Handleiding Aanmelden met Microsoft (Azure AD)

1-10-2022

Inhoud

Lijst met afbeeldingen

1 Inleiding

Het is mogelijk om Archie gebruikers te koppelen aan ‘Azure Active directory’ (AAD). Dit houdt in dat bij het aanmeldscherm in Archie (Desktop, web en app) een knop is waarop staat ‘Aanmelden met Microsoft’. Deze knop zal een venster openen waarmee de gebruiker kan inloggen met een AAD account. Dit ziet er als volgt uit bij de Archie web app (op de desktop en app is het vergelijkbaar):

FIGUUR 1. INLOGSCHERM ARCHIE MET MICROSOFT ALS IDENTITY PLATFORM

Om deze functionaliteit te kunnen benutten, dienen er een aantal stappen genomen te worden. De belangrijkste stap is een app-registratie in de ‘Azure Active Directory Admin center’ (AADAC). Daarnaast moeten er een aantal instellingen gedaan worden m.b.t. gebruikersprofielen voor iedere Archie gebruiker (ook in AADAC). Als laatste moet in Archie systeembeheer een aantal instellingen worden gedaan om Archie aan AAD te koppelen.

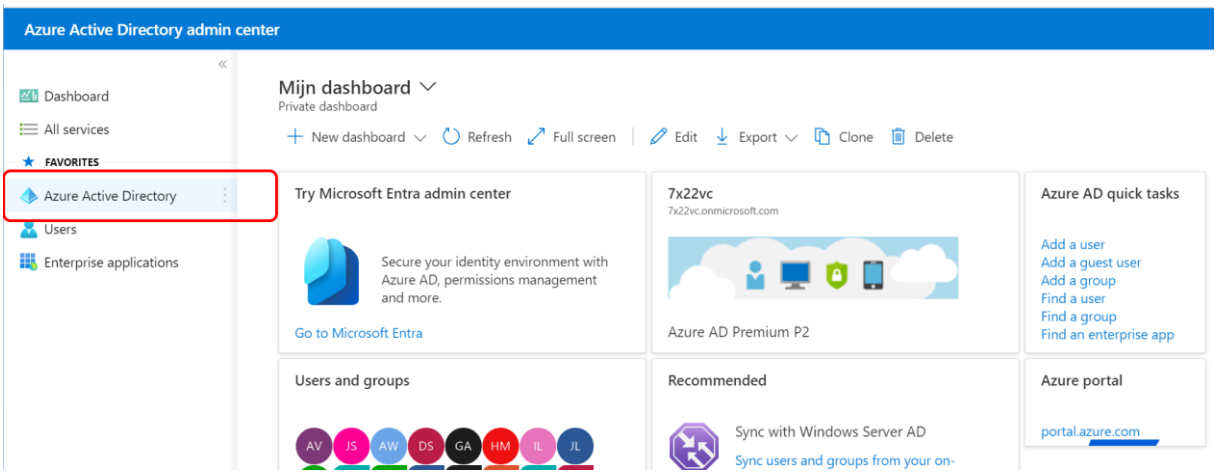
Door gebruik te maken van AAD ligt de verantwoordelijkheid van het aanmelden niet meer bij Archie, maar bij Microsoft. In dit geval wordt Microsoft de Identity Provider (IP) en Archie de Service Provider (SP).

2 App-registratie in AADAC

Om gebruik te kunnen maken van 'Aanmelden met Microsoft' moet er bij AADAC een app worden geregistreerd. Ga hiervoor naar AADAC en log in met een account dat in het domein de rechten heeft om een app registratie aan te maken (een 'systeembeheerder'): https://aad.portal.azure.com/

2.1 Azure active directory openen

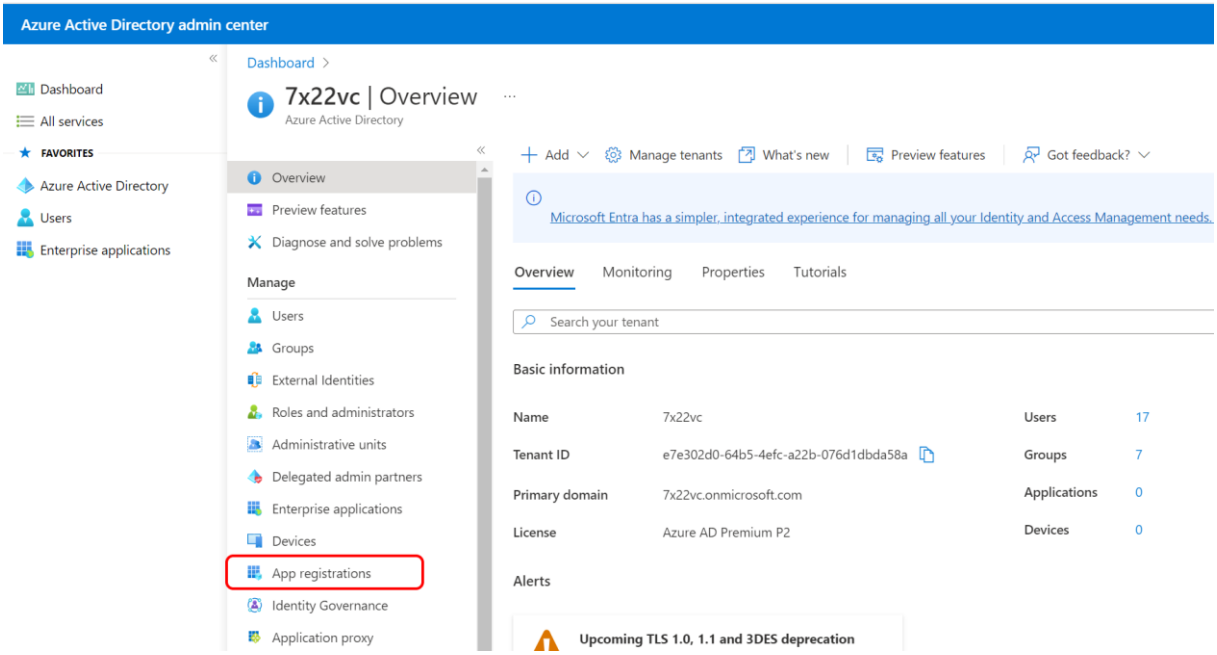
Zodra de gebruiker is ingelogd, klikt deze op 'Azure Active Directory':



FIGUUR 2. KLIK OP AZURE ACTIVE DIRECTORY

2.2 App registrations openen

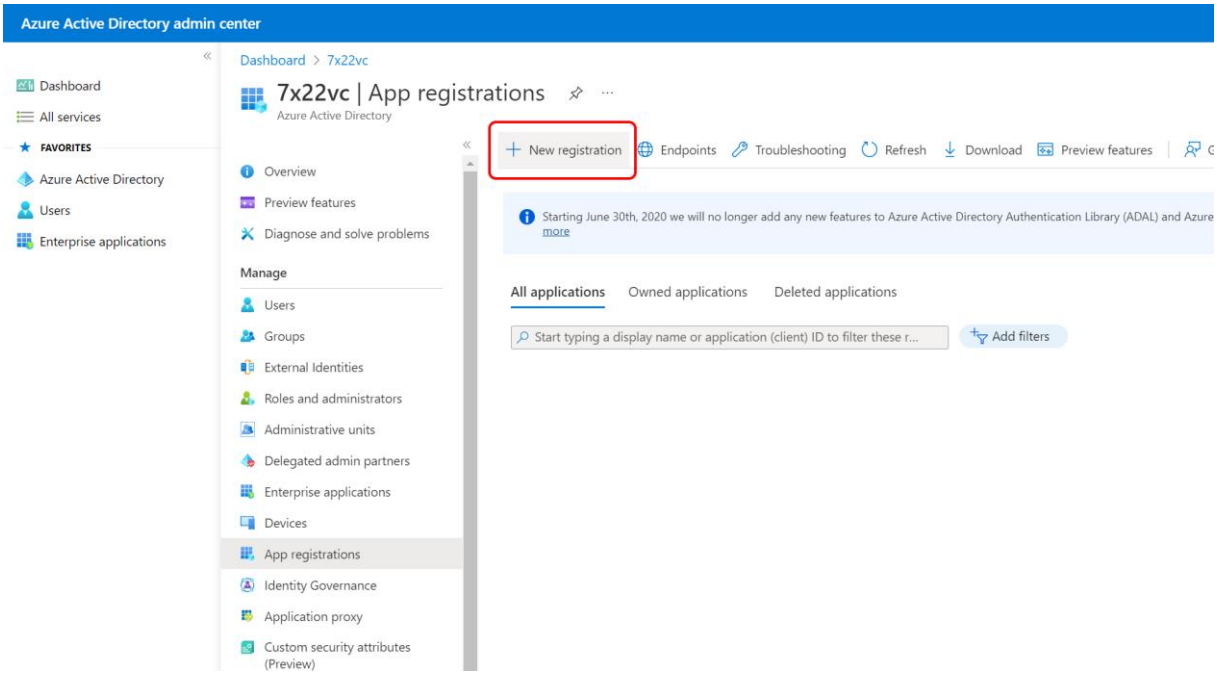
Een scherm met alle mogelijkheden voor de Active Directory verschijnt. Klik in dit scherm op 'App registrations':



FIGUUR 3. KLIK OP APP REGISTRATIONS

2.3 Nieuwe applicatie aanmaken

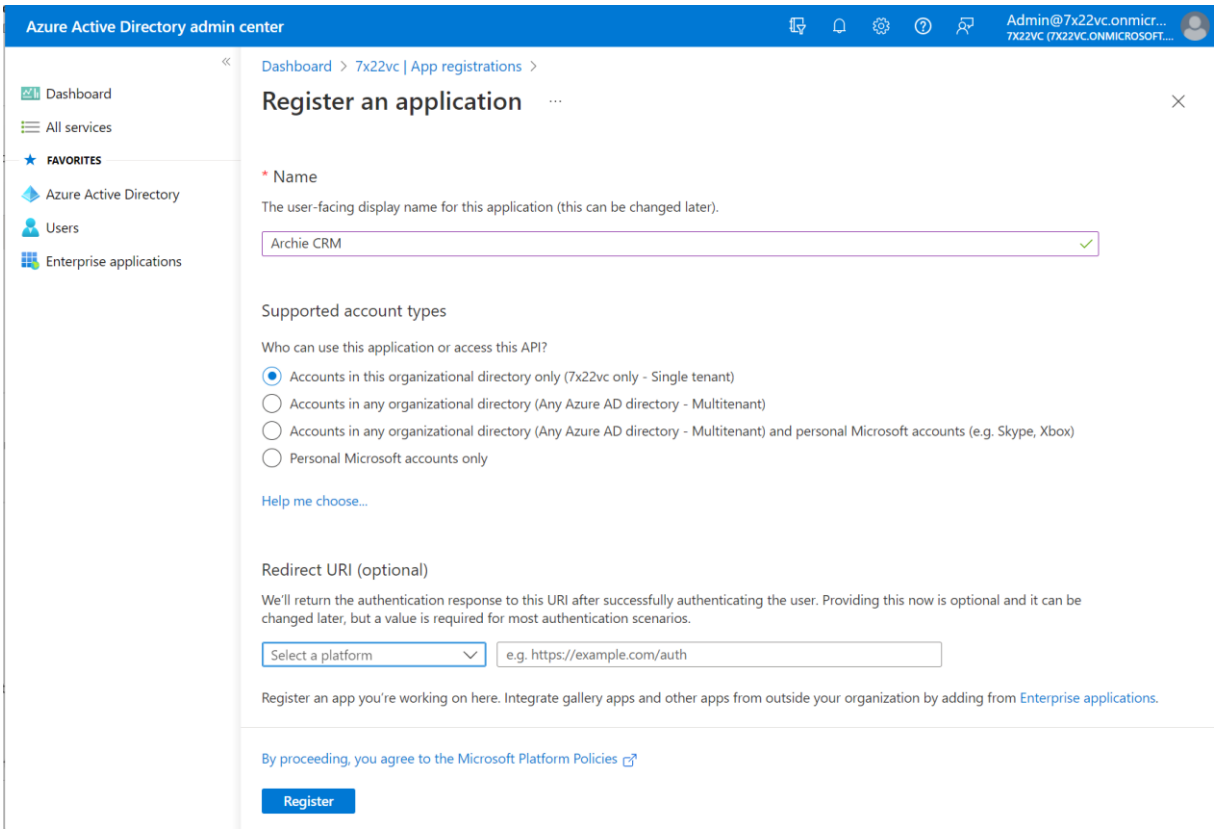
Er zal nu een overzicht verschijnen van apps die geregistreerd zijn. Het kan bijv. dat er al een app registratie staat voor de Archie OAP (Outlook Activities Plugin). Klik in dit scherm op de knop '+ New registration'.



FIGUUR 4. KLIK OP NEW APPLICATION

2.4 Registratiegegevens nieuwe applicatie invullen

Er verschijnt een scherm waarin de naam voor de applicatie moet worden gekozen. Voor deze naam mag alles worden ingevuld, maar Archie CRM is een voor de hand liggende naam. Kies bij ‘Supported account types’ voor ‘Accounts in this organizational directory only’ (Single tenant) en vul voor ‘Redirect URI’ niets in. Klik daarna op ‘Register’.

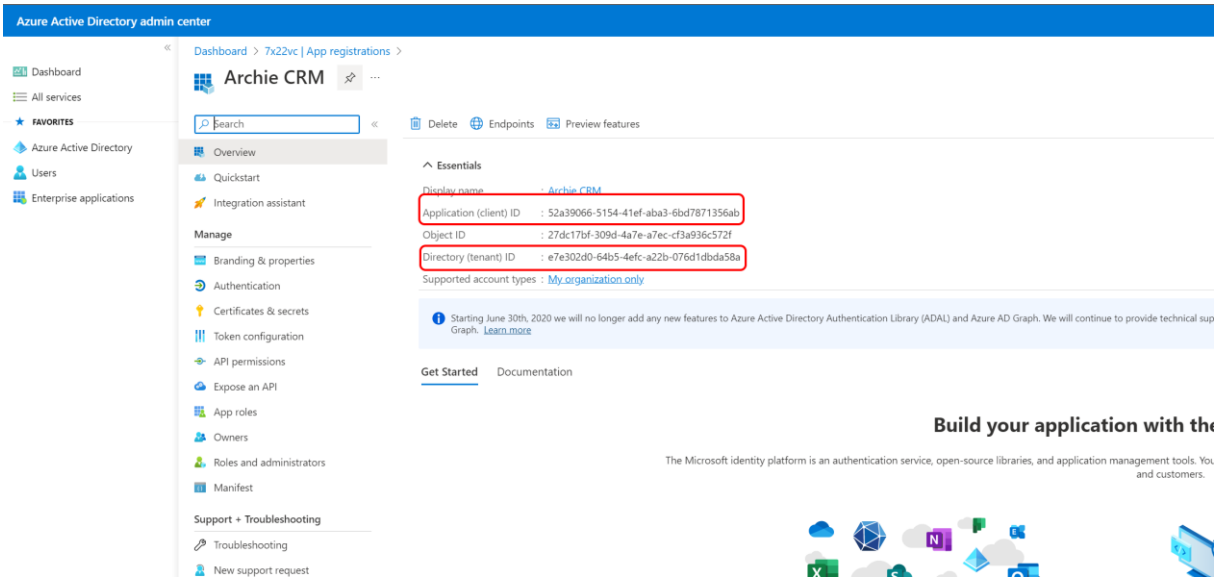


FIGUUR 5. REGISTREREN VAN EEN NIEUWE APPLICATIE (ARCHIE CRM)

2.5 Noteren client ID en tenant ID

Zodra de app is geregistreerd, zal het app overzicht verschijnen. Hierop staan belangrijke gegevens die verderop nodig zijn. Noteer de volgende gegevens:

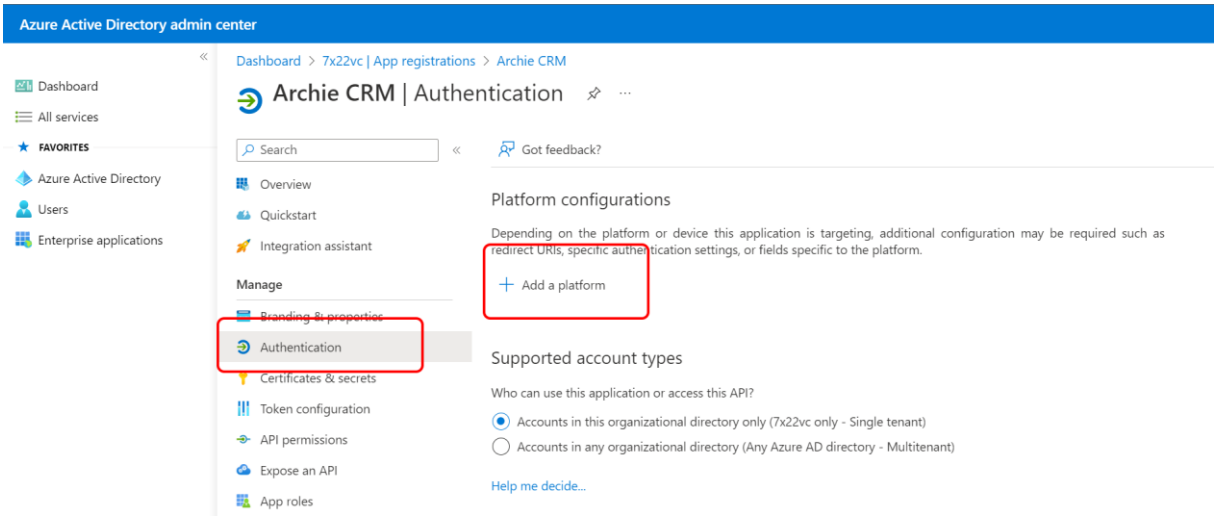
- Application (client) ID
- Directory (tenant) ID



FIGUUR 6. APPLICATION (CLIENT ID) EN DIRECTORY (TENANT) ID

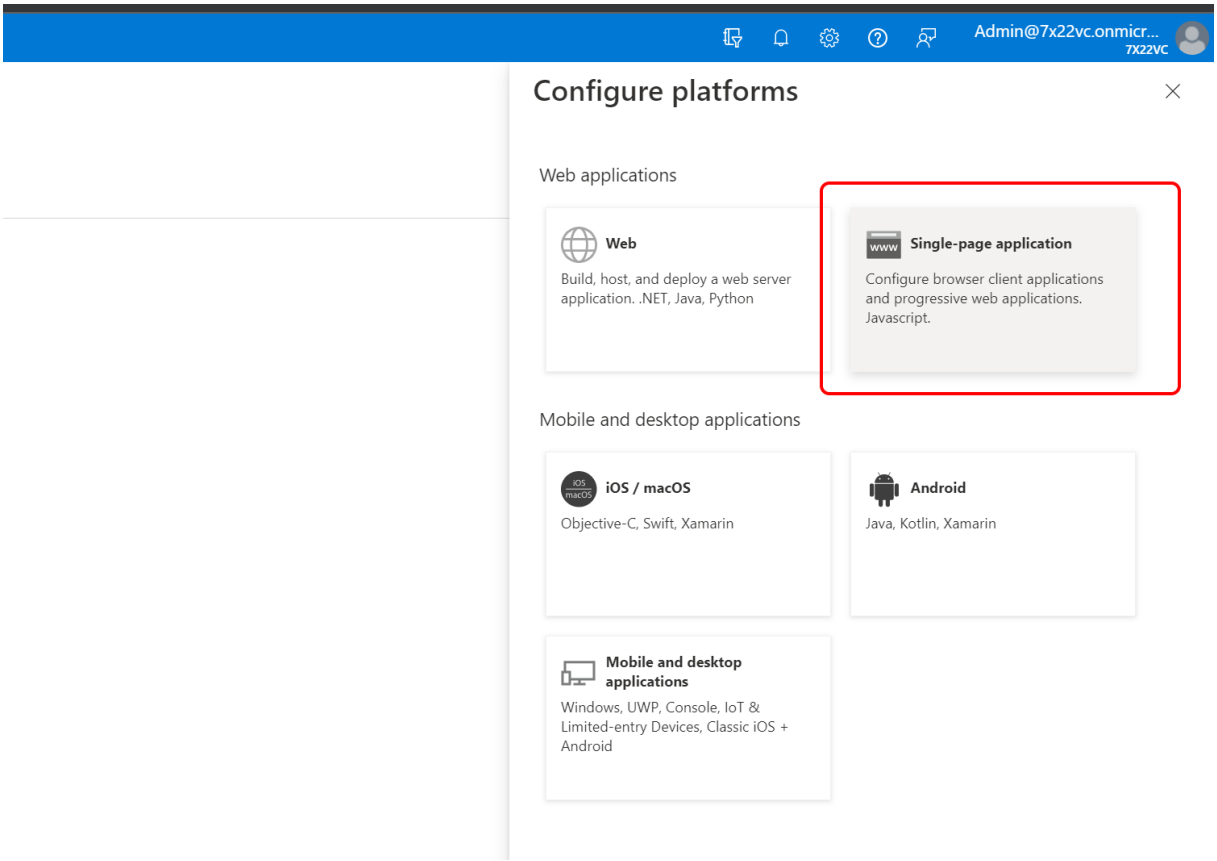
2.6 SPA platform toevoegen

Klik nu links op ‘Authentication’ en daarna op ‘+ Add a platform’:



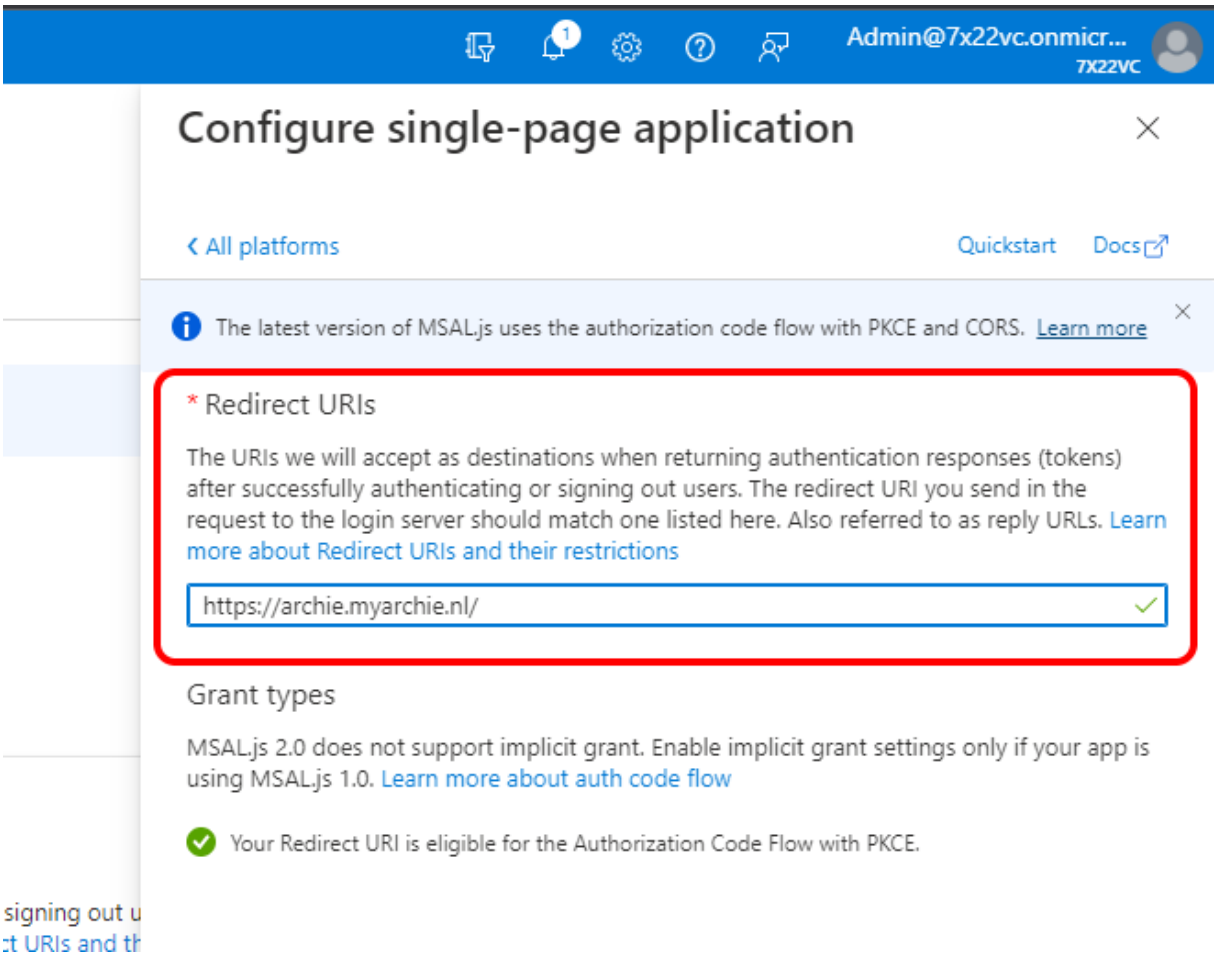
FIGUUR 7. AUTHENTICATION, ADD A PLATFORM

Er moeten twee platforms worden toegevoegd, een ‘Single-page application’ (SPA) en een ‘Mobile and desktop application’ (MDA). De eerste die wordt toegevoegd is de SPA. Klik in het scherm dat rechts verschenen is op Single-page application.



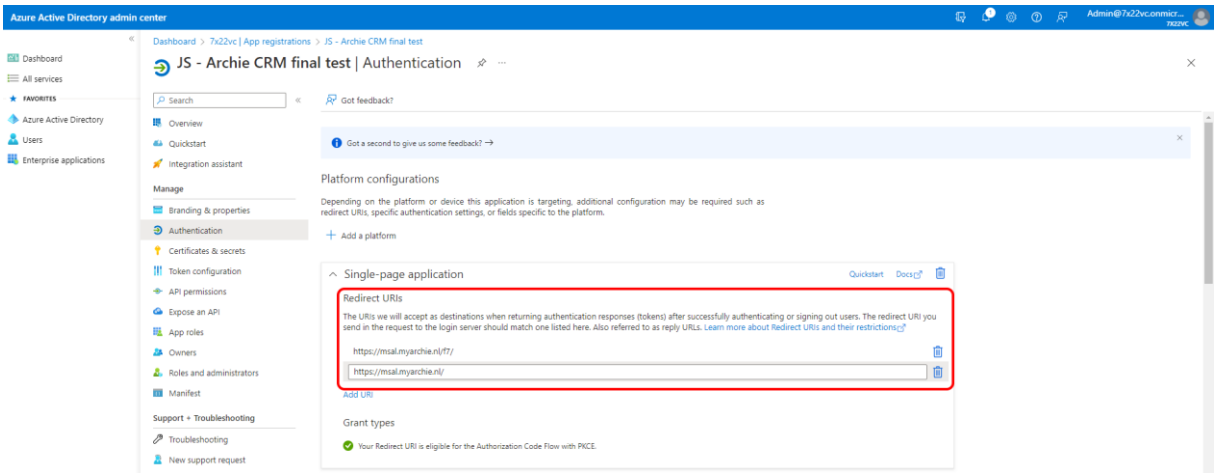
FIGUUR 8. TOEVOEGEN SINGLE-PAGE APPLICATION

Bij het toevoegen van een SPA moet de ‘Redirect URI’ worden ingevoerd. Deze is het URL van de web app, voor cloud klanten is dit als volgt: https://klantcode.myarchie.nl/ (**LET OP! Er moet met een slash (/) worden afgesloten)**, bijv. https://archie.myarchie.nl/. Laat de rest staan zoals het is ingevuld en klik op ‘Configure’.



FIGUUR 9. REDIRECT URI INVULLEN SPA

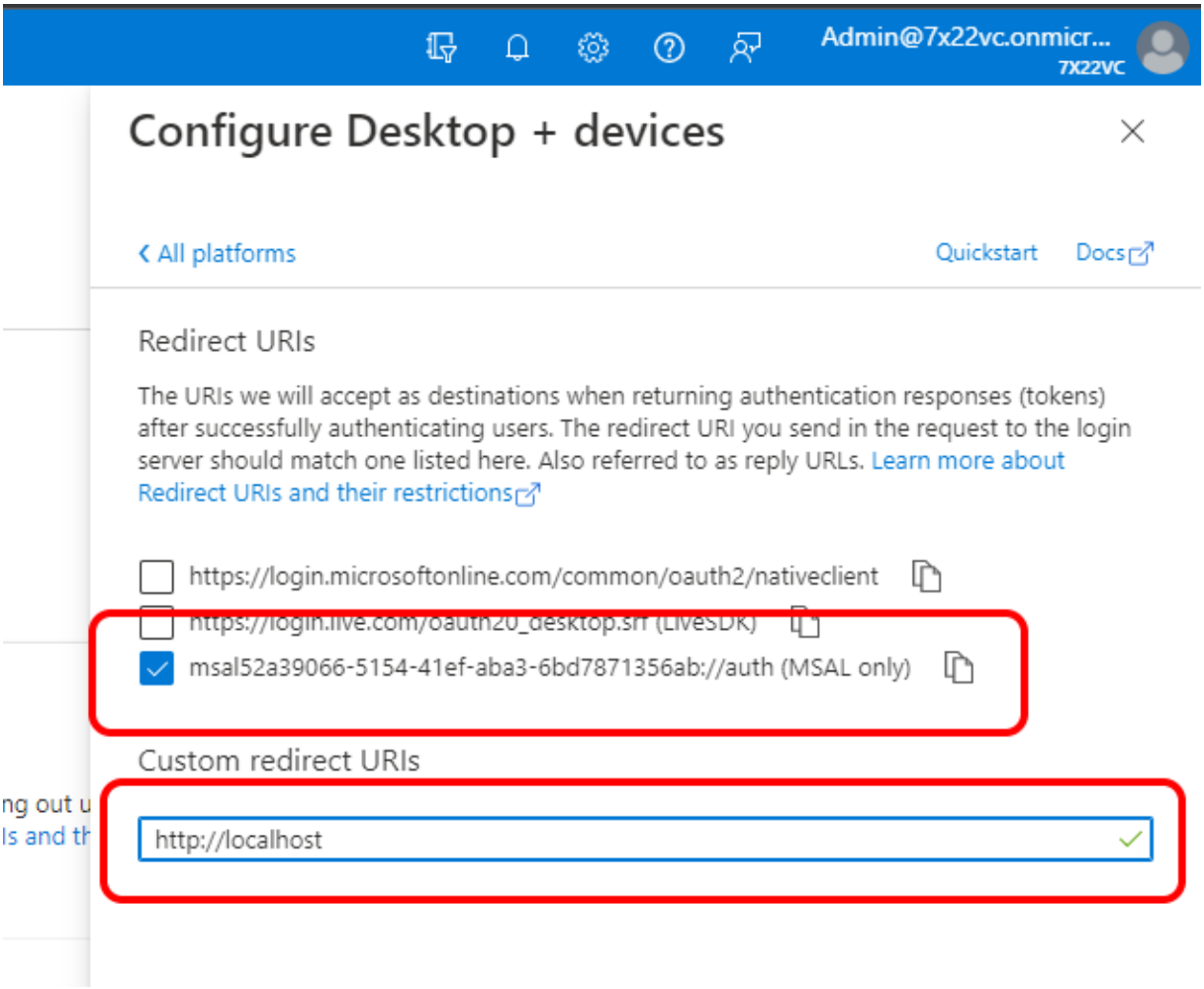
De SPA is nu toegevoegd. Klik nu in het blok ‘Single-page application’ op Add URI en vul nu hetzelfde URL in, maar dan met /f7/ erachter (Let weer op de slash achter f7). Klik daarna op ‘Save’.



FIGUUR 10. KLIK EERST OP ADD URI EN VUL DAARNA HET URL + /F7/ IN.

2.7 MDA platform toevoegen

Klik nu nogmaals in het scherm op '+ Add a platform' (zie Figuur 7) en kies dan voor 'Mobile and desktop applications'. Vink in het volgende scherm de optie 'MSAL only' aan (msal[clientid]://auth), vul daarna bij 'Custom redirect URIs' de waarde 'http://localhost'[1] in en klik op 'Configure'.

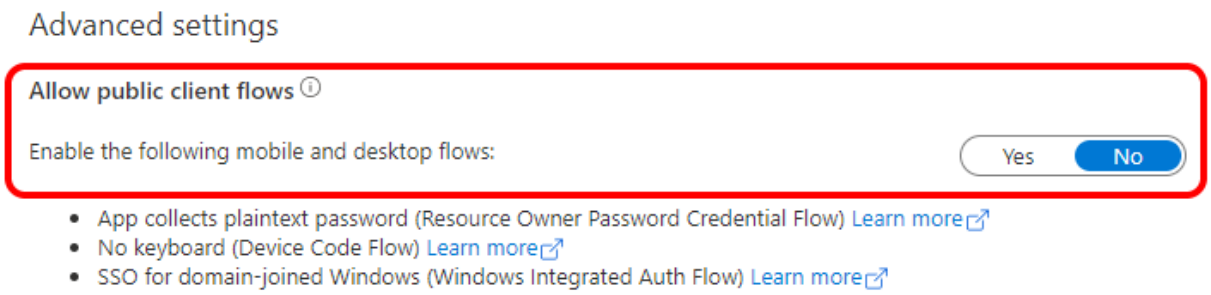


FIGUUR 11. MOBILE EN DESKTOP CONFIGURATIE

[1] Het is mogelijk een poort op te geven, bijv. http://localhost:37005, maar dit wordt afgeraden. Dit kan worden gebruikt als poort 80 bij de gebruikers van Archie in gebruik is. Als hier een andere poort wordt opgegeven, dan moet bij het instellen van Archie systeembeheer hier ook dezelfde poort worden opgegeven.

2.8 Allow public client flows inschakelen

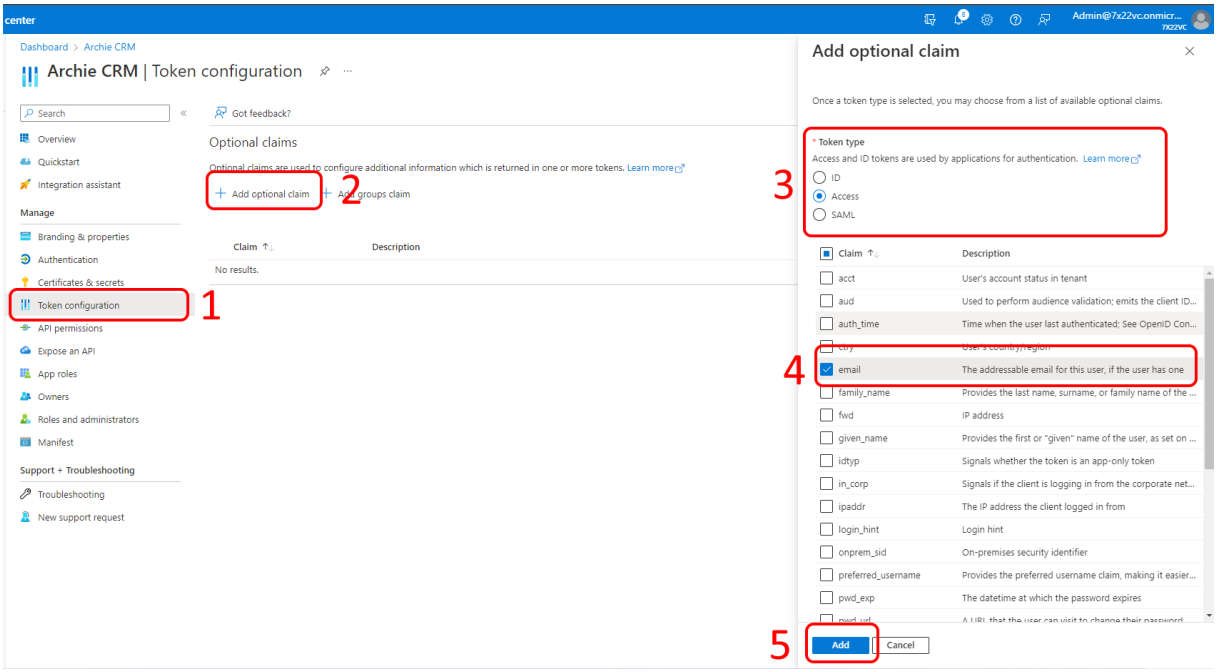
Scroll nu naar beneden en zet 'Allow public client flows' op YES onder 'Advanced settings' en klik daarna op 'Save' onderin het scherm.



FIGUUR 12. ALLOW PUBLIC CLIENT FLOWS OP 'YES' ZETTEN

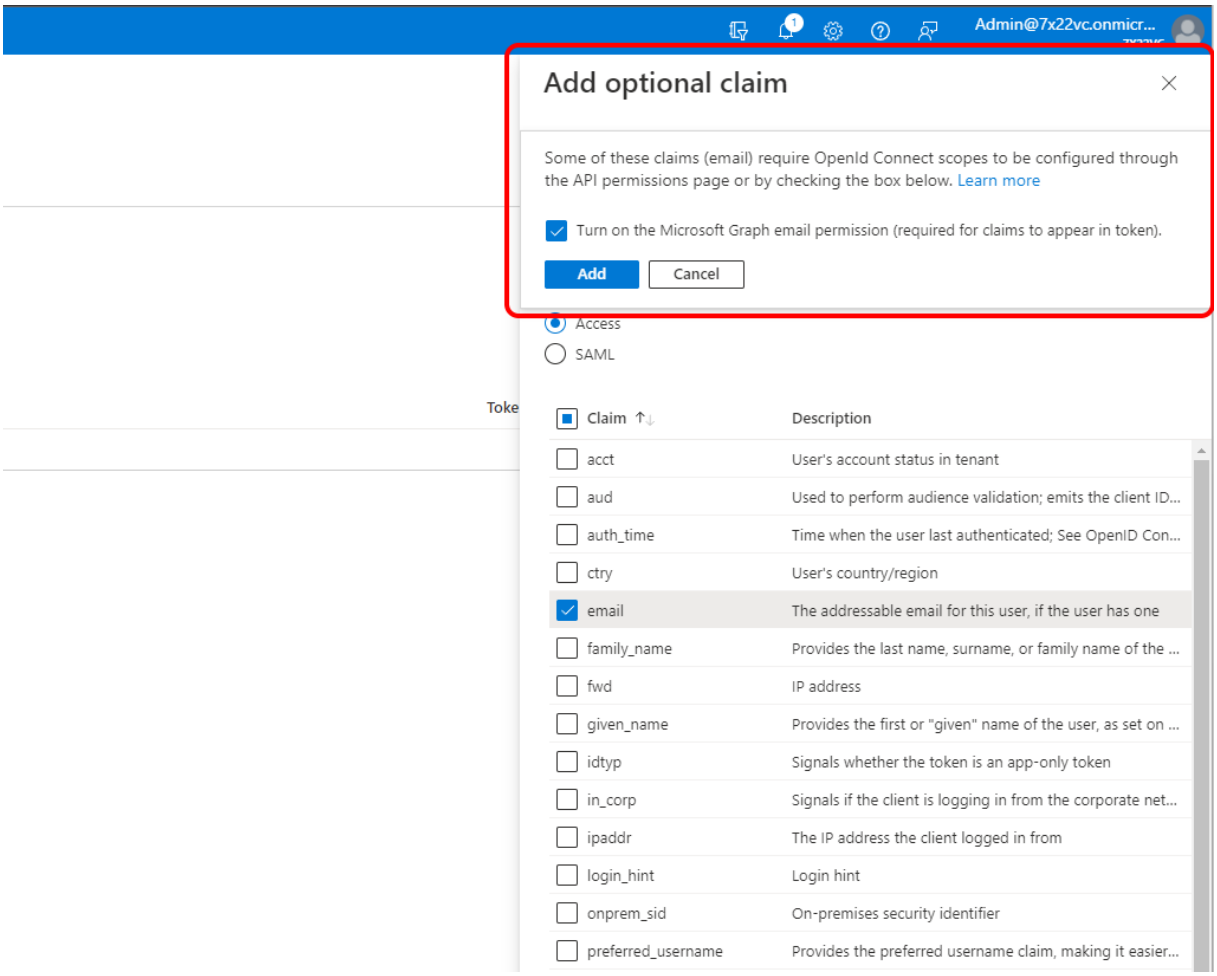
2.9 Toevoegen email claim bij 'Token configuration'

Klik nu op het tabblad 'Token configuration' (1) en daarna op '+ Add optional claim' (2), Access (3), vink email aan (4) en klik daarna op Add (5).



FIGUUR 13. TOKEN CONFIGURATION: EMAIL CLAIM TOEVOEGEN

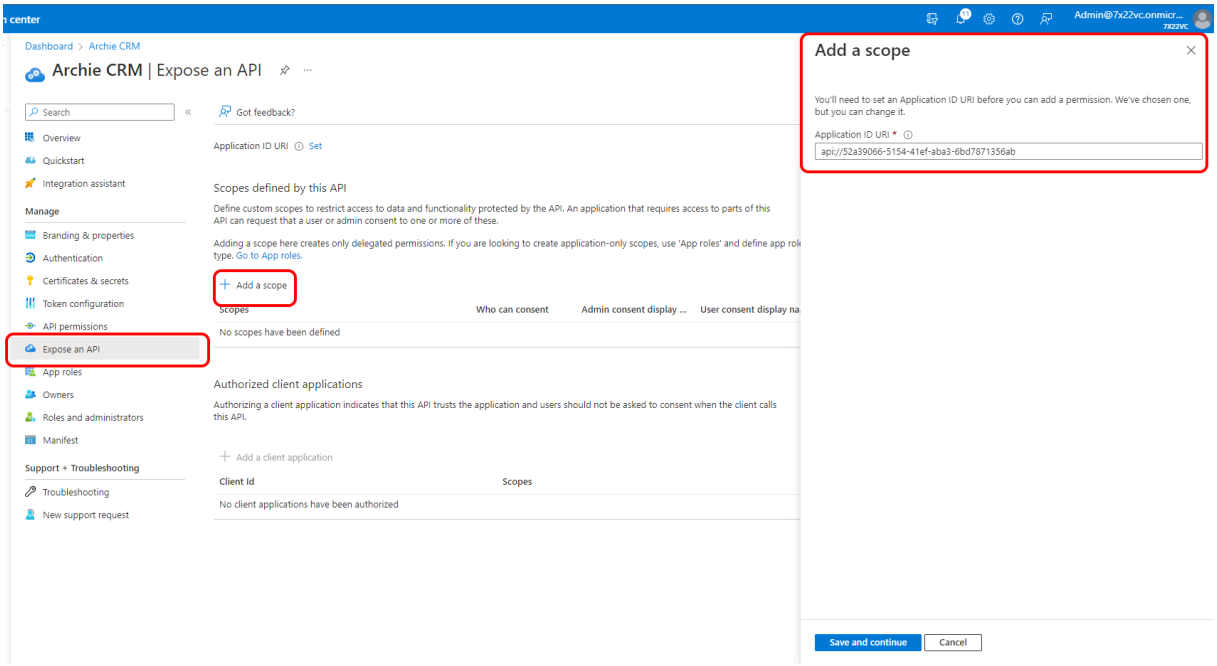
Er verschijnt nu in het dialoog 'Add optional claim' een soort (onduidelijk) sub dialoog. In dat dialoog wordt gevraagd om een extra API permission. Vink dit aan en druk op 'Add'.



FIGUUR 14. TOEKENNEN EXTRA CLAIM BIJ TOEVOEGEN EMAIL CLAIM

2.10 Scope toevoegen

Klik nu links op ‘Expose an API’. Klik dan op ‘Add a scope’. Er zal een popup verschijnen met de goede Application ID URI alvast ingevuld (met client id erin). Klik nu op ‘Save and continue’ (onderin het scherm).

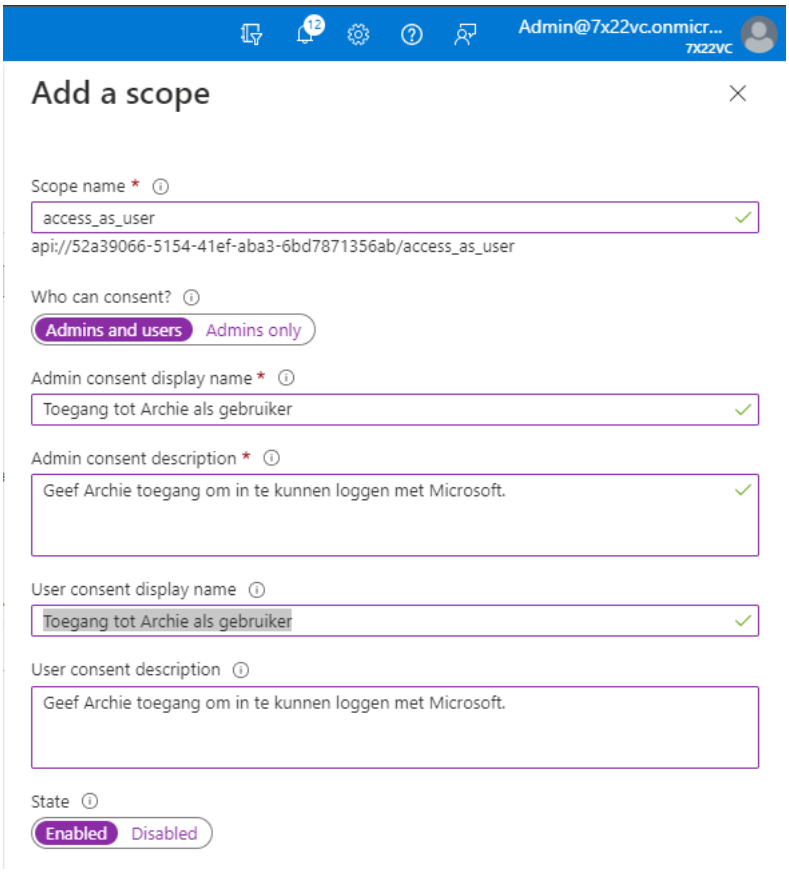


FIGUUR 15. TOEVOEGEN VAN EEN SCOPE

Vul in het volgende scherm de volgende waarden in:

1. Scope name: access_as_user
2. Who can consent? ‘Admins and users’
3. Admin consent display name: zelf instelbaar, bijv. Toegang tot Archie als gebruiker
4. Admin consent description: zelf instelbaar, bijv. Geef Archie toegang om in te kunnen loggen met Microsoft.
5. User consent display name: zelf instelbaar, bijv. Toegang tot Archie als gebruiker
6. User consent description: zelf instelbaar, bijv. Geef Archie toegang om in te kunnen loggen met Microsoft.

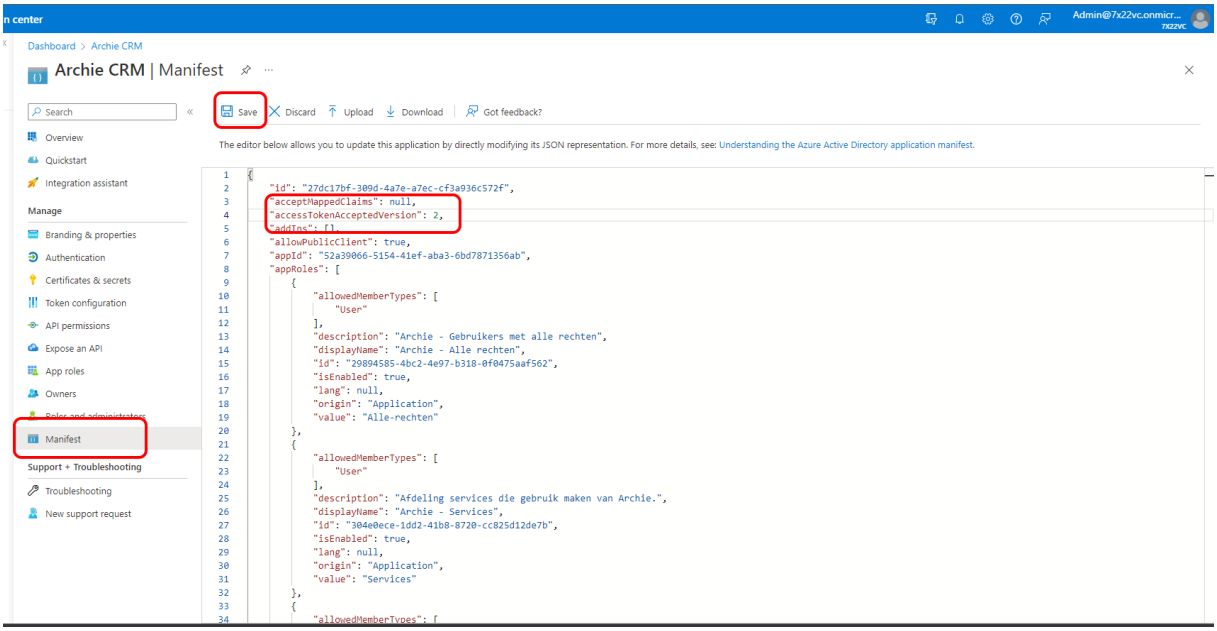
Klik daarna op ‘Add scope’.



FIGUUR 16. GEGEVENS SCOPE INVULLEN

2.11 accessTokenAcceptedVersion aanpassen naar '2'

Ga nu naar het tabblad Manifest en verander bovenin het manifest de waarde van accessTokenAcceptedVersion van null naar de waarde 2 en klik daarna op 'Save'.

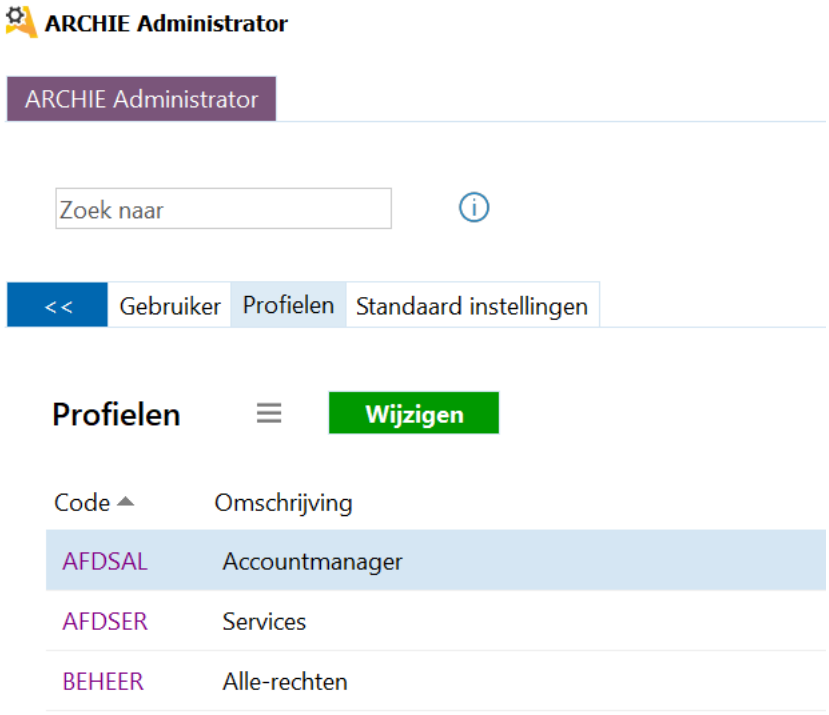


FIGUUR 17. AANPASSEN ACCESSTOKENACCEPTEDVERSION IN HET MANIFEST BESTAND

3 Toekennen rollen (profielen binnen Archie)

3.1 Inleiding

Als de applicatie is geregistreerd, moeten twee standaard rollen en rollen voor de profielen die in Archie systeembeheer gemaakt zijn nog worden toegevoegd in de applicatie om het autorisatieniveau van de gebruikers te kunnen toekennen. In ons geval hebben we drie profielen gedefinieerd in Archie systeembeheer: Accountmanager, Services en Alle-rechten. Let erop dat de omschrijving van het profiel **GEEN** spaties kan bevatten, zie volgende afbeelding:



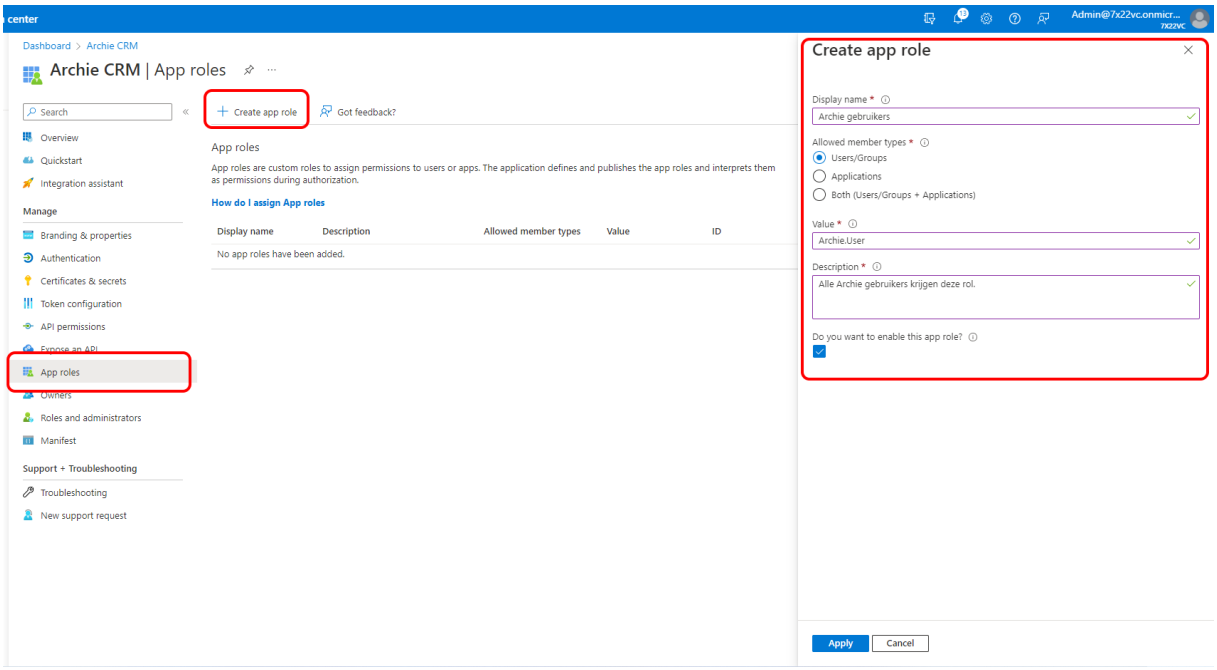
FIGUUR 18. PROFIELEN IN ARCHIE SYSTEEMBEHEER

In ons geval moeten er dus vijf rollen worden geregistreerd in de AAD:

1. Een rol voor iedere Archie gebruiker (standaard Archie.User, deze naam is instelbaar)
2. Een rol voor iedere Archie beheerder (standaard Archie.Admin, maar deze naam is instelbaar)
3. Een rol voor 'Accountmanager'
4. Een rol voor 'Services'
5. Een rol voor 'Alle-rechten'

3.2 App roles toevoegen

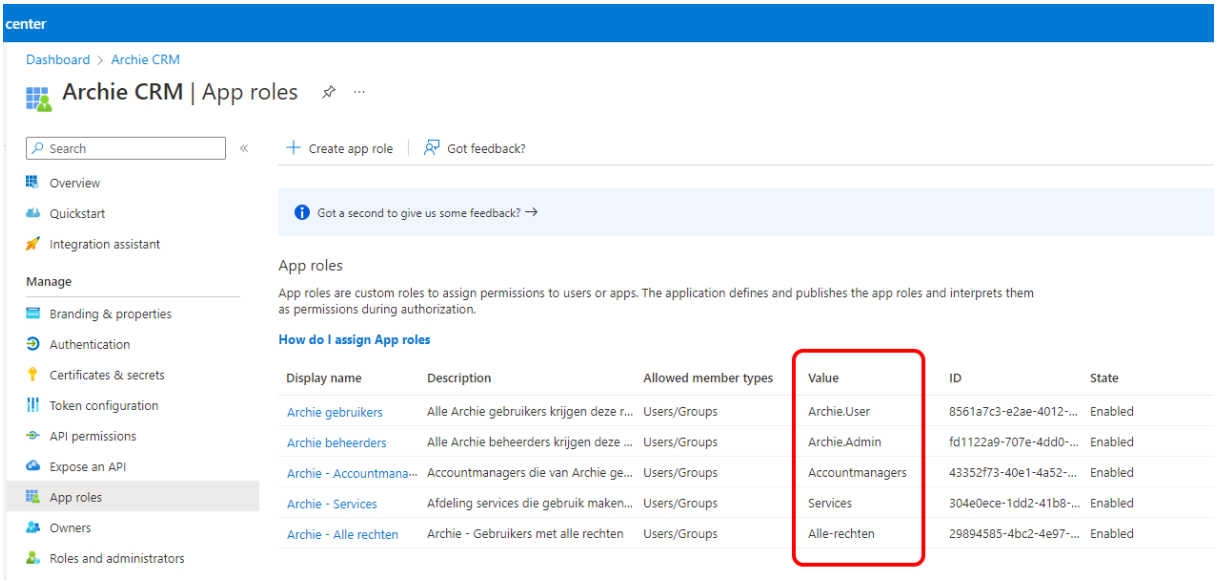
Klik bij de app registration van Archie CRM in AADAC nu op het tabblad ‘App roles’, daarna op ‘+ Create app role’ en vul daarna de gegevens in voor rol 1 (Archie.User). De member type is altijd ‘Users/Groups’. Let erop dat bij de value ‘Archie.User’ wordt ingevuld, tenzij er is gekozen voor een andere (niet standaard naam). Klik daarna op ‘Apply’.



FIGUUR 19. APP ROLE TOEVOEGEN

Doe nu hetzelfde voor de rollen 2 t/m 5. Let erop dat bij rol 3 t/m 5 bij de ‘Value’ waarde de **OMSCHRIJVING VAN HET ARCHIE PROFIEL** wordt ingevoerd en **NIET DE CODE VAN HET PROFIEL**. Dus niet AFDSAL, maar Accountmanager bij rol 3.

Als alle stappen gevolgd zijn, dan ziet het scherm er ongeveer uit zoals op de volgende afbeelding. Let erop (nogmaals), dat bij de Value kolom de **OMSCHRIJVING** van het Archie profiel en **niet de CODE** van het Archie profiel is ingevuld.



FIGUUR 20. ALLE ROLLEN/PROFIELEN ZIJN TOEGEVOEGD

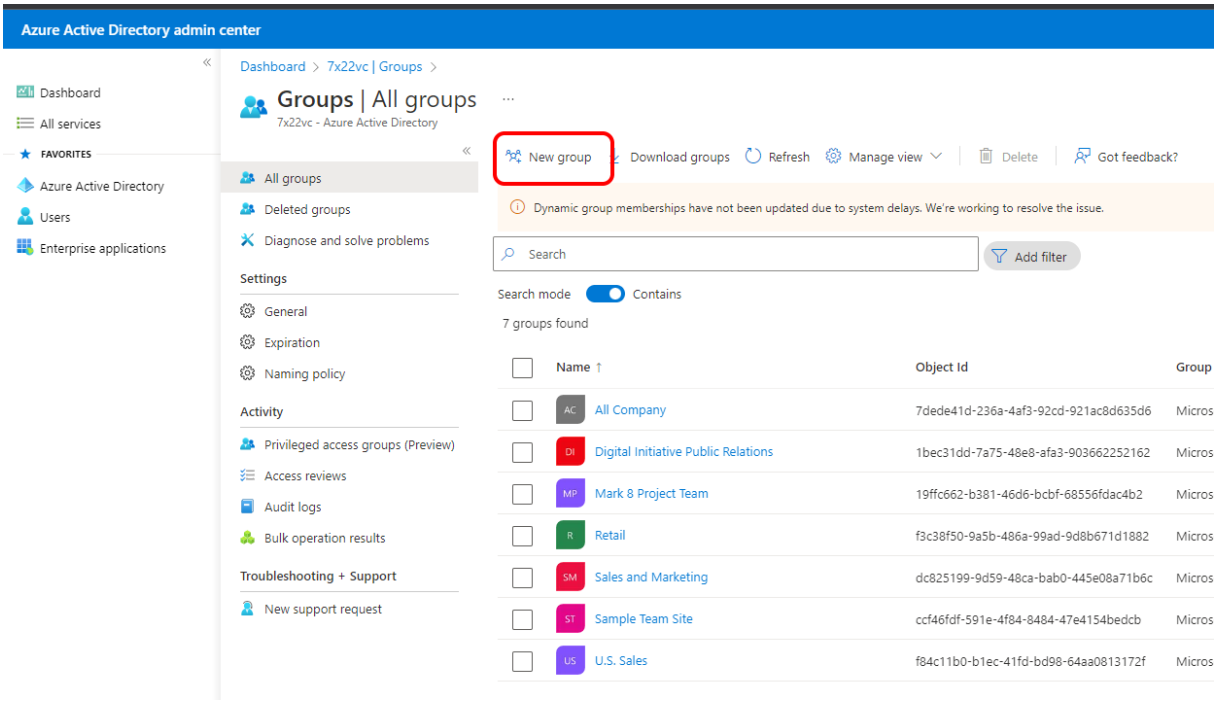
4 Koppelen van Archie rollen aan AAD gebruikers

4.1 Inleiding

Alle Archie gebruikers moeten in de AAD worden gekoppeld aan de Archie app registration (standaard de Archie.User rol) en iedere gebruiker moet ook een profiel gekoppeld krijgen. Deze profielen zijn in het vorige hoofdstuk toegevoegd aan de app registration. Dit kan op verschillende manieren en valt deels buiten de scope van dit document. In dit document wordt een voorbeeld getoond hoe de rechten toe te kennen zijn op basis van groepsautorisatie, maar dit kan ook per gebruiker worden toegepast. Per groep houdt in dat er een groep wordt aangemaakt (bijv. Archie gebruikers), in deze groep worden een aantal AAD gebruikers toegevoegd die toegang moeten krijgen tot Archie en daarna wordt deze groep gekoppeld aan de 'Enterprise application', zodat de gebruikers zich daadwerkelijk kunnen aanmelden.

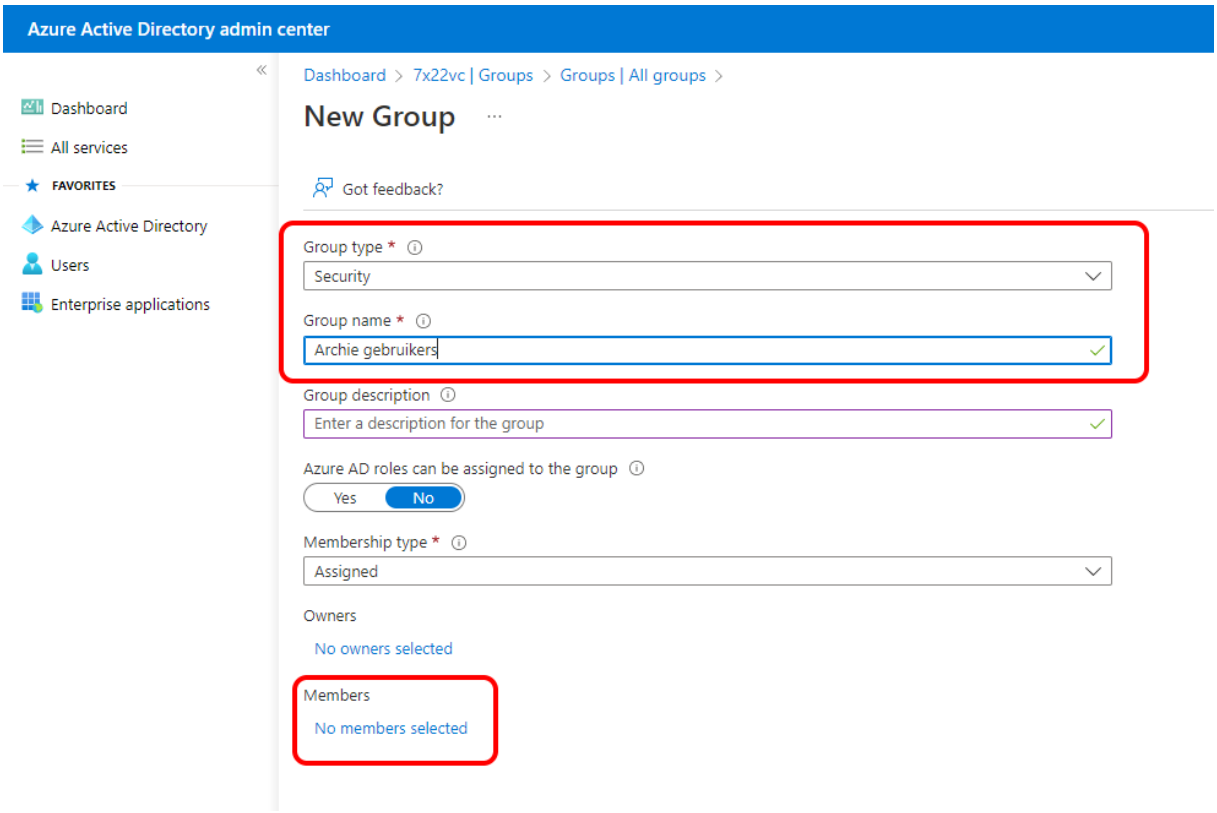
4.2 Groep voor Archie gebruikers aanmaken

Klik (in AADAC) op 'Azure Active Directory' en daarna op 'Groups'. In het scherm dat verschijnt kan een nieuwe groep worden aangemaakt met de 'New group' actie:



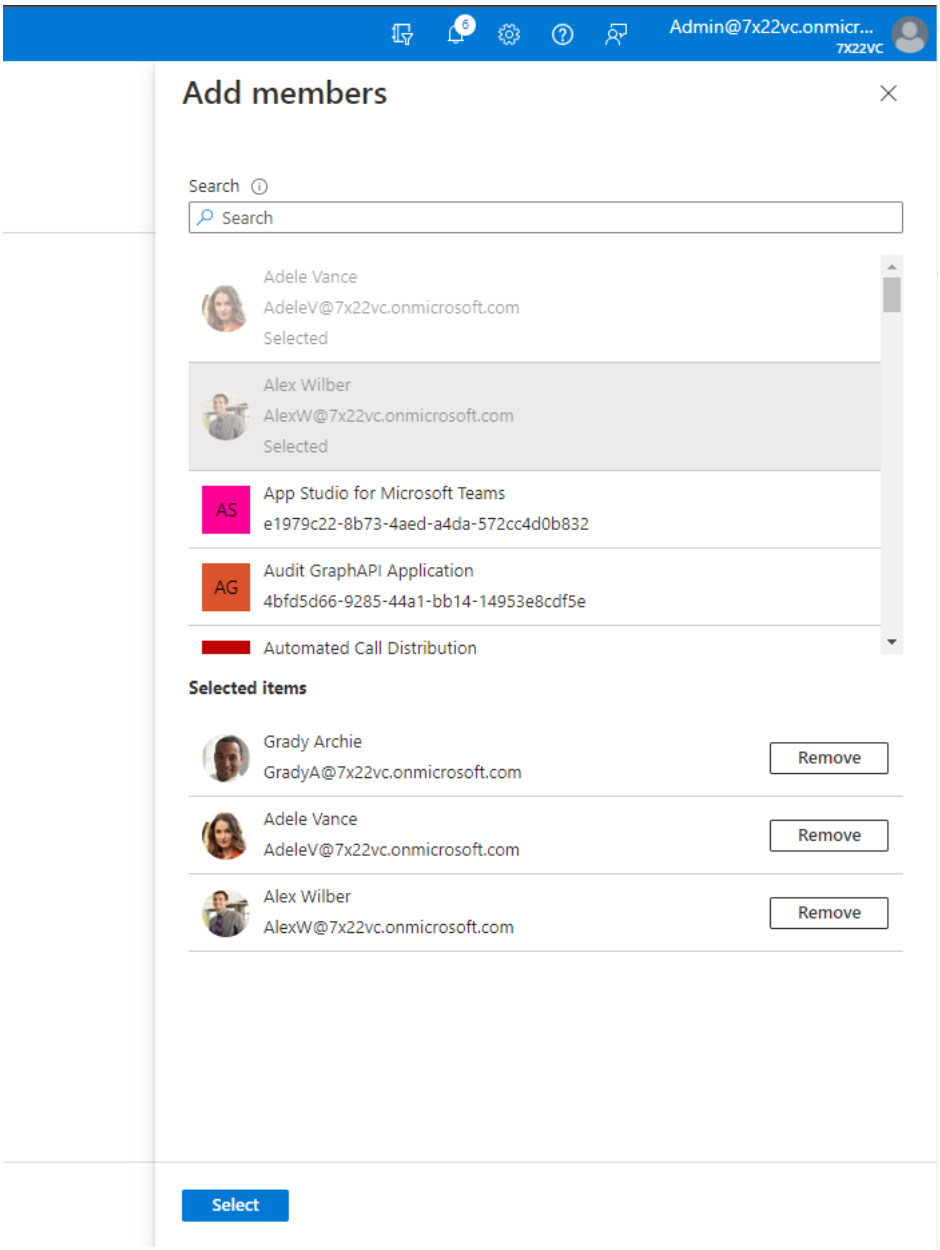
FIGUUR 21. TOEVOEGEN NIEUWE GROEP

Bij het toevoegen van de nieuwe groep, stel de waarde bij group type in op 'Security' en geef de groep een naam, bijv. 'Archie gebruikers'. Geef eventueel een omschrijving op en klik daarna bij members op 'No members selected'.



FIGUUR 22. GEGEVENS NIEUWE GROEP INVULLEN

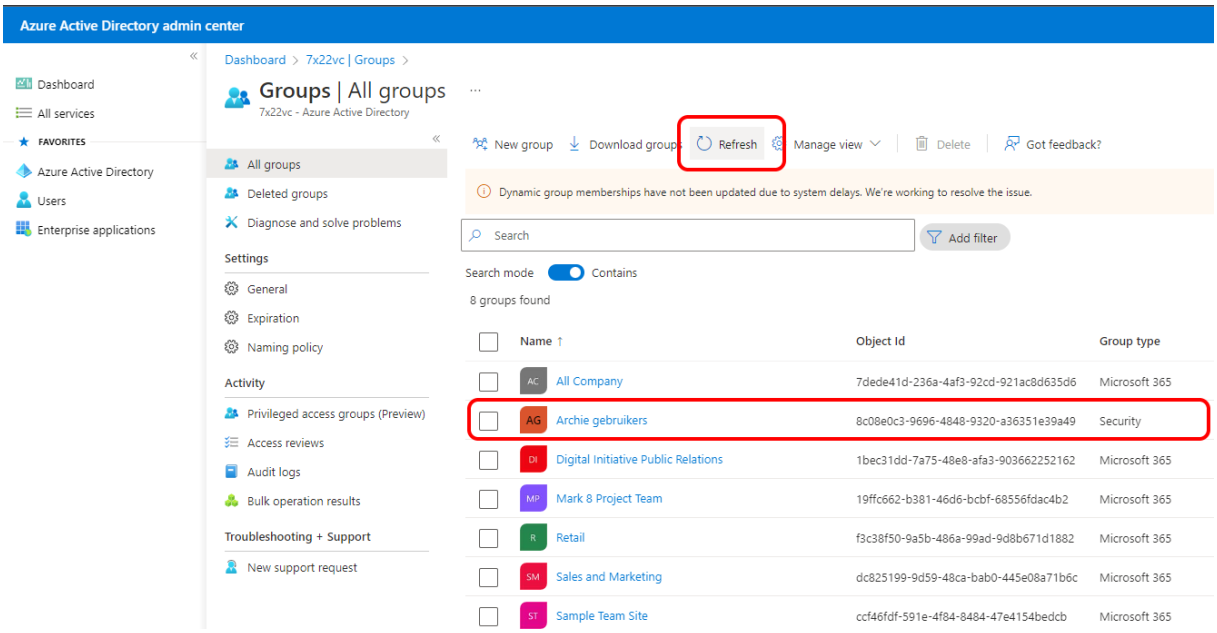
Selecteer in het geopende dialoog alle gebruikers die Archie kunnen gebruiken en klik daarna op ‘Select’. Deze lijst kan later worden aangepast.



FIGUUR 23. GEBRUIKERS VOOR DE GROEP SELECTEREN

Als de gebruikers zijn geselecteerd, klik dan op ‘Create’ onderin het scherm.

LET OP! De groep lijkt nu niet te zijn aangemaakt in de lijst. Wacht ongeveer een minuut en klik dan op 'Refresh' boven in het scherm en de groep zal uiteindelijk wel verschijnen.



FIGUUR 24. VERTRAGING BIJ HET VERSCHIJNEN VAN DE GROEP

4.3 Stap 2: Groep voor Archie beheerders aanmaken

Volg nogmaals dezelfde stappen voor alle Archie systeembeheerders. Noem die groep Archie systeembeheerders en maak alle gebruikers die Archie systeembeheerder zijn lid van deze groep.

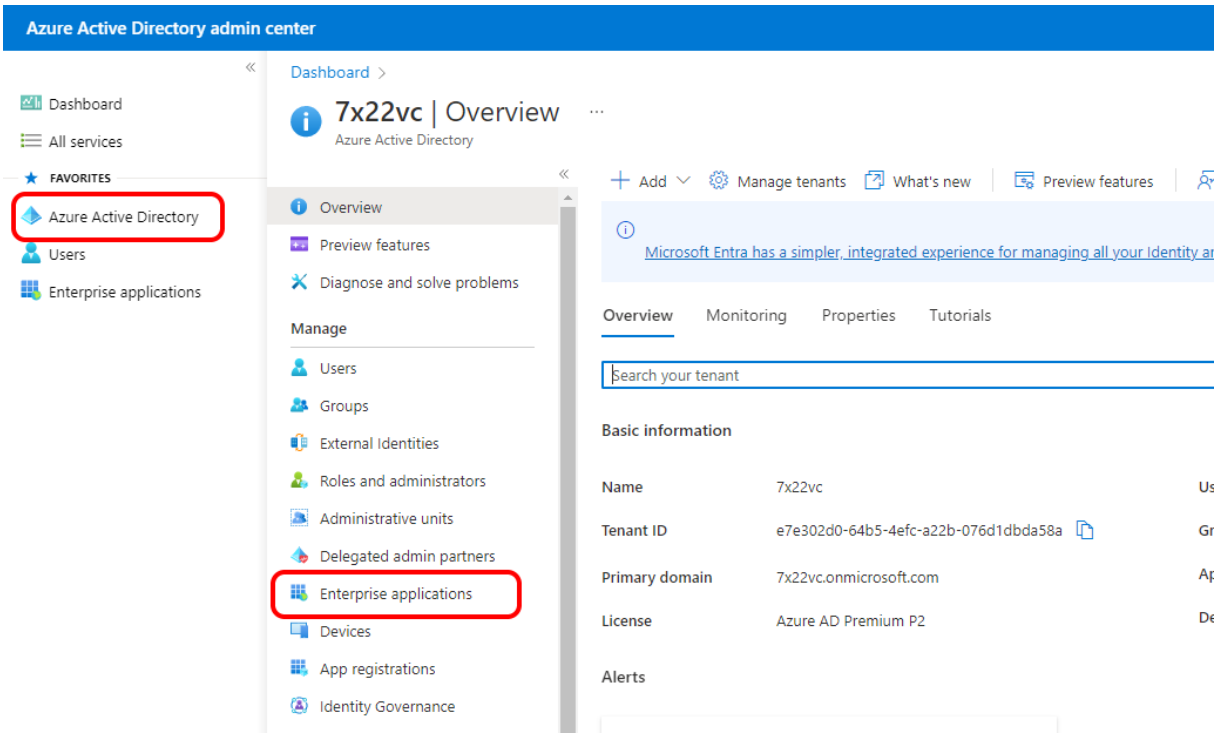
4.4 Stap 3: Groepen voor profielen

Volg nogmaals dezelfde stappen voor alle profielen die in Archie zijn. Noem die groep bijv. Archie profiel – [naam profiel] en maak alle gebruikers die van dat profiel moeten krijgen lid van deze groep.

5 Rollen toekennen ‘Enterprise application’.

5.1 Inleiding

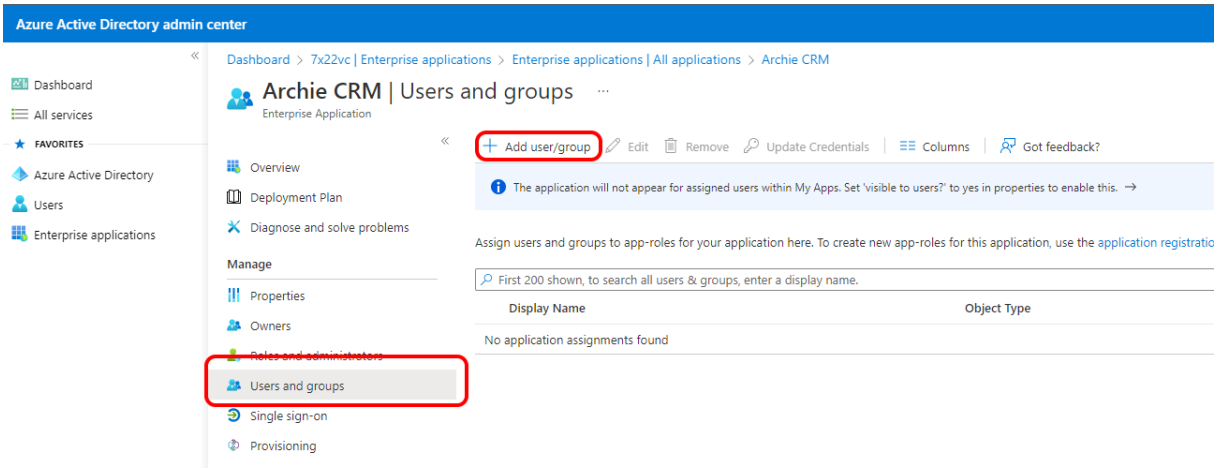
De aangemaakte groepen (Archie gebruikers, Archie beheerders en de profielen) moeten nu nog gekoppeld worden aan de ‘app registration’. Dit kan in de ‘Enterprise application’. Klik (in AADAC) op ‘Azure Active Directory’ en daarna op ‘Enterprise applications’.



FIGUUR 25. OPENEN 'ENTERPRISE APPLICATIONS'

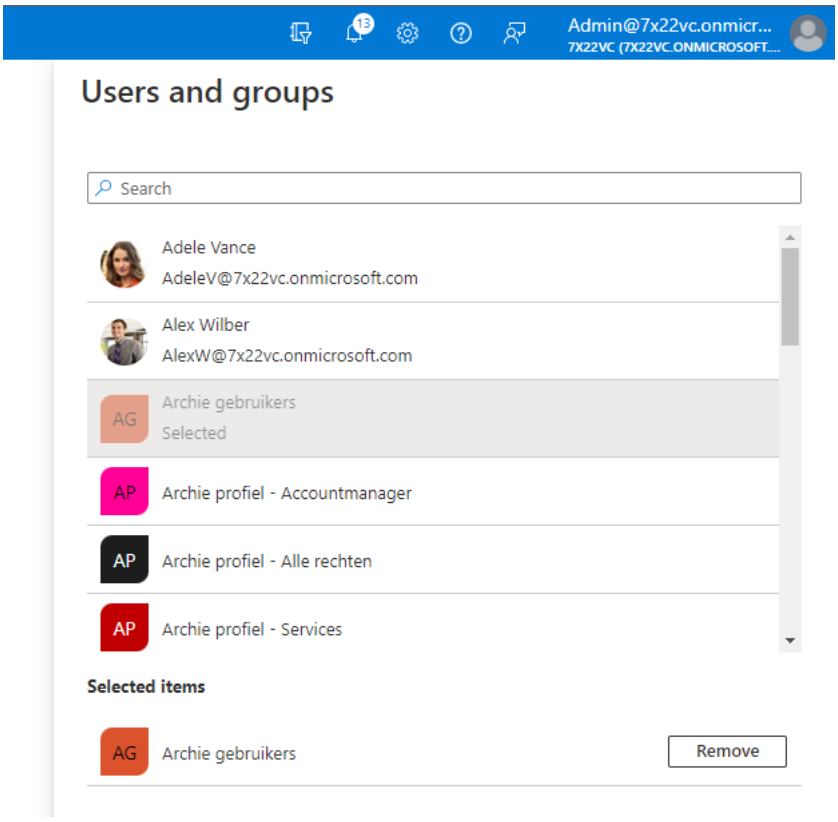
5.2 Groep en rol toekennen aan Archie gebruikers

Het scherm met enterprise applications verschijnt. Klik hier de aangemaakte app aan (Archie CRM). Het scherm van de Archie CRM enterprise application opent. Klik nu op 'Users and Groups'. Een leeg grid zal verschijnen. Klik nu op '+ Add user/group'.



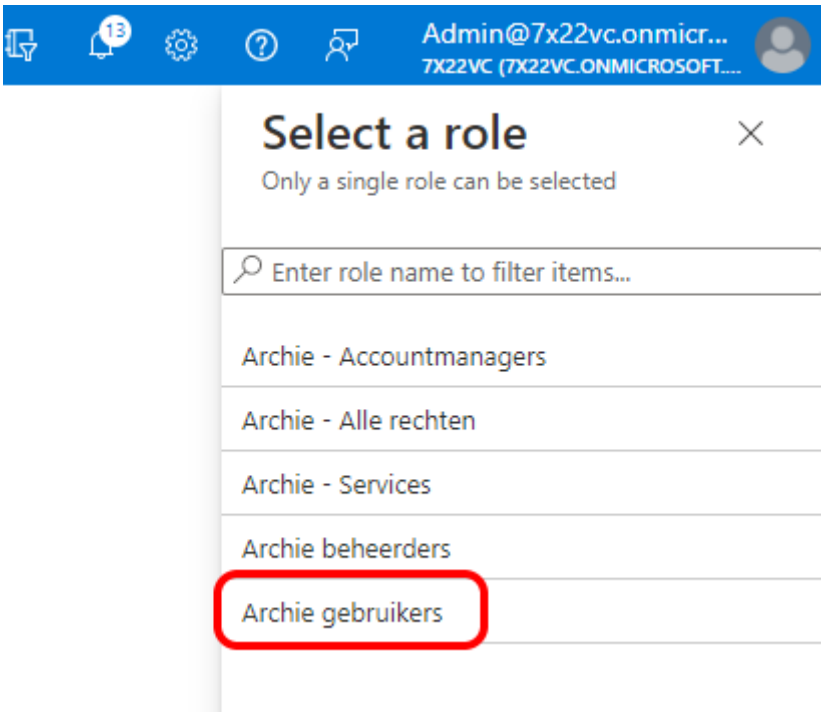
FIGUUR 26. TOEVOEGEN GEBRUIKER/GROEP

Er verschijnt nu een scherm waarin één van de gemaakte groepen kan worden gekoppeld aan één van de gemaakte rollen. Klik hiervoor eerst op 'None selected' bij 'Users and groups'. Selecteer daar dan 'Archie gebruikers' en klik op 'Select'.



FIGUUR 27. 'ARCHIE GEBRUIKERS' GROEP SELECTEREN

De groep is geselecteerd. Klik nu op ‘None selected’ onder ‘Select a role’. Kies in dit scherm voor de ‘Archie gebruikers’ rol. En daarna op select.



FIGUUR 28. SELECTEER DE ‘ARCHIE GEBRUIKERS’ ROL

De groep en rol zijn nu geselecteerd. Klik nu op ‘Assign’ en de rol is toegekend aan de groep.

5.3 Stap 2: groep en rol toekennen aan Archie beheerders

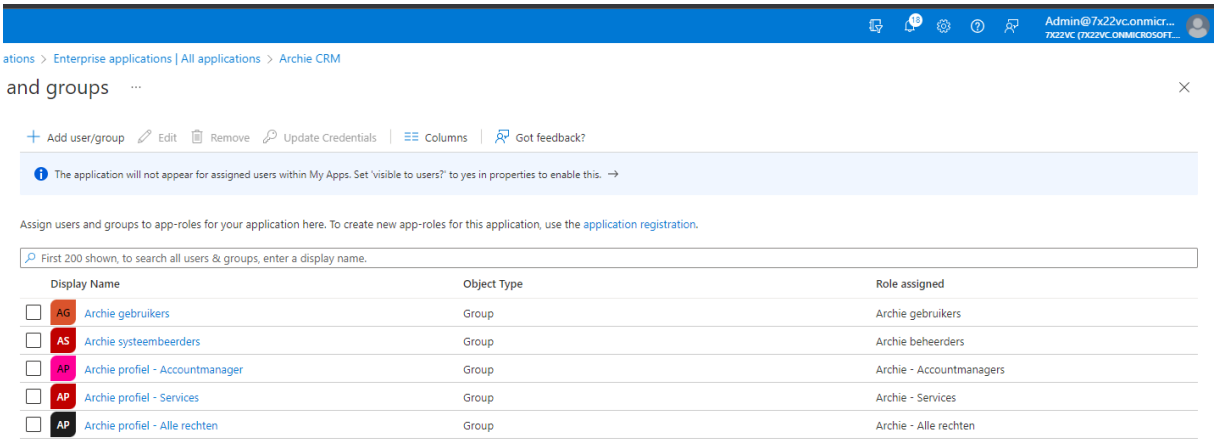
Volg nogmaals dezelfde stappen voor alle Archie systeembeheerders. Selecteer dan de Archie systeembeheerders groep en selecteer de Archie beheerders rol.

5.4 Stap 3: groep en rol toekennen aan profielen

Volg nogmaals dezelfde stappen voor alle profielen die in Archie zijn. Noem die groep bijv. Archie profiel – [naam profiel] en maak alle gebruikers die van dat profiel moeten krijgen lid van deze groep.

5.5 Wijzigingen Archie gebruikers/rollen binnen Archie

Als alle stappen zijn gevolgd ziet het scherm er ongeveer zo uit:

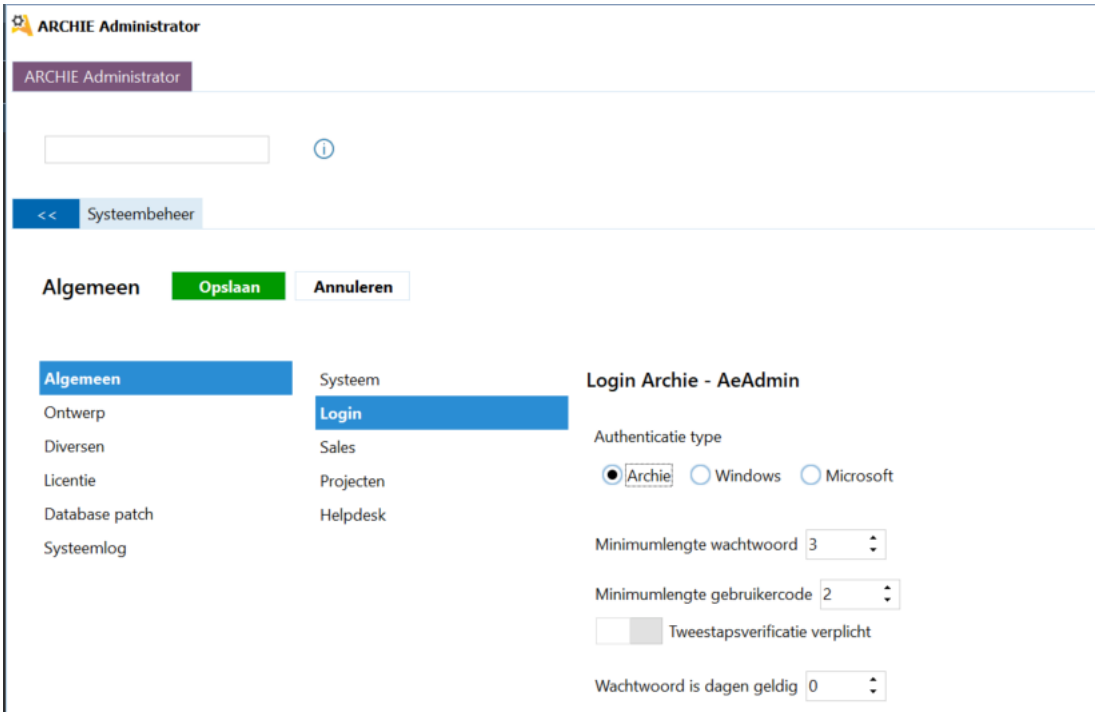


FIGUUR 29. ROLLEN ZIJN AAN ALLE GROEPEN TOEGEKEND

Op deze manier kan toegang tot Archie of Archie systeembeheer worden geregeld door simpelweg gebruikers toe te voegen of verwijderen uit de Archie gebruikers of Archie systeembeheerders groep. Hiervoor hoeft niets te worden aangepast in de app registratie. Dit kan een AAD gebruikersbeheerder doen. Hetzelfde geldt voor gebruikers die binnen Archie een andere rol (profiel) krijgen. Bij het gebruikersbeheer wordt de betreffende gebruiker lid gemaakt van een andere groep (bijv. Alle rechten i.p.v. Accountmanager) en in Archie zal dan automatisch dat profiel worden toegekend.

6 Instellen Archie systeembeheer

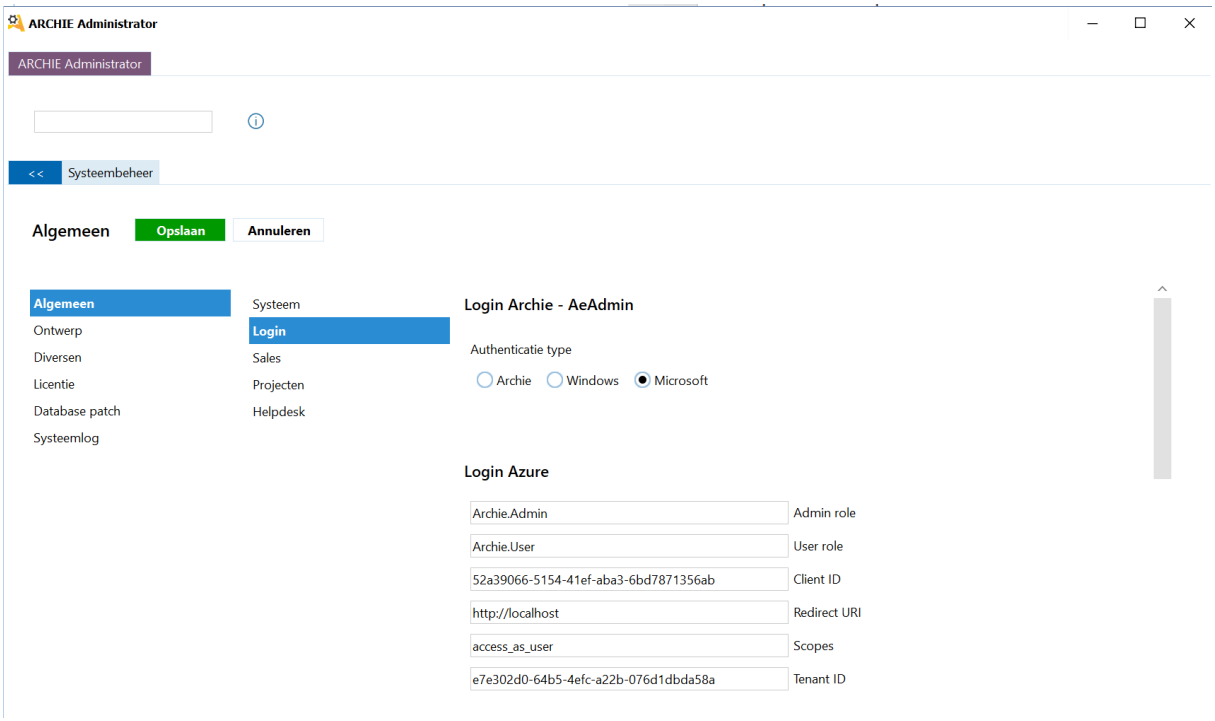
Om ‘Aanmelden met Microsoft’ in te schakelen, dient deze te worden geconfigureerd in Archie systeembeheer. Hiervoor hebben we een aantal gegevens nodig die eerder in het document zijn gemaakt of ingevuld. Start Archie systeembeheer en ga naar ‘Systeembeheer’. Klik daarna onder het tabblad ‘Algemeen’ op ‘Login’:



FIGUUR 30. ARCHIE SYSTEEMBEHEER: LOGIN OPENEN

Klik nu op wijzigen en daarna op ‘Microsoft’ en vul de volgende gegevens in:

1. Admin role: Archie.Admin (tenzij anders bepaald in vorige hoofdstuk)
2. User role: Archie.User (tenzij anders bepaald in vorige hoofdstuk)
3. Client ID: client id opgeschreven aan het begin van de handleiding. Te vinden in ‘Overview’ van de app registration in AADAC.
4. Redirect URI: http://localhost (vaste waarde, niet veranderen, tenzij bij paragraaf 2.7 op pagina 11 een andere poort is ingesteld. In dat geval moet deze alternatieve poort hier worden ingevoerd)
5. Scopes: access_as_user (vaste waarde, niet veranderen)
6. Tenant ID: tenant id opgeschreven aan het begin van de handleiding. Te vinden in ‘Overview’ van de app registration in AADAC.



FIGUUR 31. INSTELLEN ARCHIE LOGIN (MICROSOFT)

7 User provisioning

Archie is nu ingesteld. Het kan tot een minuut duren voordat de Archie API de instellingen heeft doorgevoerd. Als dit is gebeurd, dan kan de gebruiker Archie opstarten. En zal er een knop verschijnen ‘Aanmelden met Microsoft’. Zodra een gebruiker zich aanmeldt, dan zal worden gekeken of de gebruiker zich al eerder met Microsoft heeft aangemeld. Als dit niet zo is, dan wordt gekeken of er een Archie gebruiker is met hetzelfde e-mail adres als de Microsoft gebruiker en als ook dat niet zo is, dan wordt een nieuwe gebruiker aangemaakt.

Nadat de Archie gebruiker is gekozen of aangemaakt, zal user provisioning worden toegepast. Deze zorgt er bijv. voor dat de gebruiker een naam krijgt. Ook zorgt user provisioning ervoor dat het juiste profiel aan de gebruiker wordt gekoppeld. Als een gebruiker een andere rol krijgt, dan wordt het Archie profiel ook automatisch aangepast. Als er in Archie geen enkel profiel overeenkomt met een rol in AAD, dan krijgt de gebruiker automatisch een protectgroep ‘prt’ (kleine letters). Dit betekent dat de gebruiker **NIKS** mag zien. Zodra een profiel gevonden kan worden dat overeenkomt met een rol, zal deze ‘prt’ groep weer worden verwijderd.