



In the Aranda SERVICE DESK ASDK V8 configuration processes, learn about the configuration for Oauth/Microsoft Modern Authentication.

OAuth 2.0 Authentication - Microsoft

Preconditions

1. An Azure account with permissions to manage applications in Azure Active Directory (Azure AD). Any of the following Azure AD roles include the required permissions:

- Application Manager.
- Application developer.
- Cloud application manager.

2. POSTMAN application for the refresh_token.

Creating an Application in Azure

How to build an app in Azure

1. Access the Azure portal [View Microsoft Azure](#), search and select Azure Active Directory.

The screenshot shows the Microsoft Azure portal interface. On the left, there is a sidebar with various service icons and links. An arrow points to the 'Azure Active Directory' icon, which is highlighted with a yellow background. The main content area displays a dashboard for Azure Active Directory, including sections for 'Administración de costos', 'Grupos de recursos', 'Suscripciones', 'Todos los recursos', and 'Proveedores de servicios'. Below this, there is a table showing resource usage statistics. At the bottom of the sidebar, the 'Azure Active Directory' link is also highlighted with a yellow background.

2. In the Administer Search and select Application logs, click New Registration.

The screenshot shows the 'Aranda Software Corp | Registros de aplicaciones' page in the Azure Active Directory section. The left sidebar has 'Administrar' selected, with 'Registros de aplicaciones' highlighted. The main area shows a message about the deprecation of ADAL and Graph, followed by tabs for 'Todas las aplicaciones', 'Aplicaciones propias' (which is selected), and 'Aplicaciones eliminadas'. A search bar and a 'Agregar filtros' button are present. Below, a table lists registered applications, showing columns for Nombre para mostrar, Id. de aplicación, Fecha de c..., and Certificados y secretos. Two entries are listed, both marked as 'Current'.

3. The name field is filled in and the desired option is selected under (Supported Account Types), click Register.

The screenshot shows the 'Registrar una aplicación' (Register an application) form. It starts with a 'Nombre' (Name) field containing 'Nombre de la Aplicación'. Below it is a section titled 'Tipos de cuenta compatibles' (Compatible account types) with three options: 'Solo cuentas de este directorio organizativo (solo de Aranda Software Corp: inquilino único)', 'Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: multiinquilino)', and 'Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: multiinquilino) y cuentas de Microsoft personales (como Skype o Xbox)'. The first option is selected. At the bottom, there is a checkbox for accepting Microsoft platform terms and a red-outlined 'Registrar' (Register) button.

4. Once your app is registered, save the following data that is required for configuration in Aranda apps.

- Application ID (Client) -> Client ID.

Click on the option (Endpoints).

- OAuth 2.0 authorization endpoint (v2) -> authorization URL.
- OAuth 2.0 (v2) token endpoint -> token URL.

Microsoft Azure | Buscar recursos, servicios y documentos (G+) | ARANDA SOFTWARE CORP

Inicio > Aranda Software Corp | Registros de aplicaciones > AutModerna

Información general

Buscar (Ctrl+ /)

Eliminar Puntos de conexión Características en versión preliminar

¿Tiene un segundo? Nos encantaría conocer su opinión sobre la plataforma de identidad de Microsoft (anteriormente Azure AD para desarrolladores).

^ Información esencial

Nombre para mostrar: AutModerna
Id. de aplicación (cliente): [REDACTED]
Identificador de objeto: [REDACTED]
Id. de directorio (inquilino): [REDACTED]
Tipos de cuenta compatibles: Solo mi organización

Credenciales de cliente: 0 certificado_1secreto
URI de redirección: 2 web_0 SPA_0 cliente público
URI de id. de aplicación: Agregar un URI de id. de aplicación
Aplicación administrada en directorio local: AutModerna

Microsoft Azure | Buscar recursos, servicios y documentos (G+) | ARANDA SOFTWARE CORP

Inicio > Aranda Software Corp | Puntos de conexión

Nombre de la aplicación: Normbre

Punto de conexión de autorización de OAuth 2.0 (v2): https://login.microsoftonline.com/[REDACTED]/oauth2/v2.0/authorize

Punto de conexión de token de OAuth 2.0 (v2): https://login.microsoftonline.com/[REDACTED]/oauth2/v2.0/token

Punto de conexión de autorización de OAuth 2.0 (v1): https://login.microsoftonline.com/[REDACTED]/oauth2/authorize

Punto de conexión de token de OAuth 2.0 (v1): https://login.microsoftonline.com/[REDACTED]/oauth2/token

Documento de metadatos de OpenID Connect: https://login.microsoftonline.com/[REDACTED]/.well-known/openid-configuration

Punto de conexión de la API de Microsoft Graph: https://graph.microsoft.com

Documento de metadatos de federación: https://login.microsoftonline.com/[REDACTED]/federationmetadata/2007-06/federationmetadata.xml

Configure your application in the Azure portal

When you have the application created and have the data saved, you proceed to configure the application as follows:

How to set up authentication

1. You enter the Azure portal > Azure Active Directory > Menu > Application Logs > select the created application from the list that appears in the view.
2. In the Administer Search and select > Authentication then in Add a platform, select the Web.

Microsoft Azure | Buscar recursos, servicios y documentos (G+) | ARANDA SOFTWARE CORP

Inicio > Aranda Software Corp | Registros de aplicaciones > Nombre de la Aplicación

Nombre de la Aplicación | Autenticación | Configurar plataformas

Buscar (Ctrl+ /)

Configuraciones de p

En función de la plataforma configura más elementos, como la plataforma.

+ Agregar una plataforma

Aplicaciones web

Web: Permite compilar, hospedar e implementar una aplicación de servidor web .NET, Java y Python.

Aplicación de página única: Configure aplicaciones cliente de explorador y aplicaciones web progresivas. JavaScript.

Tipos de cuenta com

Quién puede usar esta aplicación:

- Solo cuentas de este directorio
- Cuentas en cualquier dirección

Guardar Descarta

Aplicaciones móviles y de escritorio

iOS/macOS: Objective-C, Swift, Xamarin

Android: Java, Kotlin, Xamarin

3. In the redirect URI field, we add the following value http://localhost, and then select Configure.

Creation of the Secret

1. To create the secret, enter the Azure portal > Azure Active Directory > Menu > Application Logs > select the created application from the list that appears in the view.
2. In the Administer Search and select Certificates and secrets > Then click New client secret.

3. At the Hearing Add a client secret fill in the field Description, configure the Expires which corresponds to the duration of the secrecy. Then select Add (It is important to always keep this duration in mind since, when it expires, if it is not updated, authentication will fail.)

4. The value of the secret is only visible when it is created, so it must be saved for later use and retained for the configurations required in Aranda products.

- Client Secret Value -> Client Secret.

User and group settings

In this configuration, the email account(s) that will be able to access the application are associated.

1. You enter the Azure portal> Menu> Azure Active Directory> Business Applications> select the created application from the list that appears in the view.

2. In the Administer Search and select Users and groups> and then Add User or Group.

3. In the Add Mapping view, select None selected> Then look for the email account(s) you want to add, when you have all the emails selected click on Select.

4. Finally select Assign.

Refresh Token Request

How to request the Azure Refresh Token

For refresh request_token, you must use the Postman desktop application and perform the following actions:

1. Create a new collection in Postman and select OAuth 2.0 in the authorization type.

2. At the hearing, the fields must be filled in as follows:

The screenshot shows the Postman interface with the following details:

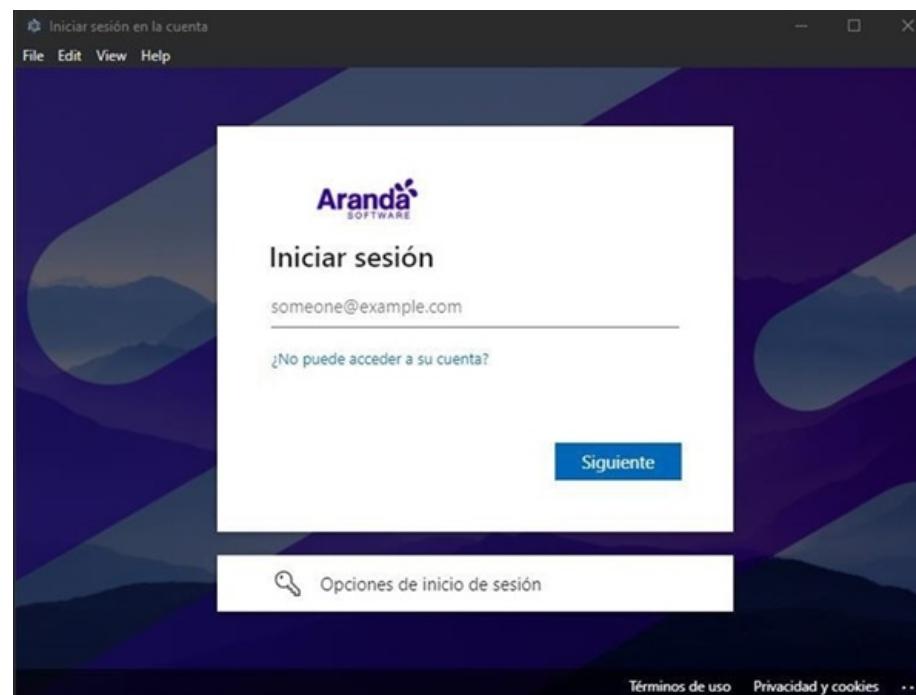
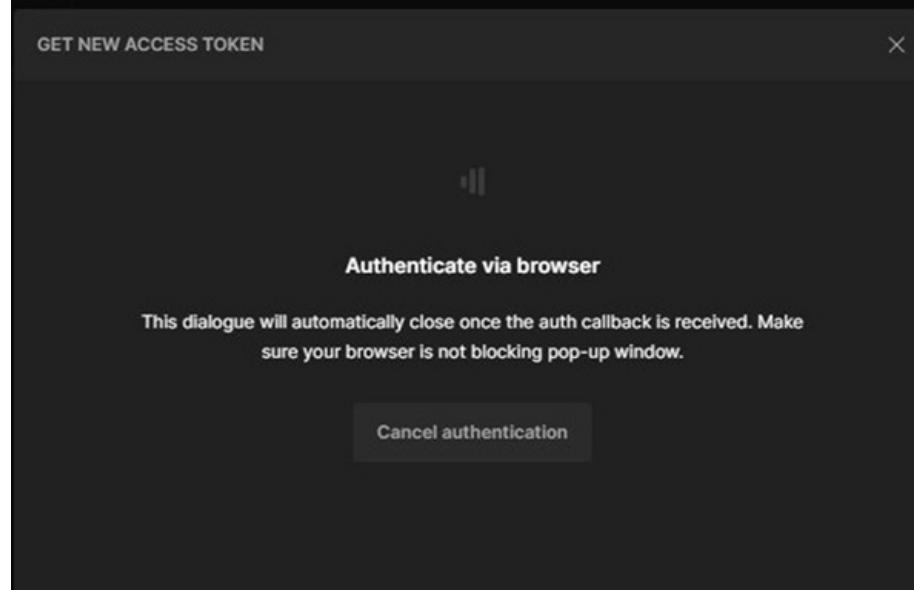
- Authorization Method:** OAuth 2.0
- Add auth data to:** Request Headers
- Current Token:** Available Tokens (Access Token selected)
- Header Prefix:** Bearer
- Configure New Token:**
 - Token Name:** Enter a token name...
 - Grant Type:** Authorization Code
 - Callback URL:** http://your-application.com/registered.
 - Auth URL:** https://example.com/login/oauth/authz
 - Access Token URL:** https://example.com/login/oauth/acce
 - Client ID:** Client ID
 - Client Secret:** Client Secret
 - Scope:** e.g. read.org
 - State:** State
 - Client Authentication:** Send as Basic Auth header

Field	Description
Type	OAuth 2.0
Add auth data to	Request Headers
Access Token	Available Token
Header Prefix	Bearer
Token Name	Name you want for the token
Grant Type	Authorization Code
Callback URL	http://localhost
Auth URL	Enter the value of OAuth 2.0 authorization endpoint (v2) .
Access Token URL	Enter the value of OAuth 2.0 (v2) token endpoint .
Client ID	Enter the value of Application ID (client) .
Client Secret	Enter the Secret Customer Value .
Scope	offline_access https://outlook.office.com/SMTP.Send https://outlook.office.com/IMAP.AccessAsUser.All https://outlook.office.com/POP.AccessAsUser.All
State	It can be left blank.
Client Authentication	Send as Basic Auth header

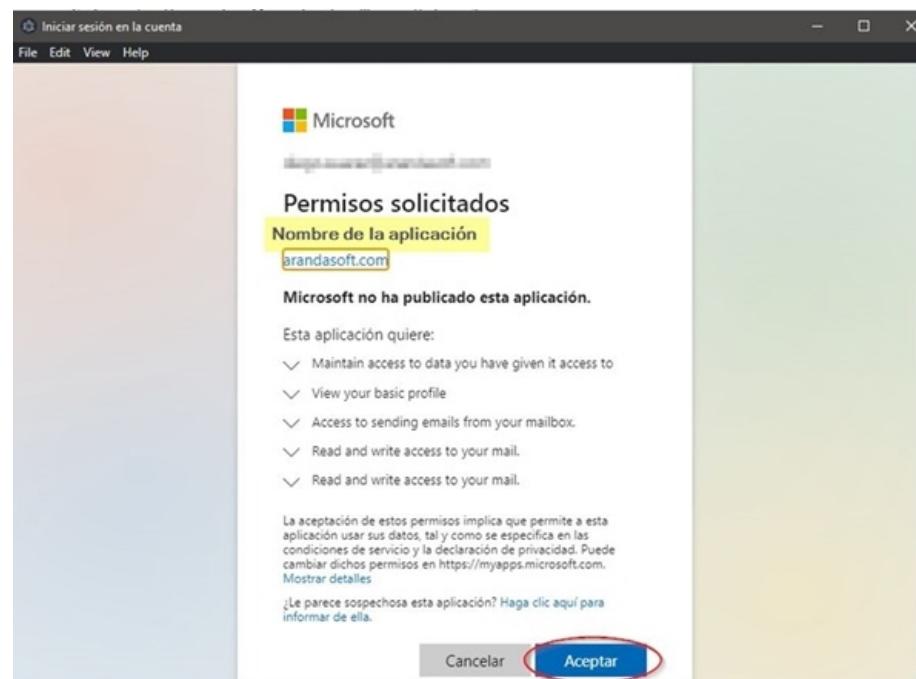
3. When entering all the information select Get New Access Token.

▷ Note: To ensure the correct generation of the Refresh_Token, it is essential to check the URLs entered in the Scope and make sure that they do not contain line breaks or white spaces at the beginning or end.

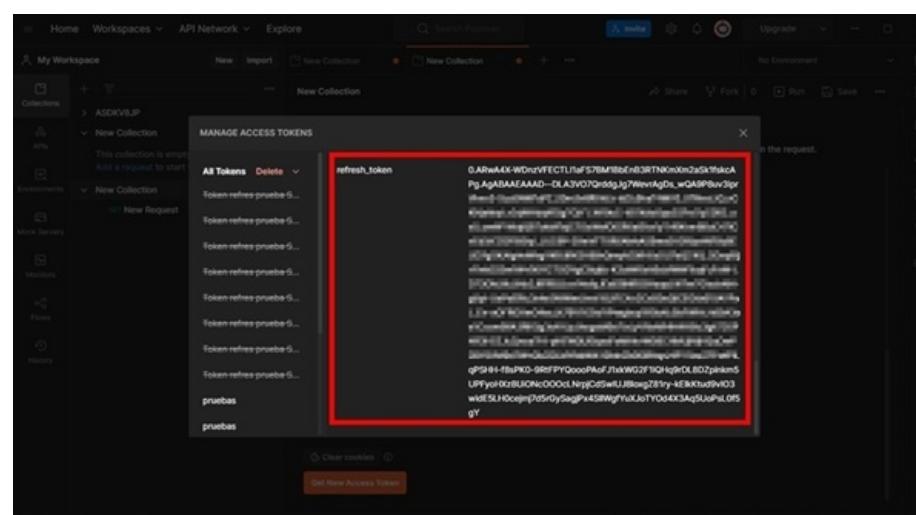
4. Two windows open, one window to enter the access credentials and the other where the Token application process is displayed.



5. The session must be logged in with one of the accounts added in the [User and Group Settings](#), when the entry is made correctly, the session will request that we accept the requested permissions.



5. After accepting the permissions, you must proceed to copy the refresh_token, save this token since it will be used in the configurations of (Mail) and (Case creator) in the Aranda applications.



Preconditions

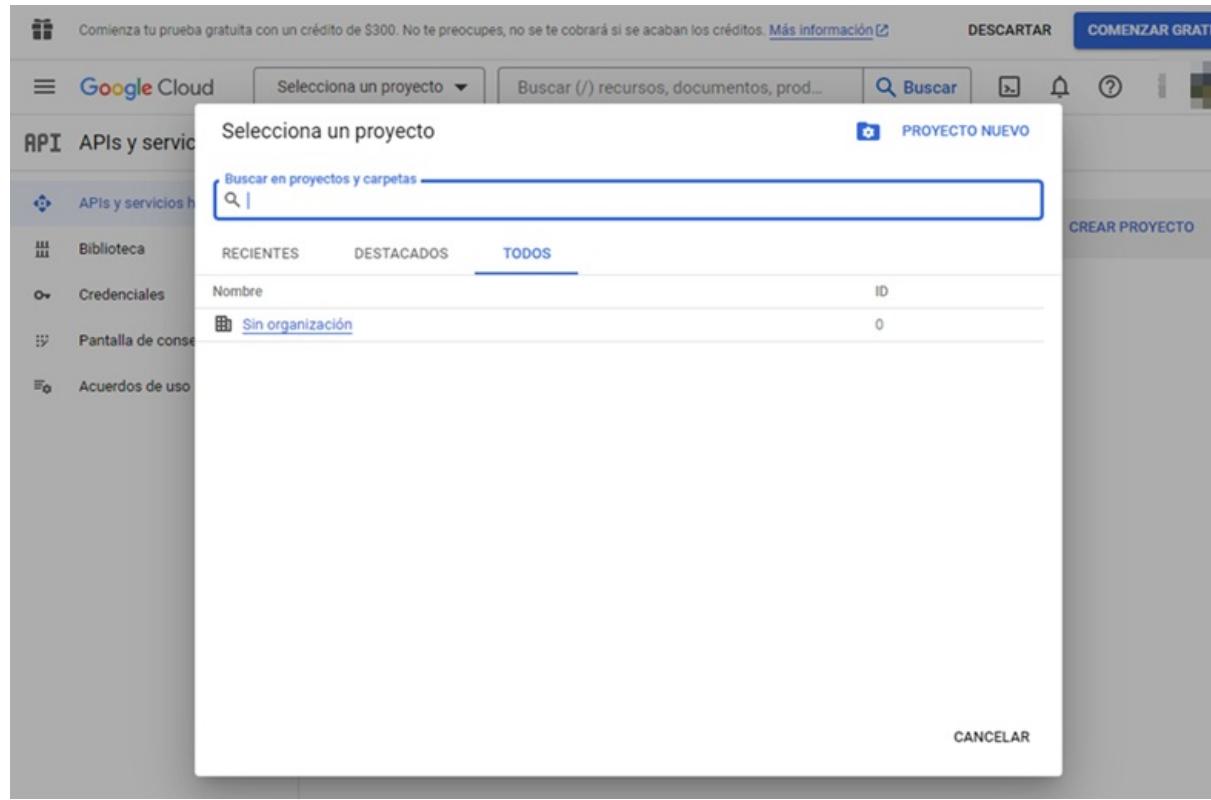
1. A Google Account with one of the Admin, Billing Admin, or Project Billing Manager roles. It can also be the same one you'll use to send and receive emails.
2. POSTMAN application for the refresh_token.

Creating a project on Google

▷ Note: If you already have a project set up on Google, you can skip this step.

How to create a project on Google

1. Access to the [Google Cloud Console](#) with the Google Account designated for this process, select the drop-down menu Select a project in the top navigation menu. Then, click the NEW PROJECT.



2. In the window New project Enter the four requested fields following the recommendations and click the CREATE.

Nombre del proyecto *	Nombre del Proyecto
ID del proyecto *	nombre-del-proyecto-123
El ID del proyecto puede contener letras minúsculas, números o guiones. Debe empezar con una letra en minúscula y terminar con una letra o un número.	
Organización *	Nombre de la Organización
Selecciona una organización para vincularla a un proyecto. No podrás cambiar esta selección más adelante.	
Ubicación *	Nombre de la Organización
Organización o carpeta superior	
CREAR	CANCELAR

▷ Note: If in the field Organization only the option is listed No organization is that the user with whom the project is being created does not have the required permissions.

3. The window is enabled Notifications. Click the SELECT PROJECT For the project created:

The screenshot shows the Google Cloud Console interface. In the top left, it says "Google Cloud". To its right is a dropdown menu labeled "Nombre del Proyecto". On the far right are icons for search, refresh, notifications, help, and more. The main navigation bar has "API" selected, followed by "APIs y servicios". Under this, "APIs y servicios habilitados" is highlighted. The main content area is titled "Notificaciones" and shows a notification: "Crear proyecto: Nombre del Proyecto Hace unos instantes" with a "SELECCIONAR PROYECTO" button. Below it is a link "VER TODAS LAS ACTIVIDADES". At the bottom of the notifications panel is a timestamp "12:00 p.m.". A modal window is open in the center, displaying the message: "Estás viendo el proyecto \"Nombre del Proyecto\" en la organización \"Nombre de la Organización\"". There is also a note: "Este proyecto es el que has seleccionado." and a close button "X".

4. In the drop-down menu Select a project You will be able to display the name of the created project.

Create and configure your app on Google

When the project is created and selected, proceed with the creation of an OAuth application as follows:

How to create an app on Google

1. In the Google Cloud Console section APIs and services Select the option OAuth Consent Screen and the type of user

- Select Internal if you're using a GSuite admin tenant and you're creating the app exclusively for your organization.
- Select External if you're trying a separate Gmail account.

The screenshot shows the Google Cloud Console interface. The navigation bar has "API" selected, followed by "APIs y servicios". Under this, "Pantalla de consentimiento de OAuth" is highlighted. The main content area is titled "Pantalla de consentimiento de OAuth". It contains a descriptive text: "Elige cómo deseas configurar y registrar tu app, incluidos los usuarios objetivo. Puedes asociar una sola app con tu proyecto." Below this is a section titled "User Type". It shows two radio buttons: " Interno" and " Externos". The "Internos" section includes text: "Solo está disponible para los usuarios de tu organización. No necesitarás enviar tu app para verificarla. [Obtén más información sobre el tipo de usuario](#)". The "Externos" section includes text: "Está disponible para cualquier usuario de prueba con una Cuenta de Google. Tu app se iniciará en modo de prueba y solo estará disponible para los usuarios que agregues a la lista de usuarios de prueba. Una vez que la app esté lista para enviarse a producción, puedes que debas verificarla. [Obtén más información sobre el tipo de usuario](#)". At the bottom is a blue "CREAR" button.

2. Click the CREATE. 3. In the window OAuth Consent Screen Enter the fields App Name, User Support Email in the Application Information and Email addresses in the Developer Contact Information according to the recommendations of each field(the other fields are optional). Then, click the SAVE & CONTINUE.

API APIs y servicios

Editar el registro de la app

1 Pantalla de consentimiento de OAuth — 2 Permisos —

3 Resumen

Información de la aplicación

Esta información aparece en la pantalla de consentimiento y permite que los usuarios finales sepan quién eres y cómo comunicarse contigo

Nombre de la aplicación * _____
Nombre de la Aplicación _____

El nombre de la aplicación que solicita el consentimiento

Correo electrónico de asistencia del usuario * _____
usuario@dominio.com

Para que los usuarios se comuniquen contigo si tienen preguntas sobre su consentimiento. [Más información](#)

Logotipo de la app

Este es tu logotipo. Ayuda a que las personas reconozcan tu app y aparece en la pantalla de consentimiento de OAuth.

Después de subir un logotipo, deberás enviar tu app para verificarla, a menos que esté configurada solo para uso interno o tenga el estado de publicación "Prueba". [Más información](#)

Dominios autorizados

Cuando un dominio se usa en la pantalla de consentimiento o en la configuración del cliente de OAuth, debe contar con un registro previo aquí. Si debes verificar la app, ve [Google Search Console](#) para comprobar si tus dominios están autorizados. [Más información](#) sobre el límite de dominios autorizados.

+ AGREGAR UN DOMINIO

Información de contacto del desarrollador

Direcciones de correo electrónico * _____
usuario@dominio.com

Google enviará notificaciones sobre cualquier cambio en tu proyecto a estas direcciones de correo electrónico.

GUARDAR Y CONTINUAR **CANCELAR**

4. In the window Permissions Click the ADD OR REMOVE PERMISSIONS.

API APIs y servicios

Editar el registro de la app

1 Pantalla de consentimiento de OAuth — 2 Permisos —

3 Resumen

Los permisos representan lo que solicitas que los usuarios autoricen para la app y permiten que tu proyecto tenga acceso a tipos específicos de datos privados del usuario de sus Cuentas de Google. [Más información](#)

AGREGAR O QUITAR PERMISOS

5. In the window Update selected permissions in the Add permissions manually Enter the value <https://mail.google.com/> and click the ADD TO TABLE. Then in UPDATE.

Actualiza los permisos seleccionados

 Solo se muestran los permisos de las APIs habilitadas. Si deseas agregar un permiso faltante a esta pantalla, encuentra y habilita la API en la [Biblioteca de APIs de Google](#) o usa el recuadro para pegar permisos que aparece a continuación. Actualiza la página para ver las APIs nuevas que habilites en la biblioteca.

Filtro Ingresar el nombre o el valor de la propiedad		
<input type="checkbox"/> API ↑	Alcance	Descripción para el usuario
<input type="checkbox"/>	.../auth/userinfo.email	See your primary Google Account email address
<input type="checkbox"/>	.../auth/userinfo.profile	See your personal info, including any personal info you've made publicly available
<input type="checkbox"/>	BigQuery API	Ver tus datos en todos los servicios de Google Cloud y ver la dirección de correo electrónico de tu Cuenta de Google
<input type="checkbox"/>	BigQuery API	Manage your data and permissions in Cloud Storage and see the email address for your Google Account
<input type="checkbox"/>	BigQuery API	Ver tus datos en Google Cloud Storage.
<input type="checkbox"/>	BigQuery API	Administrar tus datos de Cloud Storage y ver la dirección de correo electrónico de tu Cuenta de Google

Filas por página: 10 ▾ 1 – 10 de 24 < >

Agrega permisos manualmente

Si los permisos que quieras agregar no aparecen en la tabla que se muestra más arriba, puedes ingresarlos aquí. Cada permiso debe estar en una línea nueva o debe separarse con comas. Proporciona la string completa del permiso (comienza con "https://"). Cuando termines, haz clic en "Agregar a la tabla".

`https://mail.google.com/`

AGREGAR A LA TABLA

ACTUALIZAR

6. In the window Permissions Verify that the permission has been added in the Your restricted permissions and click the SAVE & CONTINUE to advance to the window Summary where you can view the data from the new application. 7. Select the option Credentials, click the CREATE CREDENTIALS and select the OAuth Client ID.

API APIs y servicios  Credenciales  + CREAR CREDENCIALES  BORRAR 

 APIs y servicios habilitados Clave de API Identifica tu proyecto con una clave de API simple para verificar la cuota y el acceso

 Biblioteca ID de cliente de OAuth Solicita el consentimiento del usuario para que tu app pueda acceder a sus datos

 Credenciales Cuenta de servicio Habilita la autenticación de servidor a servidor en el nivel de la app mediante cuentas robot

 Pantalla de consentimiento Ayúdame a elegir Responde algunas preguntas para decidir qué tipo de credencial usar

 Acuerdos de uso de páginas

<input type="checkbox"/>	Nombre	Fecha de creación	Tipo	ID de cliente	Acciones
No hay clientes de OAuth para mostrar					

Cuentas de servicio [Administrar cuentas de servicio](#)

<input type="checkbox"/>	Correo electrónico	Nombre	Acciones
No hay cuentas de servicio para mostrar			

8. In the window Create OAuth Client ID In the field Application Type, select the Web application.

API APIs y servicios   Crear ID de cliente de OAuth

 APIs y servicios habilitados Un ID de cliente se usa con el fin de identificar una sola app para los servidores de OAuth de Google. Si la app se ejecuta en varias plataformas, cada una necesitará su propio ID de cliente. Consulta [Configura OAuth 2.0](#) para obtener más información. [Obtén más información](#) sobre los tipos de clientes de OAuth.

 Biblioteca

 Credenciales

 Pantalla de consentimiento ...

 Acuerdos de uso de páginas

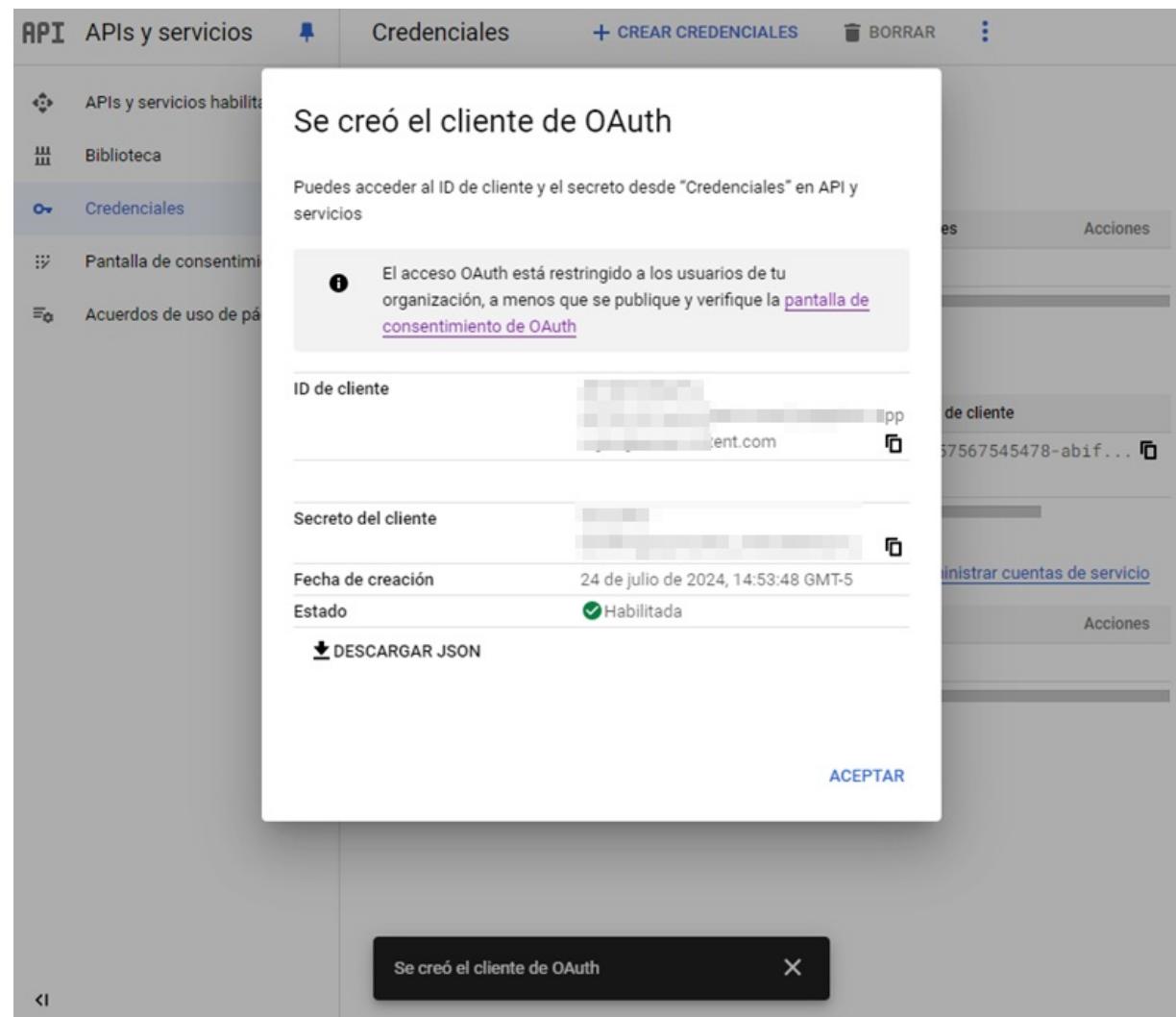
Tipo de aplicación *

- Aplicación web
- Android
- Extensión de Chrome
- iOS
- TVs y dispositivos de entrada limitada
- App de escritorio
- Plataforma universal de Windows (UWP)

9. In the window Create OAuth Client ID in the Authorized redirect URIs add the URI <http://localhost> and click the CREATE.

The screenshot shows the 'Crear ID de cliente de OAuth' (Create OAuth Client ID) page. On the left, there's a sidebar with options like 'APIs y servicios habilitados', 'Biblioteca', 'Credenciales' (which is selected), 'Pantalla de consentimiento ...', and 'Acuerdos de uso de páginas'. The main area has a back arrow and the title 'Crear ID de cliente de OAuth'. A 'Nombre *' field contains 'Cliente web 1'. Below it, a note says: 'Los dominios de los URI que agregues a continuación se incorporarán automáticamente a tu pantalla de consentimiento de OAuth como dominios autorizados.' A 'Orígenes autorizados de JavaScript' section follows, with a note 'Para usar con solicitudes de un navegador' and a '+ AGREGAR URI' button. Another section for 'URI de redireccionamiento autorizados' is shown with a note 'Para usar con solicitudes de un servidor web', a 'URI 1 *' field containing 'http://localhost', and a '+ AGREGAR URI' button. At the bottom are 'CREAR' and 'CANCELAR' buttons.

10. In the window The OAuth client was created save the following data that is required for configuration in Aranda applications and in the generation of the [Refresh Token](#).



- Application ID(Client) -> Client ID.
- Client Secret Value -> Client Secret.
- OAuth 2.0(v2) token endpoint -> <https://oauth2.googleapis.com/token>.

Google Refresh Token Application

How to apply for the Google Refresh Token

For refresh request_token, you must use the Postman desktop application and perform the following actions:

1. Create a new collection in Postman and select OAuth 2.0 in the authorization type.

Untitled Request

GET Enter URL or paste text

Params Authorization Headers (6) Body Scripts Settings

Auth Type

OAuth 2.0

Inherit auth from parent
No Auth
Basic Auth
Bearer Token
JWT Bearer
Digest Auth
OAuth 1.0
 OAuth 2.0
Hawk Authentication
AWS Signature
NTLM Authentication [Beta]
API Key
Akamai EdgeGrid
ASAP (Atlassian)

Current Token

Token

Header Prefix ⓘ

Auto-refresh Token
Your expired token will be auto-renewed before sending a request.

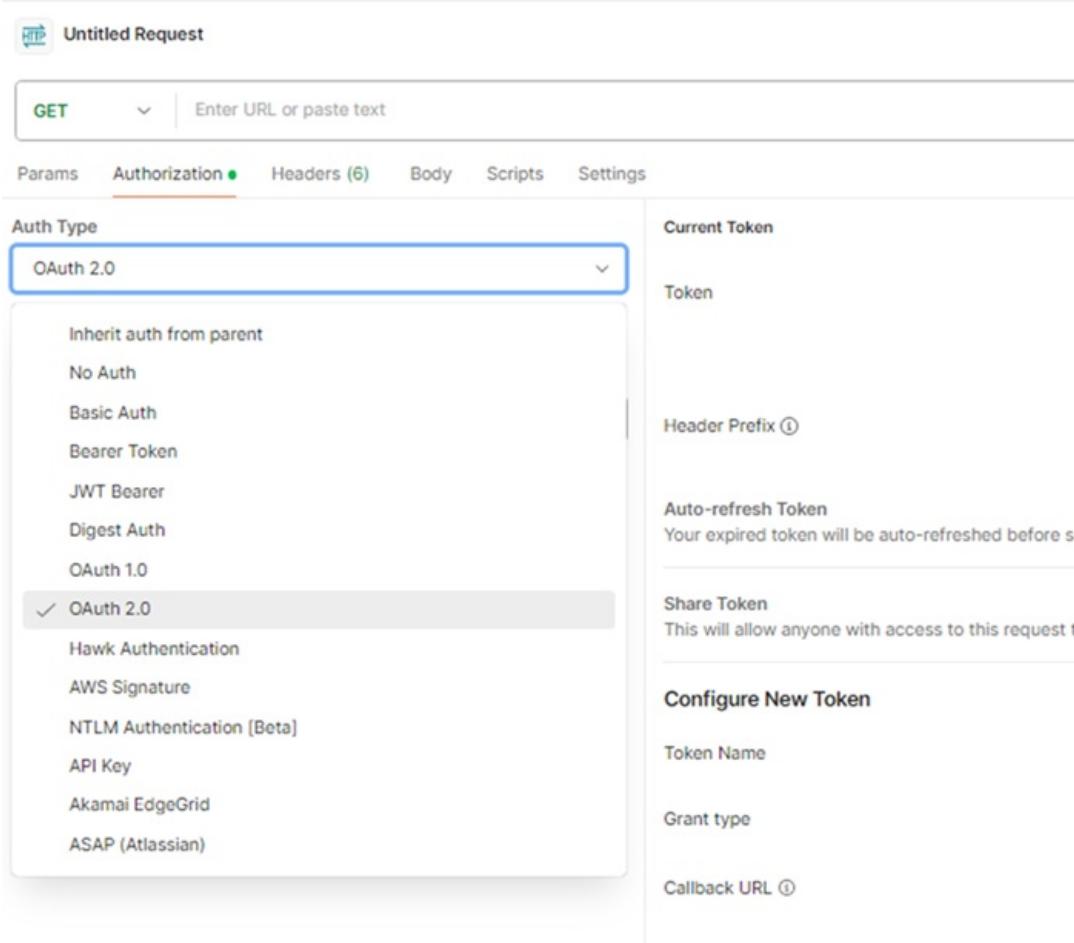
Share Token
This will allow anyone with access to this request to view and use it.

Configure New Token

Token Name

Grant type

Callback URL ⓘ



2. In the view, enter the fields as follows:

Untitled Request

GET Enter URL or paste text

Params Authorization Headers (6) Body Scripts Settings

Auth Type

OAuth 2.0

The authorization data will be automatically generated when you send the request. Learn more about [OAuth 2.0](#) authorization.

Add authorization data to Request Headers

Current Token

Token Available Tokens

Token Prefix Bearer

Header Prefix ⓘ

Auto-refresh Token
Your expired token will be auto-renewed before sending a request.

Share Token
This will allow anyone with access to this request to view and use it.

Configure New Token

Token Name Pruebas Google

Grant type Authorization Code

Callback URL ⓘ http://localhost

Authorize using browser

Auth URL ⓘ https://accounts.google.com/o/oauth2/v2/...

Access Token URL ⓘ https://oauth2.googleapis.com/token

Client ID ⓘ 

Client Secret ⓘ 

Scope ⓘ https://mail.google.com/

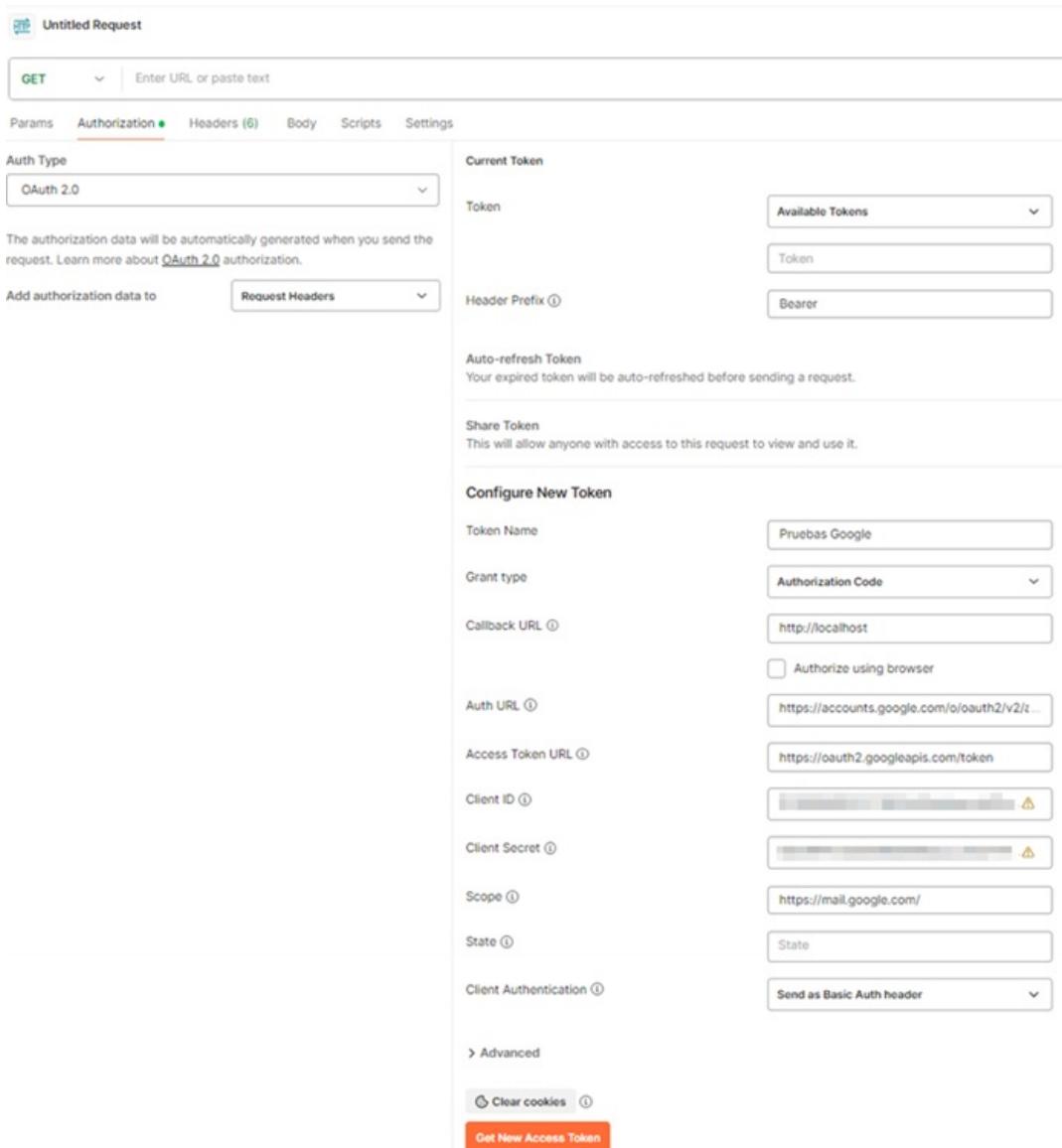
State ⓘ State

Client Authentication ⓘ Send as Basic Auth header

> Advanced

Clear cookies ⓘ

Get New Access Token

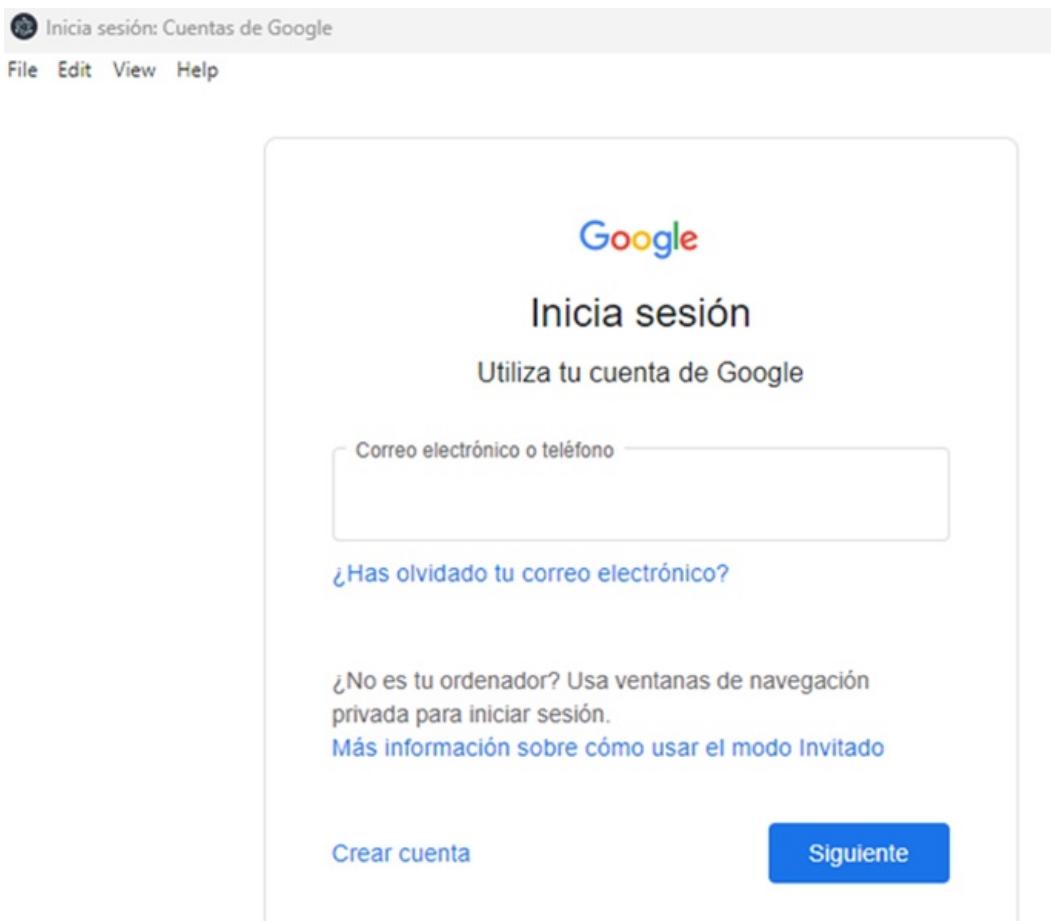


Field	Description
Type	OAuth 2.0
Add auth data to	Request Headers
Access Token	Available Token
Header Prefix	Bearer
Token Name	Name you want for the token
Grant Type	Authorization Code
Callback URL	http://localhost
Auth URL	https://accounts.google.com/o/oauth2/v2/auth?access_type=offline
Access Token URL	https://oauth2.googleapis.com/token
Client ID	Enter the value of Application ID (client) .
Client Secret	Enter Secret Customer Value .
Scope	https://mail.google.com/
State	It can be left blank.
Client Authentication	Send as Basic Auth header

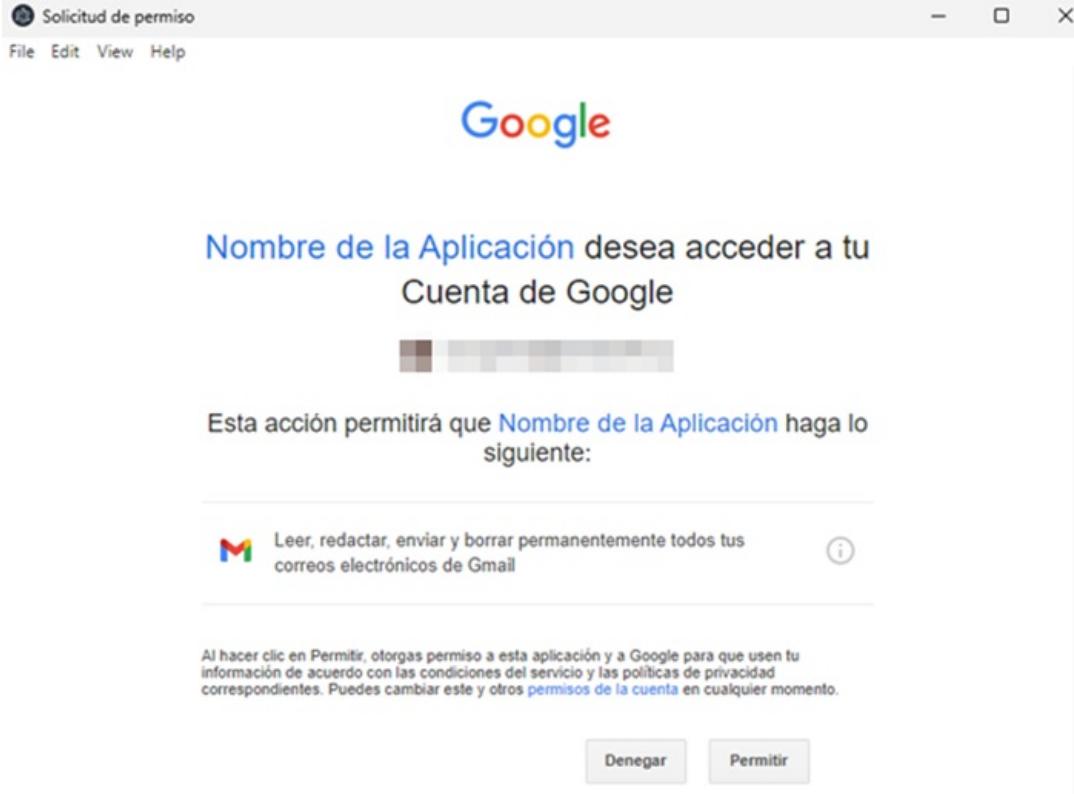
3. When entering all the information select Get New Access Token.

▷ Note: To ensure the correct generation of the Refresh_Token, check the URLs entered and make sure they do not contain line breaks or white spaces, both at the beginning and at the end.

4. The Google Account sign-in window is enabled; Enter the email and password to which the Refresh Token is required to be generated.



5. The session must be held with accounts associated with the organization; If the entry is successful, the session prompts them to accept the required permissions.



5. When accepting permissions, copy and save the refresh_token, as it will be used in the Mail and Case creator settings in Aranda applications.

Token Details		Use Token
Token Name	Pruebas Google	
Access Token		
Token Type	Bearer	
expires_in	3599	
refresh_token	1//0SEDO-1_g0AUH-3M3bu2QW4rc	
scope	https://mail.google.com/	

▷ Note: A refresh token may stop working for reasons such as:

- The user revokes permissions to the app.
- The refresh token is not used for six months.
- The user changed the password and the refresh token contains Gmail permissions.
- The user account exceeded the maximum amount of (live) refresh tokens granted.

For more information, please consult Google's documentation: [Update token expiration](#)