
# Tot plugin Azure AD

# Control de versiones

| Versión | Fecha de modificación | Responsable | Aprobador | Resumen de cambios |
|---|---|---|---|---|
| 1.0 | 28/10/2022 | Anjana Producto | Anjana Producto | Creación del documento |

# Introducción

Este plugin se usa en coordinación con los plugins de tecnologías de almacenamiento conectadas a Azure AD para provisionar los grupos que representan a los DSA y adicionalmente gestiona las membresías que representan la aceptación de los DSA por parte de los usuarios.

# Modelo de integración

## Gobierno activo

De forma general los DSA de Anjana Data serán representados como grupos en Azure AD, y los firmantes de dichos DSA serán miembros de dichos grupos.

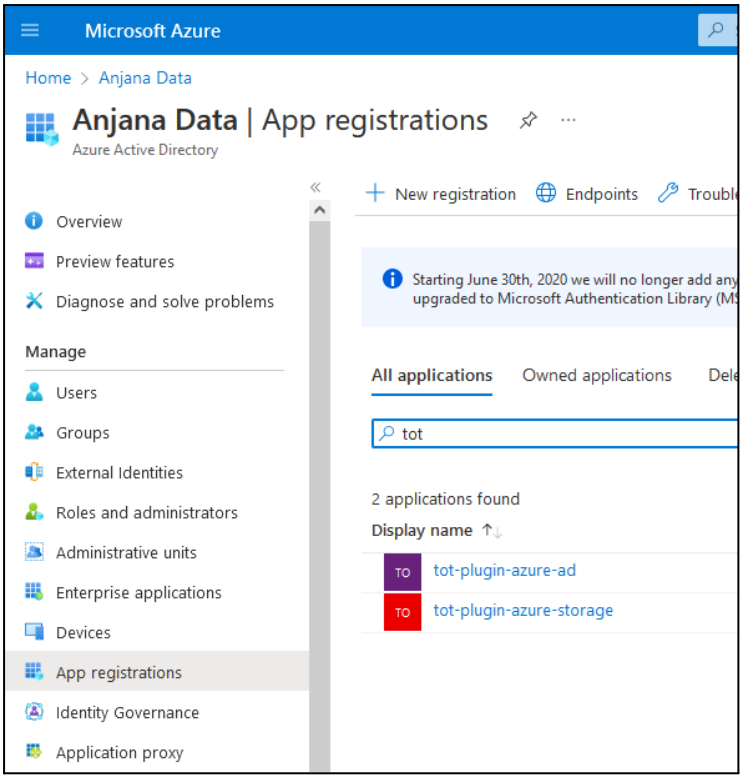
# Credenciales requeridas

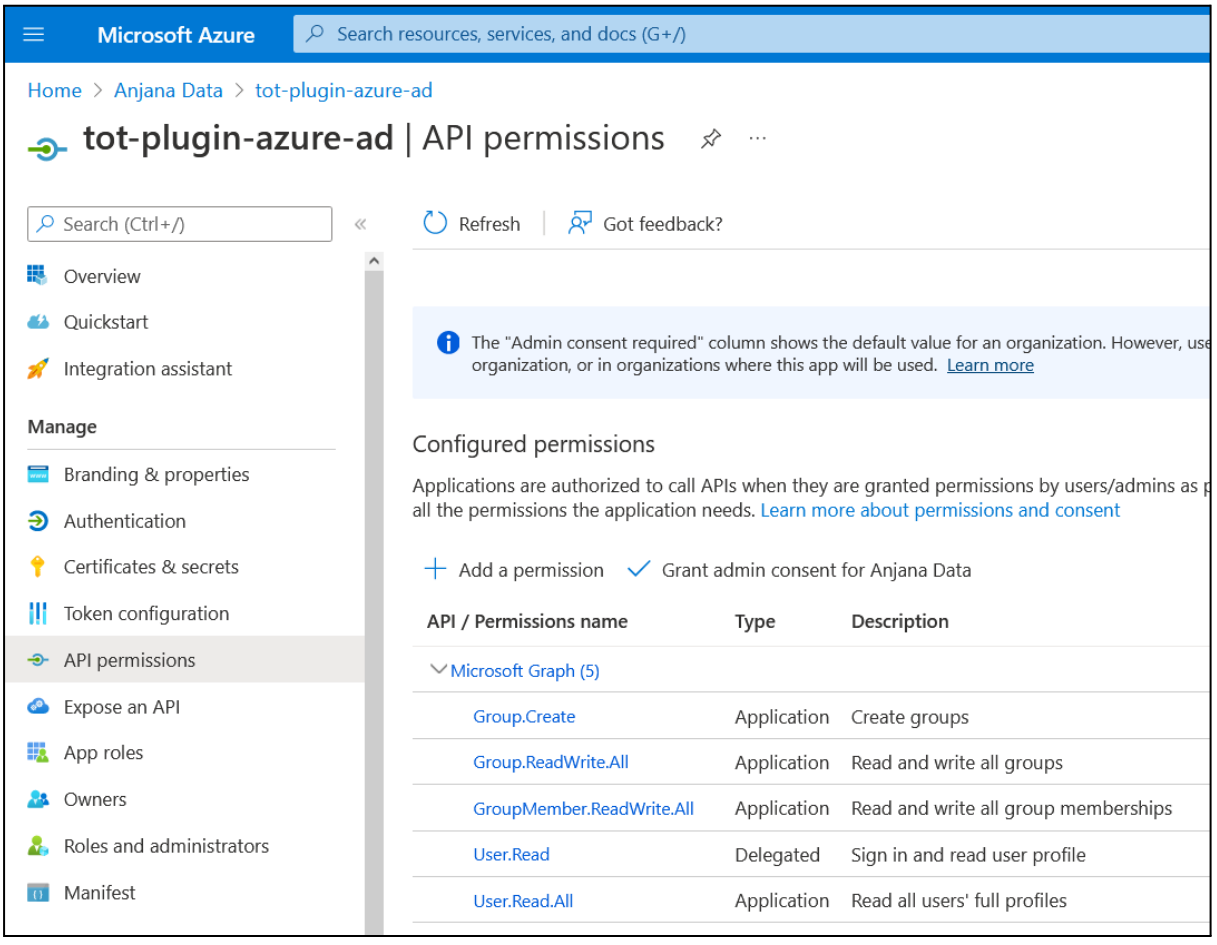
Es necesario registrar una aplicación en Azure AD y generar el necesario clientID y secret para que el plugin pueda autenticar y adquirir los permisos necesarios para cada funcionalidad.

## Gobierno activo

La acciones realizadas por este plugin son las siguientes:

- Crear grupos: Se crearán grupos que representen a DSAs que pasen a estado aprobado. Para ello es necesario que la aplicación registrada tenga el permiso de “Group.Create” para poder crear los grupos.
- Lectura usuarios: Se requiere la lectura de los campos para realizar la membresía. “User.Read”
- Añadir/Eliminar usuarios en grupos: En los grupos creados por el plugin se van a añadir y eliminar usuarios (el plugin no crea ni borra usuarios del Active Directory) en base a las adherencias y deshaderencias sobre el DSA. Para ello la aplicación requiere los permisos “User.Read” para poder localizar los usuarios y “GroupMember.ReadWrite.All” para poder modificar los miembros del grupo con los usuarios localizados.
- Eliminar grupos: El plugin eliminará aquellos grupos que representen a DSA que pasen a estados expirados de forma automática en Anjana. Para ello la aplicación requiere el permiso “Group.ReadWrite.All” para poder borrar grupos.


Microsoft Azure
Home > Anjana Data
Anjana Data | App registrations
Azure Active Directory
New registration
Endpoints
Overview
Preview features
Diagnose and solve problems
Manage
Users
Groups
External Identities
Roles and administrators
Administrative units
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Starting June 30th, 2020 we will no longer add any
upgraded to Microsoft Authentication Library (MS
All applications
Owned applications
tot
2 applications found
Display name
TO
tot-plugin-azure-ad
TO
tot-plugin-azure-storage


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Anjana Data > tot-plugin-azure-ad
tot-plugin-azure-ad | API permissions
Search (Ctrl+/)
Refresh
Got feedback?
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
The "Admin consent required" column shows the default value for an organization. However, use
organization, or in organizations where this app will be used. Learn more
Configured permissions
Applications are authorized to call APIs when they are granted permissions by users/admins as p
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
Microsoft Graph (5)
Group.Create
Application
Create groups
Group.ReadWrite.All
Application
Read and write all groups
GroupMember.ReadWrite.All
Application
Read and write all group memberships
User.Read
Delegated
Sign in and read user profile
User.Read.All
Application
Read all users' full profiles

# Limitaciones Azure

El número máximo de usuarios en un grupo es de 100. Lo que significa que en un DSA que gobierne objetos en azure no puede tener más de 100 personas adheridas (incluyendo owners), a partir de la 100 no se podrá aplicar gobierno activo.

# Configuración necesaria

```yaml
server:
 port: 15009

totplugin:
 location: http://totpluginazuread:15009/plugin/azure/ad/api/v1
 server:
   url: http://totserver:15000/tot/
   keep-alive-seconds: 60
 aris:
   - ari: "anja:totplugin:im:/microsoft/azure/ad/"
 connection:
   pathSeparator: "/"
   clientId: "1x0xx2b1-380e-407e-9f7e-bea8a5sa496f"
   tenantId: "xxx11d52-8710-418d-bb06-9fb94eg04ded"
   secret: "Xx-bGup3orJ-M4~.7H~oF~zhI343VL5M-q"
   scopes: "https://graph.microsoft.com/.default"
 groupPrefix: Dsa_
```

Server:

- port: El puerto en el que se va a desplegar el plugin.
- keep-alive-seconds: Tiempo de espera entre intentos de registro del plugin

TotPlugin (apartado con la configuración específica del plugin):

- Location: URL del plugin cuando está desplegado (lo que se debe modificar es el host y el puerto, la ruta de entrada no debe modificarse)
- Server:
  - Url: URL de tot
- Aris:
  - ari: ARI usada para registrarse en Tot y poder ser referido y llamado según eventos en Anjana.
- Connection (apartado con la configuración relativa a las credenciales de conexión con Azure AD):
  - pathSeparator: El símbolo que se usa como separador de path
  - clientId: El id de la aplicación registrada para conectarse con Azure AD.
  - tenantId: El tenant id de la suscripción de la cuenta de Azure.
  - secret: La contraseña de la aplicación registrada para conectarse con Azure AD.
  - scopes: El scope al que el plugin interactúa con Azure, en este caso con el graph de microsoft que es el encargado de los grupos y usuarios.

- groupPrefix: El prefijo que se concatena a los nombres de los grupos. El nombre completo del grupo lo formará el prefijo más el nombre y la versión.