



## Integración Azure

<b>Control de versiones</b>	<b>2</b>
<b>Modelo de integración</b>	<b>3</b>
Autenticación y autorización (Oauth2)	3
Configuración de autenticación	3
Configuración de autorización	4
Gobierno activo	5
Nomenclatura de los grupos	5
<b>Credenciales requeridas</b>	<b>5</b>
Autenticación y autorización (Oauth2)	5
Gobierno activo	9
<b>Emulación SSO vía Oauth2</b>	<b>10</b>

## Control de versiones

<b>Versión</b>	<b>Fecha de modificación</b>	<b>Responsable</b>	<b>Aprobador</b>	<b>Resumen de cambios</b>
1.0	28/10/2022	Anjana Producto	Anjana Producto	Creación del documento
2.0	16/03/2023	Anjana Producto	Anjana Producto	Corrección de la variable client-secret en la Configuración de autenticación

# Modelo de integración

## Autenticación y autorización (Oauth2)

Anjana Data se integra mediante circuito estándar para “Web apps” el cual se describe por el fabricante en la siguiente documentación.

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow>

<https://docs.microsoft.com/en-us/azure/active-directory/develop/app-sign-in-flow>

<https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-flows-app-scenarios>

Para la recuperación de información relativa a perfil de usuario y grupos de autorización se explota la api Microsoft Graph.

<https://docs.microsoft.com/en-us/graph/overview>

La funcionalidad está directamente embebida en el microservicio de gestión de autenticación y autorización Zeus, se habilita y configura mediante el fichero de configuración de dicho microservicio.

## Configuración de autenticación

En la propiedad `security.authentication.oidc.providers` colgarán los distintos proveedores de autenticación que tengamos. En el caso de Azure debemos poner las siguientes propiedades:

- name: Azure AD
  - *El nombre que se mostrará en la pantalla de login*
- authorize-url:  
`https://login.microsoftonline.com/<tenant>/oauth2/v2.0/authorize?client_id=${security.authentication.oidc.providers.azure.client-id}&response_type=code&response_mode=query&scope=${security.authentication.oidc.providers.azure.scopes}&redirect_uri=${security.authentication.oidc.providers.azure.redirect-uri}`
- authorize-url-portuno:  
`https://login.microsoftonline.com/<tenant>/oauth2/v2.0/authorize?client_id=${security.authentication.oidc.providers.azure.client-id}&response_type=code&response_mode=query&scope=${security.authentication.oidc.providers.azure.scopes}&redirect_uri=${security.authentication.oidc.providers.azure.redirect-uri-portuno}`
- token-url: `https://login.microsoftonline.com/<tenant>/oauth2/v2.0/token`
- scopes: openid profile email user.read
- client-id: <client-id>
- client-secret: <client-secret>
- client-authentication-method: POST

- redirect-uri: https://<front-anjana>/anjana/authorized
- redirect-uri-portuno: https://<front-anjana>/admin/authorized
- username-claim: preferred\_username
- type: AZURE

Ej.

```

security:
  ...
  authentication:
    oidc:
      providers:
        azure:
          name: Anjana Azure
          authorize-url: https://login.microsoftonline.com/11111111-2222-3333-4444-555555555555
          authorize-url-portuno: https://login.microsoftonline.com/11111111-2222-3333-4444-555555555555
          token-url: https://login.microsoftonline.com/11111111-2222-3333-4444-555555555555
          scopes: openid profile email user.read
          client-id: aaaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee
          client-secret: AAAAAA.BBBBBBBB_CCCCCCCCCC~- .DDDDDDDDDDDDDDDDDD
          client-authentication-method: POST
          redirect-uri: https://anjana.client.com:8443/anjana/authorized
          redirect-uri-portuno: https://anjana.client.com:8443/admin/authorized
          username-claim: preferred_username
          type: AZURE

```

## Configuración de autorización

En la propiedad `security.authorization` colgarán los distintos proveedores de autenticación que tengamos. En el caso de Azure debemos poner sus propiedades en `security.authorization.azure-active-directory.providers.azure`:

- tenant-id: 11111111-2222-3333-4444-555555555555
- client-id: aaaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee
- client-secret: AAAAAA.BBBBBBBB\_CCCCCCCCCC~- .DDDDDDDDDDDDDDDDDD
- scopes: https://graph.microsoft.com/.default
- national-cloud: Global # One of: Global Germany China or UsGovernment. Global is default
- groupOrgUnitSeparator: separador de partes de unidad organizativa en un grupo (nunca valor ""). Esta propiedad, por tanto, debe tener valor o no ser definida) (En caso de configurar un separador distinto a '/', en el provider las OUs no se puede usar '/' como parte de un nombre de OU)
- roleOrgUnitSeparator: separador del rol del resto de la cadena en un grupo (nunca valor ""). Esta propiedad, por tanto, debe tener valor o no ser definida)
- groupPrefix: prefijo que contengan los grupos (nunca valor ""). Esta propiedad, por tanto, debe tener valor o no ser definida)

```
security:
  ...
  authorization:
    azure-active-directory:
      providers:
        azure:
          tenant-id: 11111111-2222-3333-4444-555555555555
          client-id: aaaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee
          client-secret: AAAAAA.BBBBBBBB_CCCCCCCC~-.DDDDDDDDDDDD
          scopes: https://graph.microsoft.com/.default
          national-cloud: Global # One of: Global Germany China or UsGovernment. Global is default
```

## Gobierno activo

El plugin a desplegar el cual realizará la parte de las tareas de gobierno activo que tengan que provisionar elementos sobre Azure AD es “Tot plugin AzureAD”.

Para la provisión de grupos de usuarios a los que posteriormente se asignan permisos de acceso a recursos de datos gobernados por el producto se explota la api Microsoft Graph <https://docs.microsoft.com/en-us/graph/overview>

## Nomenclatura de los grupos

El nombre del grupo debe contener el alias de la unidad organizativa y el rol que aplica a dicha unidad organizativa.

Un ejemplo de un nombre de un grupo sería : HQ/Legal-architect , donde HQ/Legal es el alias de la unidad organizativa y architect el rol.

Como se puede observar hay dos separadores:

-El separador de jerarquía de la unidad organizativa -> ‘/’ , cuyo valor es configurable gracias a la propiedad del yml: roles.separator-organizational-unit.

-El separador de la unidad organizativa y el rol -> ‘-’ , cuyo valor es configurable gracias a la propiedad del yml: roles.separator-role.

## Credenciales requeridas

La credencial puede ser única aglutinando los permisos de ambas, pero se recomienda mantenerlas por separado de cara a facilitar la monitorización y auditoría de la actividad ejercida por las mismas.

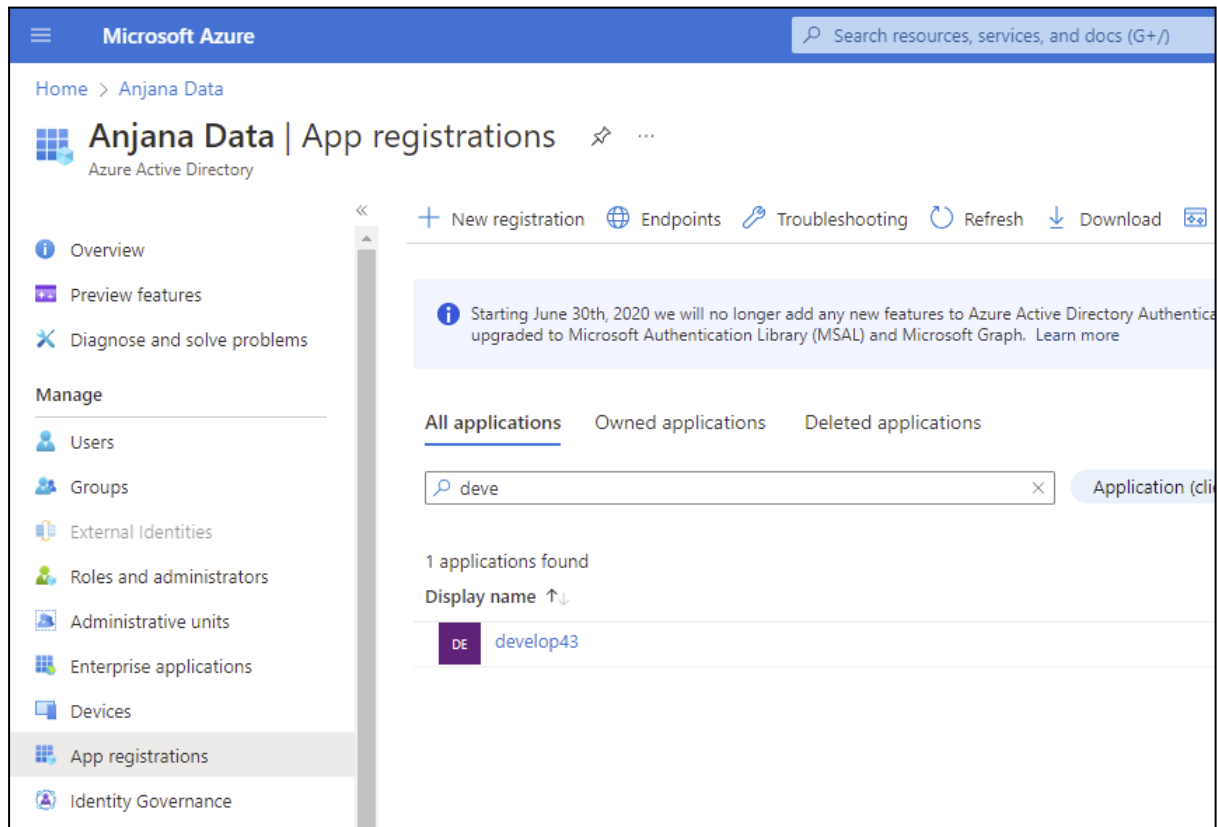
## Autenticación y autorización (Oauth2)

La funcionalidad está directamente embebida en el microservicio de gestión de autenticación y autorización Zeus, se habilita y configura mediante el fichero de configuración de dicho microservicio.

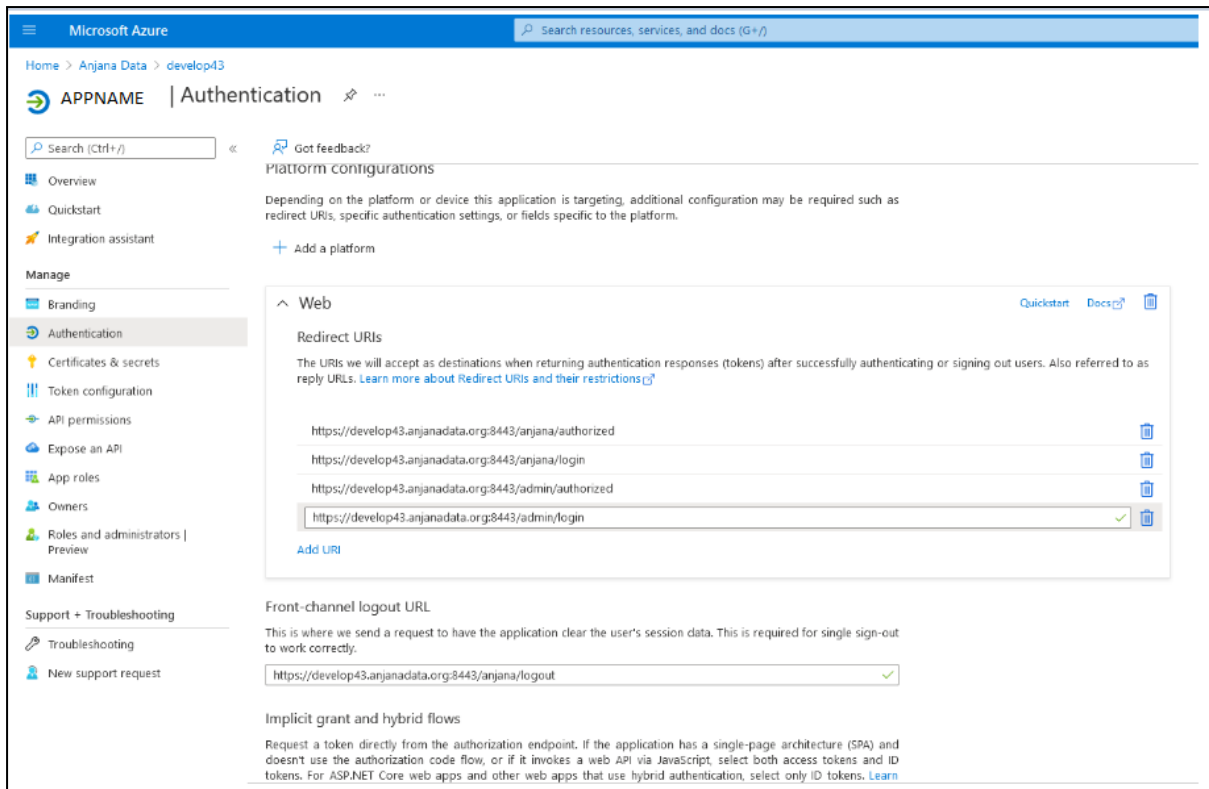
Es necesario registrar una nueva aplicación con las siguientes propiedades.

Autenticación web en la cual configuraremos las url acordes al nombre de dominio que enrute hasta el frontal de Anjana Data, es necesario dar de alta dos URL, más la de log out:

- `https://<host>:<port>/anjana/authorized`
- `https://<host>:<port>/anjana/login`
- `https://<host>:<port>/anjana/logout`



The screenshot displays the Microsoft Azure portal interface for 'Anjana Data | App registrations'. The left sidebar contains navigation options such as Overview, Preview features, Diagnose and solve problems, and a Manage section with Users, Groups, External Identities, Roles and administrators, Administrative units, Enterprise applications, Devices, App registrations, and Identity Governance. The main content area shows a search for 'deve' resulting in one application found: 'DE develop43'. A notification banner at the top indicates that starting June 30th, 2020, new features for Azure Active Directory Authentication will be discontinued in favor of Microsoft Authentication Library (MSAL) and Microsoft Graph.



Microsoft Azure

Home > Anjana Data > develop43

APPNAME | Authentication

Search (Ctrl+/) << Got feedback?

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web

Quickstart Docs Add

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

https://develop43.anjanadata.org:8443/anjana/authorized	Add
https://develop43.anjanadata.org:8443/anjana/login	Add
https://develop43.anjanadata.org:8443/admin/authorized	Add
https://develop43.anjanadata.org:8443/admin/login	Add

Add URI

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

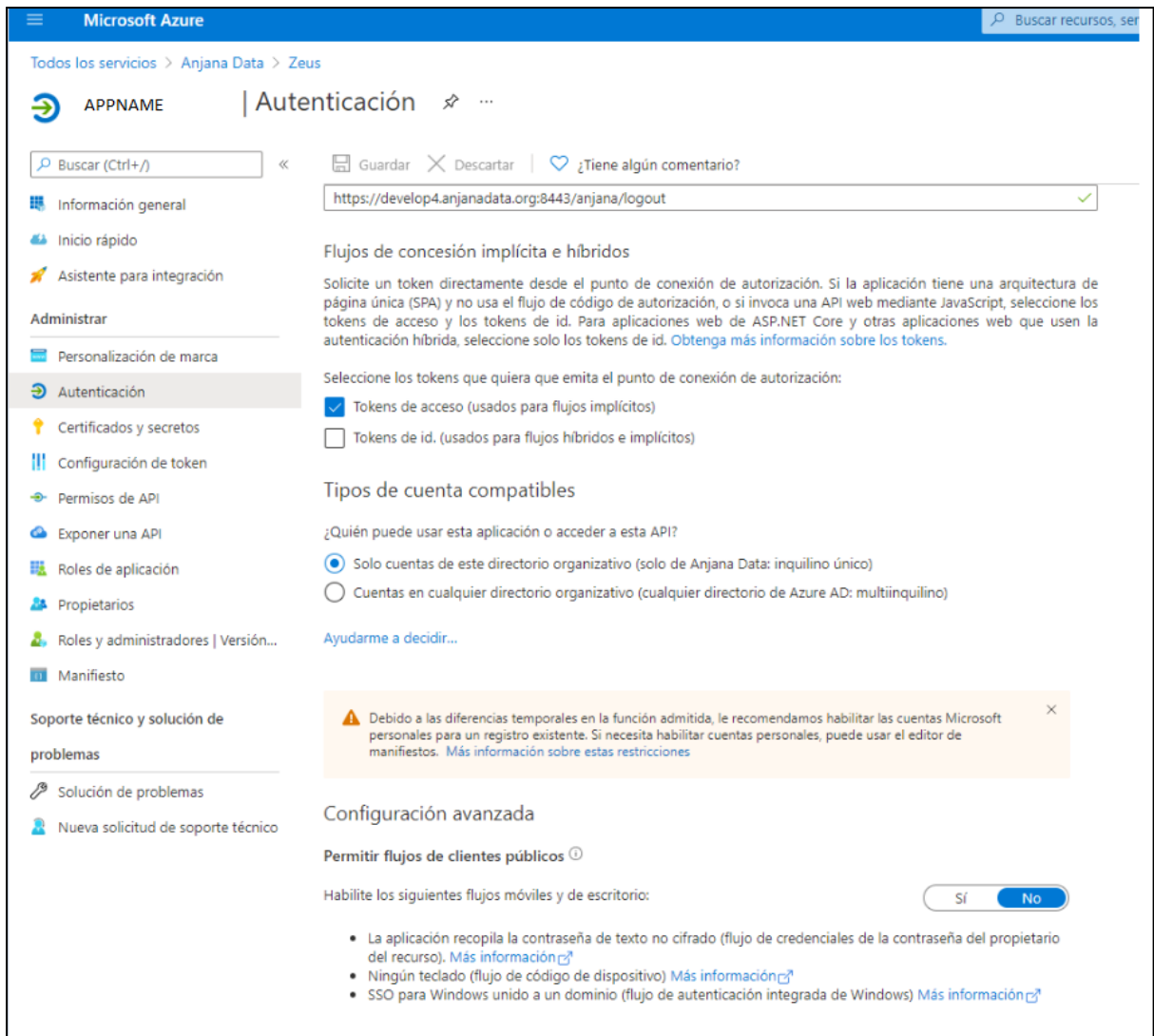
https://develop43.anjanadata.org:8443/anjana/logout

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn](#)

En base a necesidad ajustar las opciones, generalmente son las siguientes:





Microsoft Azure | Buscar recursos, ser

Todos los servicios > Anjana Data > Zeus

APPNAME | Autenticación

Buscar (Ctrl+/) | Guardar | Descartar | ¿Tiene algún comentario?

https://develop4.anjanadata.org:8443/anjana/logout

### Flujos de concesión implícita e híbridos

Solicite un token directamente desde el punto de conexión de autorización. Si la aplicación tiene una arquitectura de página única (SPA) y no usa el flujo de código de autorización, o si invoca una API web mediante JavaScript, seleccione los tokens de acceso y los tokens de id. Para aplicaciones web de ASP.NET Core y otras aplicaciones web que usen la autenticación híbrida, seleccione solo los tokens de id. [Obtenga más información sobre los tokens.](#)

Seleccione los tokens que quiera que emita el punto de conexión de autorización:

- Tokens de acceso (usados para flujos implícitos)
- Tokens de id. (usados para flujos híbridos e implícitos)

### Tipos de cuenta compatibles

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

- Solo cuentas de este directorio organizativo (solo de Anjana Data: inquilino único)
- Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: multiinquilino)

[Ayudarme a decidir...](#)

⚠ Debido a las diferencias temporales en la función admitida, le recomendamos habilitar las cuentas Microsoft personales para un registro existente. Si necesita habilitar cuentas personales, puede usar el editor de manifiestos. [Más información sobre estas restricciones](#)

### Configuración avanzada

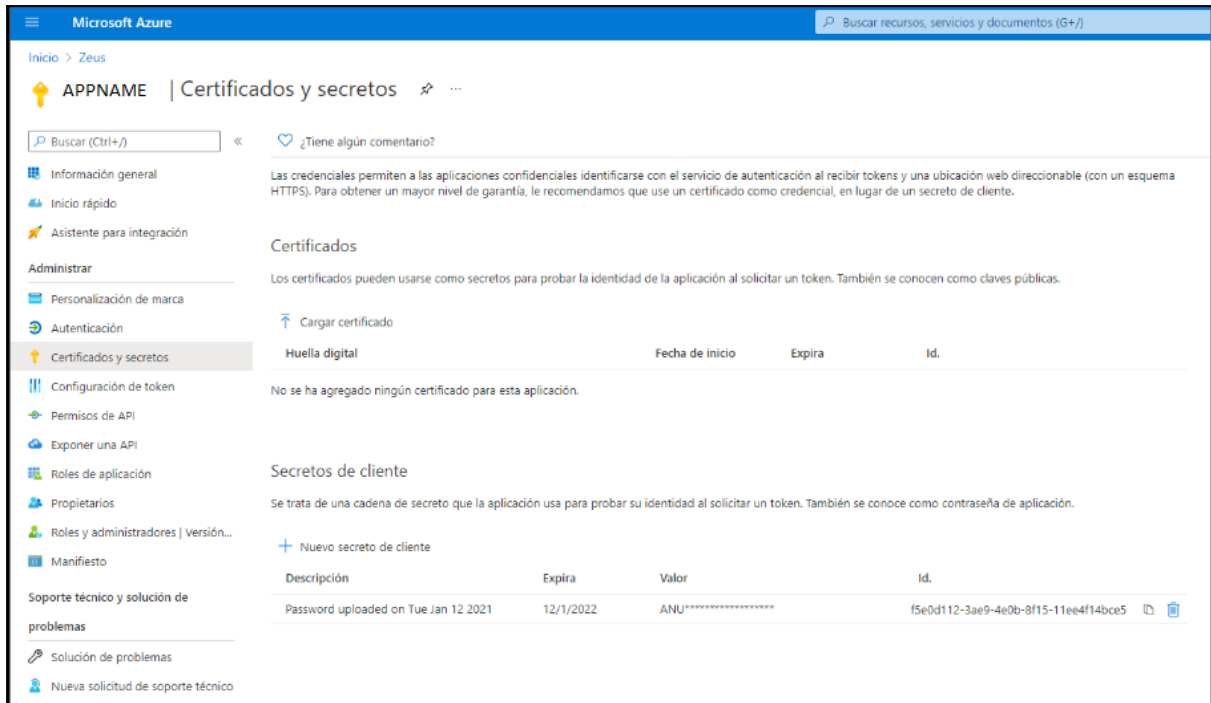
Permitir flujos de clientes públicos ⓘ

Habilite los siguientes flujos móviles y de escritorio:

Sí  No

- La aplicación recopila la contraseña de texto no cifrado (flujo de credenciales de la contraseña del propietario del recurso). [Más información](#)
- Ningún teclado (flujo de código de dispositivo) [Más información](#)
- SSO para Windows unido a un dominio (flujo de autenticación integrada de Windows) [Más información](#)

Tras ello es necesario crear cliente y secreto que posteriormente será configurado en producto



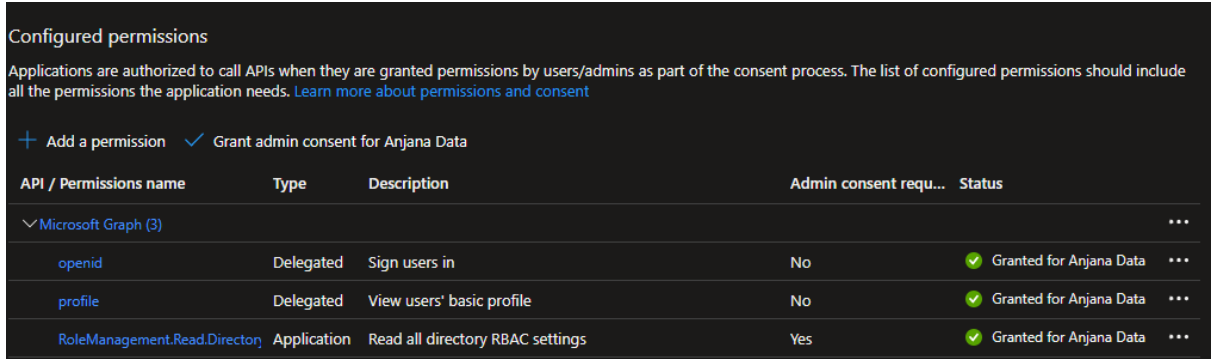
The screenshot shows the 'Certificados y secretos' (Certificates and secrets) page in the Microsoft Azure portal for an application named 'APPNAME'. The page is divided into two main sections: 'Certificados' (Certificates) and 'Secretos de cliente' (Client secrets).

**Certificados:** This section contains a 'Cargar certificado' (Upload certificate) button and a table with columns: 'Huella digital' (Fingerprint), 'Fecha de inicio' (Start date), 'Expira' (Expires), and 'Id.'. Below the table, it states: 'No se ha agregado ningún certificado para esta aplicación.' (No certificate has been added for this application).

**Secretos de cliente:** This section contains a '+ Nuevo secreto de cliente' (New client secret) button and a table with columns: 'Descripción' (Description), 'Expira' (Expires), 'Valor' (Value), and 'Id.'. The table contains one entry:

Descripción	Expira	Valor	Id.
Password uploaded on Tue Jan 12 2021	12/1/2022	ANU*****	f5e0d112-3ae9-4e0b-8f15-11ee4f14bce5

Asignar permisos de lectura necesarios para recopilar la información del usuario y sus membresías las cuales serán mapeadas de forma automática a roles y unidades organizativas en el producto



The screenshot shows the 'Configured permissions' section in the Azure portal. It includes a heading 'Configured permissions' and a paragraph explaining that applications are authorized to call APIs when granted permissions by users/admins. Below this is a table of configured permissions:

Buttons: '+ Add a permission' and 'Grant admin consent for Anjana Data' (checked).

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
openid	Delegated	Sign users in	No	Granted for Anjana Data
profile	Delegated	View users' basic profile	No	Granted for Anjana Data
RoleManagement.Read.Directory	Application	Read all directory RBAC settings	Yes	Granted for Anjana Data

Asignar usuarios a los grupos de Azure AD

## Gobierno activo

El plugin a desplegar el cual realizará la parte de las tareas de gobierno activo que tengan que provisionar elementos sobre Azure AD es "Tot plugin AzureAD", en su documentación queda descrita la credencial requerida.

## Emulación SSO vía Oauth2

El protocolo Oauth2 observa la autenticación transparente en caso de que sea posible, para lo cual solo es necesario redirigir al usuario a <https://<host>/anjana/login?provider=<identificador de provider en zeus>>, si el usuario ya está logado en dicho provider y las políticas configuradas en dicho provider hacen que no se requiera validar nuevamente la credencial, el usuario será autenticado en Anjana Data de forma totalmente transparente.