Handleiding
Inrichten ADFS voor RAP

Inhoudsopgave

1.Inleiding 3
2.Stappenplan 4
Stap 1. Open de wizard ADFS Management in Windows 4
Stap 2. Application Group 5
Stap 3. Native application 6
Stap 4. Configure a Web API 7
Stap 5. Apply Access Control Policy 8
Stap 6. Configure Application Permissions 9
Stap 7. Summary 10
Stap 8. Staan de OpenID endpoints aan? 11
Stap 9. Toevoegen Transform Rules 12
Stap 10. Toewijzen van HRM-claim 17
Stap 11. Stuur gegevens naar IJK 21
Stap 12. Ontvang de juiste nieuwe URL voor RAP 21
3 Vragen/opmerkingen of suggesties 21

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 ADFS.

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, werkt 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 heet ADFS (Active Directory Federation Services) en is Single Sign-On (SSO, eenmalige aanmelding) oplossing. Inloggen gaat met ADFS 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.

ADFS in een notendop

Active Directory Federation Services (ADFS) is door Microsoft ontwikkeld. Als onderdeel van Windows Server-besturingssystemen biedt het gebruikers geauthentiseerde toegang tot applicaties die niet op de computer staan. De medewerker klikt op een link naar RAP. Vervolgens start op de achtergrond het authenticatieproces. RAP maakt verbinding met een service 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 ADFS 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 ADFS werkt nemen we natuurlijk contact met jou als contactpersoon op om samen te kijken of het juist werkt.

Vragen

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

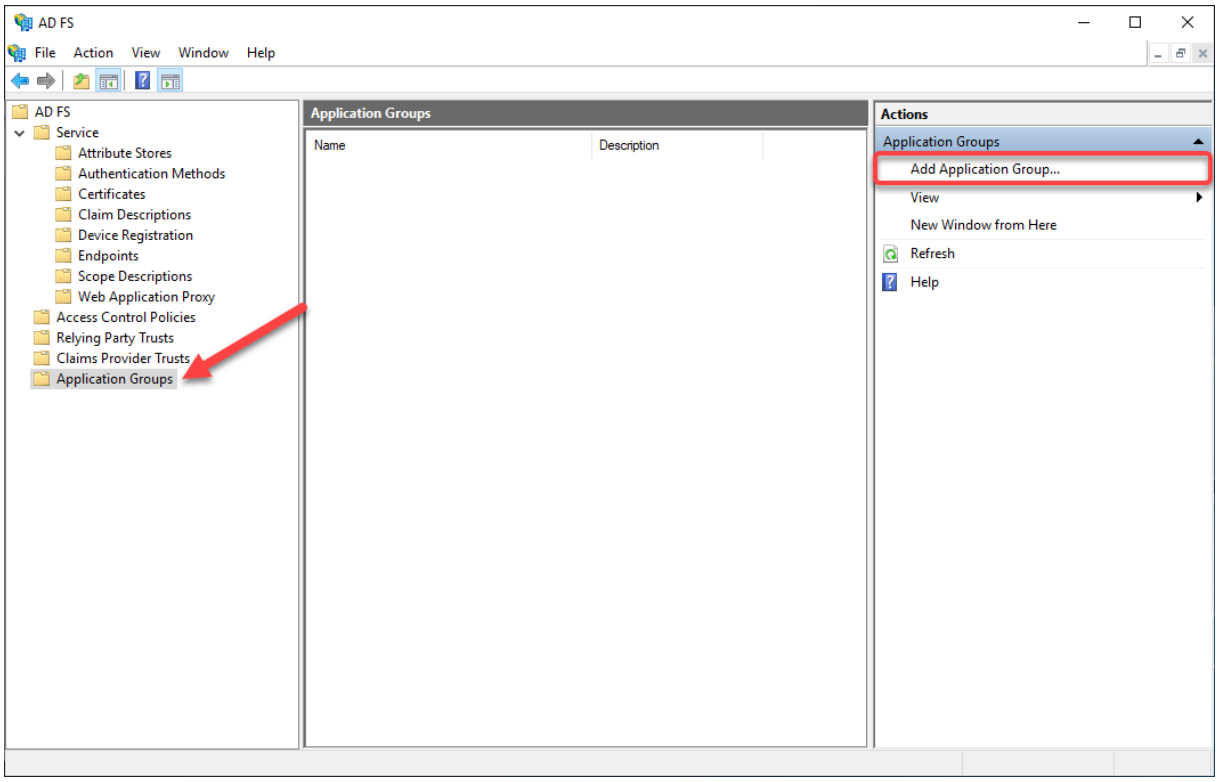
2. Stappenplan

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.

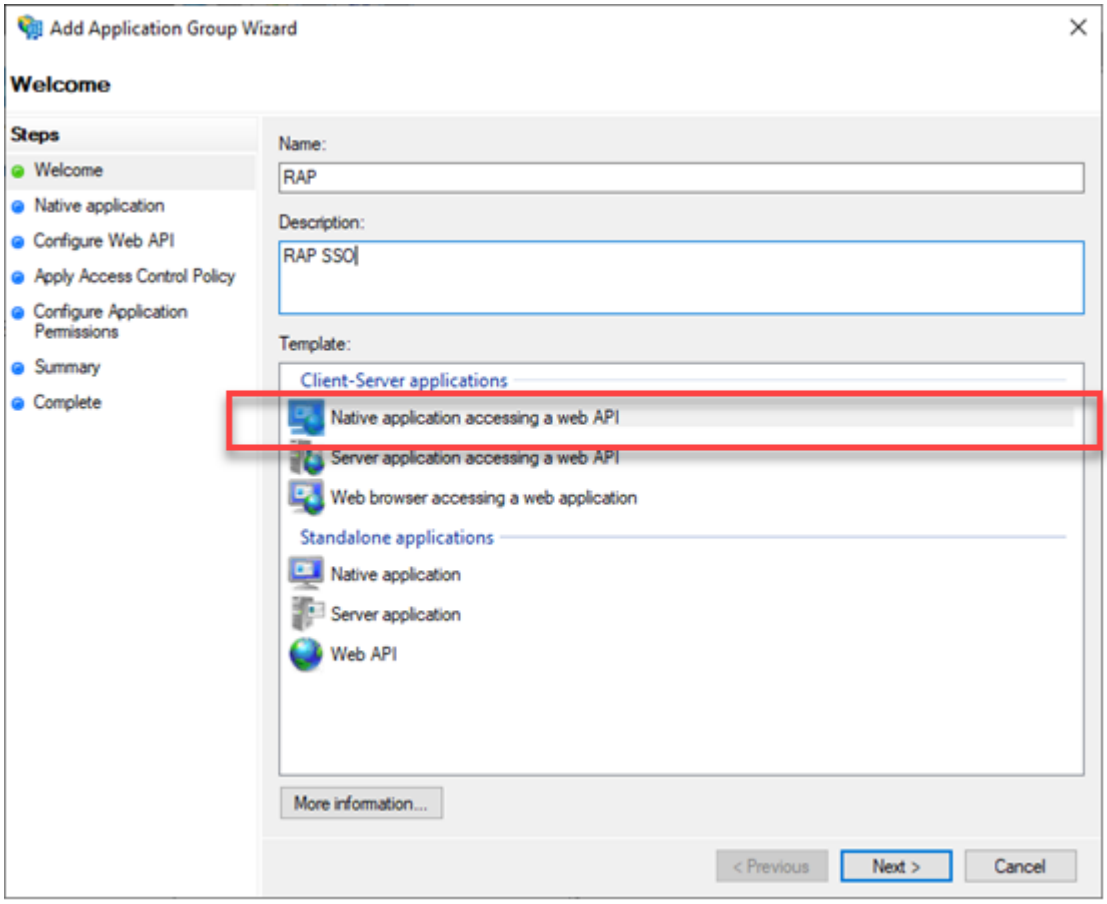
Stap 1. Open de wizard ADFS Management in Windows

Klik vervolgens op '**Application Groups**' en vervolgens op '**Add Application Group…**'



Stap 2. Application Group

Vervolgens opent een venster waarin je de naam van de Application Group en een omschrijving in kunt vullen. Geef de naam “RAP” op en de beschrijving “RAP SSO” aan de native application en klik als template ‘**Native application accessing a web API**’ aan.



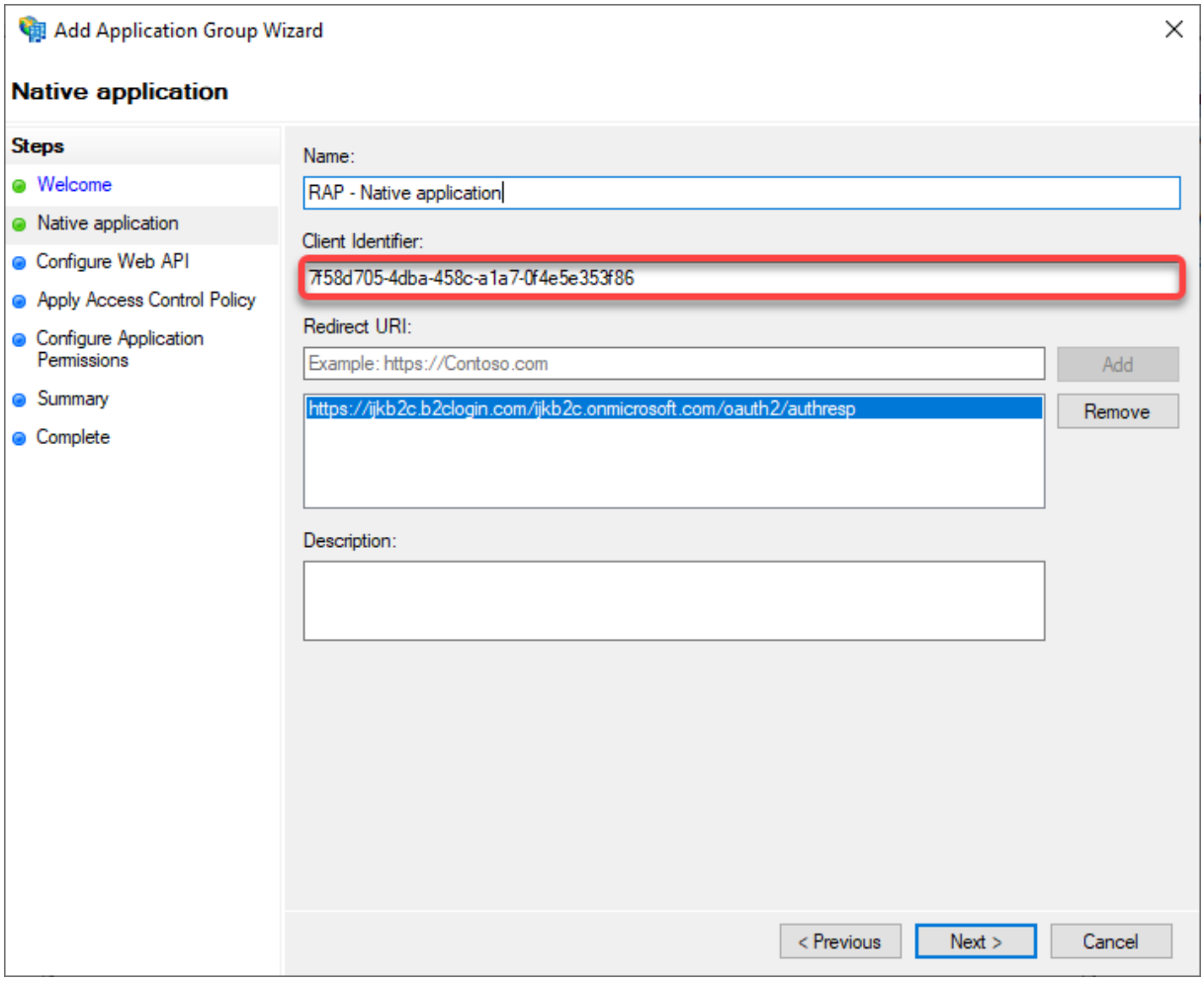
Druk op **‘Next’**

Stap 3. Native application

Vervolgens opent een venster Native application. Geef het de naam “RAP - Native application” en voer de volgende redirect URL in:

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

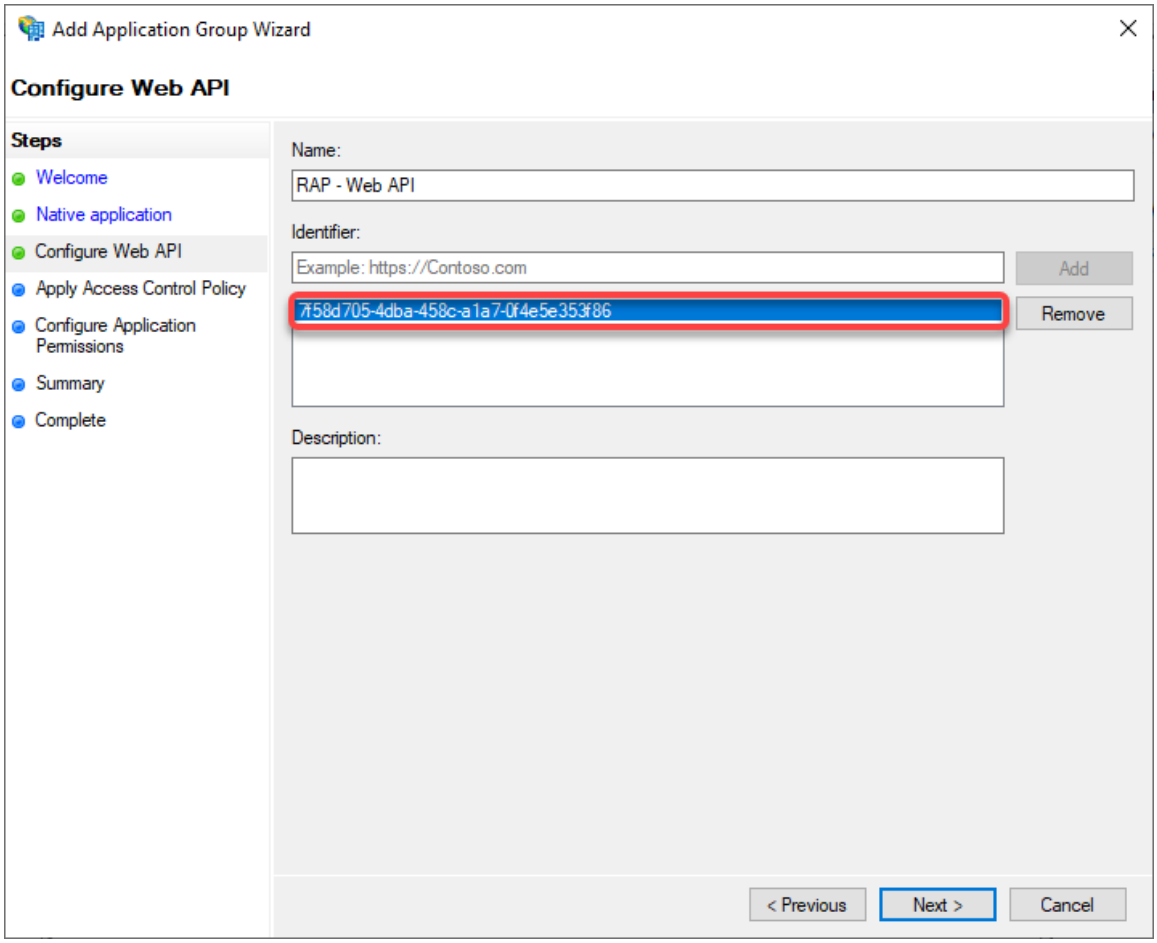
Belangrijk: kopieer de ‘**Client Identifier**’ en zet deze in bijvoorbeeld Kladblok. Deze heb je in de volgende stappen nog nodig.



Druk op **‘Next’**

Stap 4. Configure a Web API

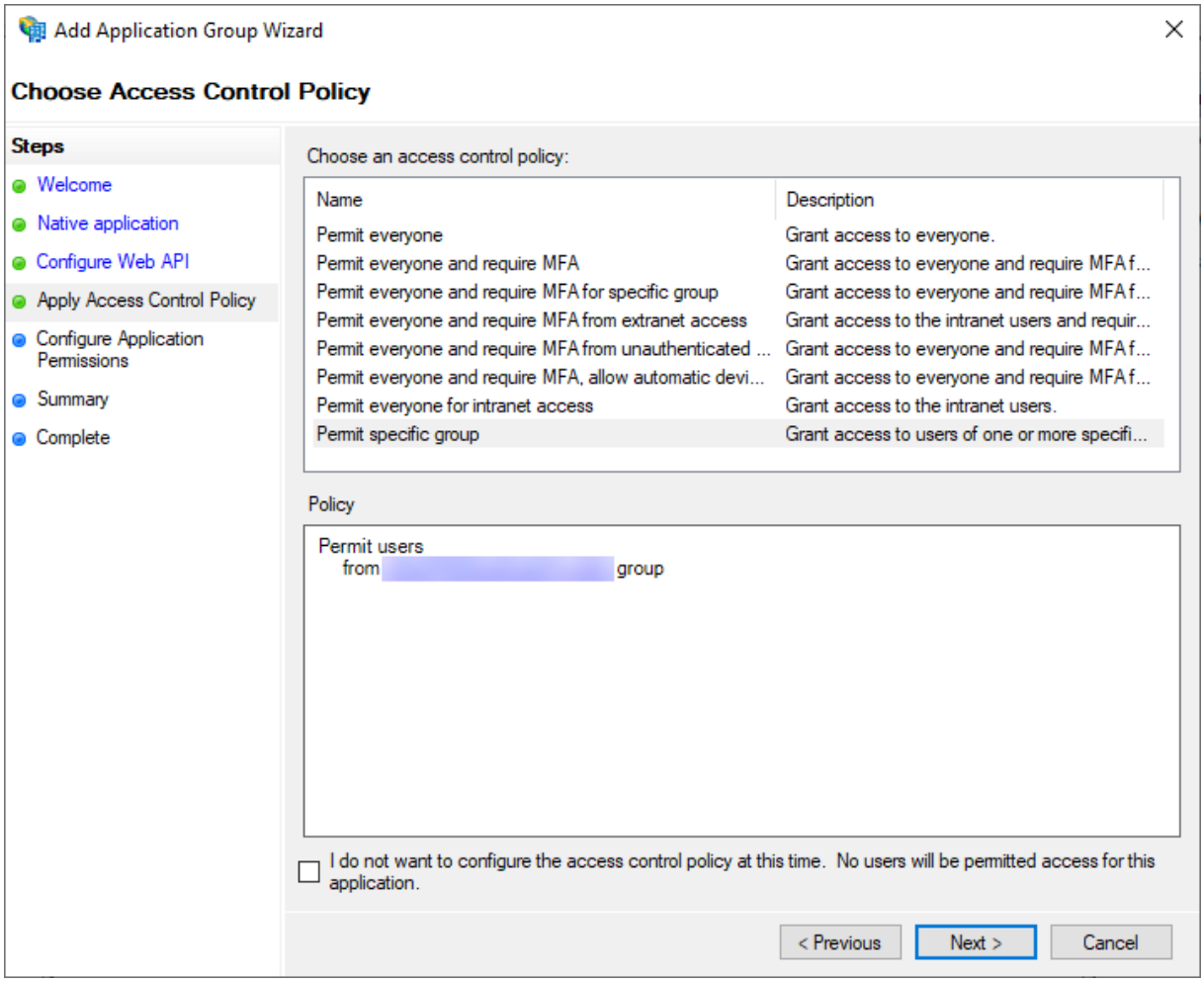
Vul in het volgende venster een naam in voor de Web API. Kies “RAP – Web API”. Vul de bij de vorige stap genoteerde ‘**Client identifier**’ in bij het tekstveld ‘**Identifier**’ en druk op ‘**Add**’.



Klik op ‘**Next**’

Stap 5. Apply Access Control Policy

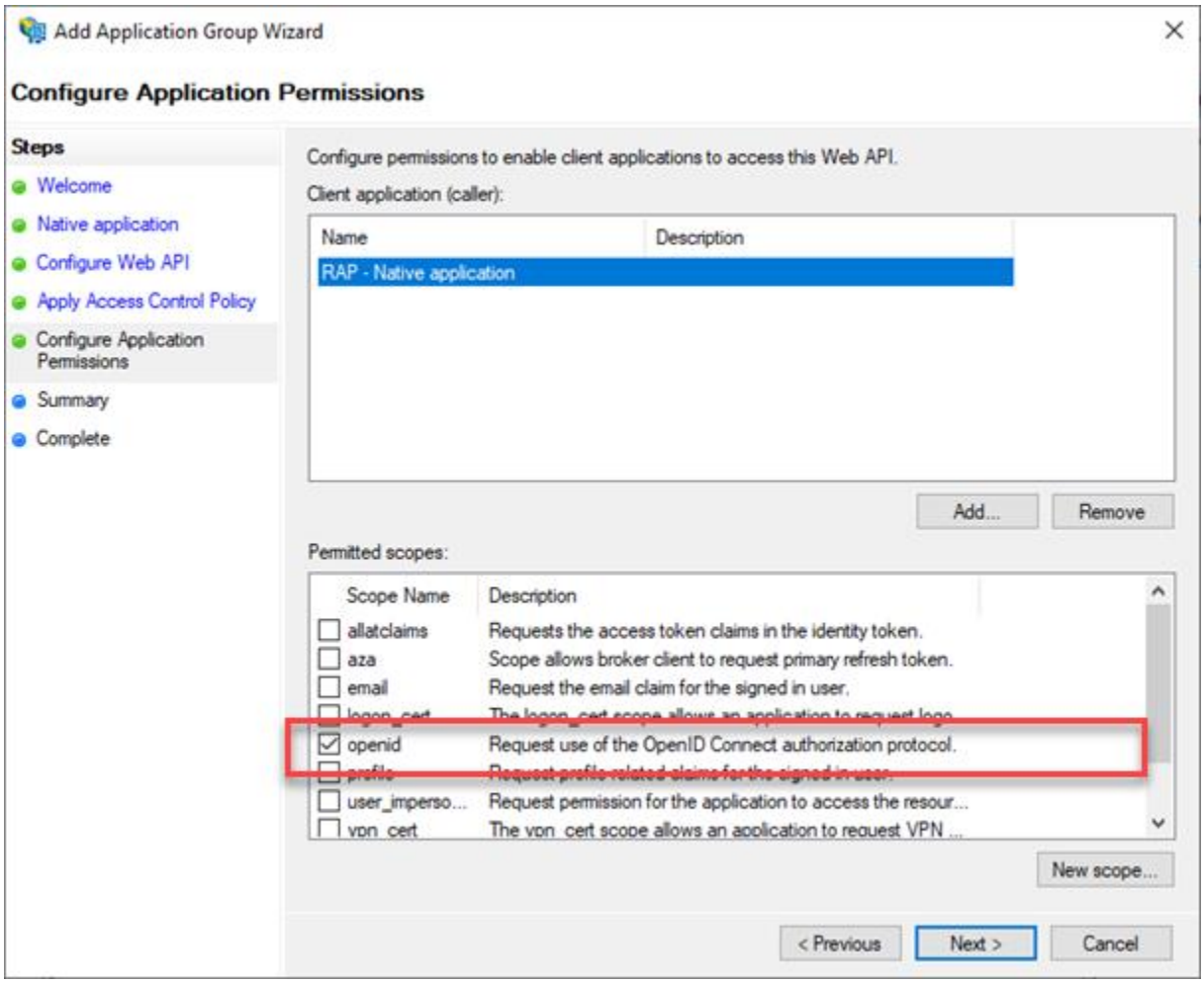
In deze stap kan toegang worden beperkt door een bepaalde policy toe te wijzen. Dit is in principe niet nodig. RAP is nadrukkelijk bedoeld voor alle medewerkers van de organisatie en werkt niet met een aantal licenties.



Klik op '**Next**'

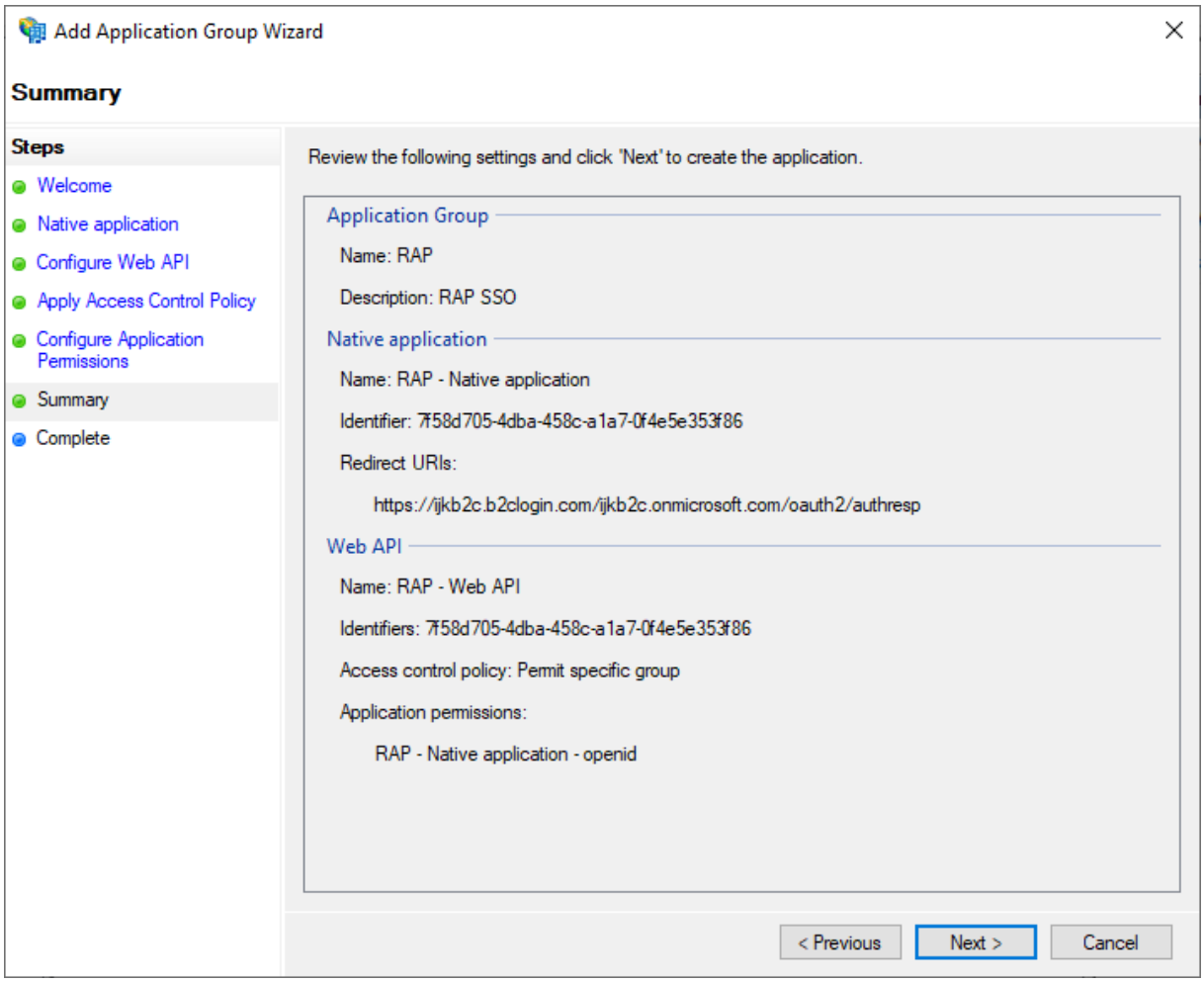
Stap 6. Configure Application Permissions

Verifieer op het volgende scherm dat '**openid**' aangevinkt is en druk op '**Next**'.



Stap 7. Summary

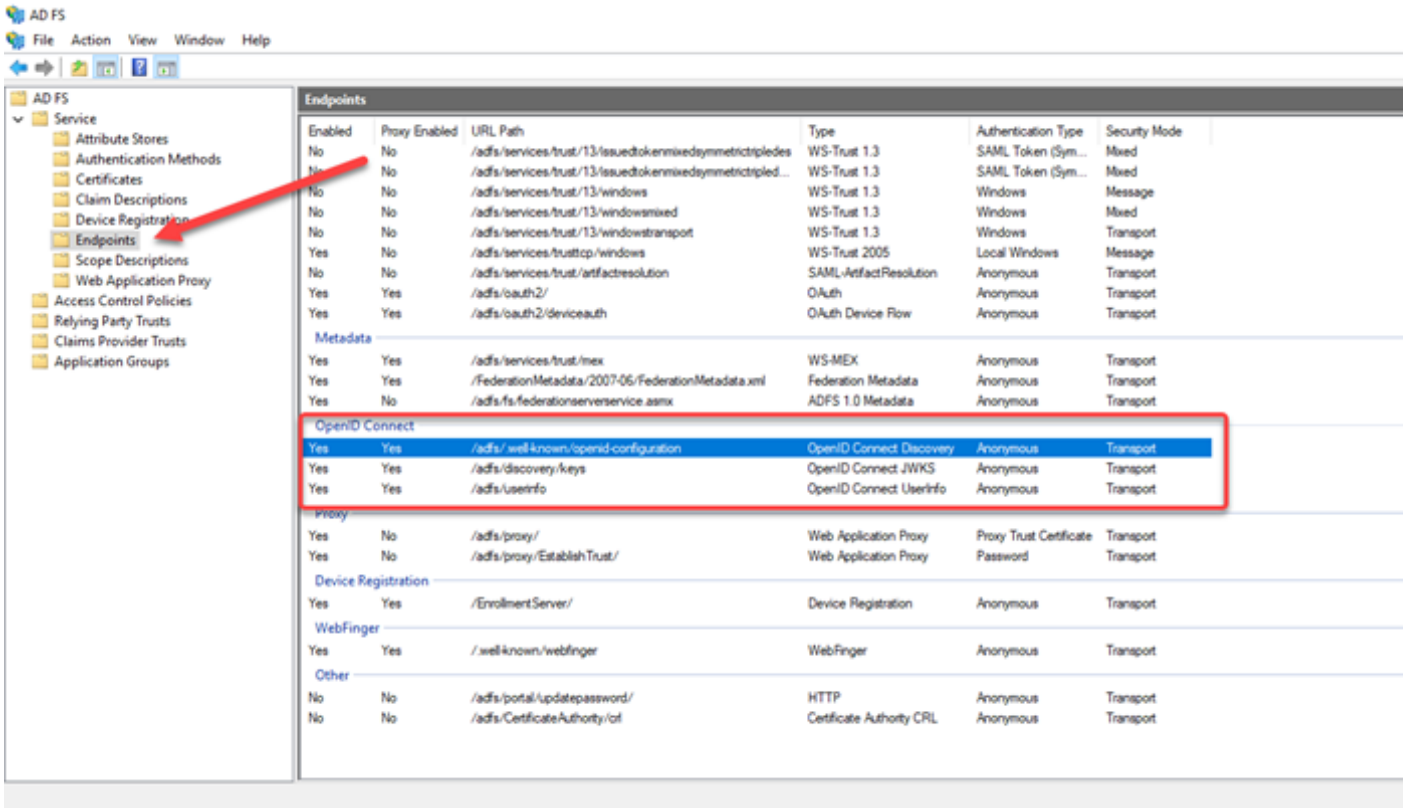
Controleer de ingevulde gegevens. Bij juistheid druk je op '**Next**' en vervolgens op '**Close**'.



Stap 8. Staan de OpenID endpoints aan?

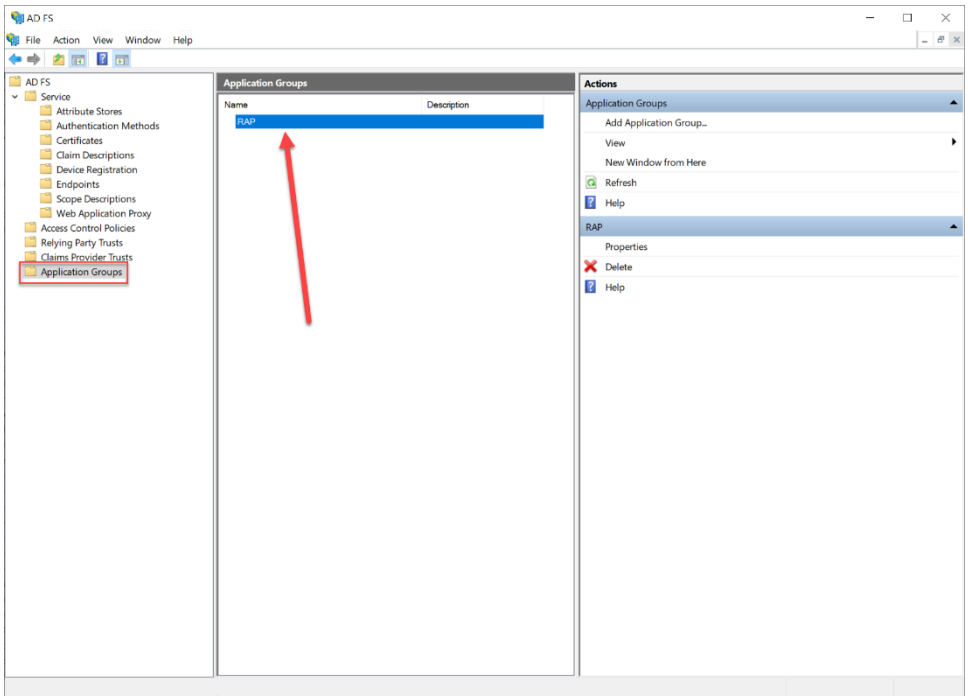
Voor de werking van de ADFS is het belangrijk dat de OpenID endpoints aan staan. Dit kan geverifieerd worden door in de linker navigatiebalk te navigeren naar **AD FS** -> **Service** -> **Endpoints**.

Vervolgens scroll je naar beneden totdat je '**OpenID**' Connect ziet. Indien de endpoints disabled zijn, zet je deze aan.

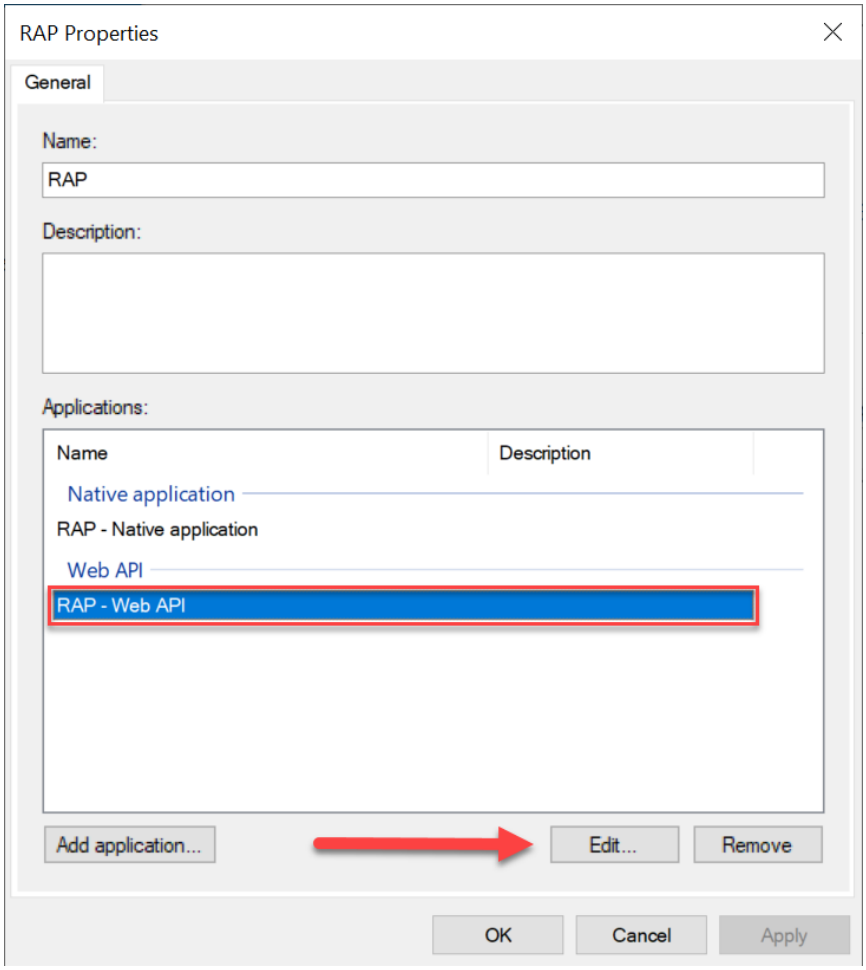


Stap 9. Toevoegen Transform Rules

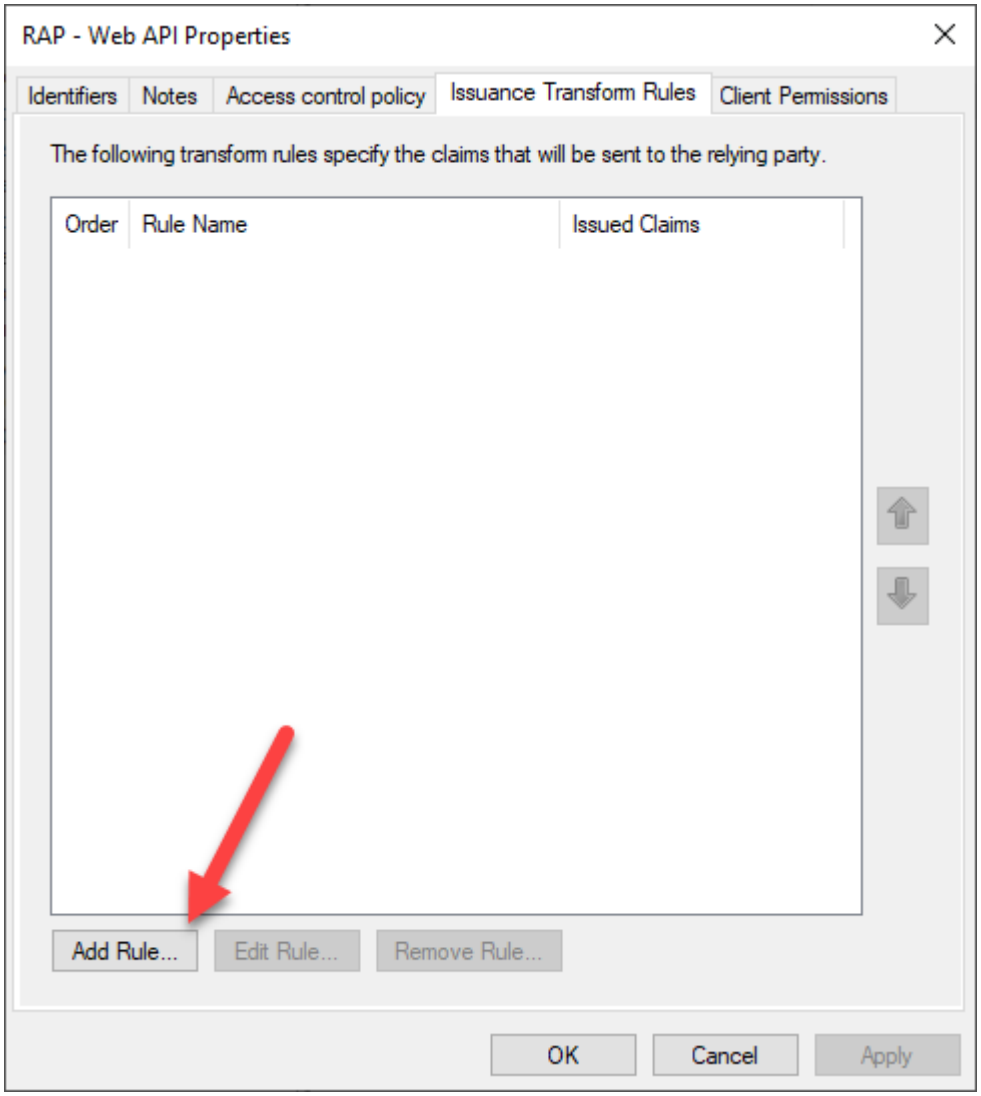
Ga terug naar '**Application Groups**' en klik op de eerder aangemaakte application group '**RAP**'.



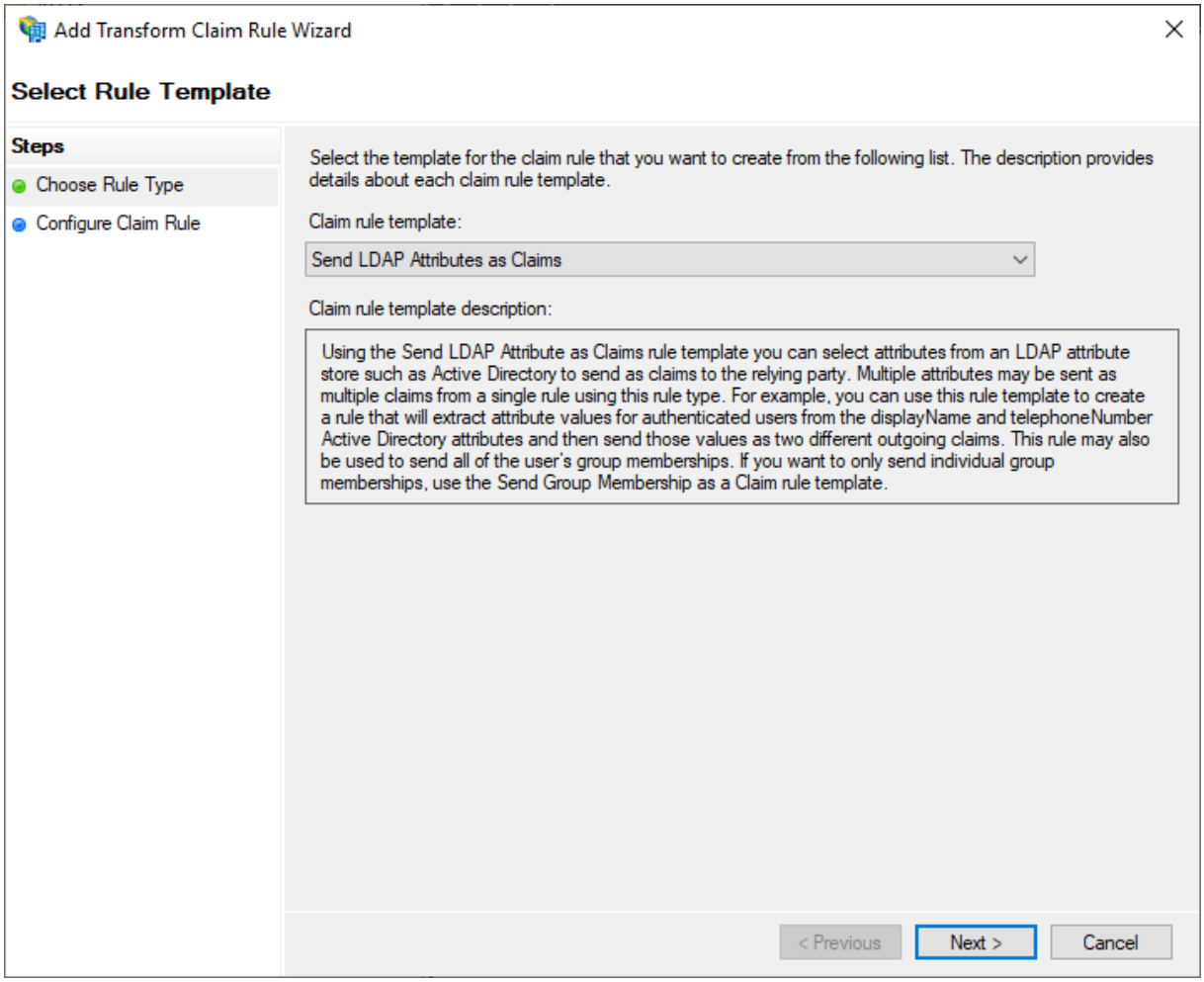
Druk vervolgens op de web api '**RAP – WEB API'** en daarna op '**Edit**...' .



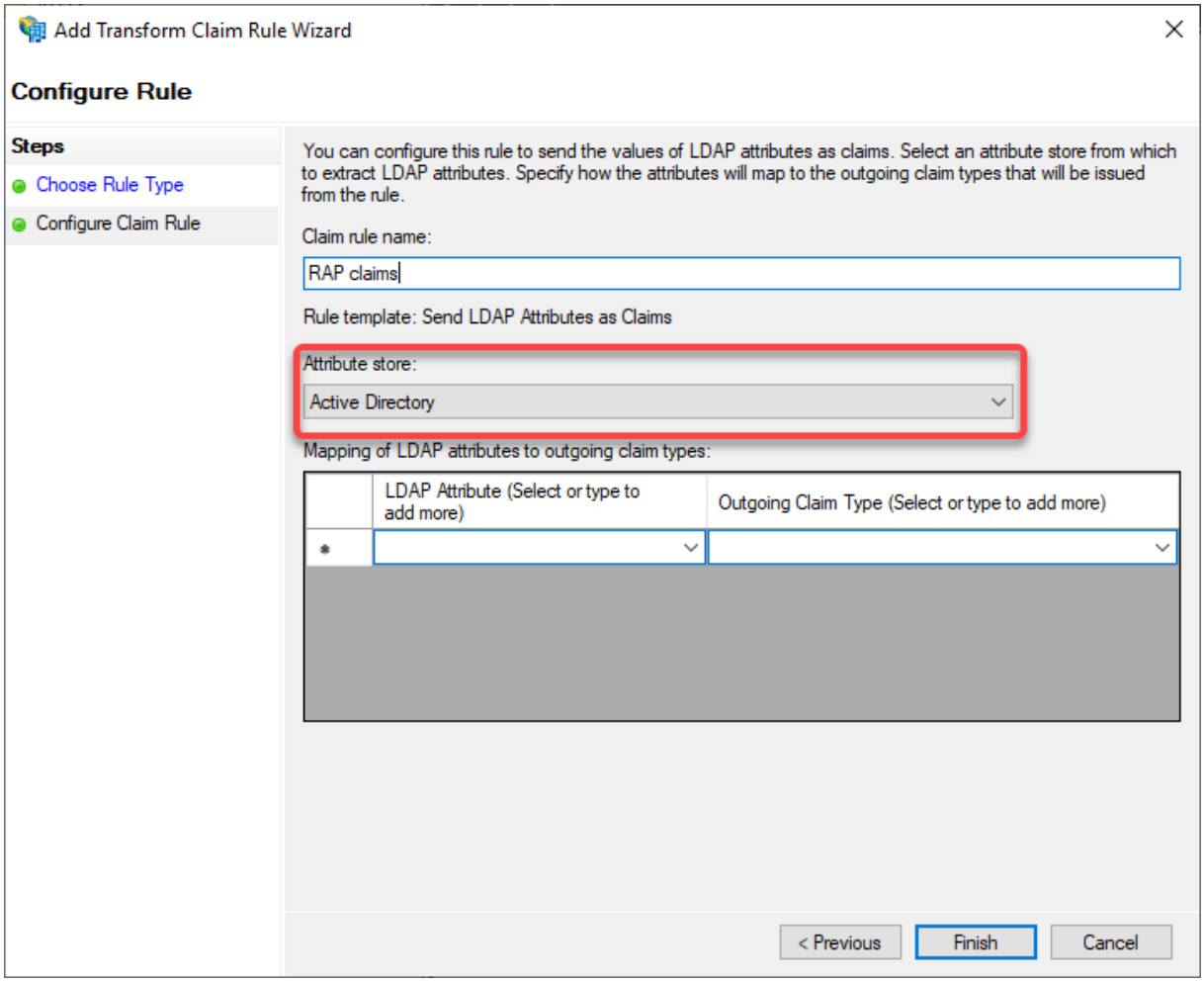
Ga naar het tabblad '**Issuance Transform Rules**' en klik op '**Add Rule…**' .



Op het volgende scherm selecteer je **'Send LDAP Attributes as Claims'** om de informatie over de gebruiker door te sturen.



Zodra je op **'Next'** klikt zie je het onderstaande scherm:



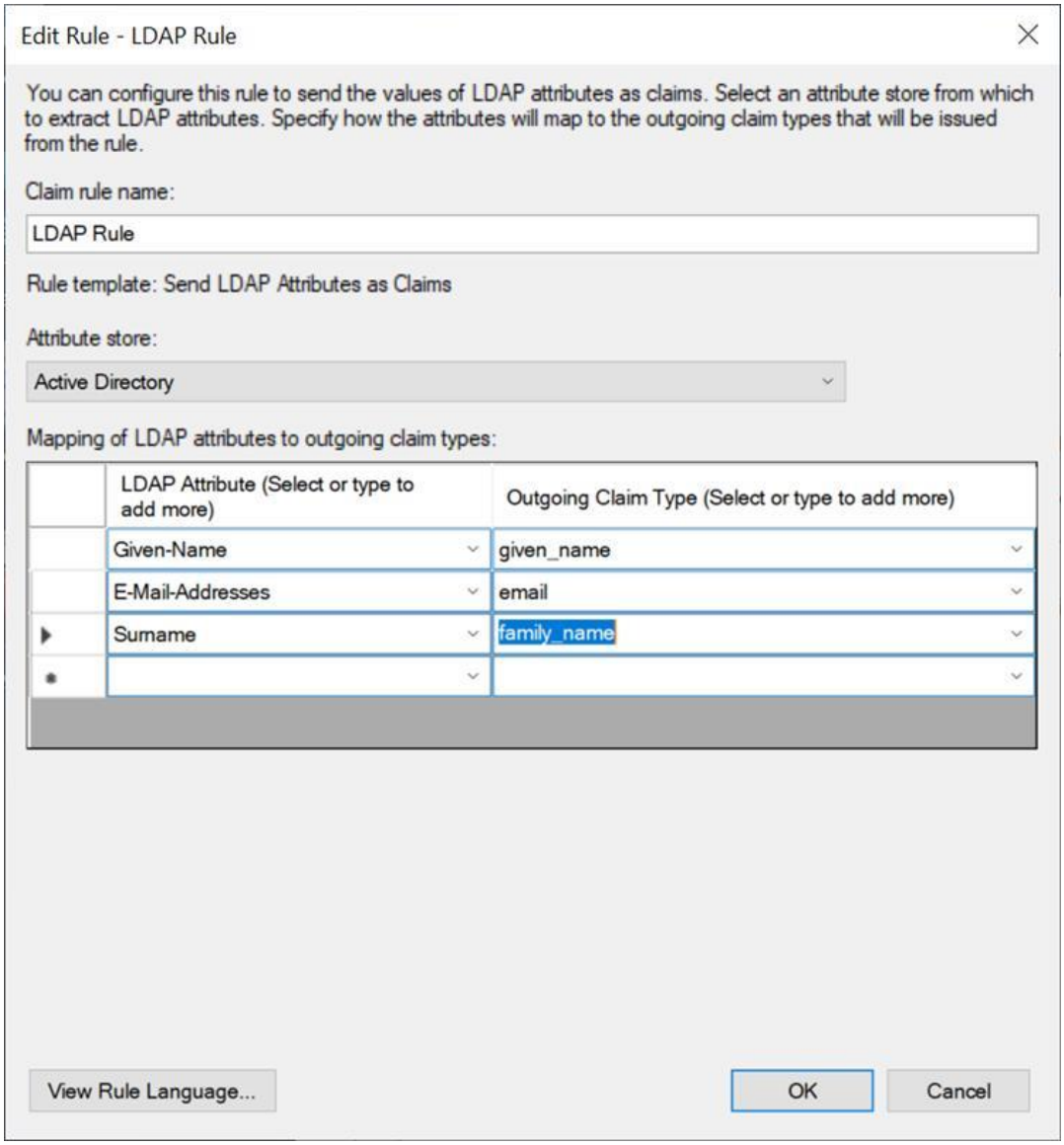
Geef het de naam “RAP claims”. Vervolgens kun je in de tabel bronvelden in de eerste kolom invullen en doelvelden in de tweede.

Vul hier het volgende in.

LDAP Attribute	Outgoing Claim type
Given-Name	given_name
E-Mail-Address	email
Surname	family_name

Let op! Vergeet niet om Active Directory als ‘**Attribute store**’ aan te selecteren.

Na het invoeren van deze waardes ziet het scherm er zo uit. Controleer dit en klik vervolgens op '**OK**'.

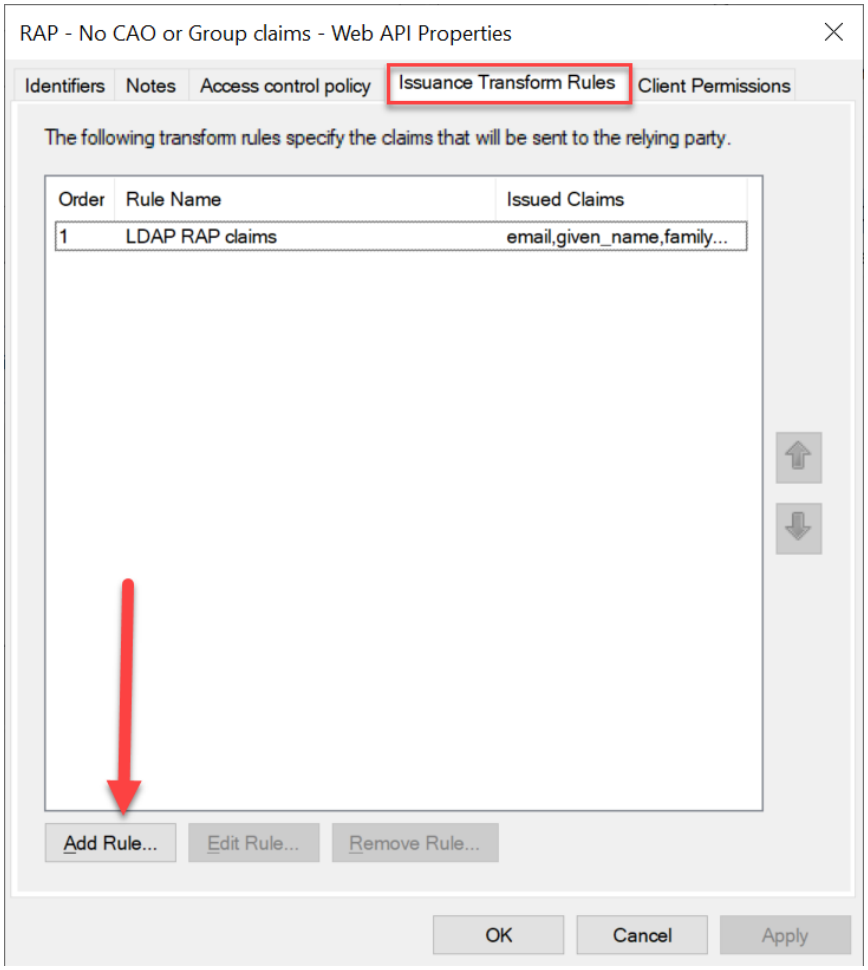


Stap 10. Toewijzen van HRM-claim

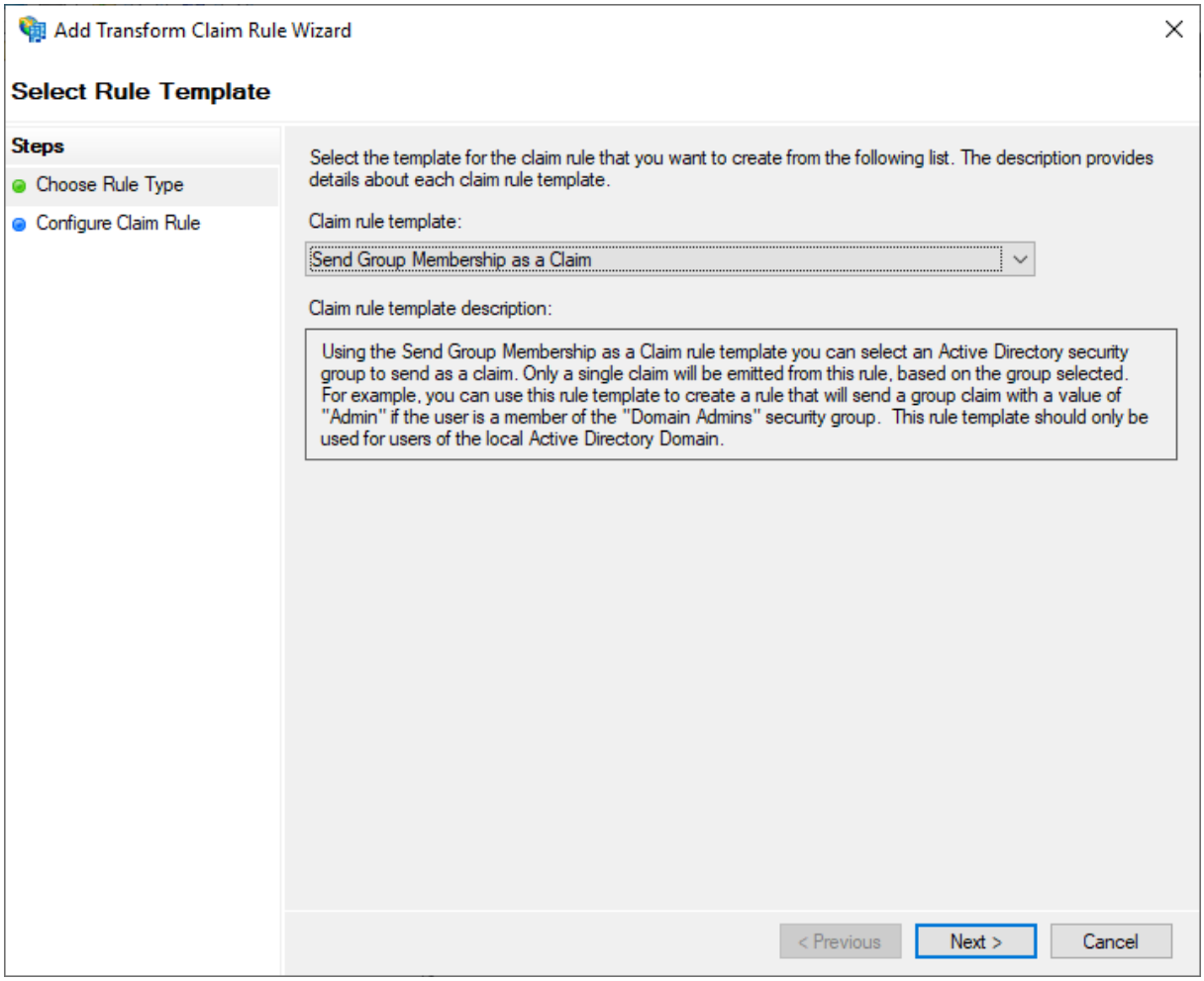
RAP bestaat uit twee versies een deel voor medewerkers en een deel voor HRM'ers. Om te zorgen dat de iedere medewerker van de HRM-afdeling (bestaande uit onder andere HRM-adviseurs, medewerkers personeels- en salarisadministratie, beleidsadviseurs) toegang krijgt, is het noodzakelijk om de HRM-claim toe te voegen. Mocht je twijfelen over wie tot deze doelgroep behoort, neem contact op met je collega's van HRM.

Maken van een HRM-claim

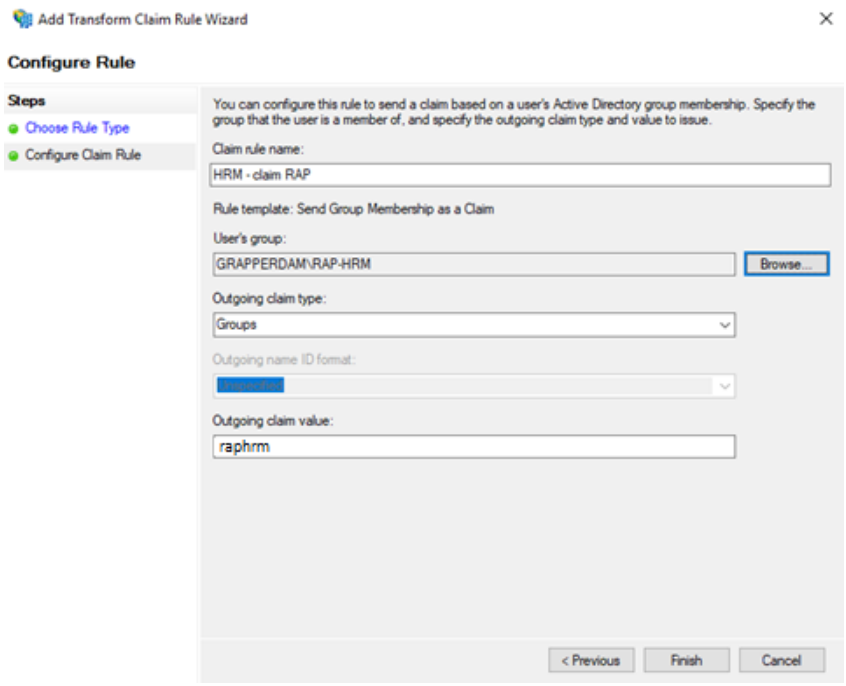
Dit gaat als volgt open wederom de '**RAP- Web API Properties** (zie stap 9)'. Klik vervolgens op '**Insuance Transform rules',** kies vervolgens **'Add Rule'.**



Kies voor '**Send Group Membership as a Claim**'


Add Transform Claim Rule Wizard
Select Rule Template
Steps
Choose Rule Type
Configure Claim Rule
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.
Claim rule template:
Send Group Membership as a Claim
Claim rule template description:
Using the Send Group Membership as a Claim rule template you can select an Active Directory security group to send as a claim. Only a single claim will be emitted from this rule, based on the group selected. For example, you can use this rule template to create a rule that will send a group claim with a value of "Admin" if the user is a member of the "Domain Admins" security group. This rule template should only be used for users of the local Active Directory Domain.
< Previous
Next >
Cancel

Klik op **'Next'**


Add Transform Claim Rule Wizard
Configure Rule
Steps
Choose Rule Type
Configure Claim Rule
You can configure this rule to send a claim based on a user's Active Directory group membership. Specify the group that the user is a member of, and specify the outgoing claim type and value to issue.
Claim rule name:
HRM - claim RAP
Rule template: Send Group Membership as a Claim
User's group:
GRAPPERDAM\RAP-HRM
Browse...
Outgoing claim type:
Groups
Outgoing name ID format:
Outgoing claim value:
raphrm
< Previous
Finish
Cancel

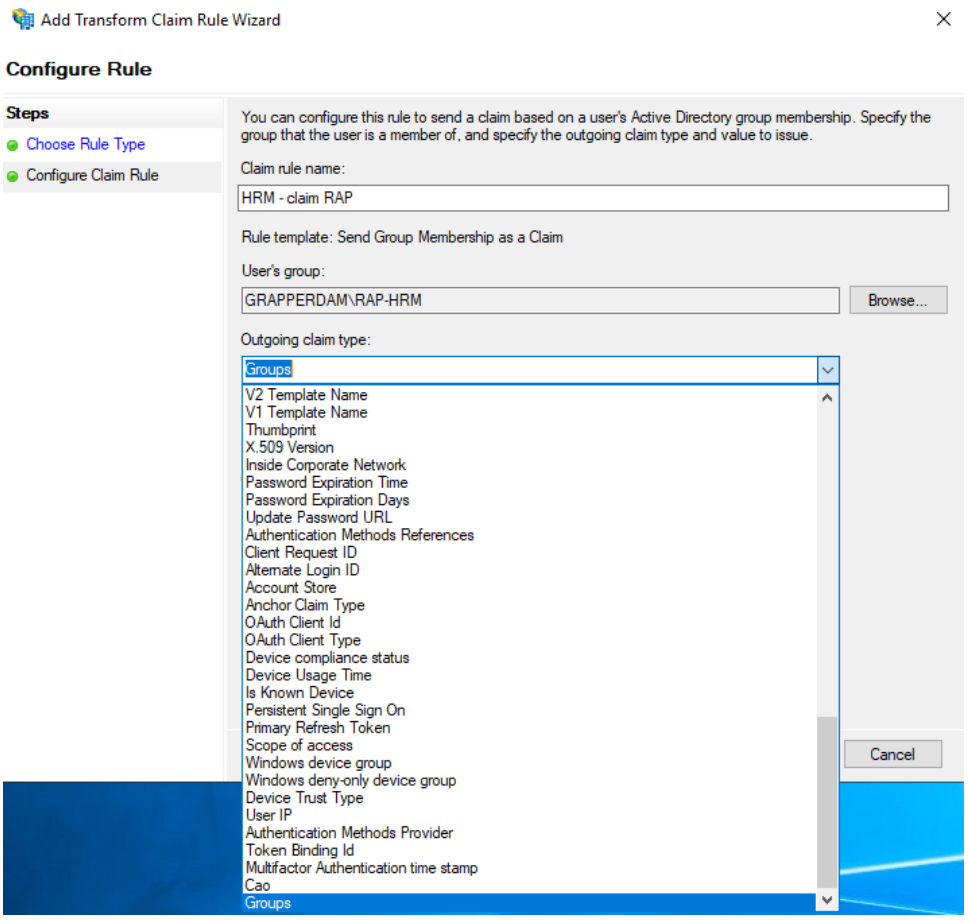
- Vul de naam '**HRM- claim RAP**' bij 'Claim rule name' in.

- Kies bij 'User's group' voor de groep van HRM-medewerkers die de claim moeten ontvangen.

Dynamische rechten
Het is verstandig om leden aan de 'HRM-claim RAP' 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.

- Kies '**Groups**' bij 'Outgoing claim type'. Dit is een keuze in het dropsdown menu

- Voer '**raphrm**' in als 'outgoing claim value'.



Klik op **'Finish'**.

Stap 11. Stuur gegevens naar IJK

Om de ADFS- koppeling te kunnen leggen, hebben wij de volgende gegevens nodig. Deze kun je mailen aan rap@ijk.nl. De meeste gegevens staan op de 'Summary' die je bij stap 7 hebt gezien.

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 '**Outgoing claim value**' voldoende. Zie Stap 10 Toewijzen van HRM-claim.

Wat	Voorbeeld	Opmerkingen
Metadata:	https://adfs.contoso.com/adfs/.well-known/openid-configuration	
Provider:	https://adfs.contoso.com /adfs	
Client ID:	9307c210-c5fb-426b-a09f-29e97b9404fb	
Outgoing claim value (HRM-Groep)	raphrm	Zie Stap 10 Toewijzen van HRM-claim Stuur de exacte gekozen naam van het veld '**Outgoing claim value'**.
Domeinen	ijk.nl; driessen.nl; jeij.nl	De domeinen waarvoor de ADFS moet werken met bijbehorende e-mailadressen.

Je hebt hiervoor een apart invulformulier ontvangen.

Stap 12. Ontvang de juiste nieuwe URL voor RAP

Wij controleren de gegevens en nemen deze op in ons systeem. Vervolgens mailen wij je 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 ADFS-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 ADFS-koppeling kan contact worden opgenomen met de afdeling RAP via rap@ijk.nl of 0492-50 66 60.