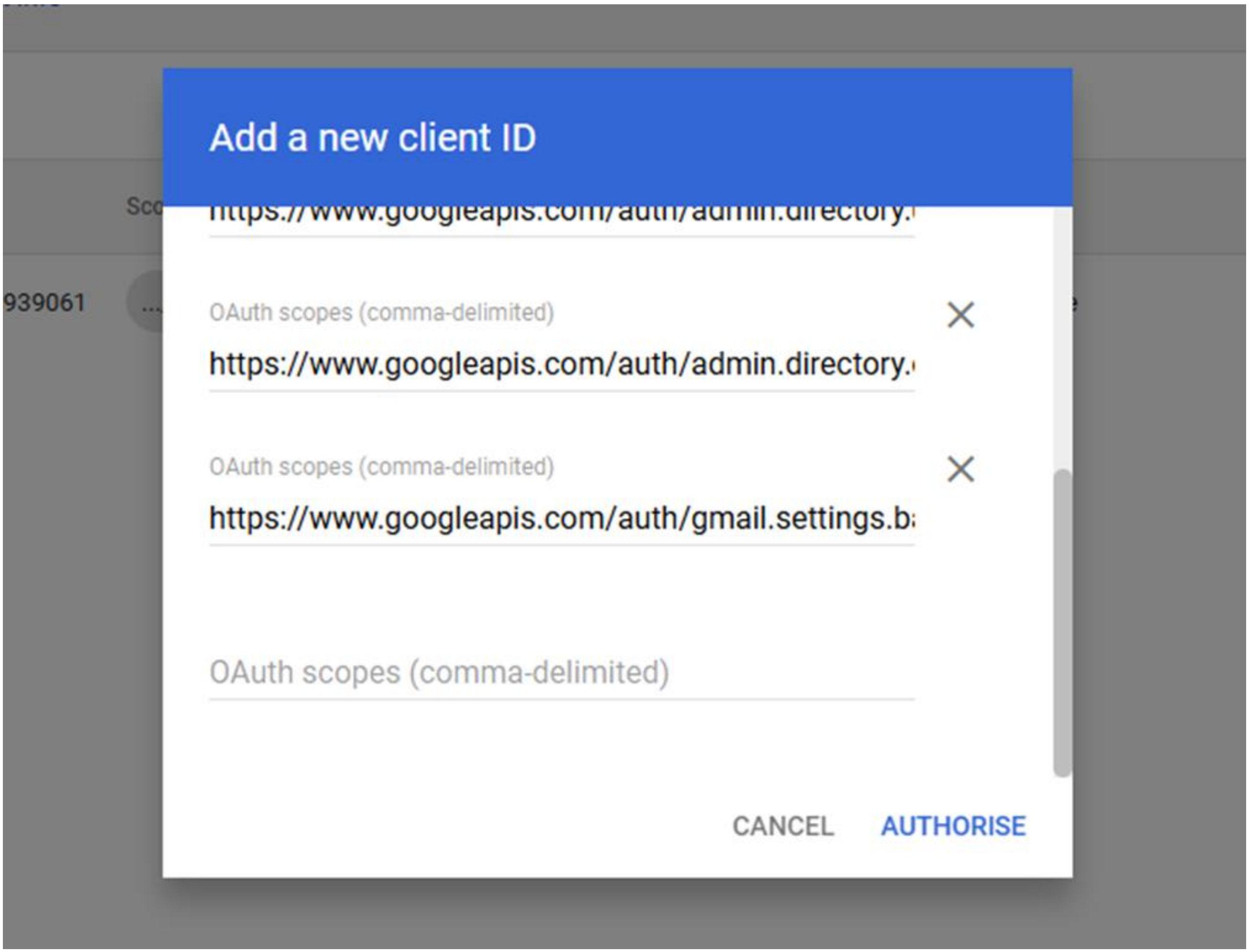


Add a new client ID

Client ID
□ Overwrite existing client ID
OAuth scopes (comma-delimited)
CANCEL
AUTHORISE

After adding the Client ID, **add** the following OAuth Scopes in the **OAuth Scopes** screen:

1. https://www.googleapis.com/auth/gmail.readonly
2. https://www.googleapis.com/auth/admin.directory.user
3. https://www.googleapis.com/auth/admin.directory.orgunit.readonly
4. https://www.googleapis.com/auth/gmail.settings.basic



Add a new client ID

https://www.googleapis.com/auth/admin.directory.

OAuth scopes (comma-delimited)
https://www.googleapis.com/auth/admin.directory.

OAuth scopes (comma-delimited)
https://www.googleapis.com/auth/gmail.settings.b

OAuth scopes (comma-delimited)

4. **Authorize:**

Click on the **Authorise** button. After adding the scopes, they will be listed on the page.

Part 2: Install the Google Workspace Marketplace App for Your Domain

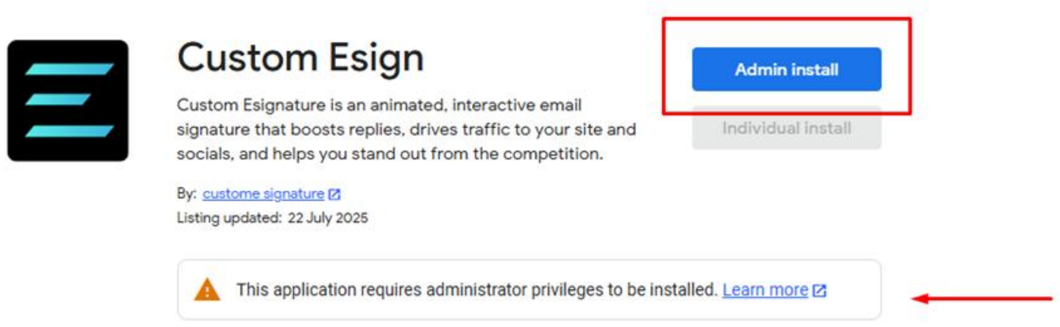
This section guides you through installing the CustomEsignature application from the Google Workspace Marketplace.

1. **Go to Google Workspace Marketplace:**

   Navigate to the Google Workspace Marketplace app page for CustomEsignature: **https://workspace.google.com/marketplace/app/custom_esign/117003538932**

2. **Install the App:**

   Click on **Install the app for your domain**. Please note that only a Google Admin user can install this application.



Custom Esign

Custom Esignature is an animated, interactive email signature that boosts replies, drives traffic to your site and socials, and helps you stand out from the competition.

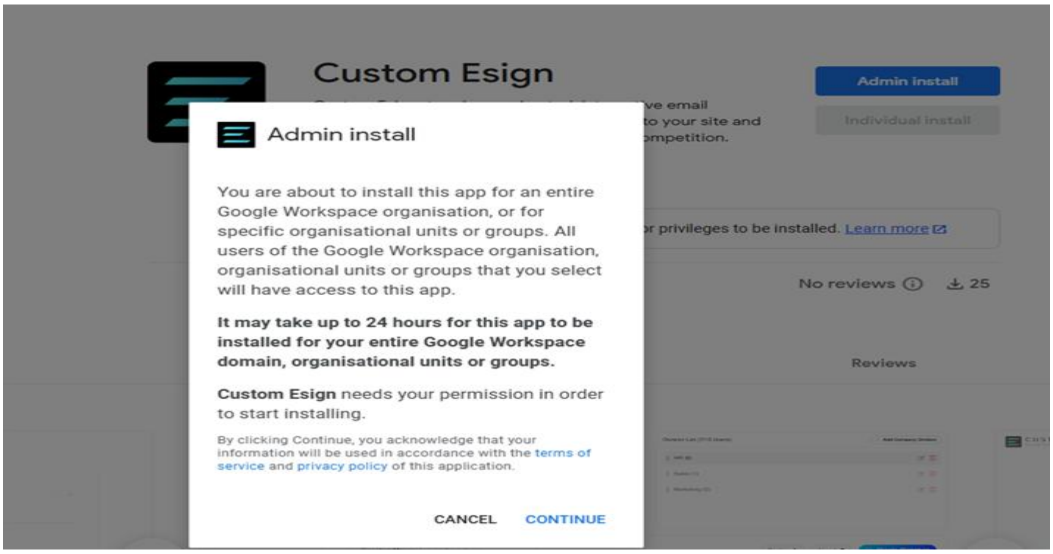
By: custome signature

Listing updated: 22 July 2025

This application requires administrator privileges to be installed. Learn more

3. **Admin Install:**

   Click on **Admin Install** and then click the button to proceed. A confirmation popup will be displayed.



Admin install

You are about to install this app for an entire Google Workspace organisation, or for specific organisational units or groups. All users of the Google Workspace organisation, organisational units or groups that you select will have access to this app.

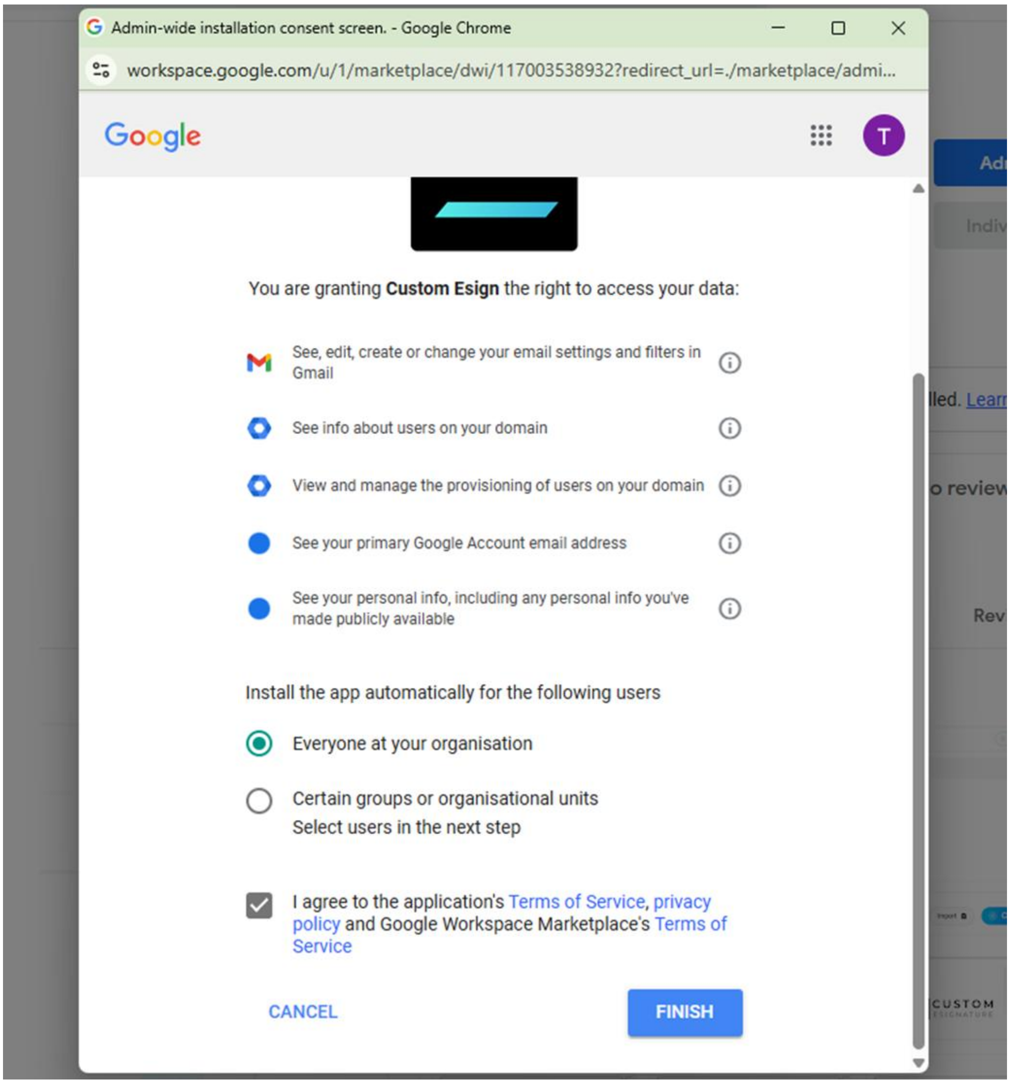
It may take up to 24 hours for this app to be installed for your entire Google Workspace domain, organisational units or groups.

Custom Esign needs your permission in order to start installing.

By clicking Continue, you acknowledge that your information will be used in accordance with the terms of service and privacy policy of this application.

4. **Grant Permission and Finish:**

Grant the necessary permissions by clicking on the **Terms & Conditions** popup. Click on the **Finish** button.


Admin-wide installation consent screen. - Google Chrome
workspace.google.com/u/1/marketplace/dwi/117003538932?redirect_url=./marketplace/admi...
Google
T

You are granting **Custom Esign** the right to access your data:

- See, edit, create or change your email settings and filters in Gmail
- See info about users on your domain
- View and manage the provisioning of users on your domain
- See your primary Google Account email address
- See your personal info, including any personal info you've made publicly available

Install the app automatically for the following users

● Everyone at your organisation

○ Certain groups or organisational units
Select users in the next step

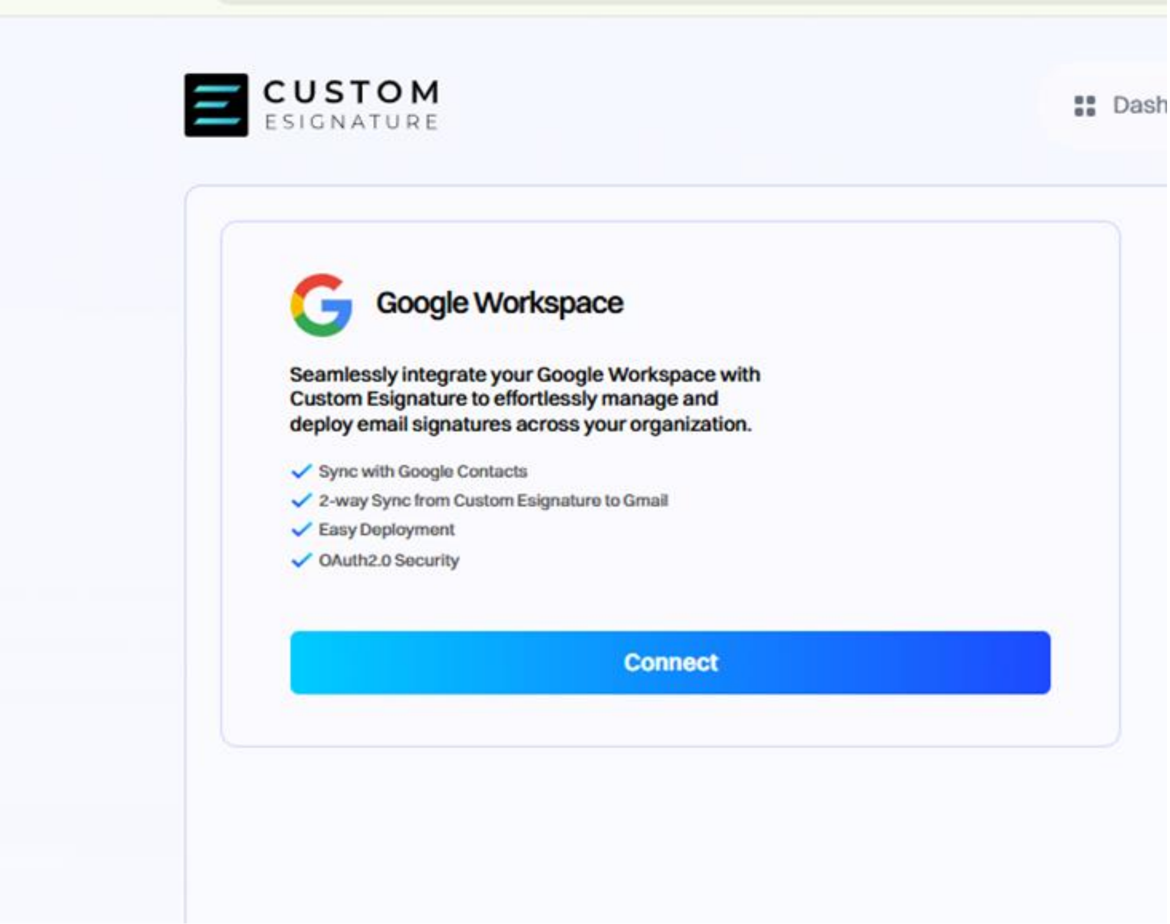
☑ I agree to the application's Terms of Service, privacy policy and Google Workspace Marketplace's Terms of Service

At this point, the integration setup within Google Workspace is complete. You will now proceed to the CustomEsignature platform to finalize the connection.

Part 3: Connect CustomEsignature with Google Workspace

This final section outlines the steps to connect your CustomEsignature account with your Google Workspace integration.

1. **Log in to CustomEsignature Dashboard:**
   Log in to your CustomEsignature dashboard.
2. **Navigate to Integrations:**
   Navigate to the **Integrations** section within your CustomEsignature dashboard.



Google Workspace

Seamlessly integrate your Google Workspace with Custom Esignature to effortlessly manage and deploy email signatures across your organization.

- ✓ Sync with Google Contacts
- ✓ 2-way Sync from Custom Esignature to Gmail
- ✓ Easy Deployment
- ✓ OAuth2.0 Security

3. **Click Connect:**
   Locate the Google Workspace integration block and click **Connect**.