



Configuración de Commons

In the configuration processes of the different Aranda applications, there are transversal concepts and functionalities that allow for the streamlining and sharing of related data for each project. This guide introduces the customer to the pre-configuration to consider for synchronizing active directory users from Microsoft Entra ID.

Microsoft Entra ID Sync

Preconditions

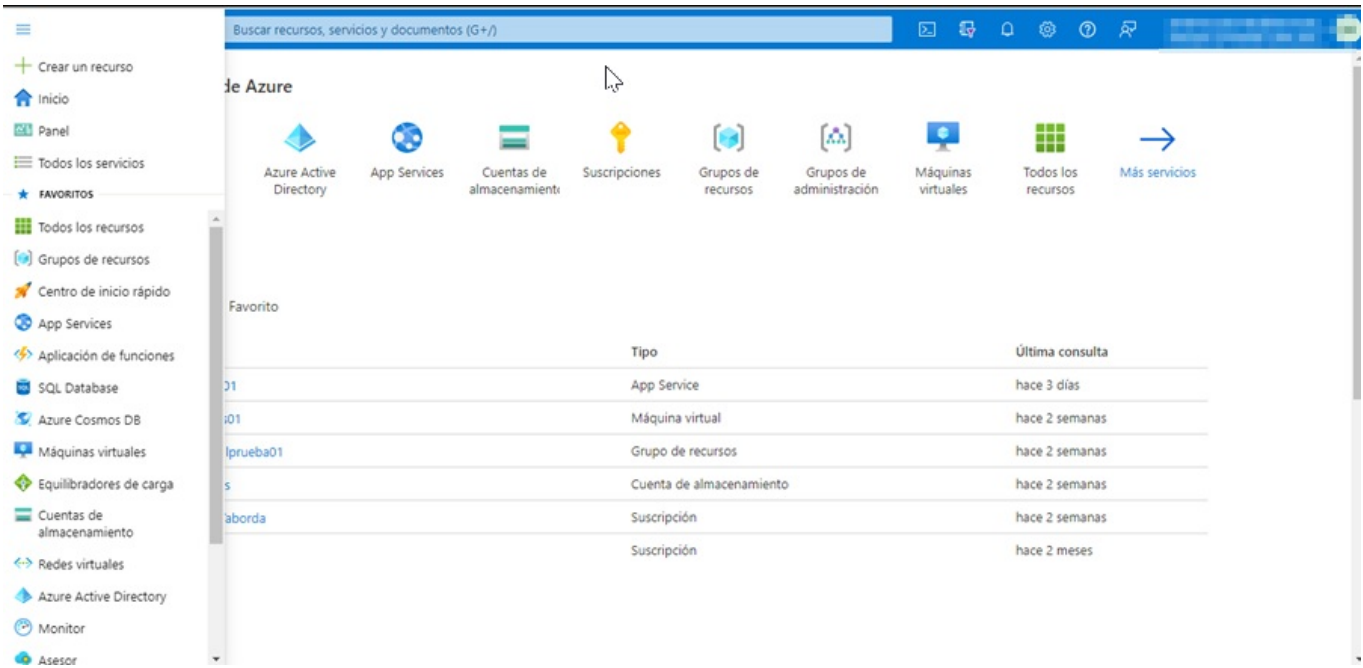
- An Azure account with permissions to manage apps in Microsoft Entra ID.
- Microsoft Roles Enter ID with the required permissions:

```
Application Manager.<br />
Application developer.<br />
Cloud application manager.<br />
```

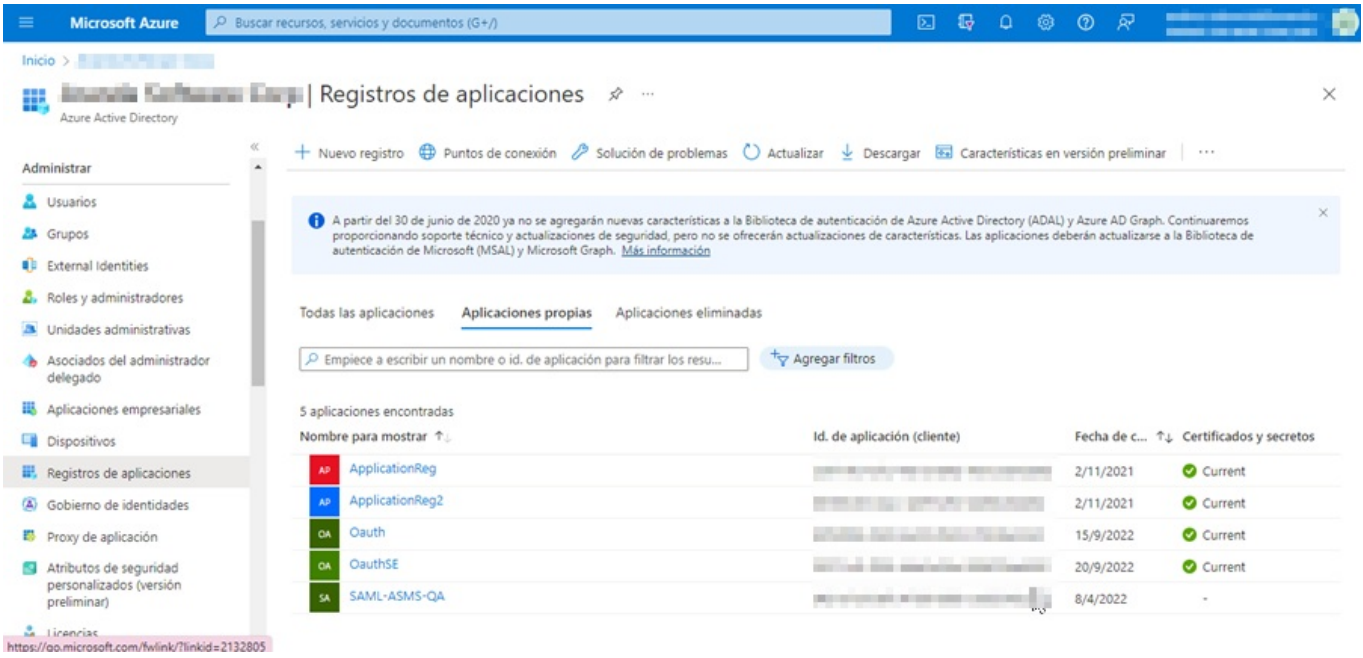
Creating an Application in Azure

How to build an app in Azure

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



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



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

Microsoft Azure | Buscar recursos, servicios y documentos (G+/I)

Inicio > | Registros de aplicaciones >

Registrar una aplicación

* Nombre

Nombre para mostrar accesible por los usuarios de esta aplicación. Se puede cambiar posteriormente.

Nombre con el que identifica la aplicación

Tipos de cuenta compatibles

¿Quién puede usar esta aplicación o acceder a esta API?

☒ Solo cuentas de este directorio organizativo (solo de Aranda Software Corp: inquilino único)

☐ Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: multiinquilino)

☐ Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: multiinquilino) y cuentas de Microsoft personales (como Skype o Xbox)

☐ Solo cuentas personales de Microsoft

[Ayúdame a elegir...](#)

Al continuar, acepta las directivas de la plataforma Microsoft.

Registrar

4. When the application is registered, save the following data that is required for configuration in LDAP synchronization with Microsoft Entra ID.

- Directory ID (tenant) = URL

▮ Note: The URL should be configured as follows: (https://login.microsoftonline.com/ + Tenant/Directory ID)

- Application ID (client) = Client id

Microsoft Azure | Buscar recursos, servicios y documentos (G+/I)

Inicio > | Registros de aplicaciones >

Eliminar Puntos de conexión Características en versión preliminar

Buscar

Información general

Inicio rápido

Asistente para integración

Administrar

Personalización de marca y propiedades

Autenticación

Certificados y secretos

Configuración de token

Permisos de API

Exponer una API

Roles de aplicación

Propietarios

Roles y administradores

Manifiesto

Información esencial

Nombre para mostrar : Credenciales de cliente : [0 certificado_5secreto](#)

Id. de aplicación (cliente) : URI de redirección : [4 web_0 SPA_0 cliente público](#)

Identificador de objeto : URI de id. de aplicación : [Agregar un URI de id. de aplicación](#)

Id. de directorio (inquilino) : Aplicación administrada ... : [OAuth](#)

Tipos de cuenta compati... : [Solo mi organización](#)

Introducción Documentación

Compilación de la aplicación con la Plataforma de identidad de Microsoft

La Plataforma de identidad de Microsoft consta de un servicio de autenticación, bibliotecas de código abierto y herramientas de administración de aplicaciones. Puede crear soluciones de autenticación modernas basadas en estándares, obtener acceso a las API y protegerlas, y agregar información de inicio de sesión para sus usuarios y clientes.

[Más información](#)

Configure your application in the Azure portal

Once you have the app created and the data saved, you can configure the app as follows:

Creation of the Secret

1. To create the secret, log in to the Azure portal > Microsoft> Menu Enter ID > Application Registrations > select the created application from the available list.
2. In the Administer Select the option Certificates and secrets > and in the information view, click the New client secret.

Microsoft Azure | Buscar recursos, servicios y documentos (G+/I)

Inicio > | Registros de aplicaciones >

Certificados y secretos

¿Tiene algún comentario?

Las credenciales permiten a las aplicaciones confidenciales identificarse con el servicio de autenticación al recibir tokens y una ubicación web direccionable (con un esquema HTTPS). Para obtener un mayor nivel de garantía, le recomendamos que use un certificado como credencial, en lugar de un secreto de cliente.

Los certificados de registro de aplicación, los secretos y las credenciales federadas se encuentran en las siguientes pestañas.

Certificados (0) **Secretos de los cliente (5)** Credenciales federadas (0)

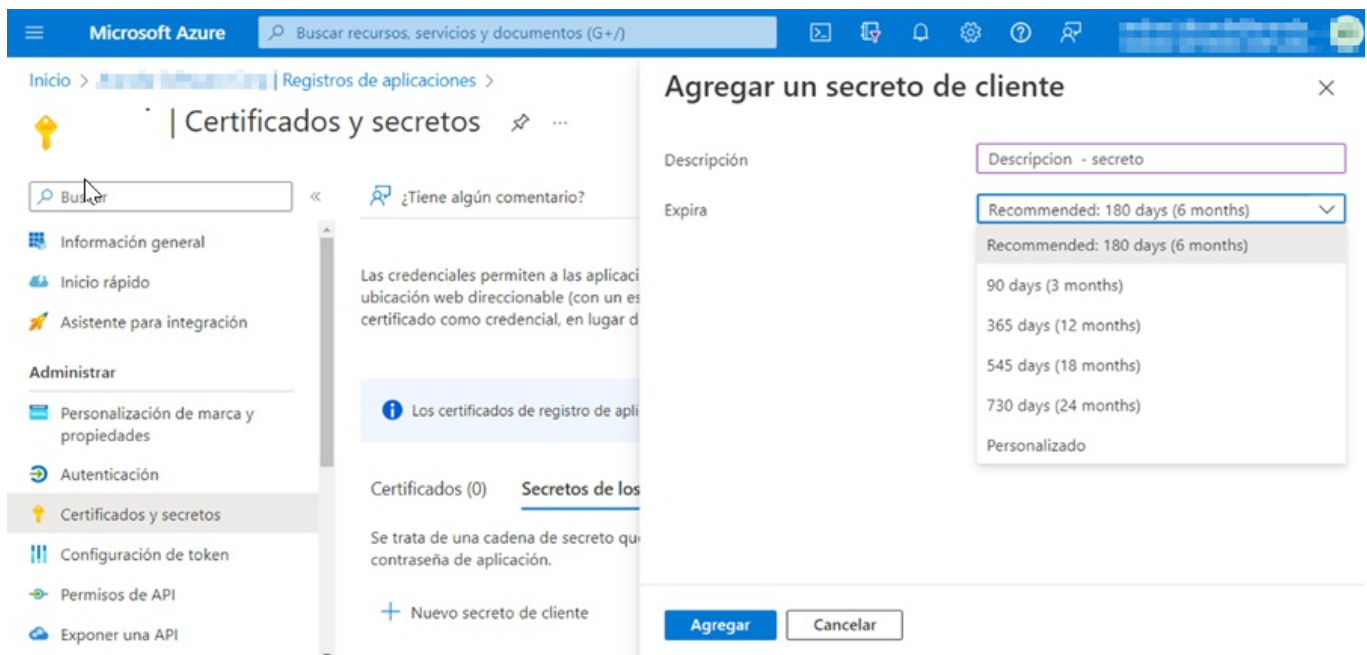
Se trata de una cadena de secreto que la aplicación usa para probar su identidad al solicitar un token. También se conoce como contraseña de aplicación.

+ Nuevo secreto de cliente

Descripción	Expira	Valor	Id. de secreto
	15/3/2023	Obg*****	
	15/3/2023	fxT*****	
Secret	26/3/2023	mRj*****	
secretonuevo	21/5/2023	9k4*****	

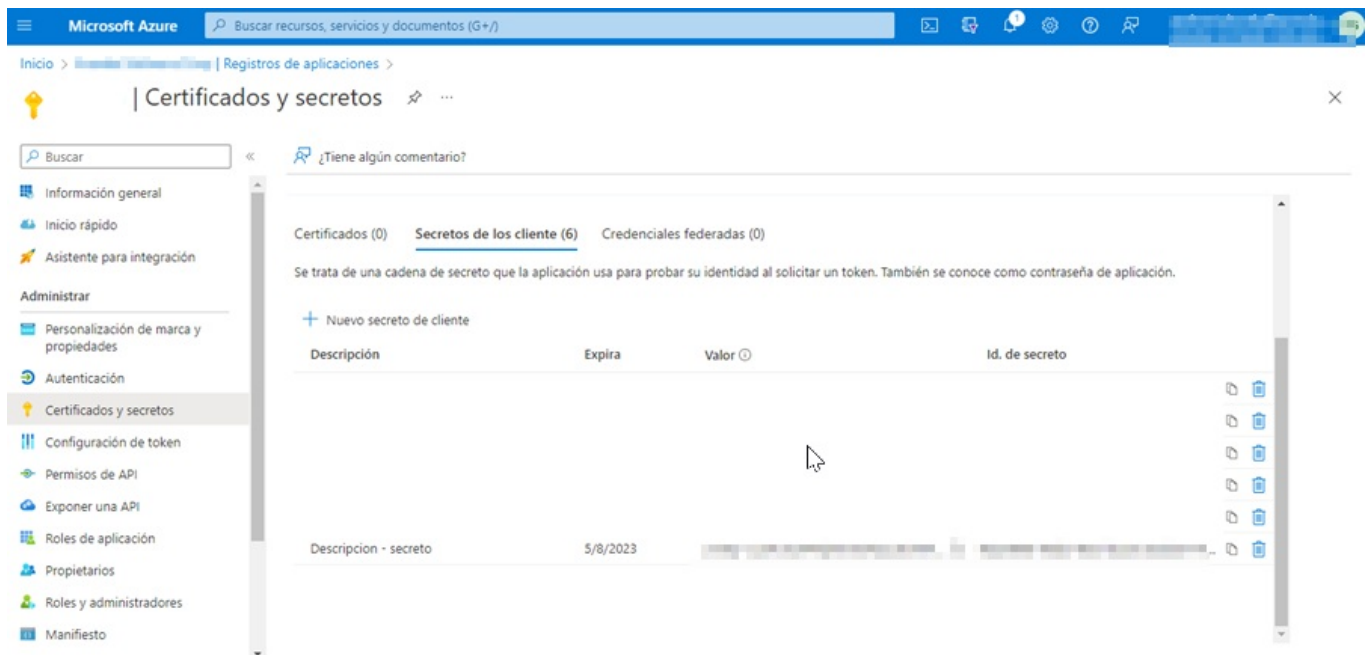
3. In the window Add a client secret fill in the field Description, define the duration of the secret in the field Expires and click the Add.

▮ Note: It is recommended not to forget the configured duration time. In case of expiration, if it is not updated, authentication will fail



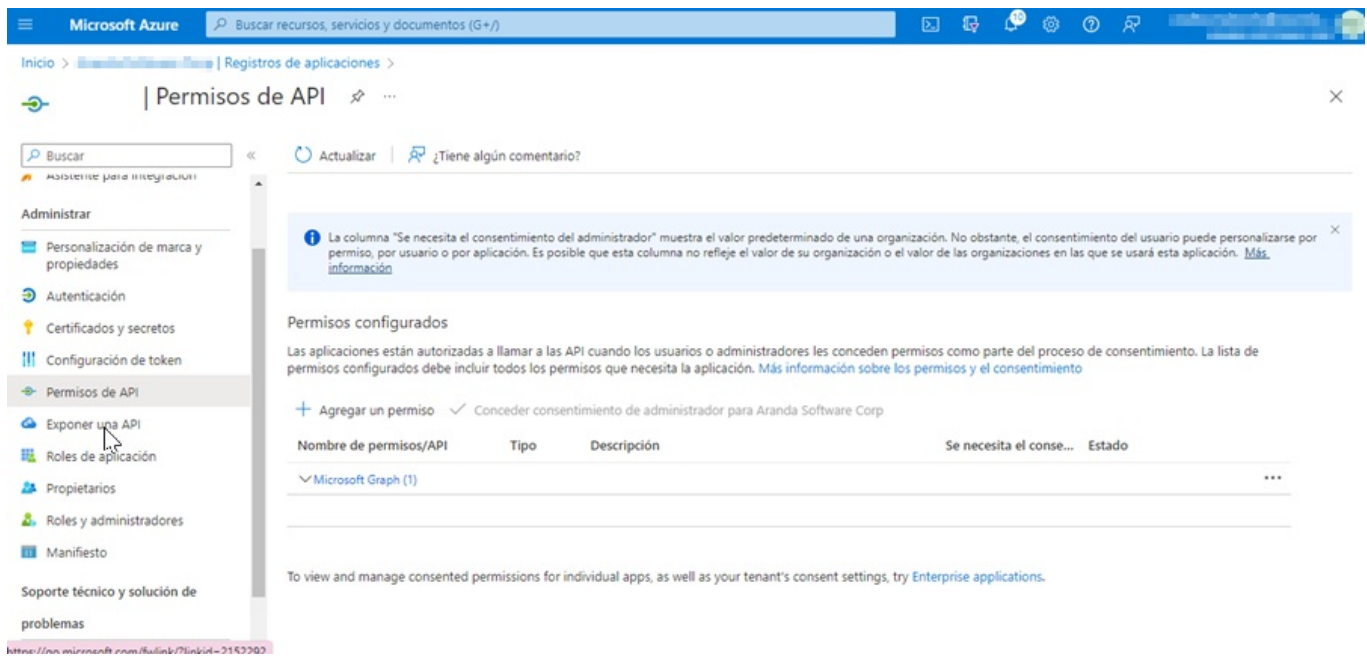
4. The value of secrecy is only visible when it is created; should be saved for later use or referenced during configurations required on Aranda products.

- Secret Customer Value = Secret Client.

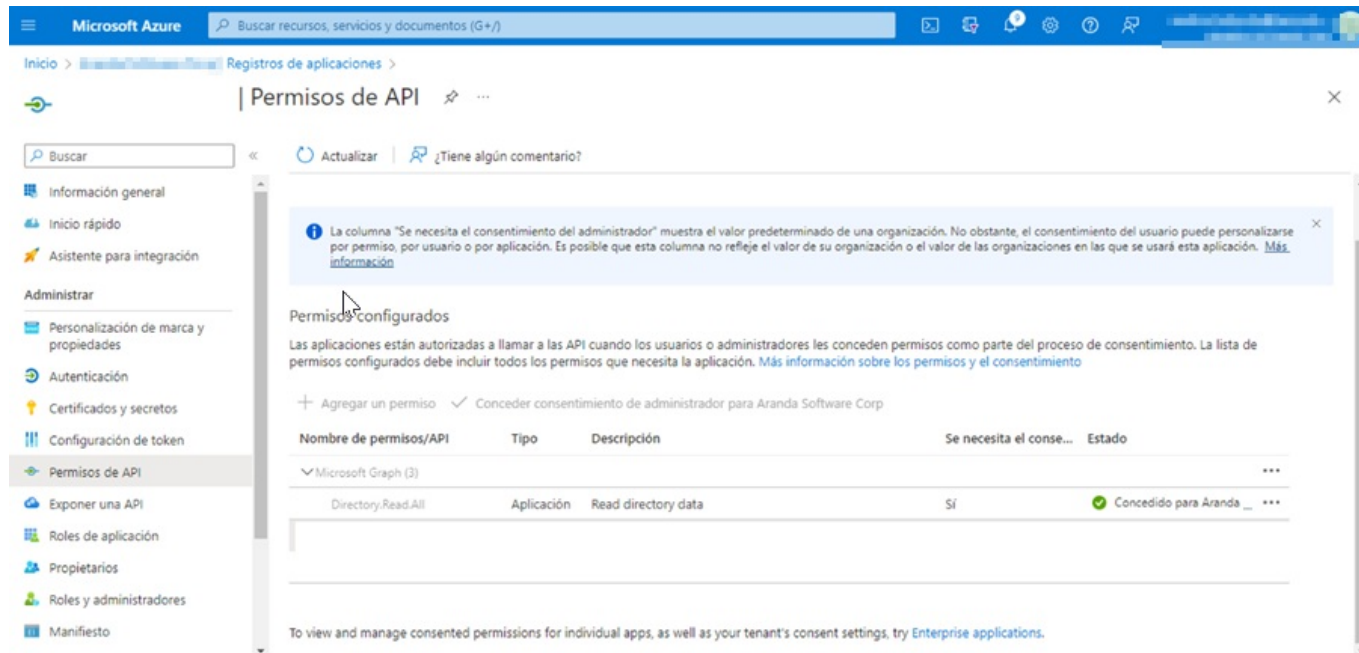
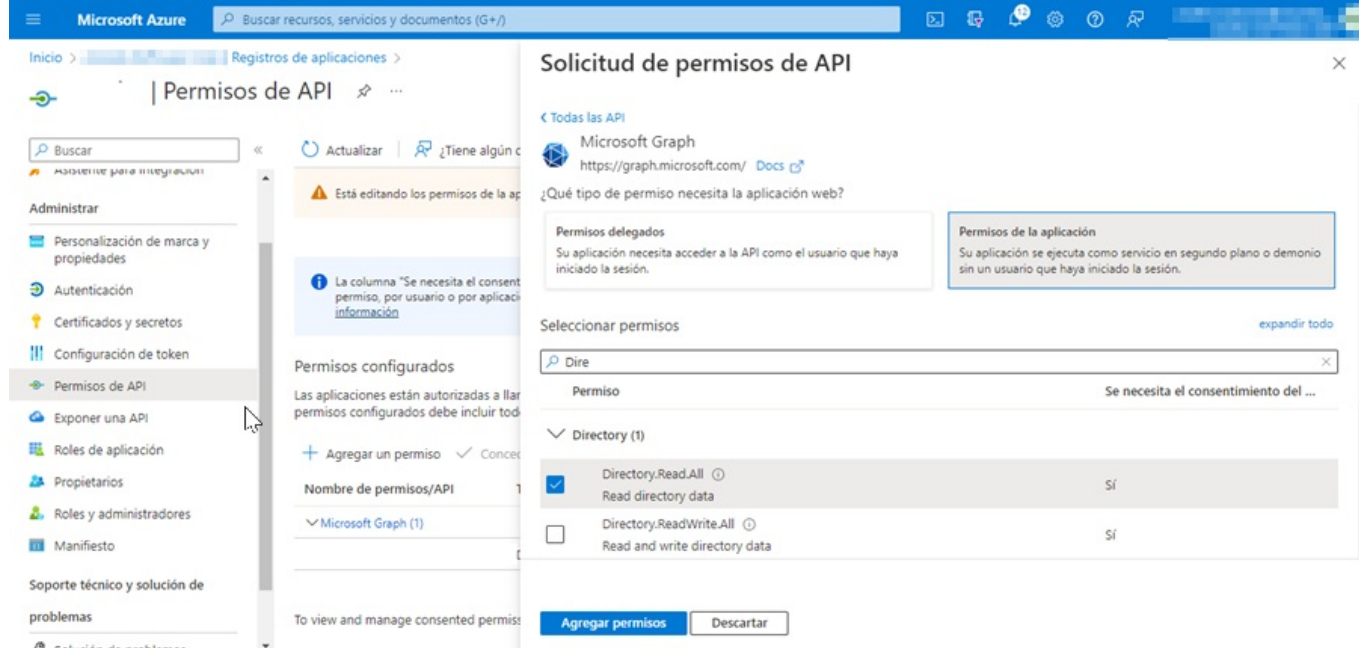


Configure API permissions

1. To configure API permissions, enter the Azure portal > Microsoft> Menu Enter ID > Application Registrations > select the created application from the available list.
2. In the Administer from the main menu, select the API permissions > and in the information view, in the Configured Permissions section, click Add a Permission.



3. In the window Request API permissions, select the Microsoft Graph > and then Application Permissions, enable permissions according to your requirements: Directory.Read.All (Read directory data). Click Add permission.



Once this process is complete, you can finish syncing with Azure AD.

Synchronization of Ldap with Microsoft Entra ID in Aranda applications

To configure Ldap with Microsoft Entra ID in Aranda apps, check the following link:

- [See Aranda Service Management ASMS Synchronization and Configuration](#)