OS2rollekatalog

Opsætning af Microsoft Entra ID integration

**Version**: 1.0.0

**Date**: 27.12.2024

**Author**: KBP

# Indholdsfortegnelse

[1 Indholdsfortegnelse 1](#_Toc2063072315)

[2 Indledning 2](#_Toc1540110874)

[3 App registration 3](#_Toc396336399)

[3.1 Oprettelse af App Registration 3](#_Toc634383270)

[3.2 Tildeling af rettigheder 5](#_Toc686815192)

[4 Anvendelse 7](#_Toc299601964)

[4.1 Sammenkobling af it-systemer og Entra Id grupper 7](#_Toc784441760)

# Indledning

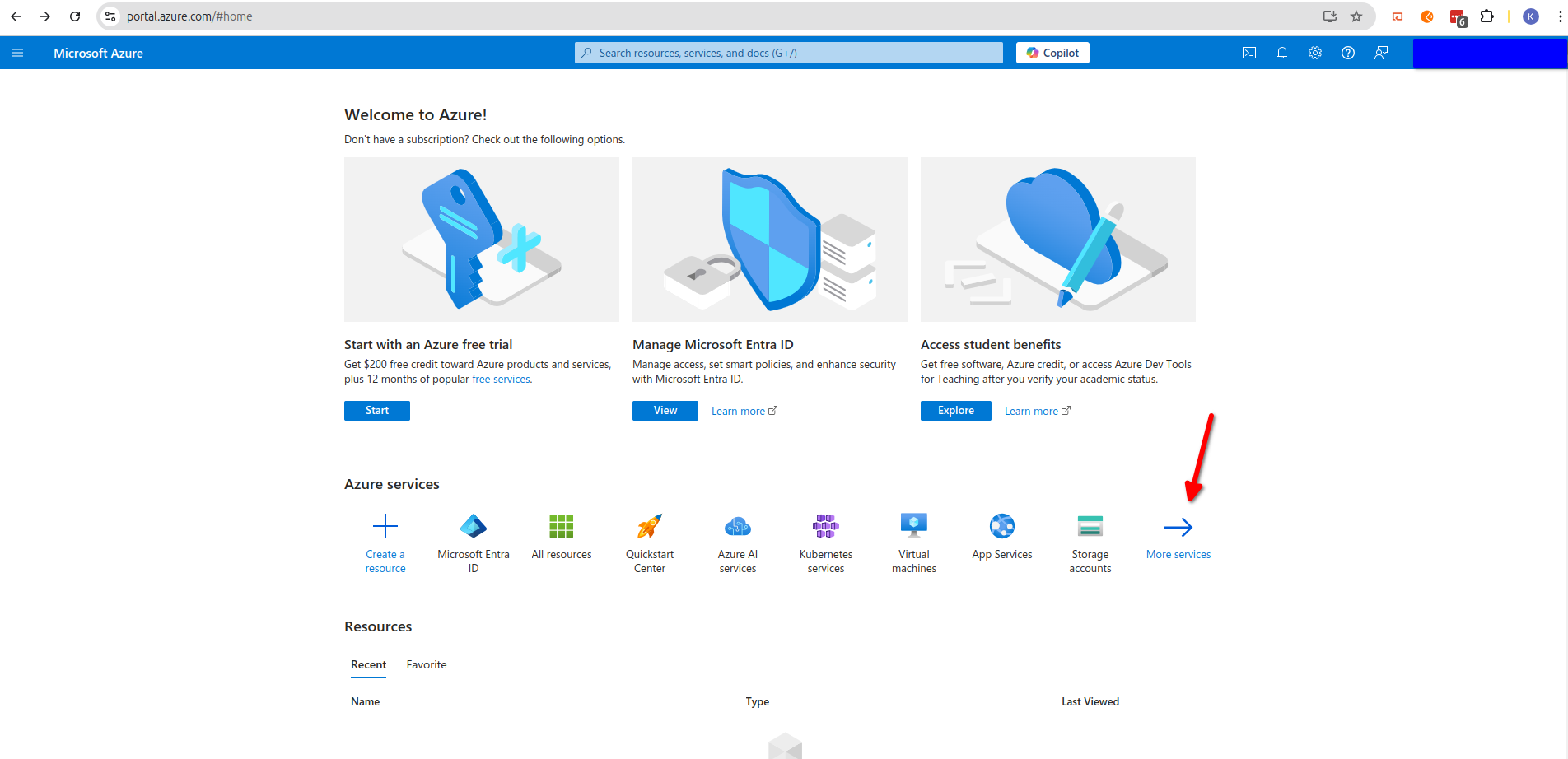
OS2rollekataloget har en indbygget integration med Microsoft Entra ID, som bruges til at styre gruppemedlemskaber i organisationen. For at aktivere denne integration skal du oprette en **App Registration** i Azure. Når App Registration er oprettet, skal de nødvendige credentials (adgangsoplysninger) sendes til Digital Identity for at fuldføre opsætningen.

# App registration

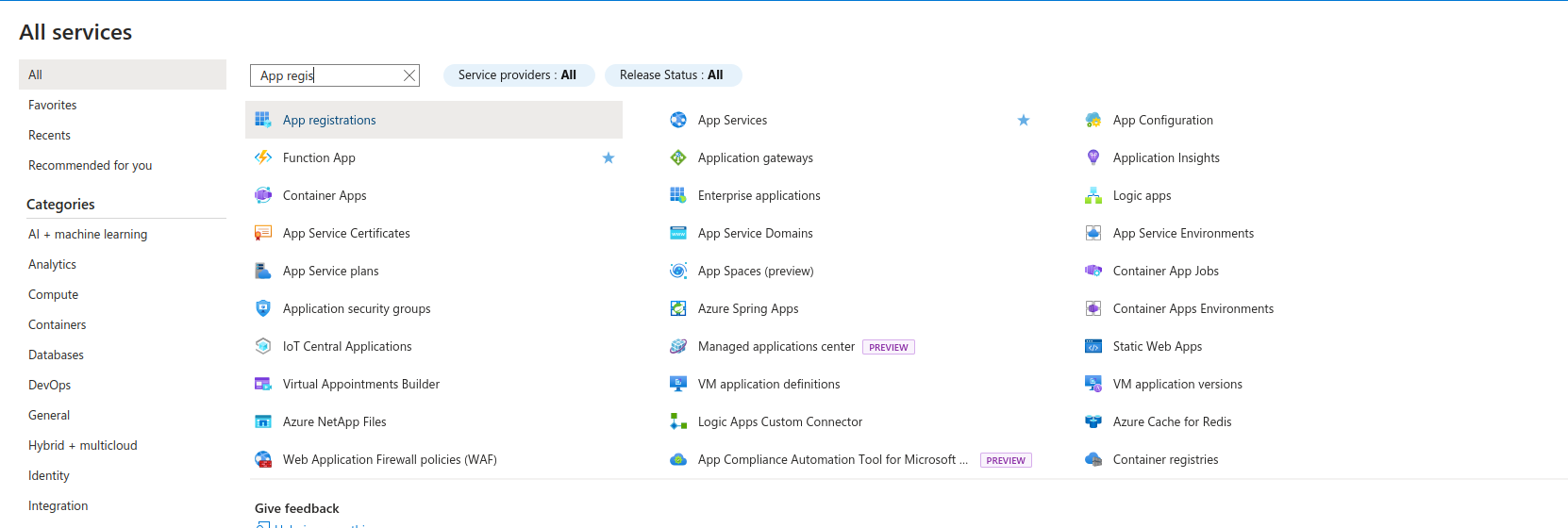
## Oprettelse af App Registration

Der logges ind i Azure på <https://portal.azure.com/>

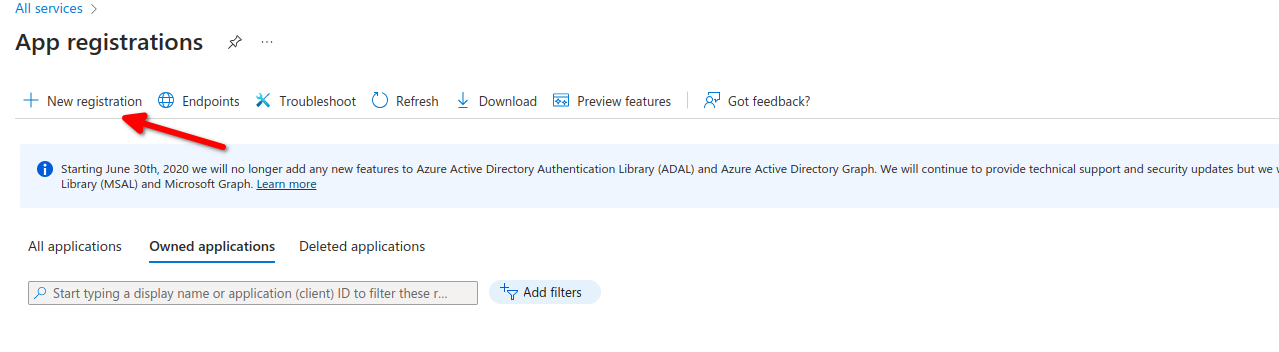
I følgende skærmbillede vælges **More services**



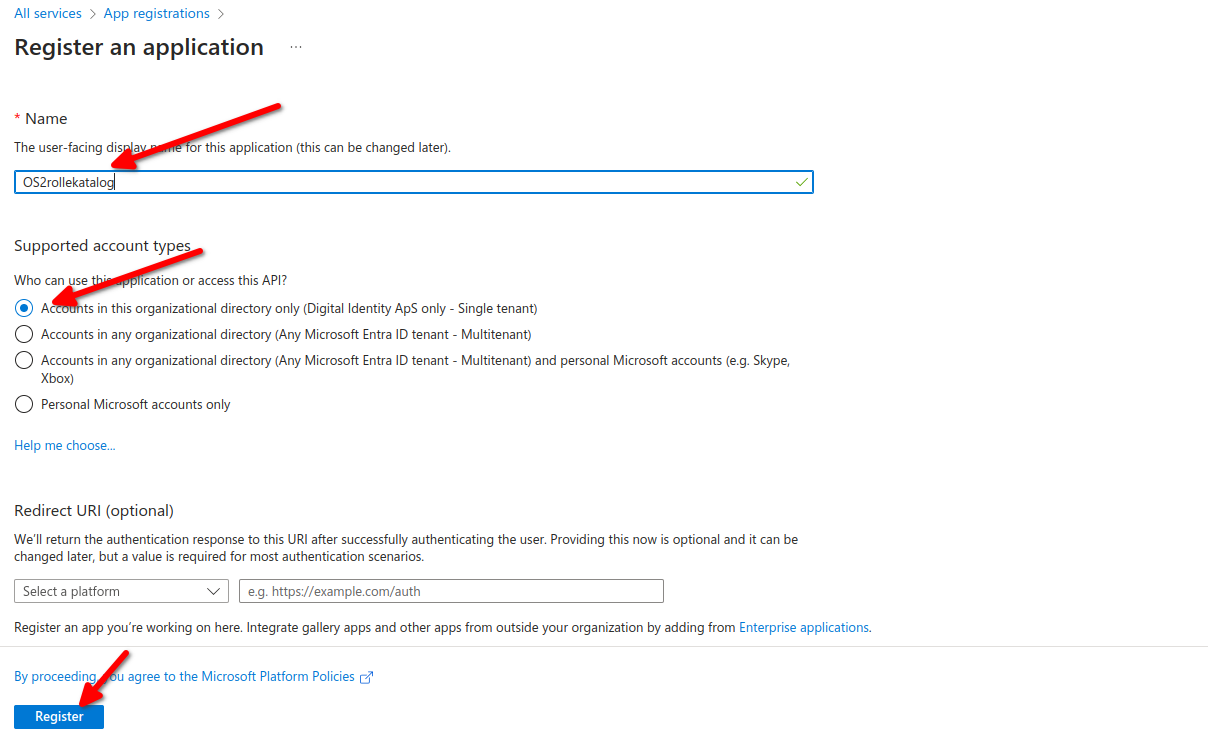
I **All services** vælges **App registrations**, søge feltet kan med fordel benyttes.



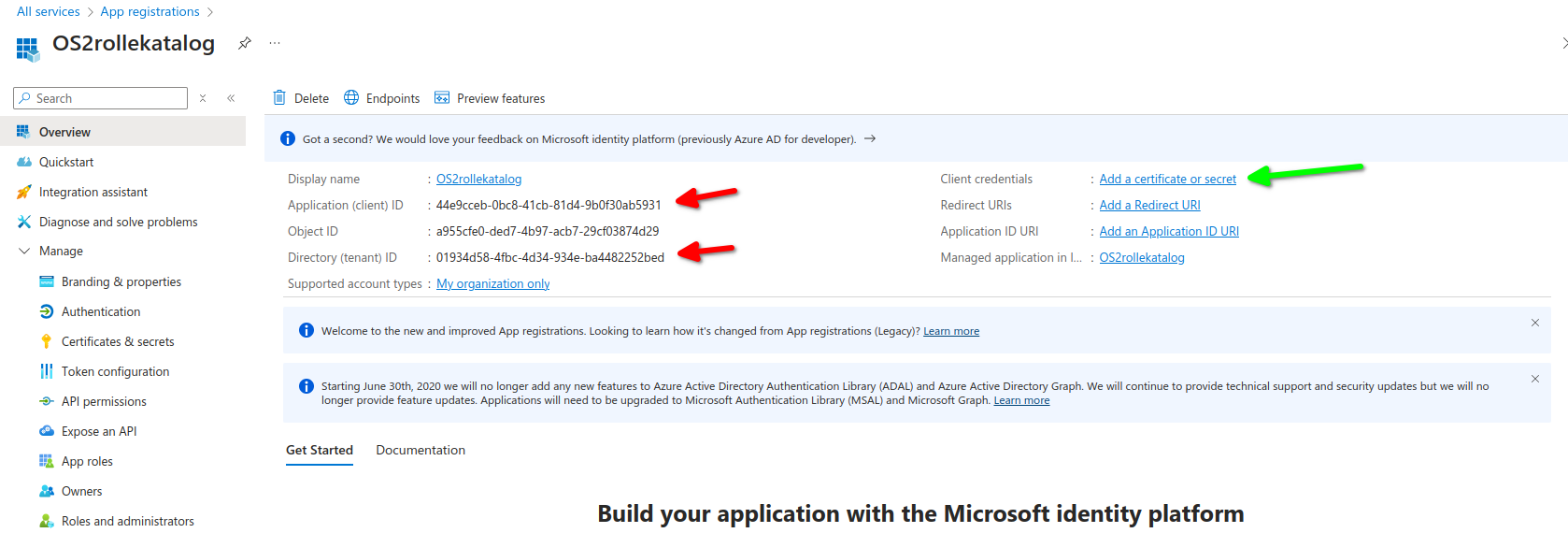
I **App registrations** billedet vælges nu **New registration**



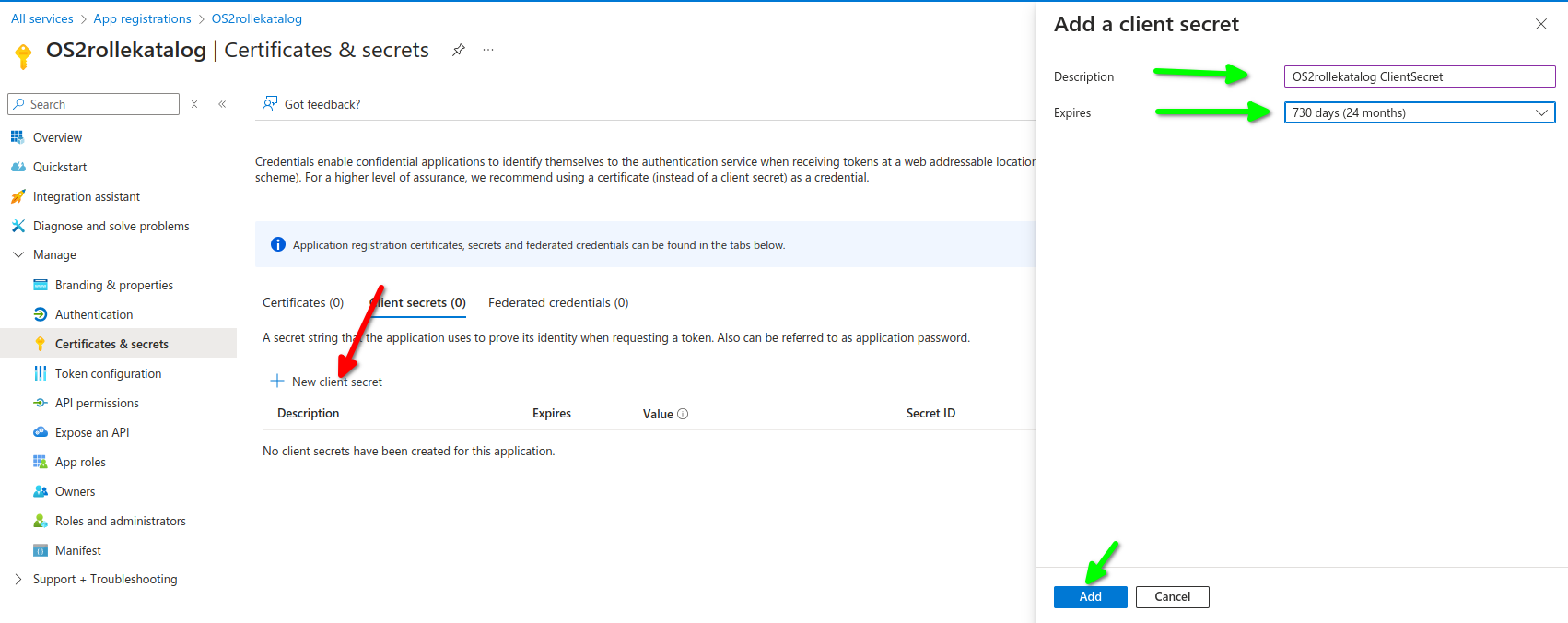
Der vælges nu et sigende navn, og der vælges **Single tenant** og der trykkes **Register**



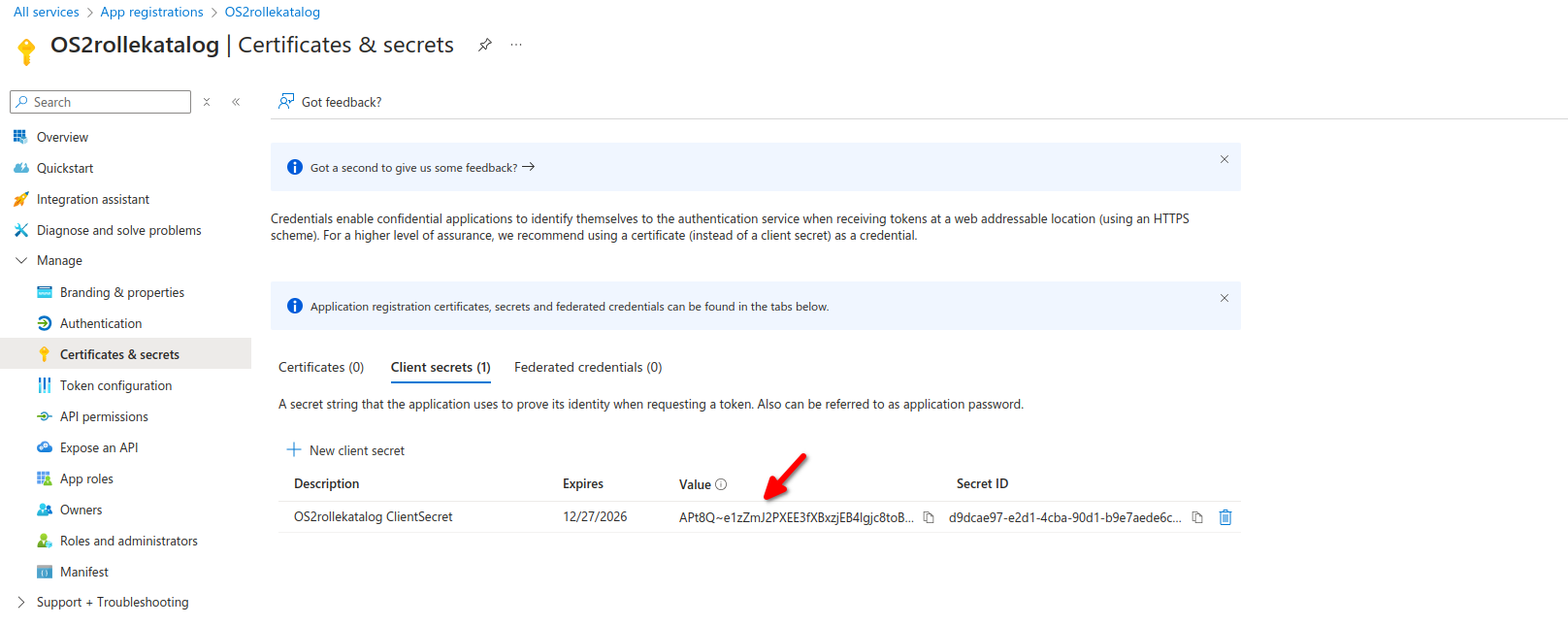
Nu er der oprettet en App registration, gem Application (client) Id og Directory (tenant) ID, disse skal sendes til Digital Identity, sammen med en client secret, som vi opretter nu ved at trykke på **Add a certificate or secret**.



Vælg nu **New client secret**, udfyld beskrivelse samt gyldighed, bemærk der skal laves en ny nøgle og sendes til Digital Identity, når den udløber, så vælg gerne lang gyldighed.



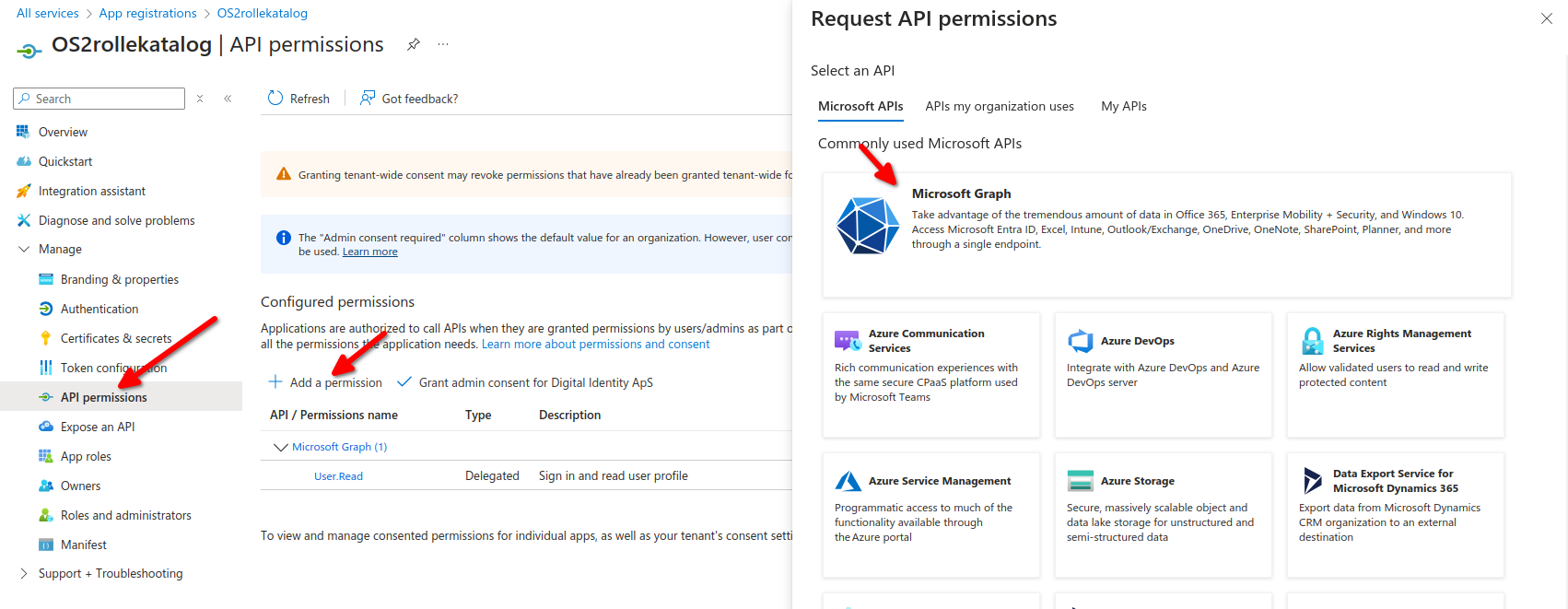
Kopier nu **Value** og send den sammen med Application (client) Id og Directory (tenant) ID til Digital-identity, på en sikker måde, fx. ved gemme det i en fil og uploade på kundenettet.



## Tildeling af rettigheder

For at rollekataloget kan læse og ændre gruppemedlemsskaber, kræves der desuden at der tilføjes rettigheder til den **App registration** som blev oprettet ovenfor.

Det gøres ved at vælge **API permissions** og **Add permissions** her vælges **Microsoft Graph**

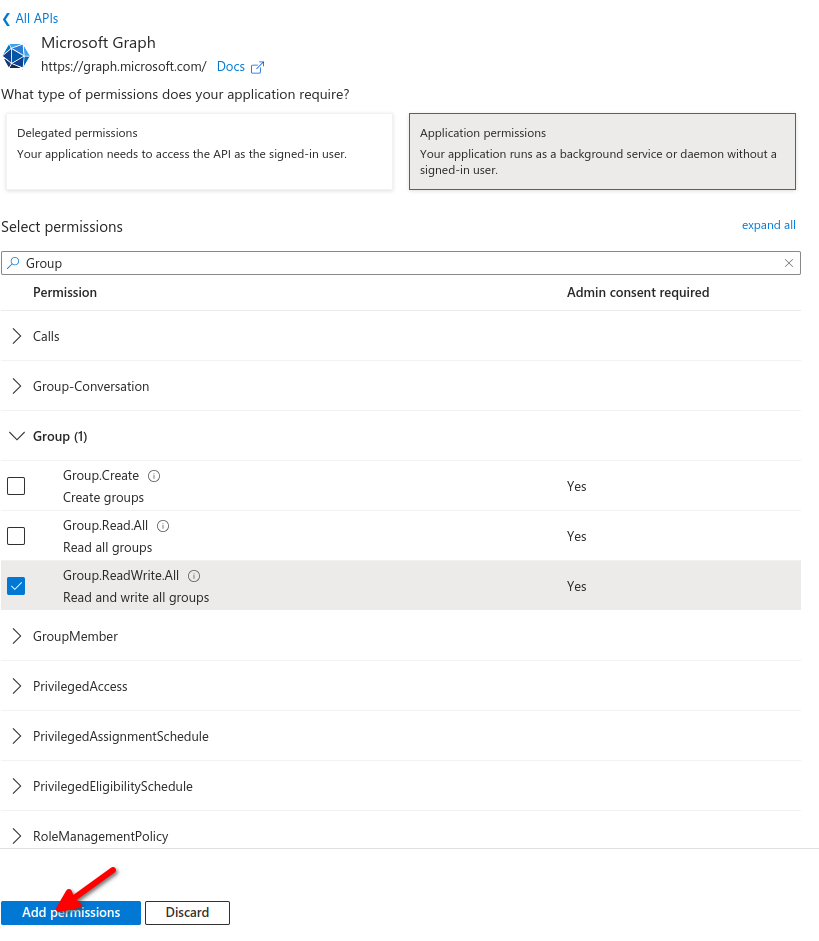


I næste skridt vælges **Application permissions** følgende vælges:

User.ReadWrite.All denne bruges til at hente brugerne.

Group.ReadWrite.All denne bruges til at ændre medlemskaber på grupperne.

Endelig vælges **Add permission**



# Anvendelse

## Sammenkobling af it-systemer og Entra Id grupper

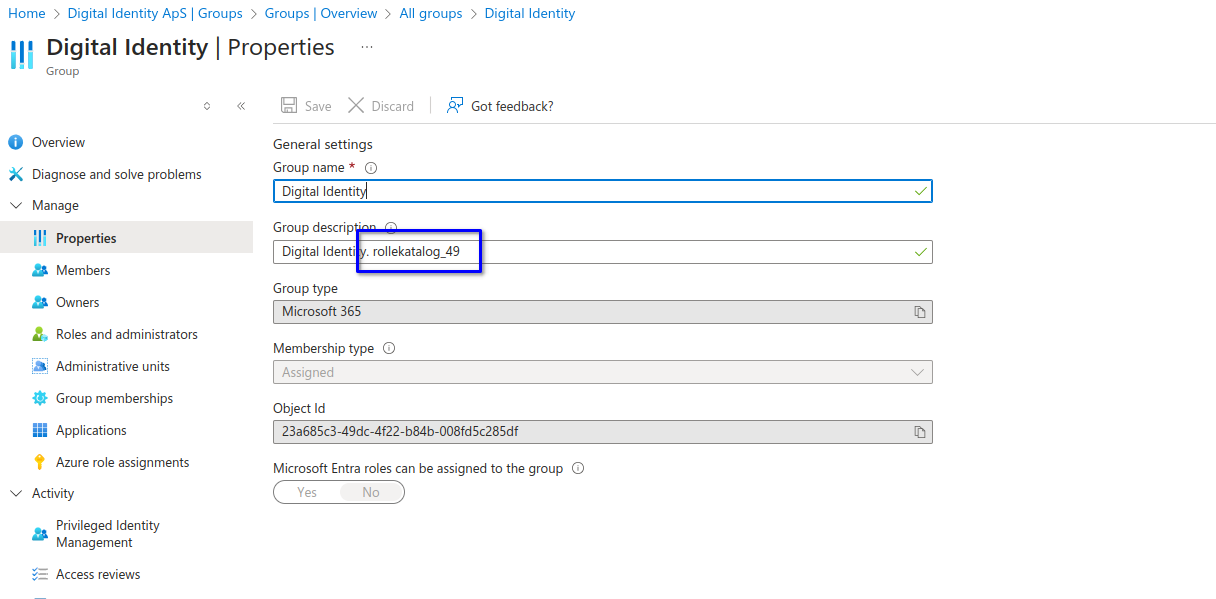
I rollekataloget oprettes et eller flere it-systemer, under synkronisering kigges ikke på it-system typen, men det giver nok mest mening at oprette dem som AD integrationer.

Gå ind på it systemet i rollekataloget og noter nummeret på it-systemet, det er det der står i adressebaren.



I azure findes den eller de grupper som der ønskes styret fra rollekataloget.

I beskrivelsen skrives rollekatalog\_49 hvis it-systemet der synkroniseres til har nummer 49, det skal bare være en del af beskrivelsen, så der kan godt stå andet i feltet også.



Rollekataloget vil nu styre gruppemedlemskaber af gruppen.

Azure grupperne behøver ikke synkronisere til det samme it-system, der kan godt oprettes flere it-systemer rollekataloget, på