



## 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)	6
Gobierno activo	9
<b>Emulación SSO vía Oauth2</b>	<b>10</b>

## Control de versiones

Versión	Fecha de modificación	Responsable	Aprobador	Resumen de cambios
1.0	22/11/2023	Anjana Producto	Anjana Producto	Creación del documento. Compatibilidad con la v4.5 de todos los módulos de Anjana

# Modelo de integración

## Autenticación y autorización (Oauth2)

Anjana Data se integra mediante circuito estándar para “Web apps”, descrito 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>

Es importante considerar que la capacidad de uso de esta API corresponde directamente con la cuota que Microsoft le tiene asignada a la cuenta del cliente con su licencia. De forma general Microsoft limita las peticiones a:

- Límite al Resource Manager  
<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/request-limits-and-throttling>
- Límite a la API Graph (15 llamadas en lapso de 5 segundos)  
<https://learn.microsoft.com/en-us/azure/governance/resource-graph/concepts/guidance-for-throttled-requests#understand-throttling-headers>

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* se configuran los distintos proveedores de autenticación que se utilizan.

En el caso de Azure es necesario configurar las siguientes propiedades:

```
security:
  authentication:
    oidc:
      providers:
        azure:
          name: Anjana Azure
          authorize-url:
https://login.microsoftonline.com/aef41d72-8720-418a-bb06-9fb98ef04ded/oauth2/v2.0/authorize?client_id=${security.authentication.oidc.provider
```

```
s.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/aef41d72-8720-418a-bb06-9fb98ef04ded/
oauth2/v2.0/authorize?client_id=${security.authentication.oidc.providers
s.azure.client-id}&response_type=code&response_mode=query&scope=${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://anjana.client.com:8443/anjana/authorized
    redirect-uri-portuno:
https://anjana.client.com:8443/admin/authorized
    username-claim: preferred_username
    workflowType: IMPLICIT
    type: AZURE
```

- name: el nombre que se mostrará en la pantalla de login

## Configuración de autorización

En la propiedad *security.authorization* se configuran los distintos proveedores de autorización que se utilizan.

En el caso de Azure es necesario configurar las siguientes propiedades:

```
security:
  authorization:
    azure-active-directory:
      providers:
        azure:
          scopes: https://graph.microsoft.com/.default
          client-id: <clientId>
          client-secret: <clientSecret>
          tenant-id: <tenantId>
          national-cloud: Global
          groupOrgUnitSeparator: "/"
          roleOrgUnitSeparator: "-"
          groupPrefix: "prefix-"
```

- `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)

## 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 Azure AD".

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<sup>1</sup>.

Como se puede observar hay dos separadores:

- El separador de jerarquía de la unidad organizativa: `'/'` , cuyo valor es configurable con la propiedad del yml: `roles.separator-organizational-unit`.
- El separador de la unidad organizativa y el rol: `'-'` , cuyo valor es configurable con 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.

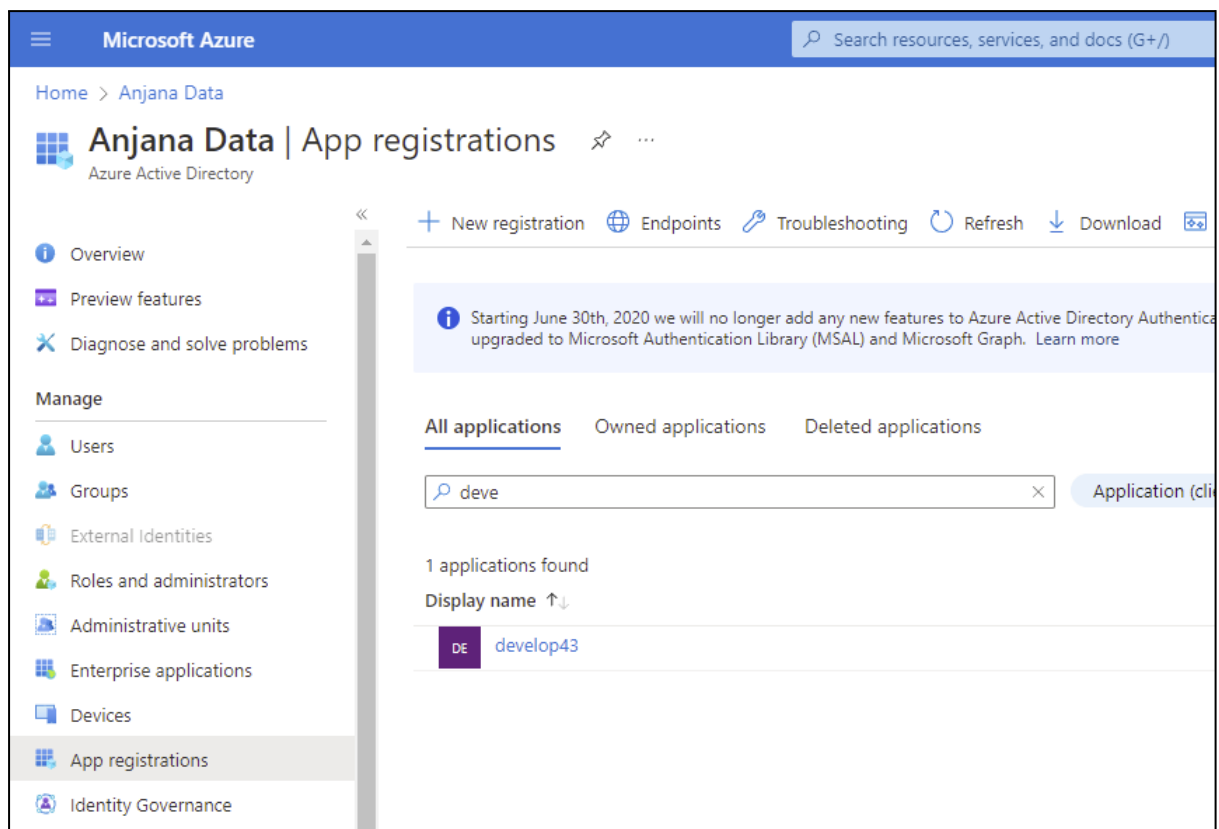
---

<sup>1</sup> Independientemente de los separadores usados en los repositorios de identidades el producto normalizará al formato estándar, por lo que en la configuración del producto ha de usarse siempre los separadores `'/'` y `'-'` para conformar el alias, por ejemplo `"UO/UO..../UO-role"`.

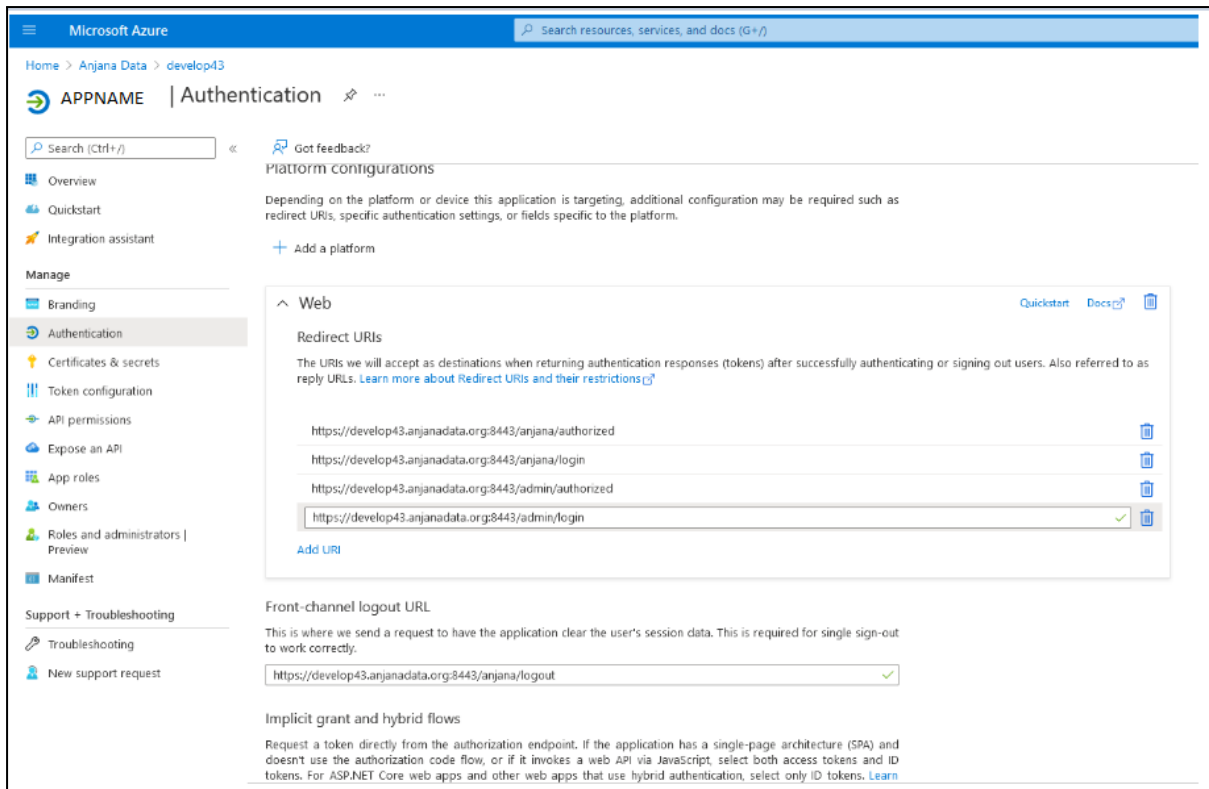
## Autenticación y autorización (Oauth2)

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.

- Para la autenticación web se deben configurar las url acorde 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 shows the Microsoft Azure portal interface for 'Anjana Data | App registrations'. The left sidebar contains navigation options like Overview, Preview features, Diagnose and solve problems, and Manage (Users, Groups, External Identities, Roles and administrators, Administrative units, Enterprise applications, Devices, App registrations, Identity Governance). The main content area shows a search bar with 'deve' entered, resulting in one application found: 'develop43'. The application is listed with a 'DE' icon and the display name 'develop43'. Above the search bar, there are tabs for 'All applications', 'Owned applications', and 'Deleted applications'. A notification banner at the top states: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more'.



Microsoft Azure

Home > Anjana Data > develop43

APPNAME | Authentication

Search (Ctrl+F) 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

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

[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.

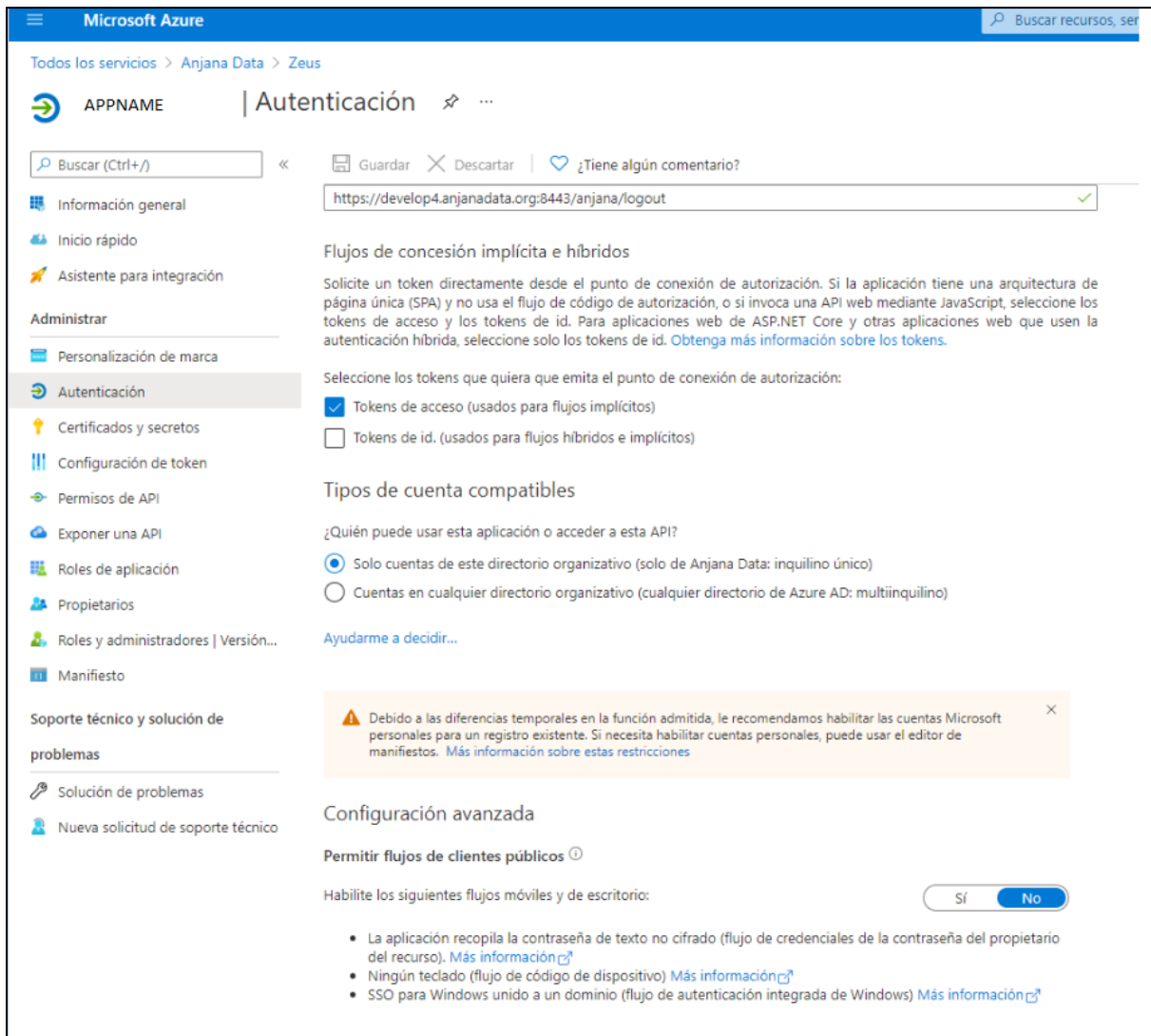
https://develop43.anjanadata.org:8443/anjana/logout ✓

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

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](#)

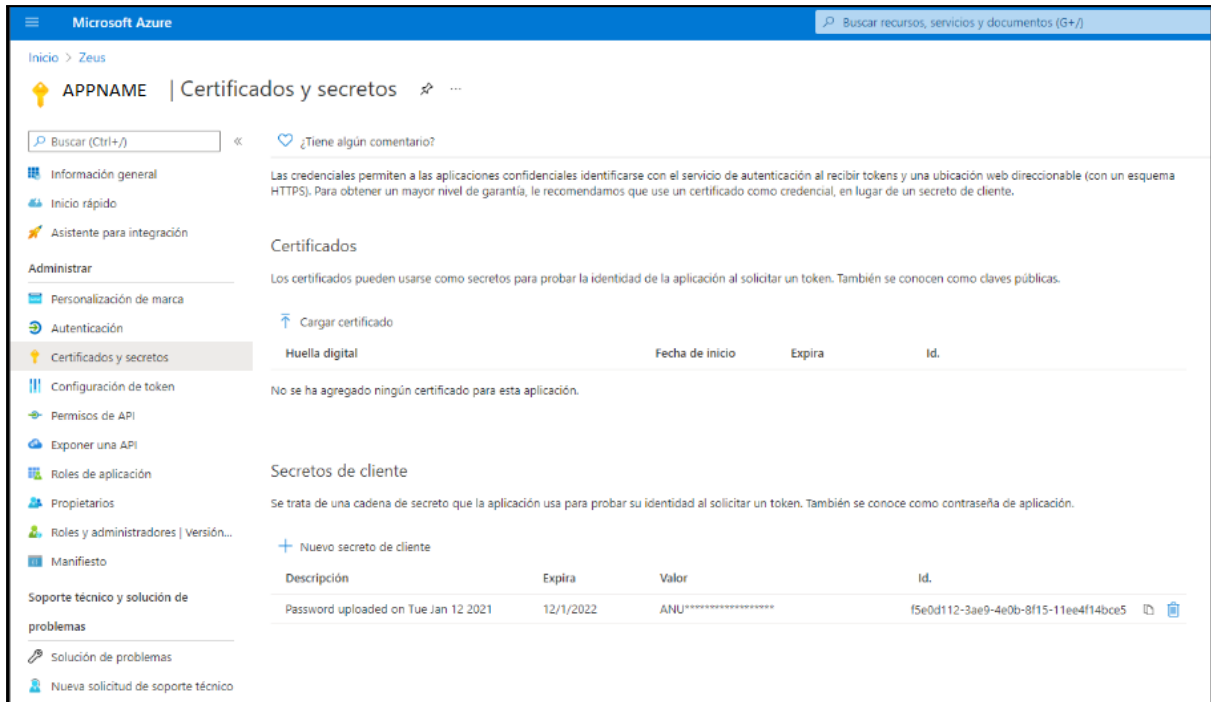
### Configuración avanzada

Permitir flujos de clientes públicos ⓘ

Habilite los siguientes flujos móviles y de escritorio: SI 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:



Microsoft Azure | APPNAME | Certificados y secretos

Inicio > Zeus

Buscar (Ctrl+/) << ¿Tiene algún comentario?

Información general: 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.

Inicio rápido

Asistente para integración

Administrar

- Personalización de marca
- Autenticación
- Certificados y secretos**
- Configuración de token
- Permisos de API
- Exponer una API
- Roles de aplicación
- Propietarios
- Roles y administradores | Versión...
- Manifiesto

SopORTE técnico y solución de problemas

- Solución de problemas
- Nueva solicitud de soporte técnico

**Certificados**

Los certificados pueden usarse como secretos para probar la identidad de la aplicación al solicitar un token. También se conocen como claves públicas.

Cargar certificado

Huella digital	Fecha de inicio	Expira	Id.
No se ha agregado ningún certificado para esta aplicación.			

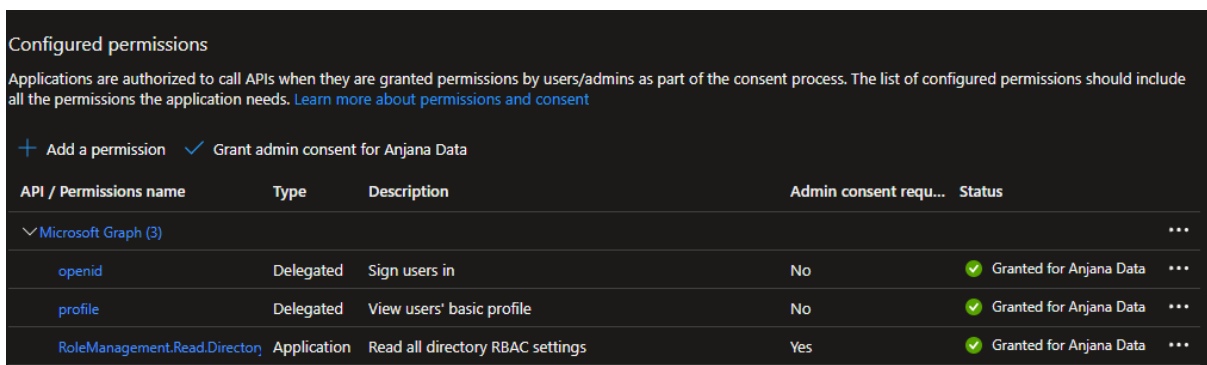
**Secretos de cliente**

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.
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 que serán mapeadas de forma automática a roles y unidades organizativas en el producto:



Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Anjana Data

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 Azure AD”, 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.