Handleiding
Inrichten Azure AD voor RAP

Inhoudsopgave

1. Inleiding

Deze handleiding helpt je om het digitale kennissysteem RAP nòg beter te gebruiken dan jij en je collega's nu al doen door gebruik te maken van Azure AD.

Je bent gewend om in te loggen met je RAP-account. Dit wordt al vergemakkelijkt door de IP-herkenning waar RAP gebruik van maakt. Wanneer het uitgaande IP-adres, het adres waarmee je internet bezoekt, van jouw organisatie bij ons bekend is dan kunnen medewerkers binnen de organisatie zonder in te loggen direct gebruik maken van RAP. Dit noemen wij IP-herkenning. Dat werkt zolang je RAP benadert met het IP-adres van je werk. Als je thuis bent, werk je soms ook met je eigen IP-adres en kom je niet automatisch in RAP.

Met de nieuwste versie van RAP hebben we hier een oplossing voor. Het nieuwe medewerkersdeel van RAP kun je namelijk koppelen aan het zakelijk account van de organisatie. Dit kan via Azure AD (Active Directory) en is een Single Sign-On (SSO, eenmalige aanmelding) oplossing. Inloggen gaat met SSO voor alle medewerkers in bijna alle gevallen automatisch en kan altijd met het zakelijke e-mailadres met bijbehorend inlogproces. Daarmee behoort inloggen met IP-herkenning tot het verleden.

Azure AD in een notendop

Azure Active Directory is door Microsoft ontwikkeld. Het is een identiteits-platform en biedt gebruikers geauthentiseerde toegang tot applicaties. De medewerker klikt op een link naar RAP. Als de gebruiker nog niet is ingelogd, verschijnt er een inlogscherm. Vervolgens start op de achtergrond het authenticatieproces. RAP maakt verbinding met de Azure AD van de klant via het OpenID connect protocol om de rechten van de gebruiker te verifiëren. Als die in orde zijn, komt de medewerker automatisch in RAP.

Handleiding voor ICT

Het inrichten van de Azure AD voor toegang tot RAP behoort in de regel tot de werkzaamheden van de afdeling ICT en is in veel gevallen een routinematige activiteit die niet veel om het lijf heeft. Het is daarom zaak om deze technisch georiënteerde handleiding naar jouw ICT-afdeling door te sturen. Zij kunnen de omzetting inplannen. De huidige versie van RAP blijft ondertussen gewoon actief. De ICT-afdeling kan bij vragen direct met ons contact opnemen.

Als de SSO is ingericht nemen we natuurlijk contact met jou als contactpersoon op om samen te kijken of het automatisch inloggen juist werkt en om aanvullende informatie te verstrekken.

Vragen

Onderstaande handleiding, in de vorm van een stappenplan, helpt met het inrichten van de Azure AD-koppeling. Bij vragen kan contact worden opgenomen met de afdeling RAP via rap@ijk.nl of 0492-50 66 60.

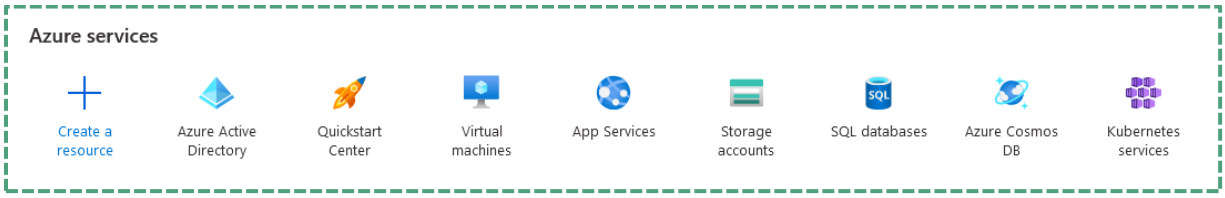
2. Stappenplan

Eenvoudig inloggen

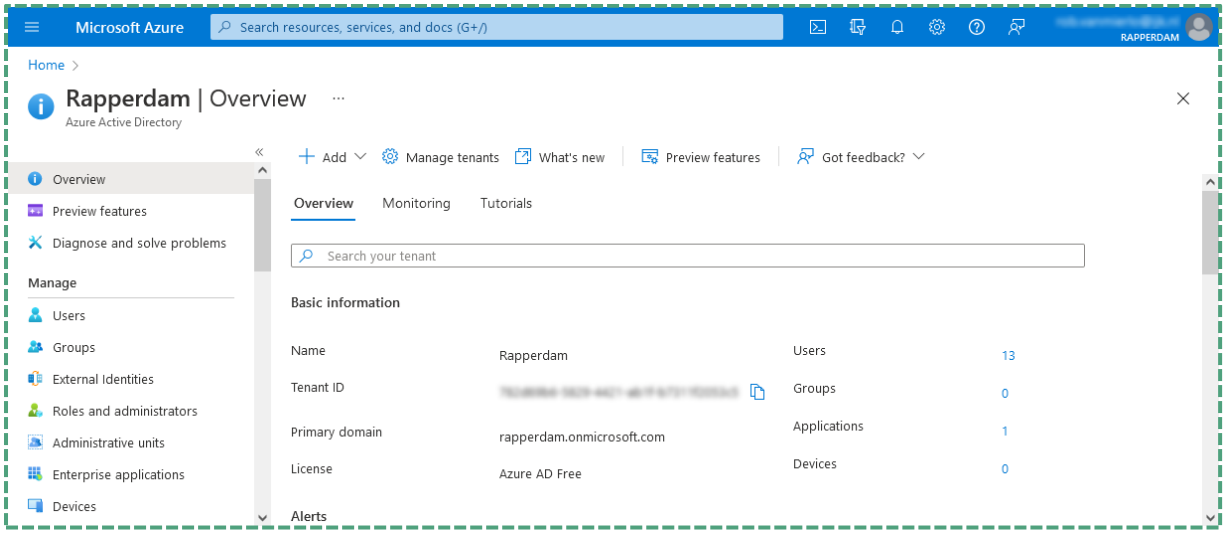
RAP is een informatieve website over arbeidsvoorwaarden en bevat geen persoonlijke of gevoelige informatie. Daarnaast is de SSO-koppeling voldoende beveiligd. Extra beveiliging met two-factor-authentication (2FA) is daarom niet geadviseerd, omdat dit het gebruikersgemak kan beïnvloeden. Houd hiermee rekening bij de inrichting.

Stap 1. Open het Azure Active Directory venster

Het Azure Active directory venster kan eenvoudig geopend worden via onderstaande snelkoppeling. Mocht deze snelkoppeling niet zichtbaar zijn, zoek er dan naar via de zoekbalk.



Het volgende venster komt in beeld.



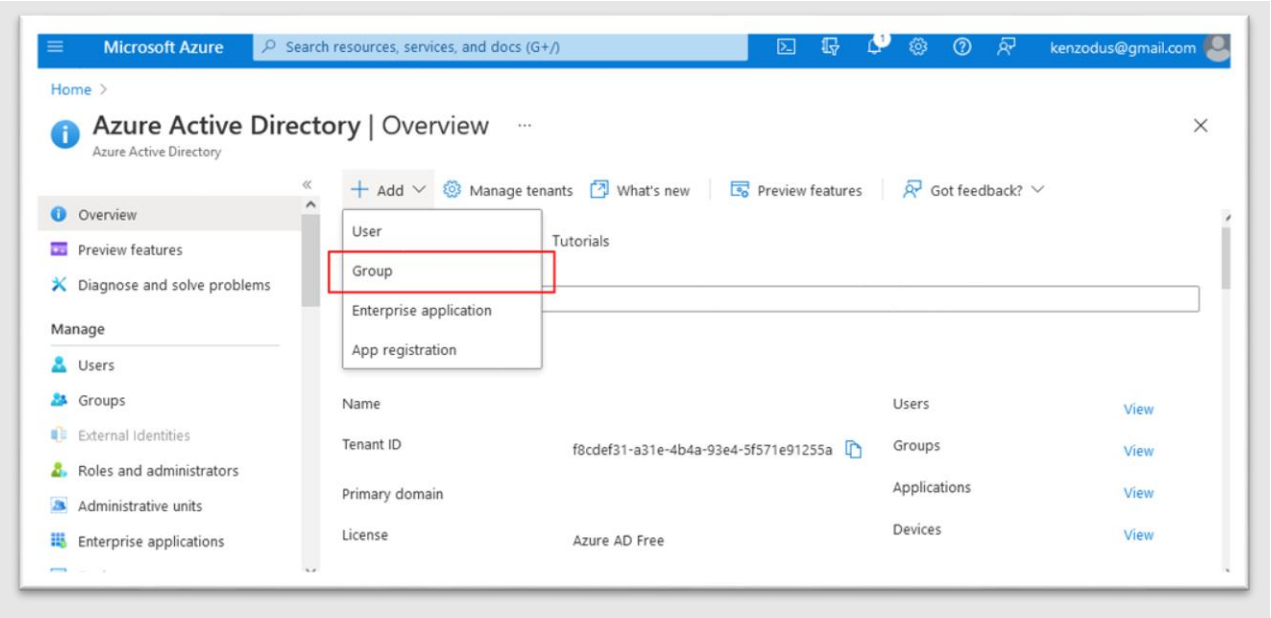
Stap 2. HRM-groep aanmaken

RAP bestaat uit twee delen, één voor medewerkers en een één voor HRM'ers. Het medewerkersdeel is vrij toegankelijk voor alle medewerkers.

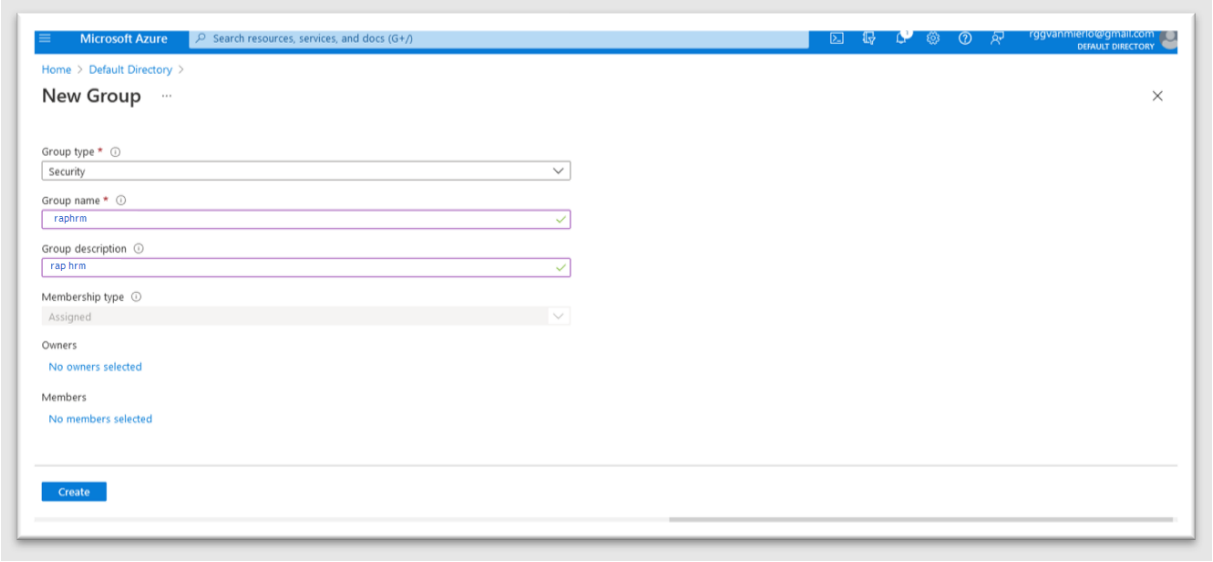
Het HRM-deel dient alleen toegankelijk te zijn voor collega's die taken hebben in het HRM-werkveld. Dit zijn in de regel de collega's van de afdeling HRM (o.a. HRM-adviseurs, medewerkers personeels- en salarisadministratie, beleidsadviseurs). Soms is het zo dat ook enkele collega's van bijvoorbeeld de afdeling financiën toegang moeten krijgen. Mocht je twijfelen over wie tot deze HRM-doelgroep behoort, neem contact op met je collega's van HRM.

Het maken van een HRM-groep doe je als volgt:

Kies voor **Group** in het **Add** dropdown menu.



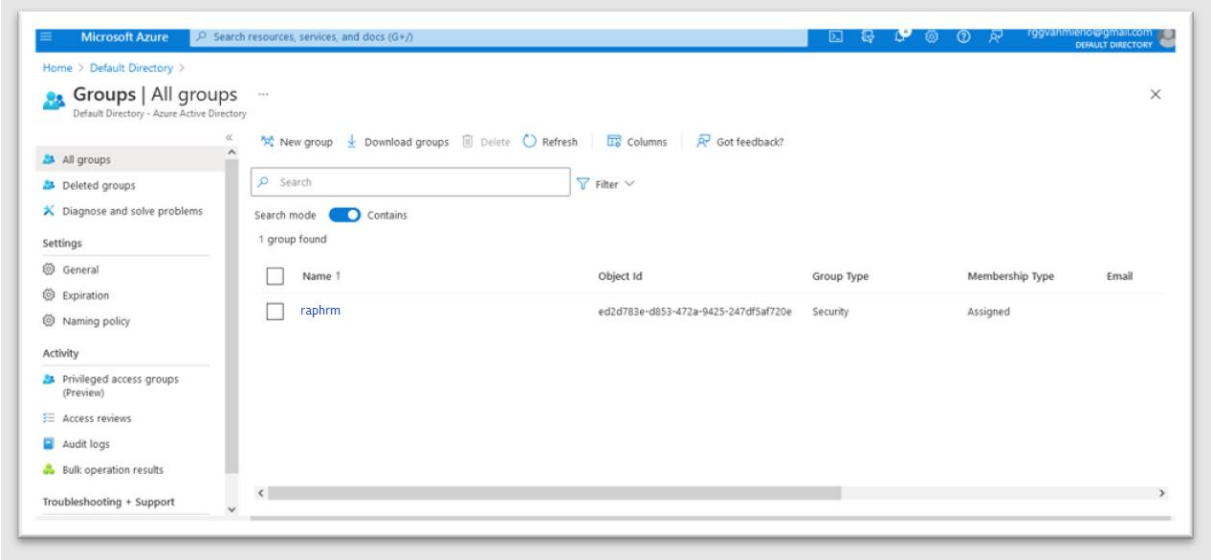
Er verschijnt een volgend venster waarin je een nieuwe groep maakt.



- Kies bij **Group type** voor **Security**
- Noteer **'raphrm'** bij **Group name**
- Noteer **'Rap hrm'** bij **Group description**

Druk op **Create** als alle velden volledig zijn ingevuld.

In het overzichtsvenster zie je dan dat de **raphrm** groep is aangemaakt.

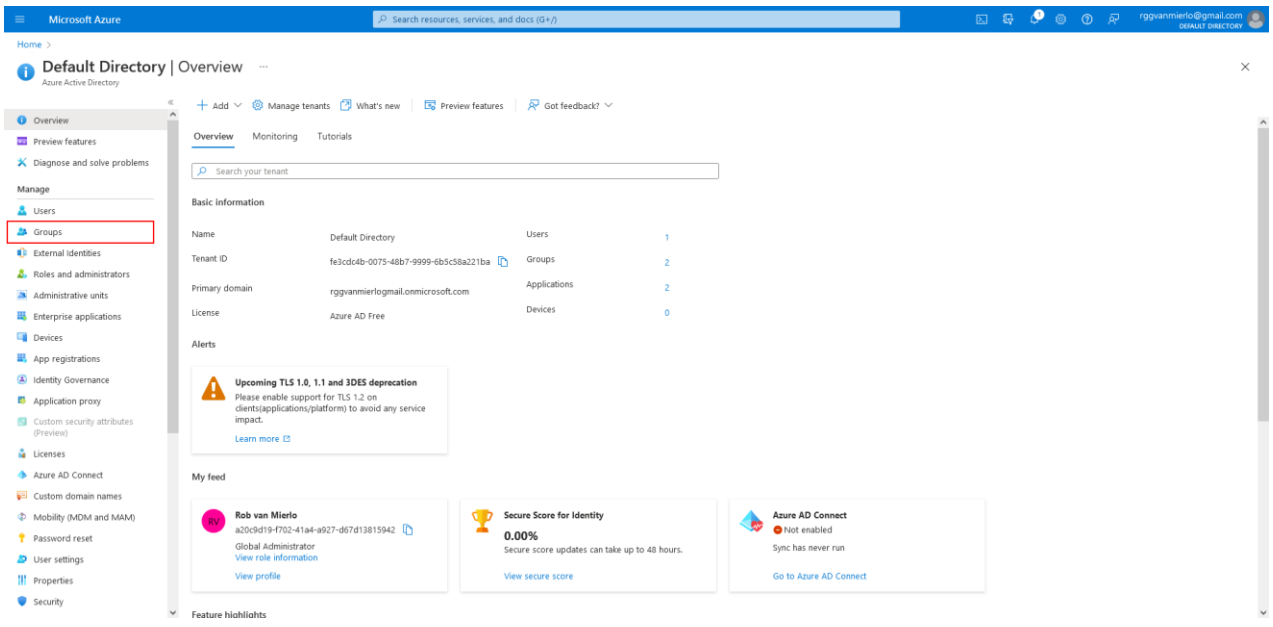


Stap 2a. Deelnemers toekennen aan de groep

Nadat de groep is aangemaakt, moeten de juiste deelnemers aan de groep worden toegewezen. Dit kan door een **groep** of een individuele **gebruiker** toe te voegen. Deze stap legt uit hoe je deelnemers toevoegt aan de **raphrm** groep.

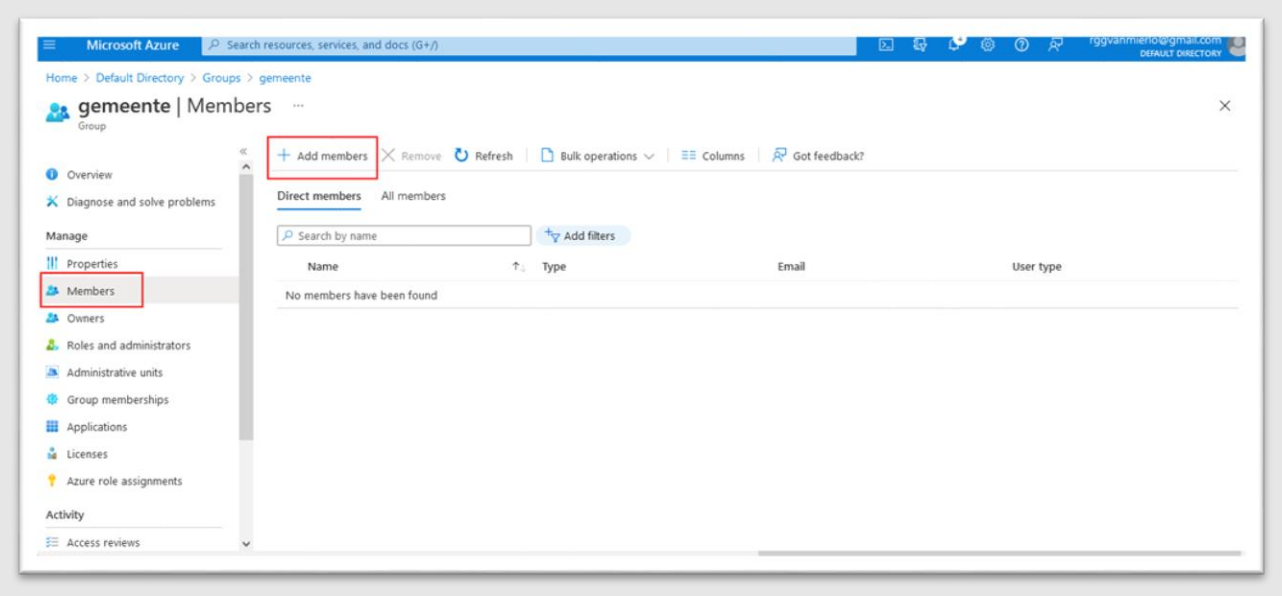
Dynamische rechten
Het is verstandig om leden aan de 'raphrm' groep toe te wijzen doormiddel van lidmaatschap aan een andere groep. Komt er in dat geval namelijk een nieuwe collega, die lid wordt van de groep die recht heeft op het HRM-deel van RAP, dan krijgt deze ook automatisch toegang tot het HRM-deel van RAP.

Ga in het linker menu naar **Manage** en klik op **Groups.**

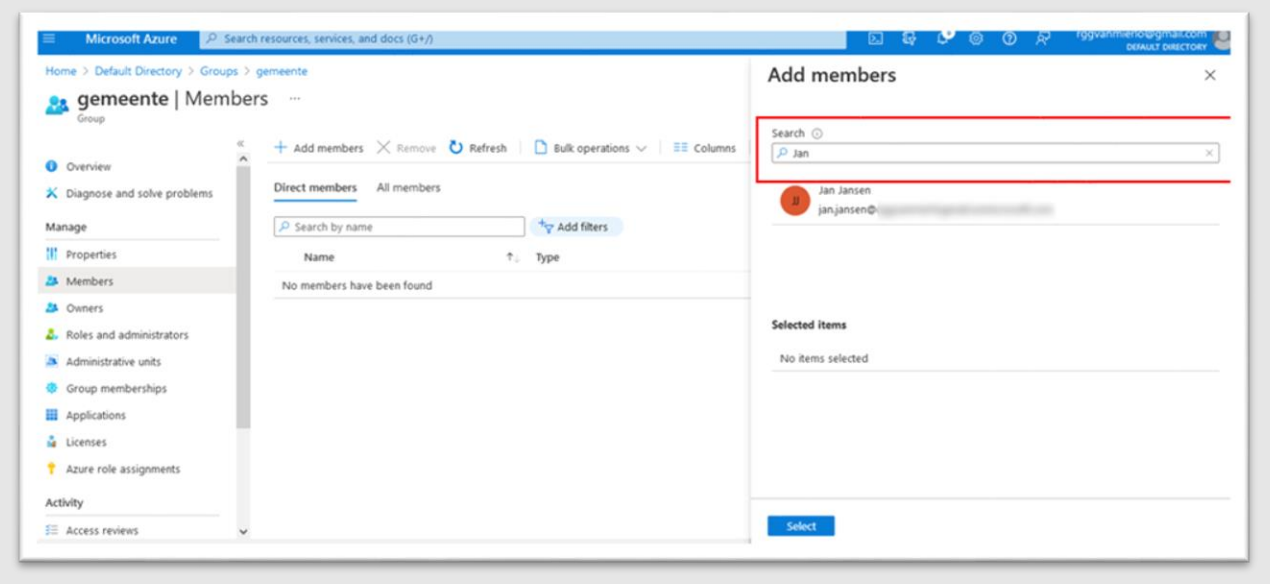


In het **Groups** overzichtsvenster zie je een overzicht van alle groepen die bekend zijn binnen Azure AD. Selecteer nu de groep **'raphrm'** waaraan je deelnemers wilt toekennen.

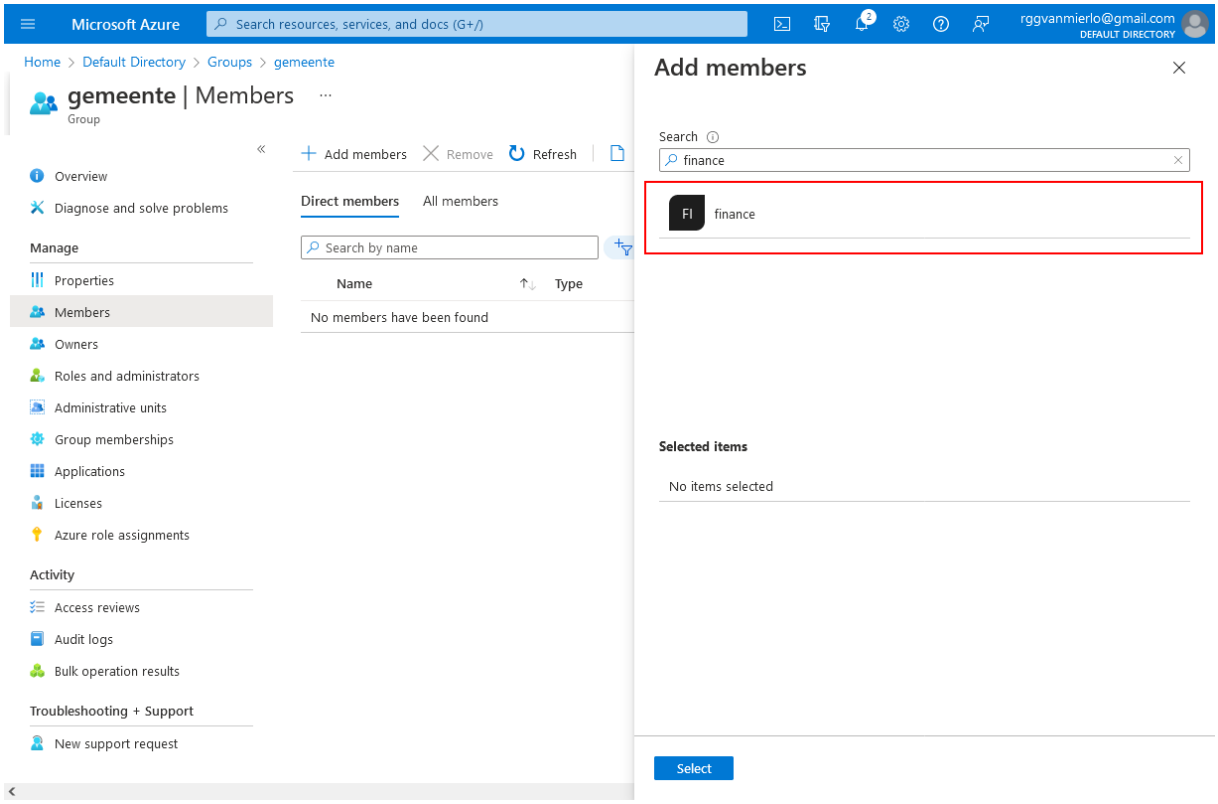
Druk in het linker menu op de knop **Members**. Druk in het **Members** venster dat verschijnt op de **Add members** knop.

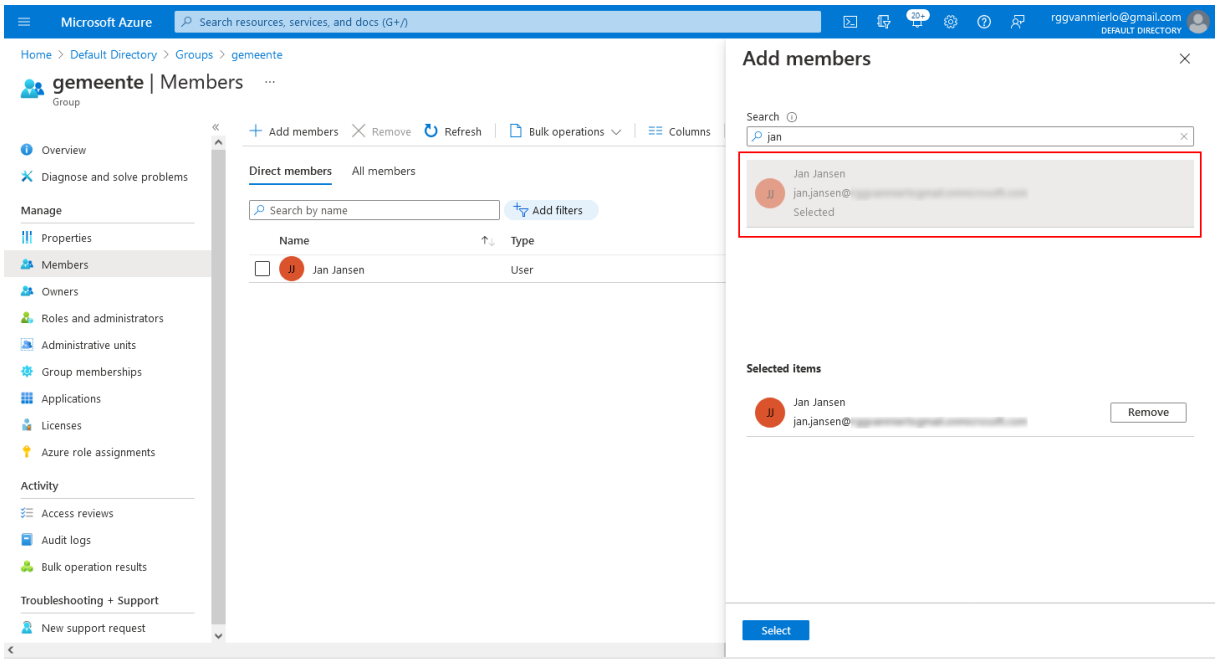


Het volgende **Add members** sub-venster verschijnt. Hier kun je deelnemers of groepen van deelnemers toevoegen.



Gebruik het **Search** veld om naar de beoogde deelnemer of groep te zoeken.





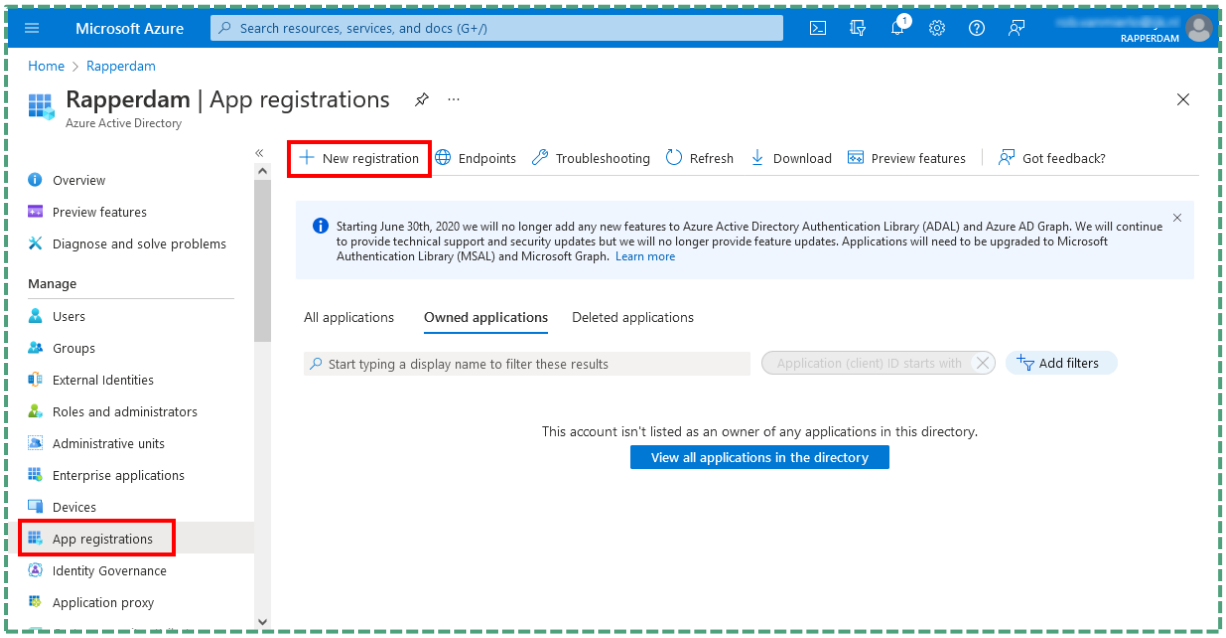
Druk op **Select** zodra de gekozen lijst van deelnemers naar wens is.

Let op: het duurt enige tijd totdat de deelnemer aan de groep is toegevoegd. Druk op de **Refresh** knop om te verifiëren of de deelnemer daadwerkelijk is toegevoegd.

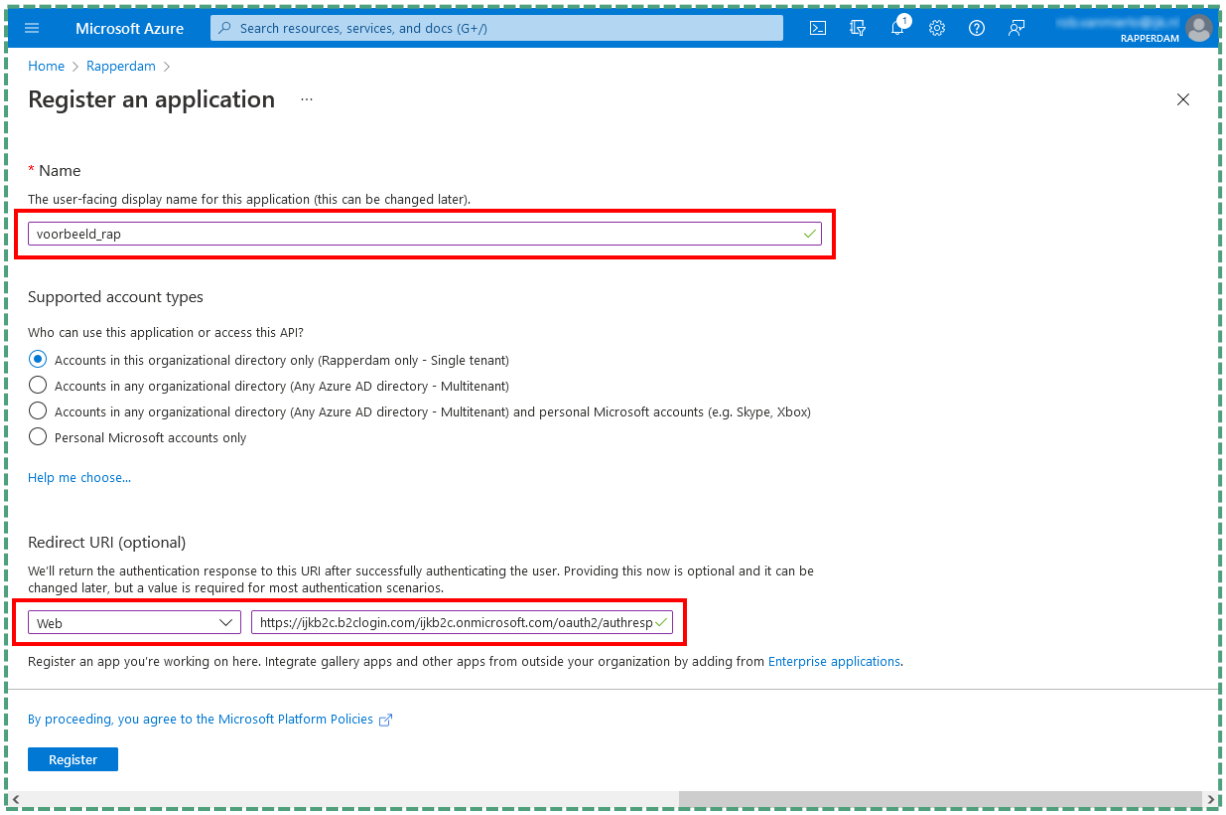
Stap 3. App registration aanmaken

Om ervoor te zorgen dat je organisatie en de RAP applicatie op een vertrouwde manier gegevens kunnen uitwisselen, dien je een **App registration** aan te maken.

- Ga hiervoor in het linker menu naar **App registrations**. Het volgende venster verschijnt.



- Druk op de knop **New registration**. Het volgende venster verschijnt.



- Noteer de naam '**rap**'

- Kies voor **'accounts in this organisational directory only (Default Directory only- Single tenant)**
- Kies bij de **Redirect URI** sectie voor de optie **Web**
- Vul onderstaande URI in:

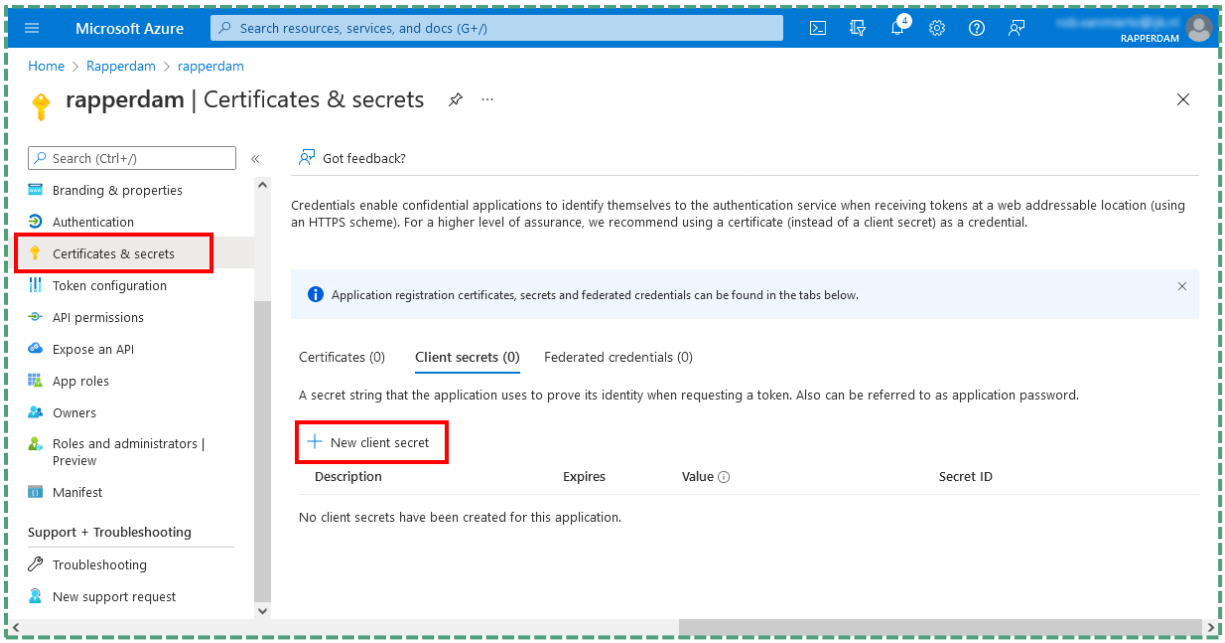
  https://ijkb2c.b2clogin.com/ijkb2c.onmicrosoft.com/oauth2/authresp

- Druk op **Register** om de App registration vast te leggen.

Stap 4. Client secret aanmaken

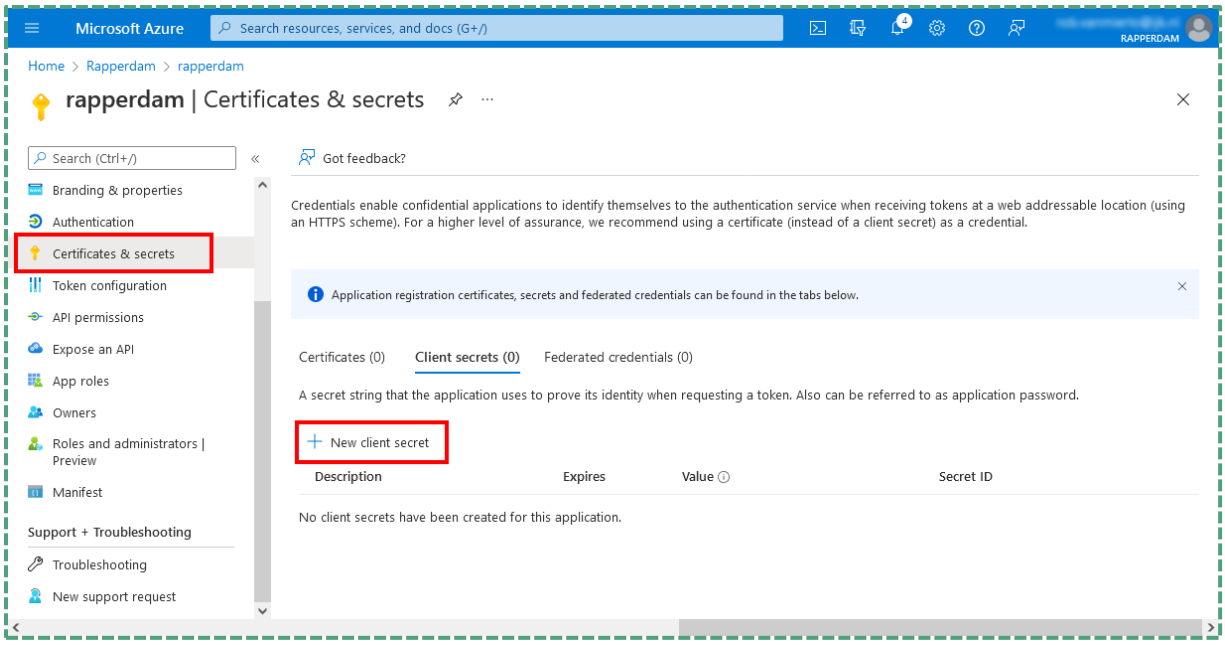
Om communicatie tussen de RAP applicatie en de Azure Active Directory van je organisatie veilig te laten verlopen, dien je een client secret aan te maken.

- Ga in het linker menu naar **Certificates & secrets**. Onderstaand venster verschijnt.



- Druk op **New client secret** om een nieuwe client secret aan te maken.

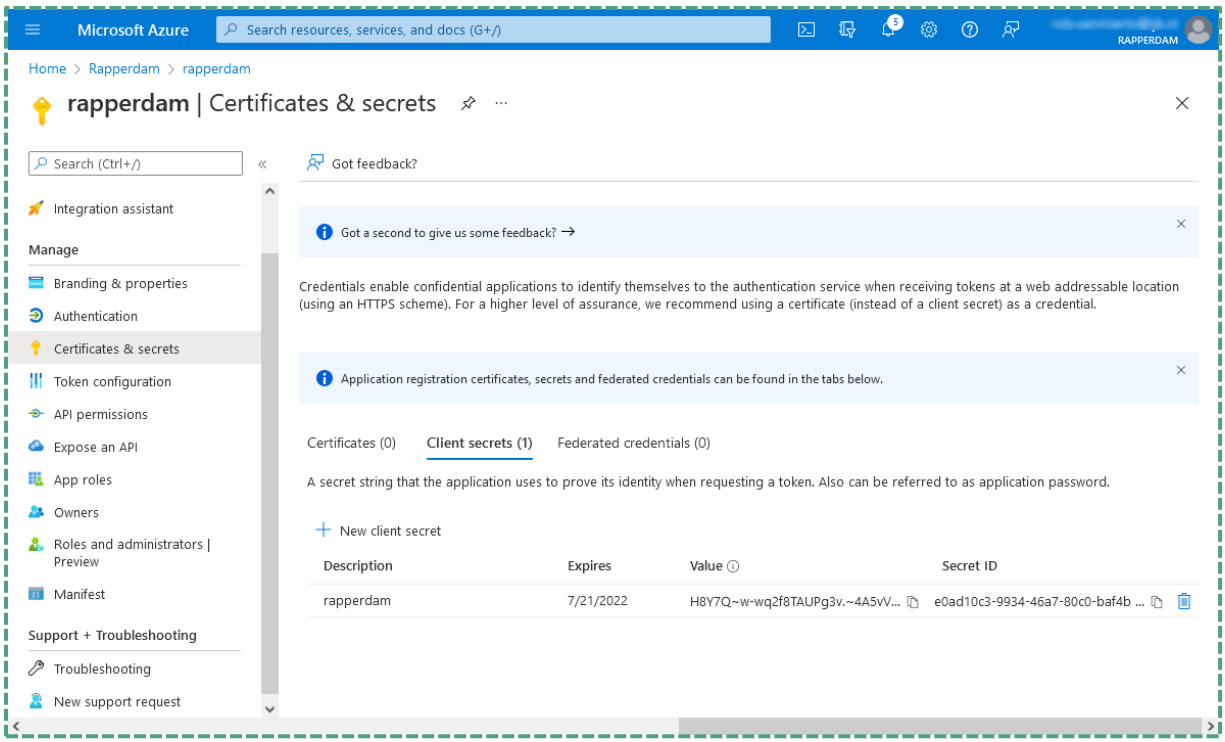
Het volgende sub-venster verschijnt.



- Noteer de naam '**rap**' bij description.
- Geef in het **Expires** veld aan hoe lang deze secret geldig is. Een lange termijn zorgt voor minder onderhoud.

- Druk op **Add** om de client secret definitief aan te maken.

  Het navolgende venster geeft een overzicht.

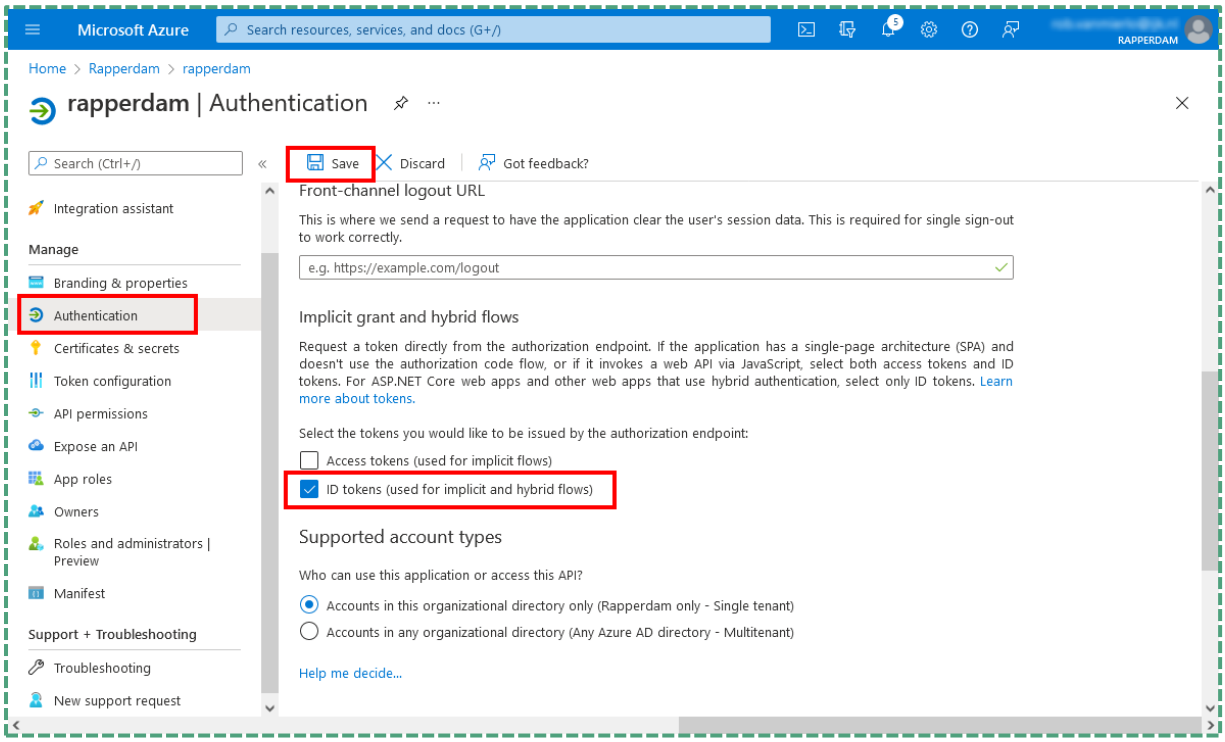


- Kopieer de **Value** en bewaar deze goed. Deze heb je later nog nodig.

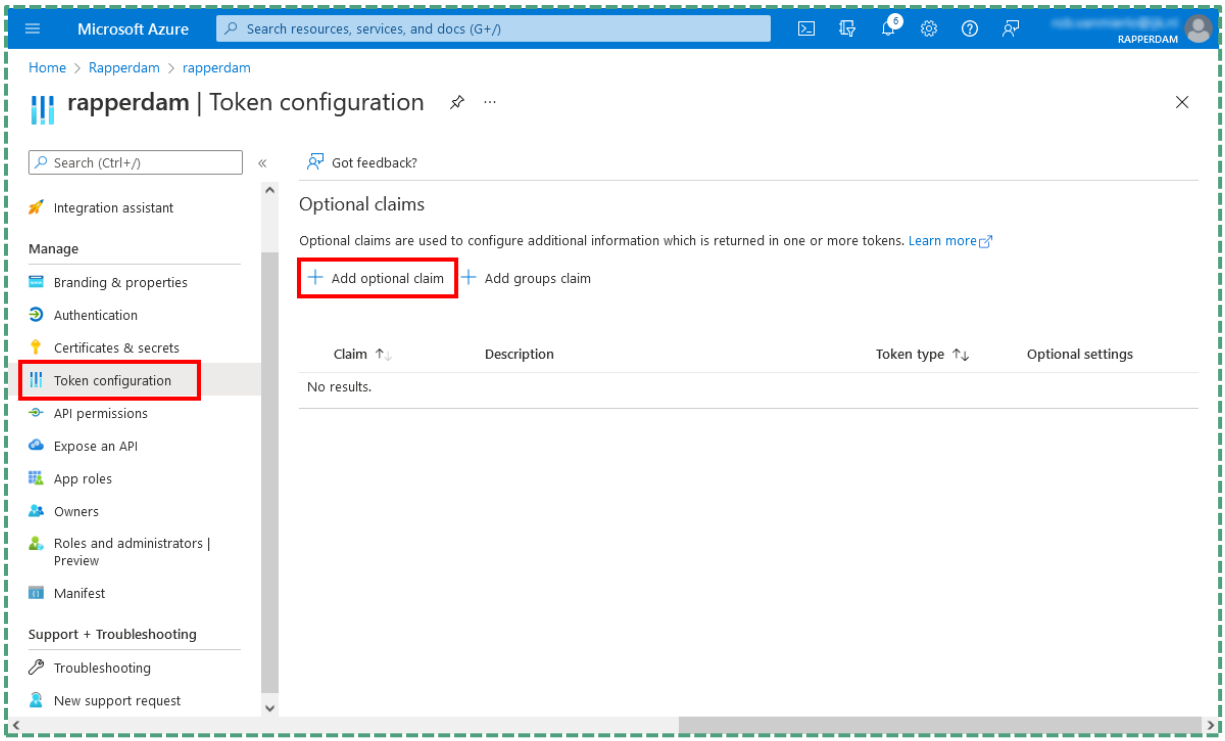
Stap 5. Token configuratie

De app van jouw organisatie wisselt gegevens uit met de RAP via een token. Met deze stap wordt vastgelegd welke gegevens uitgewisseld worden.

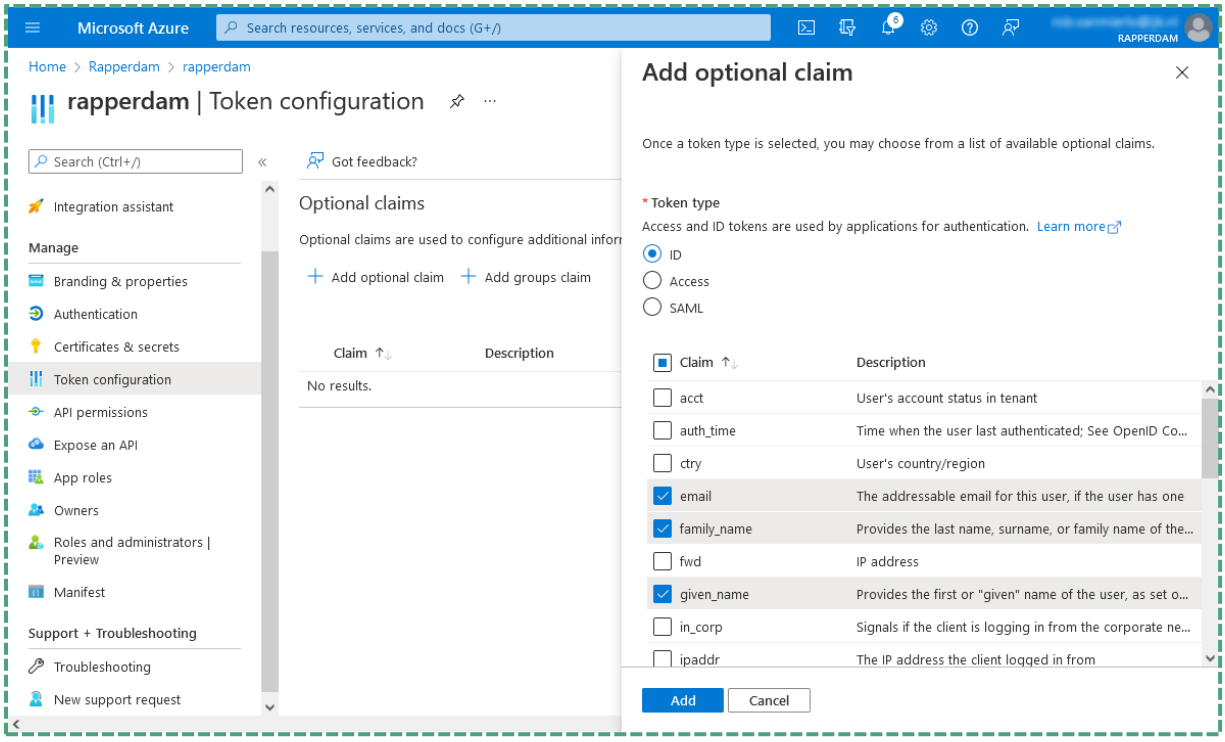
Kies in het linker menu voor **Authentication**. Het volgende venster verschijnt.



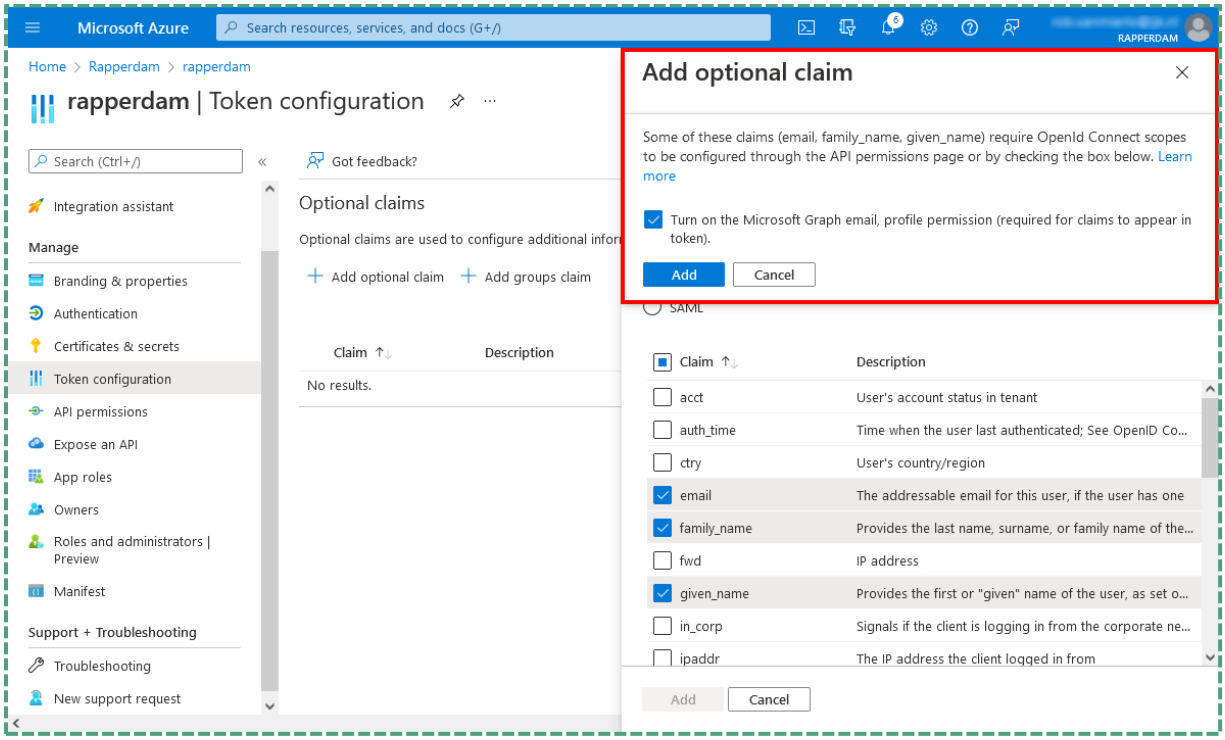
- Navigeer naar de sectie **Implicit grant and hybrid flows**.
- Vink de optie **ID tokens (used for implicit and hybrid flows)** aan.
- Laat alle andere opties onaangeroerd en druk op **Save**.
- Kies in het linker menu voor **Token configuration**. Het volgende venster verschijnt.



- Druk op **Add optional claim** om extra claims toe te voegen.
- Kies als **Token type** voor de optie **ID**, om ervoor te zorgen dat een ID token wordt uitgewisseld met de RAP. Zodra je optie hebt gekozen, verschijnen een aantal optionele claims die je mee moet geven met het token.
- Vink de claims **email**, **family_name**, **given_name** aan.
- Druk op **Add** om de gekozen claims vast te leggen.



- Waarschijnlijk krijg je nu de vraag voorgelegd om de Microsoft Graph **email** en **profile permission** toe te voegen. Dit is nodig om de ingestelde claims toe te voegen aan het token, vink de optie aan en druk vervolgens op **Add**.



Stap 6. Stuur gegevens naar IJK

Om de Azure AD koppeling te kunnen leggen, hebben wij de gegevens uit onderstaande tabel nodig. Deze kun je mailen aan rap@ijk.nl. Gebruik hiervoor het aangeleverde formulier. In het opmerkingen veld staat uitgelegd hoe je aan deze gegevens komt.

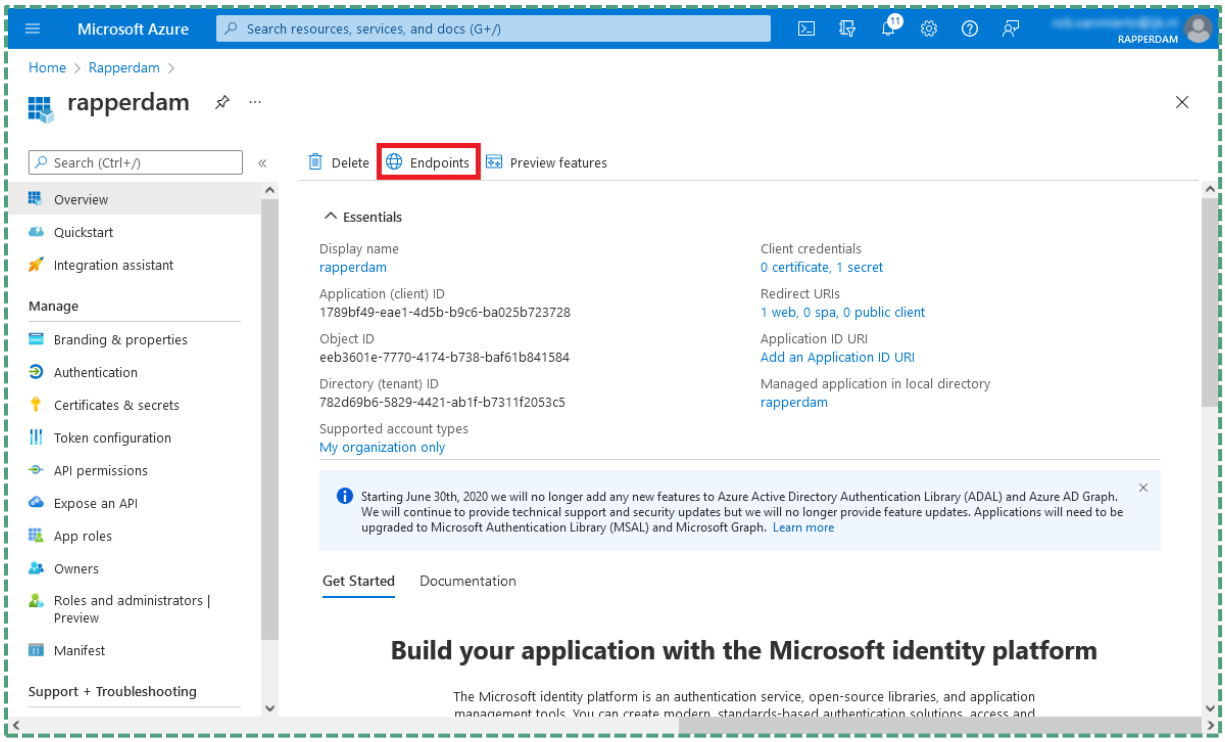
Heb je de bestaande SSO-koppeling alleen uitgebreid met de HRM-groep?
In dat geval is enkel het sturen van de exacte gekozen naam van het veld '**Group name'** voldoende. Zie Stap 2 HRM-groep aanmaken .

Wat	Voorbeeld	Opmerkingen
Metadata	https://login.microsoftonline.com/fe3cdc4b-0075-48b7-9999-6b5c58a221ba/v2.0/.well-known/openid-configuration	Zie Stap 6.1. OpenID connect metadata document url kopiëren
Client id	96631a2e-23d4-4069-9713-dba83eb5efad	Zie Stap 6.2. Client id kopiëren
Client secret id	7f682c21-b1db-4a22-87e1-5a96634c8ec6	Zie Stap 6.3 Client secret id en value kopiëren
Client secret	NV27Q~ZL6bl5-PePD4VQsdQjsPo~2I4CdOyra	
HRM-groep	raphrm	Zie Stap 2 HRM-groep aanmaken. Stuur de exacte gekozen naam van het veld '**Group name'**.
Domeinen	gemeenterapperdam.nl; bsrapperdammetje.nl; rapperdamcollege.nl; hogeschoolrapperdam.nl; waterschaprapperdam.nl; vrrapperdam.nl	De domeinen waarvoor de SSO moet werken met bijbehorende e-mailadressen.

Je hebt hiervoor een apart invulformulier ontvangen.

Stap 6.1. OpenID connect metadata document url kopiëren

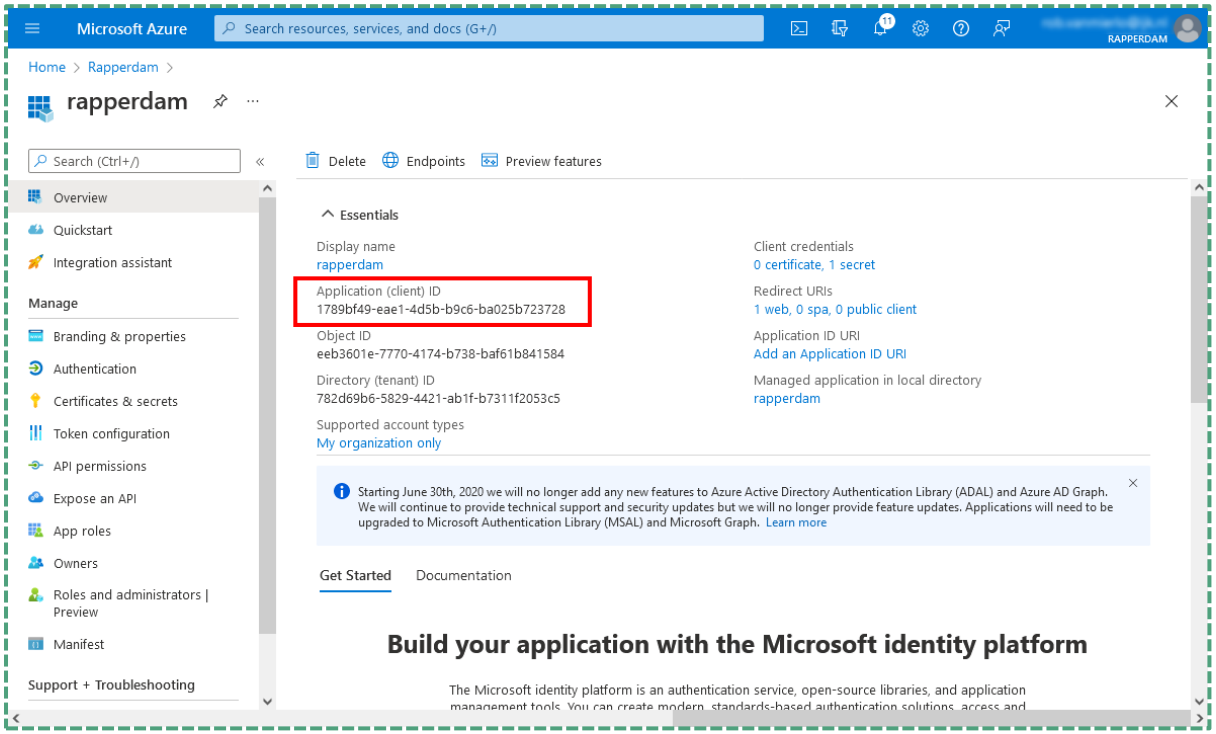
Ga in het **overview** venster van je Azure AD tenant en druk vervolgens op de **Endpoints** knop.



Het volgende **Endpoints** sub-venster verschijnt. Kopiëer de url van het **OpenID Connect metadata document** door op het copy knopje te drukken.

Stap 6.2. Client id kopiëren

Ga in het linker menu naar **Overview**.
Kopieer de client id door op het **Application (client) ID** copy knopje te drukken.

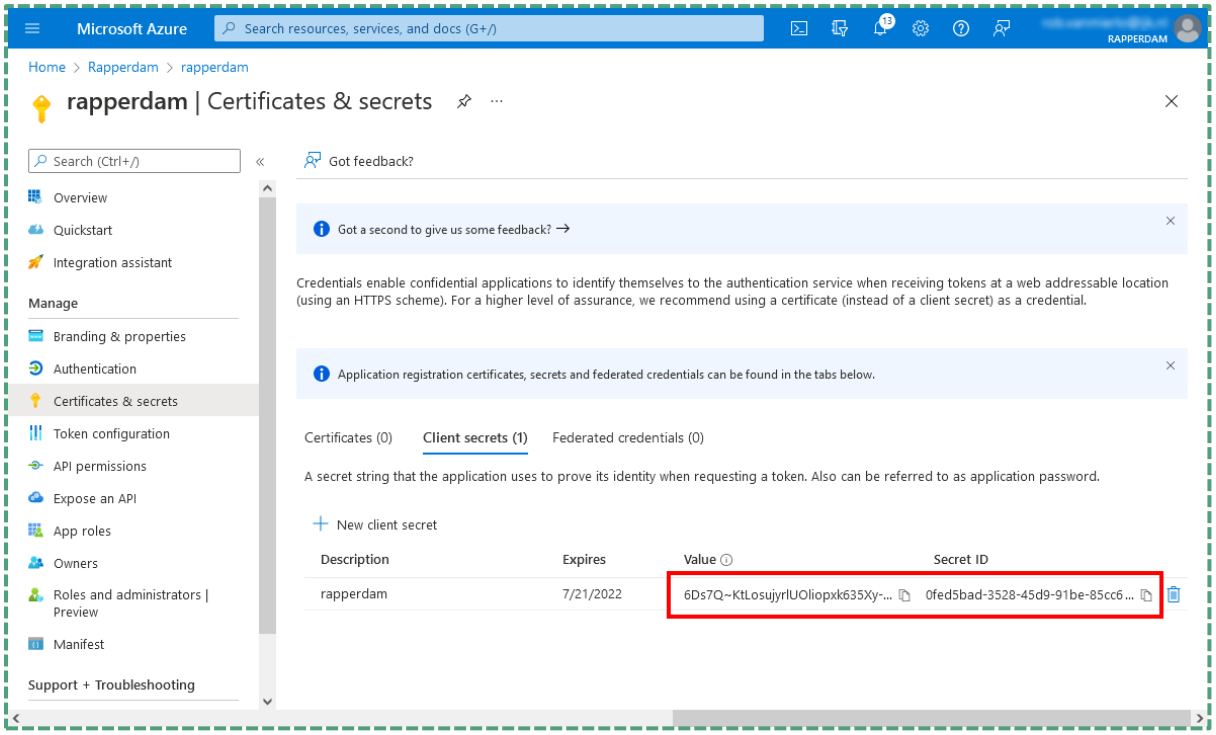


Stap 6.3 Client secret id en value kopiëren

Ga in het linker menu naar Certificates & secrets.

Kopieer de Value van de client secret door op het copy knopje te drukken.

Kopieer de Secret ID van de client secret door op het copy knopje te drukken.



Stap 7. Ontvang de juiste nieuwe URL voor RAP

Wij controleren de gegevens en nemen deze op in ons systeem. Vervolgens mailen wij jou en onze contactpersoon van RAP de juiste nieuwe URL voor het gebruik van het nieuwe medewerker deel van RAP, dat gebruik maakt van de juist gemaakte Azure AD-koppeling.

Gebruik deze URL op de plaatsen waar de collega's naar RAP worden verwezen. In de regel is dit het intranet en het Employee Self Service Portal. Mocht je vragen hebben over de juiste plaats voor de verwijzingen, neem contact met ons op.

3. Vragen/opmerkingen of suggesties

Bij alle vragen over het inrichten van de Azure AD-koppeling kan contact worden opgenomen met de afdeling RAP via rap@ijk.nl of 0492-50 66 60.