OS2skoledata

Azure AD integration

Version: 1.0.0
Date: 15.04.2023
Author: BSG

Indhold

1 Indledning 3
2 Forudsætninger 3
3 Opret integration i Azure portalen 3
3.1 Tilføj en ”Secret” 4
3.2 Tildel rettigheder til applikationen 4
4 Opsætning af integration 5

1 Indledning

I forbindelse med den tekniske implementation af OS2skoledata kan der opsættes en løbende overførsel af data til Azure AD. Denne vejledning dækker opsætningen i Azure portalen, så OS2skoledata kan få adgang.

2 Forudsætninger

Man skal have adgang til Azure portalen, og have de nødvendige rettigheder deri til at kunne oprette applikationer og brugerkonti, og tildelse disse rettigheder.

3 Opret integration i Azure portalen

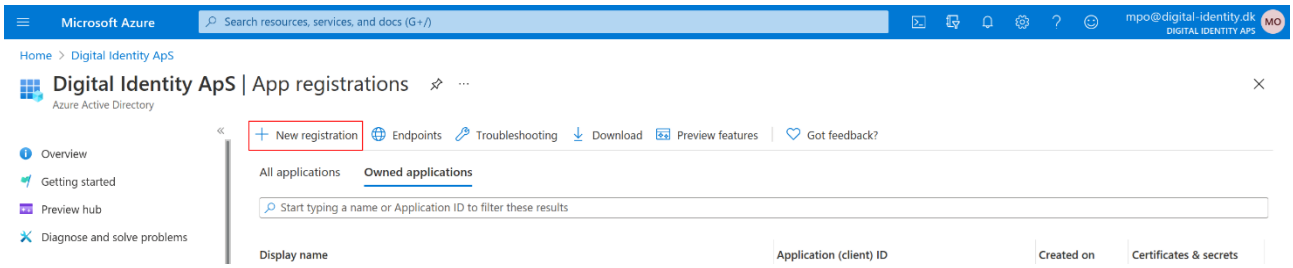
For at integrationen kan få lov til at kalde API'et på Azure AD, skal den oprettes som applikation i Azure portalen og tildeles rettigheder. Dette gøres på følgende måde

Login i Azure portalen her

https://portal.azure.com/

Klik dernæst på burger-menuen i venstre øverste hjørne (de 3 vandrette streger) og vælg "Azure Active Directory" for at navigere til AAD

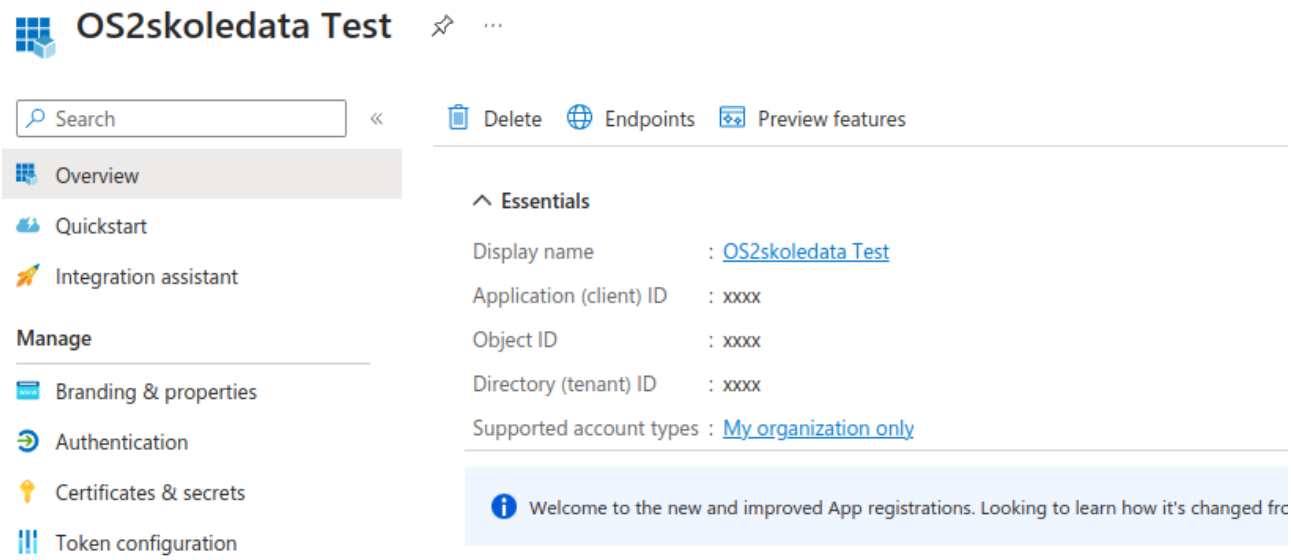
Her kan man vælge "App Registration" i menuen, og herunder klikke på linket "New Registration" som vist nedenfor



Herefter vises et skærmbillede hvor man skal udfylde stamdata for applikationen. De konkrete værdier anvendes ikke, da man ikke skal logge ind i applikationen, men fx kan man angive følgende værdier

- "OS2skoledata" som navn
- Single Tenant som "Supported Account Types"

Når applikationen er oprettet, vises en side med nedenstående oplysninger



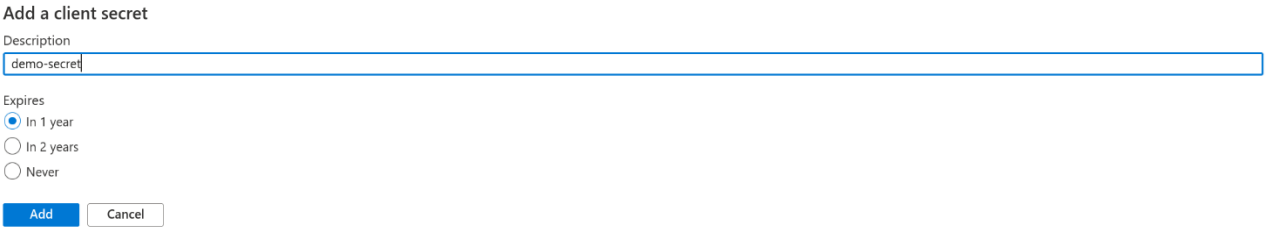
Her skal man notere følgende oplysninger

- Application (client) ID
- Directory (tenant) ID

Da de skal bruges senere i opsætningen.

3.1 Tilføj en "Secret"

Vælg nu "Add a certificate or secret og opret en ny Client Secret. Denne skal gives et navn og en udløbsdato. Bemærk at hvis man ikke kan vælge at den aldrig udløber, så skal man huske at fornye denne regelmæssigt, da integrationen ellers holder op med at virke



Når denne Secret oprettes, dannes en "Value" som er den faktiske nøgle, og denne vises kun denne ene gang, så det er vigtigt at notere den ned, da den skal bruges i opsætningen af integrationen. Hvis den går tabt skal der dannes en ny Secret.

3.2 Tildel rettigheder til applikationen

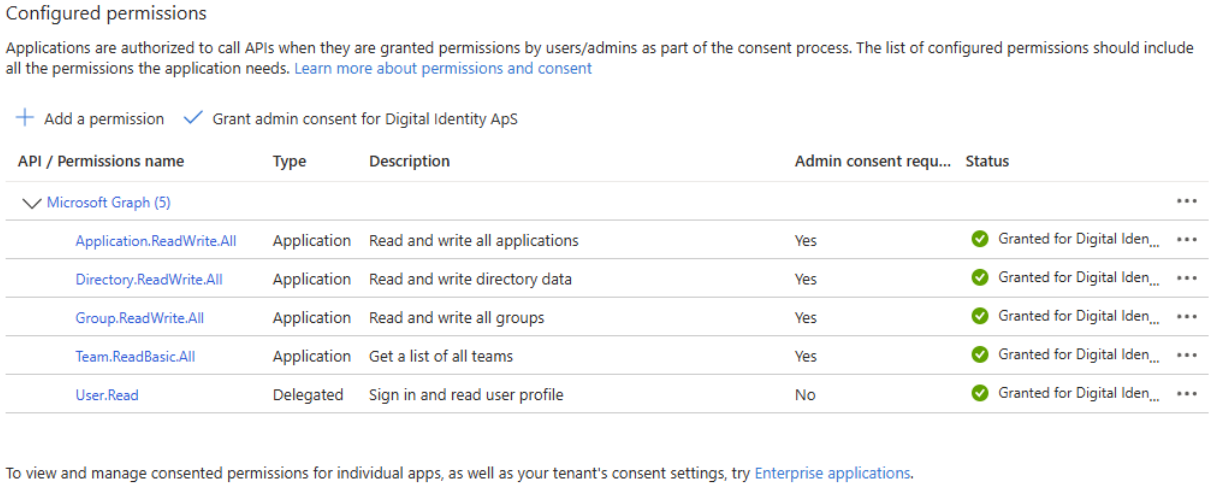
Integrationen skal bruge en række rettigheder for at kunne udlæse oplysninger fra AAD. Disse opsættes på følgende måde

1. Tryk på "API Permissions" i venstre menuen.
2. Tryk på "Add a permission"
3. Vælg "Select Microsoft APIs" og dernæst "Microsoft Graph"

Følgende rettigheder skal tildeles herunder

- Directory.ReadWrite.All (denne skal bruges, da vi tilføjer et custom OS2skoledata skema)
- Application.ReadWrite.All (denne skal bruges, da vi tilføjer et custom OS2skoledata skema)
- User.Read
- Team.ReadBasic.All (hvis OS2skoledata skal oprette teams)
- Group.ReadWrite.All

Når alle er tilvalgt, trykkes på ”Add permission”, og rettigheden er nu tildelt.



Endeligt skal der tildeles et såkald ”Admin consent”, hvilket gøres på følgende måde

1. Tryk på knappen ”Grant admin consent for ...”
2. Vælg ”Yes” i den billede der kommer frem

4 Opsætning af integration

Digital Identity opsætter selve integrationen, og skal bruge de oplysninger der er noteret ovenfor. Hvis adgangen udløber, er det vigtigt at den fornyes inden udløb, og at dette håndteres af kommunen som har adgang til Azure portalen.