



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.

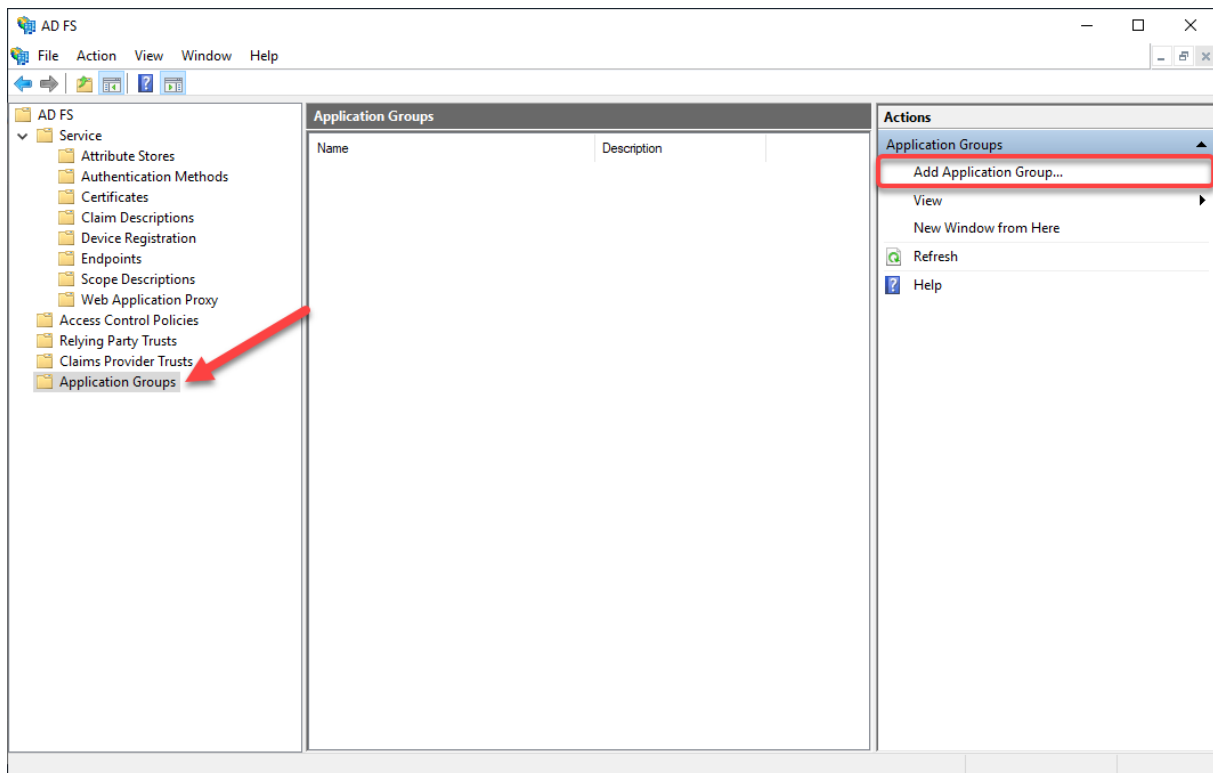
2. Stappenplan

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.

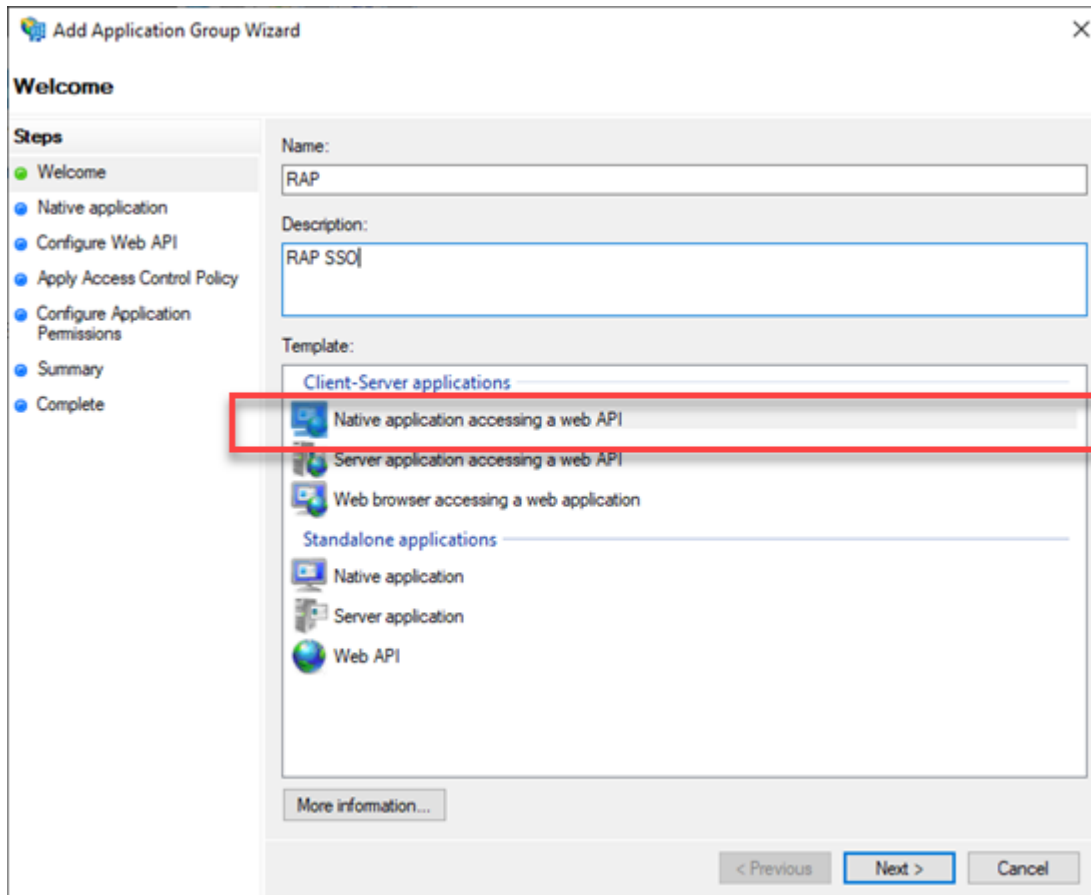
Stap 1. Open de wizard ADFS Management in Windows

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



Step 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.



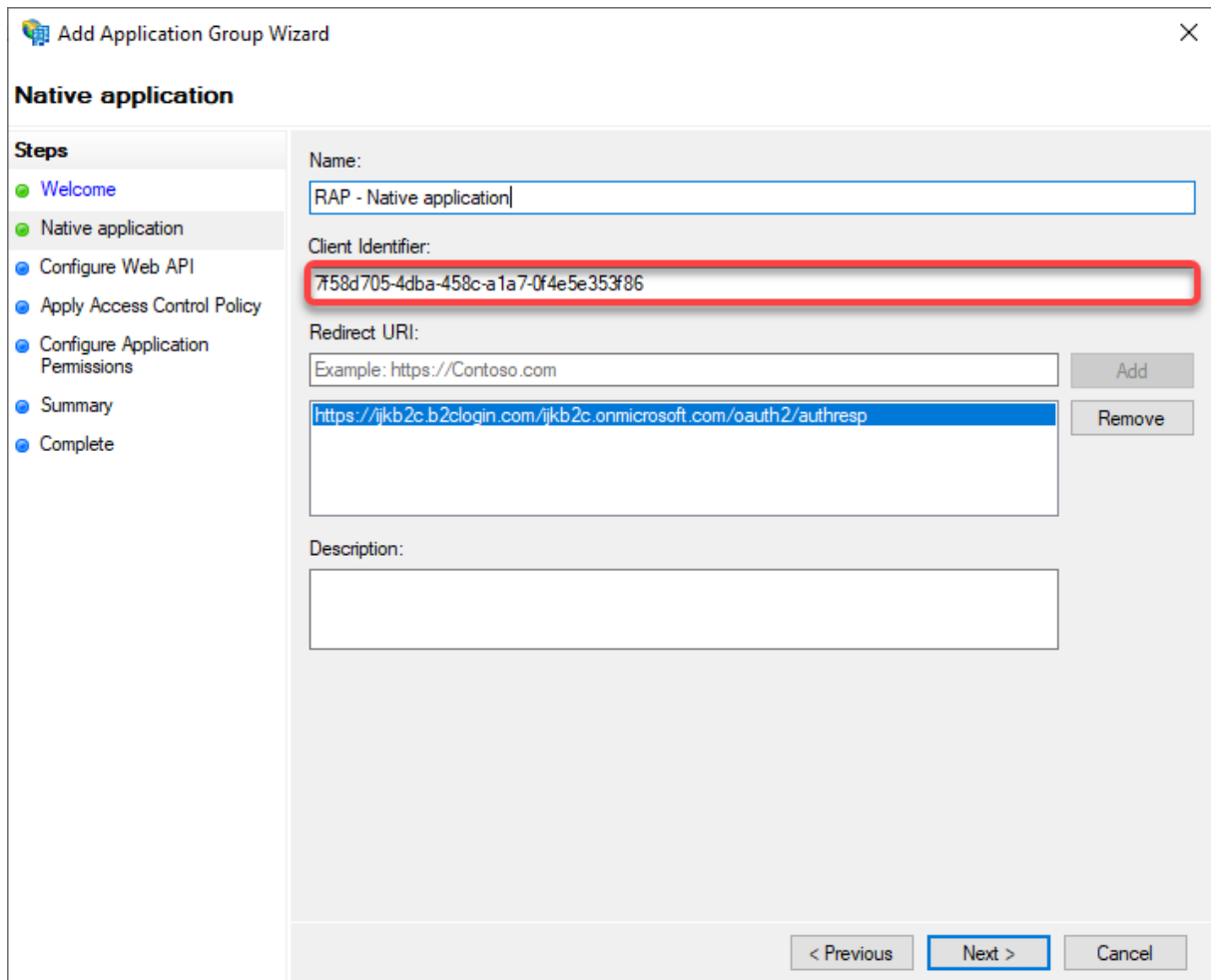
Druk op 'Next'

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.



The screenshot shows the 'Add Application Group Wizard' dialog box, specifically the 'Native application' step. The dialog has a title bar with a close button (X) and a Microsoft logo. On the left, there is a 'Steps' pane with a list of steps: Welcome, Native application (selected), Configure Web API, Apply Access Control Policy, Configure Application Permissions, Summary, and Complete. The main area contains the following fields and controls:

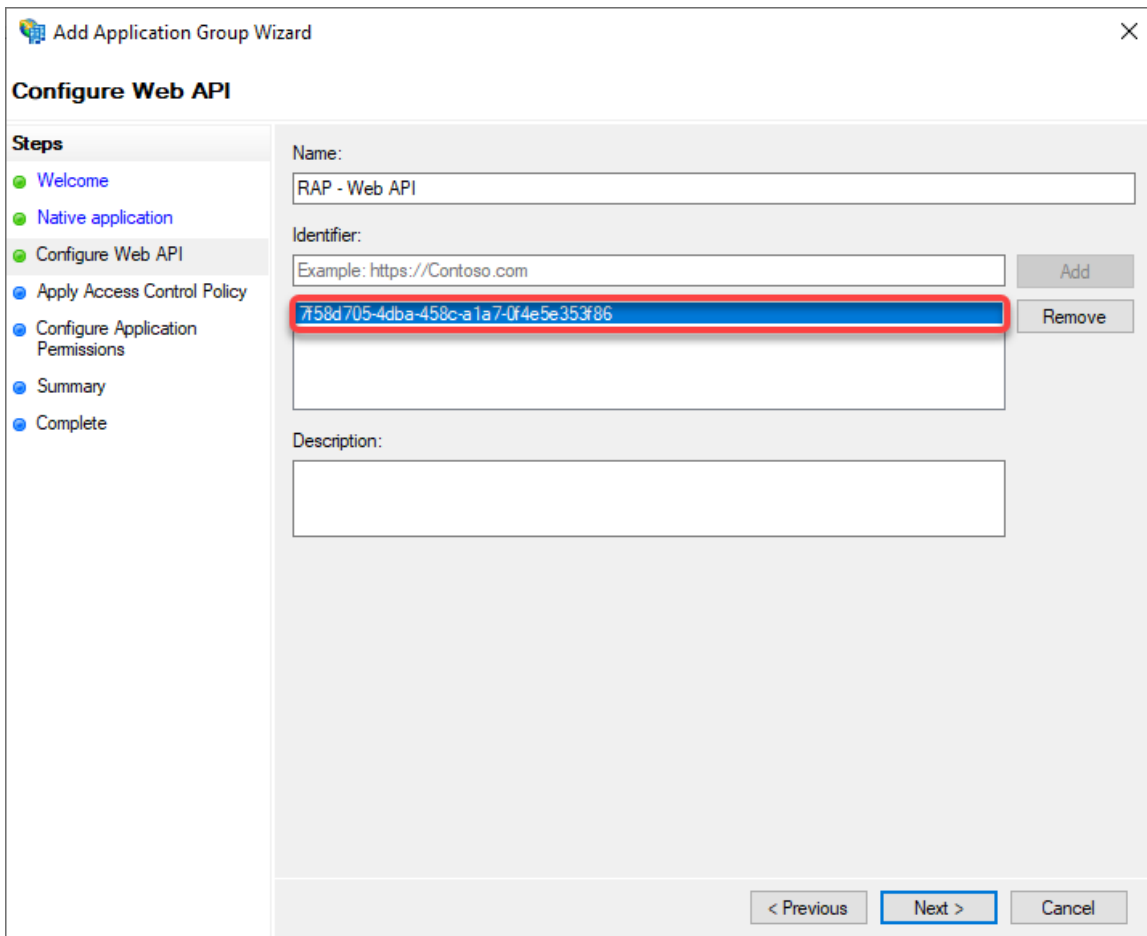
- Name:** A text box containing 'RAP - Native application'.
- Client Identifier:** A text box containing '7f58d705-4dba-458c-a1a7-0f4e5e353f86', which is highlighted with a red rectangular border.
- Redirect URI:** A text box with the placeholder 'Example: https://Contoso.com'. Below it, a list box contains the URL 'https://ijkb2c.b2clogin.com/ijkb2c.onmicrosoft.com/oauth2/authresp', which is selected. To the right of the list box are 'Add' and 'Remove' buttons.
- Description:** An empty text box.

At the bottom of the dialog, there are three buttons: '< Previous', 'Next >' (highlighted with a blue border), and 'Cancel'.

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 'Identificer' en druk op 'Add'.



The screenshot shows the 'Add Application Group Wizard' dialog box, specifically the 'Configure Web API' step. The dialog has a title bar with a close button (X) and a small icon. On the left, there is a 'Steps' pane with a list of steps: 'Welcome', 'Native application', 'Configure Web API' (highlighted), 'Apply Access Control Policy', 'Configure Application Permissions', 'Summary', and 'Complete'. The main area contains the following fields and controls:

- Name:** A text box containing 'RAP - Web API'.
- Identifier:** A text box with the placeholder 'Example: https://Contoso.com'. Below it, a list of identifiers is shown, with '7f58d705-4dba-458c-a1a7-0f4e5e353f86' selected and highlighted with a red border. To the right of the list are 'Add' and 'Remove' buttons.
- Description:** An empty text box.

At the bottom of the dialog, there are three buttons: '< Previous', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

Klik op 'Next'

Step 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.

The screenshot shows the 'Add Application Group Wizard' dialog box, specifically the 'Apply Access Control Policy' step. The dialog has a title bar with a close button (X) and a subtitle 'Add Application Group Wizard'. The main content area is titled 'Choose Access Control Policy'. On the left, there is a 'Steps' sidebar with the following items: Welcome, Native application, Configure Web API, Apply Access Control Policy (highlighted), Configure Application Permissions, Summary, and Complete. The main area contains a table of access control policies and a 'Policy' section.

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require MFA f...
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA f...
Permit everyone and require MFA from extranet access	Grant access to the intranet users and requir...
Permit everyone and require MFA from unauthenticated ...	Grant access to everyone and require MFA f...
Permit everyone and require MFA, allow automatic devi...	Grant access to everyone and require MFA f...
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more specifi...

Policy

Permit users from [] group

I do not want to configure the access control policy at this time. No users will be permitted access for this application.

< Previous Next > Cancel

Klik op 'Next'

Stap 6. Configure Application Permissions

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

The screenshot shows the 'Add Application Group Wizard' dialog box, specifically the 'Configure Application Permissions' step. The wizard is titled 'Add Application Group Wizard' and has a close button (X) in the top right corner. The main title is 'Configure Application Permissions'. On the left, there is a 'Steps' pane with the following items: Welcome, Native application, Configure Web API, Apply Access Control Policy, Configure Application Permissions (highlighted), Summary, and Complete. The main area contains the following text: 'Configure permissions to enable client applications to access this Web API.' Below this is the 'Client application (caller):' section, which contains a table with two columns: 'Name' and 'Description'. The table has one row: 'RAP - Native application'. Below the table are 'Add...' and 'Remove' buttons. The 'Permitted scopes:' section contains a table with two columns: 'Scope Name' and 'Description'. The table has the following rows: 'allatclaims' (unchecked), 'aza' (unchecked), 'email' (unchecked), 'logon_cert' (unchecked), 'openid' (checked and highlighted with a red box), 'profile' (unchecked), 'user_imperso...' (unchecked), and 'von_cert' (unchecked). Below the table is a 'New scope...' button. At the bottom of the dialog are '< Previous', 'Next >', and 'Cancel' buttons.

Steps

- Welcome
- Native application
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Configure permissions to enable client applications to access this Web API.

Client application (caller):

Name	Description
RAP - Native application	

Add... Remove

Permitted scopes:

Scope Name	Description
<input type="checkbox"/> allatclaims	Requests the access token claims in the identity token.
<input type="checkbox"/> aza	Scope allows broker client to request primary refresh token.
<input type="checkbox"/> email	Request the email claim for the signed in user.
<input type="checkbox"/> logon_cert	The logon_cert scope allows an application to request logon...
<input checked="" type="checkbox"/> openid	Request use of the OpenID Connect authorization protocol.
<input type="checkbox"/> profile	Request profile-related claims for the signed-in user.
<input type="checkbox"/> user_imperso...	Request permission for the application to access the resour...
<input type="checkbox"/> von_cert	The von_cert scope allows an application to request VPN ...

New scope...

< Previous Next > Cancel

Stap 7. Summary

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

Add Application Group Wizard

Summary

Steps

- Welcome
- Native application
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary**
- Complete

Review the following settings and click 'Next' to create the application.

Application Group

Name: RAP
Description: RAP SSO

Native application

Name: RAP - Native application
Identifier: 7f58d705-4dba-458c-a1a7-0f4e5e353f86
Redirect URLs:
https://ijkb2c.b2clogin.com/ijkb2c.onmicrosoft.com/oauth2/authresp

Web API

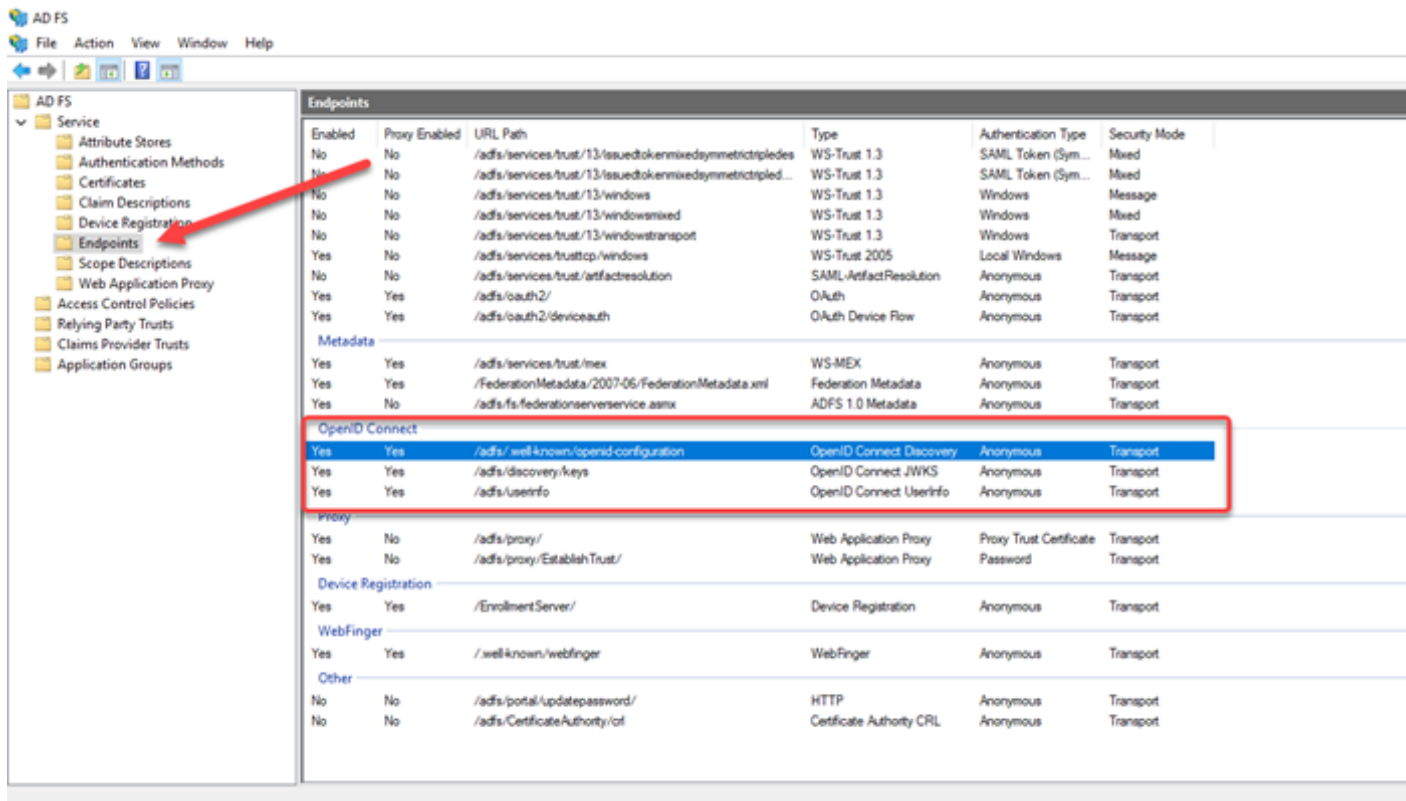
Name: RAP - Web API
Identifiers: 7f58d705-4dba-458c-a1a7-0f4e5e353f86
Access control policy: Permit specific group
Application permissions:
RAP - Native application - openid

< Previous **Next >** Cancel

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.

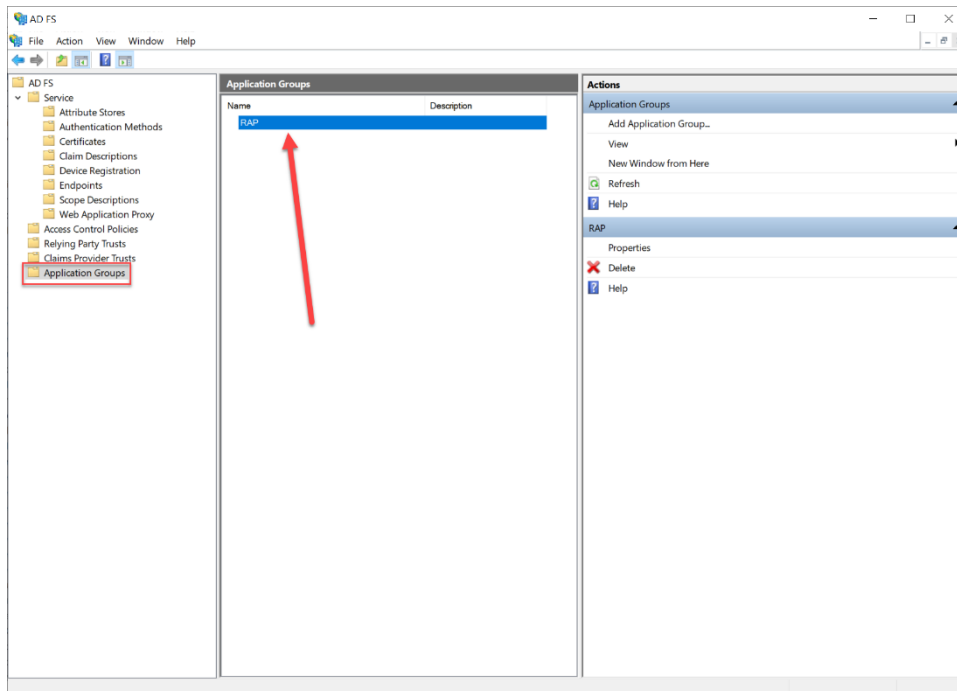


The screenshot shows the ADFS Management console interface. The left-hand navigation pane is expanded to 'Service' > 'Endpoints', with a red arrow pointing to the 'Endpoints' folder. The main area displays a table of endpoints. The 'OpenID Connect' section is highlighted with a red box, and the first three rows in this section are selected with a blue highlight.

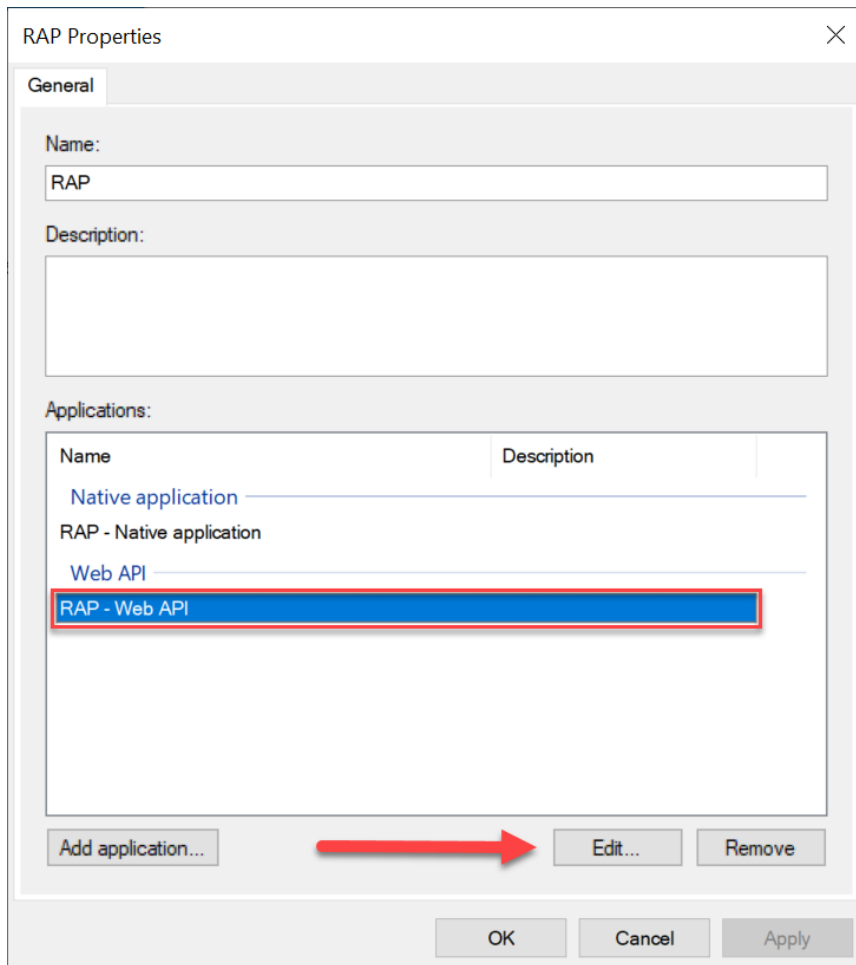
Enabled	Proxy Enabled	URL Path	Type	Authentication Type	Security Mode
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictriplede...	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictriple...	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/windows	WS-Trust 1.3	Windows	Message
No	No	/adfs/services/trust/13/windowsmixed	WS-Trust 1.3	Windows	Mixed
No	No	/adfs/services/trust/13/windowstransport	WS-Trust 1.3	Windows	Transport
Yes	No	/adfs/services/trusttp/windows	WS-Trust 2005	Local Windows	Message
No	No	/adfs/services/trust/artifactresolution	SAML-ArtifactResolution	Anonymous	Transport
Yes	Yes	/adfs/oauth2/	OAuth	Anonymous	Transport
Yes	Yes	/adfs/oauth2/deviceauth	OAuth Device Flow	Anonymous	Transport
Metadata					
Yes	Yes	/adfs/services/trust/mex	WS-MEX	Anonymous	Transport
Yes	Yes	/FederationMetadata/2007-05/FederationMetadata.xml	Federation Metadata	Anonymous	Transport
Yes	No	/adfs/fs.federationservice.asmx	ADFS 1.0 Metadata	Anonymous	Transport
OpenID Connect					
Yes	Yes	/adfs/.well-known/openid-configuration	OpenID Connect Discovery	Anonymous	Transport
Yes	Yes	/adfs/discovery/keys	OpenID Connect JWKS	Anonymous	Transport
Yes	Yes	/adfs/userinfo	OpenID Connect UserInfo	Anonymous	Transport
Proxy					
Yes	No	/adfs/proxy/	Web Application Proxy	Proxy Trust Certificate	Transport
Yes	No	/adfs/proxy/EstablishTrust/	Web Application Proxy	Password	Transport
Device Registration					
Yes	Yes	/EnrollmentServer/	Device Registration	Anonymous	Transport
WebFinger					
Yes	Yes	/.well-known/webfinger	WebFinger	Anonymous	Transport
Other					
No	No	/adfs/portal/updatepassword/	HTTP	Anonymous	Transport
No	No	/adfs/CertificateAuthority/cf	Certificate Authority CRL	Anonymous	Transport

Stap 9. Toevoegen Transform Rules

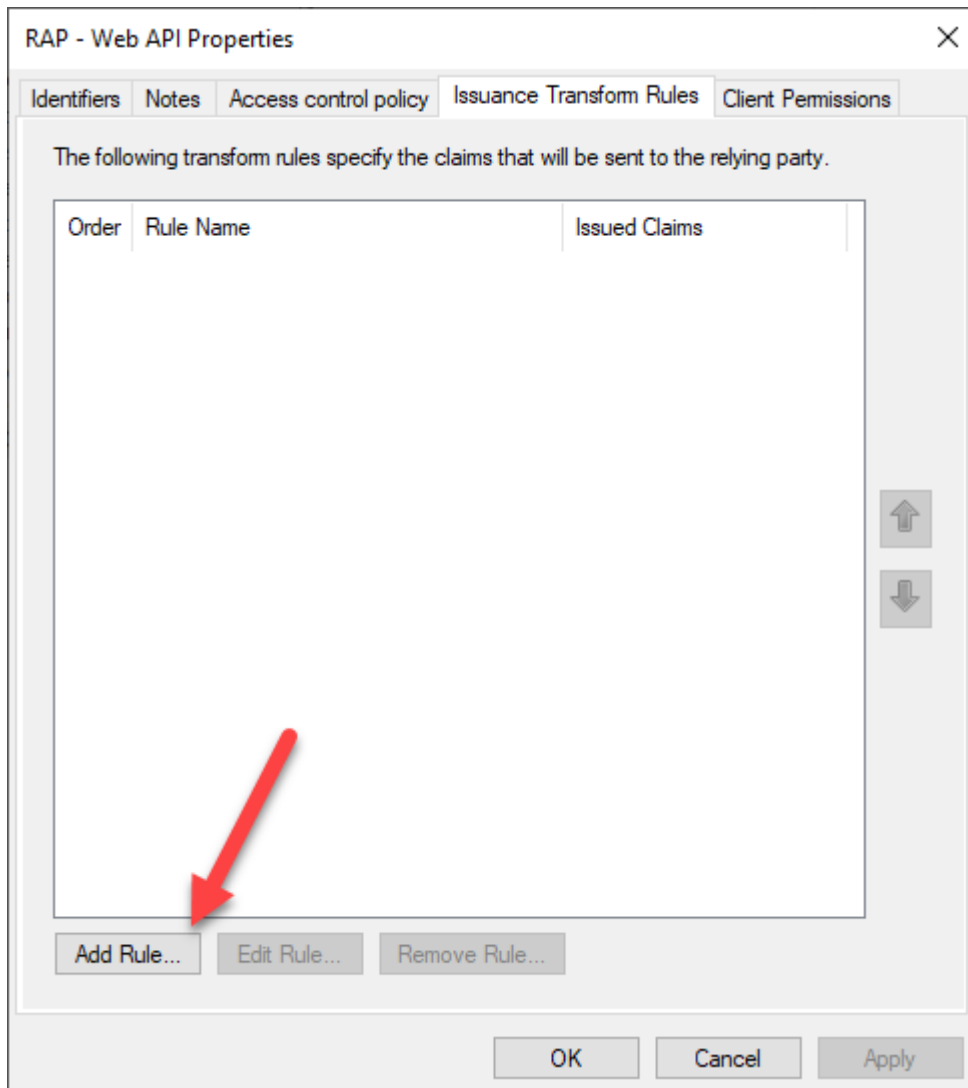
Ga terug naar 'Application Groups' en klik op de eerder aangemaakte application group 'RAP'.



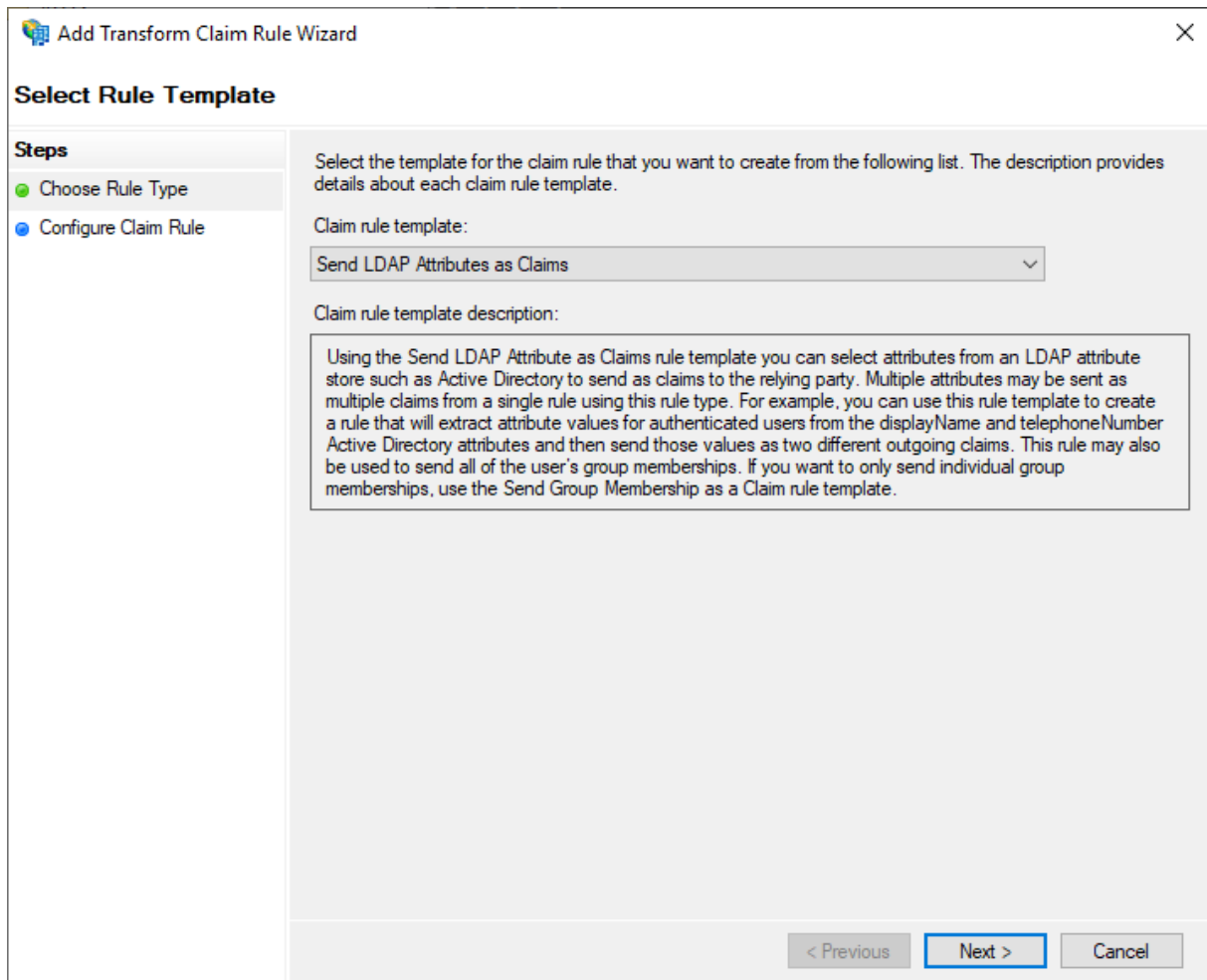
Druk vervolgens op de web api 'RAP – WEB API' en daarna op 'Edit...'



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:

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
*	<input type="text"/>	<input type="text"/>

< Previous Finish Cancel

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 waarden ziet het scherm er zo uit. Controleer dit en klik vervolgens op 'OK'.

Edit Rule - LDAP Rule [X]

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
LDAP Rule

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	Given-Name	given_name
	E-Mail-Addresses	email
▶	Surname	family_name
•		

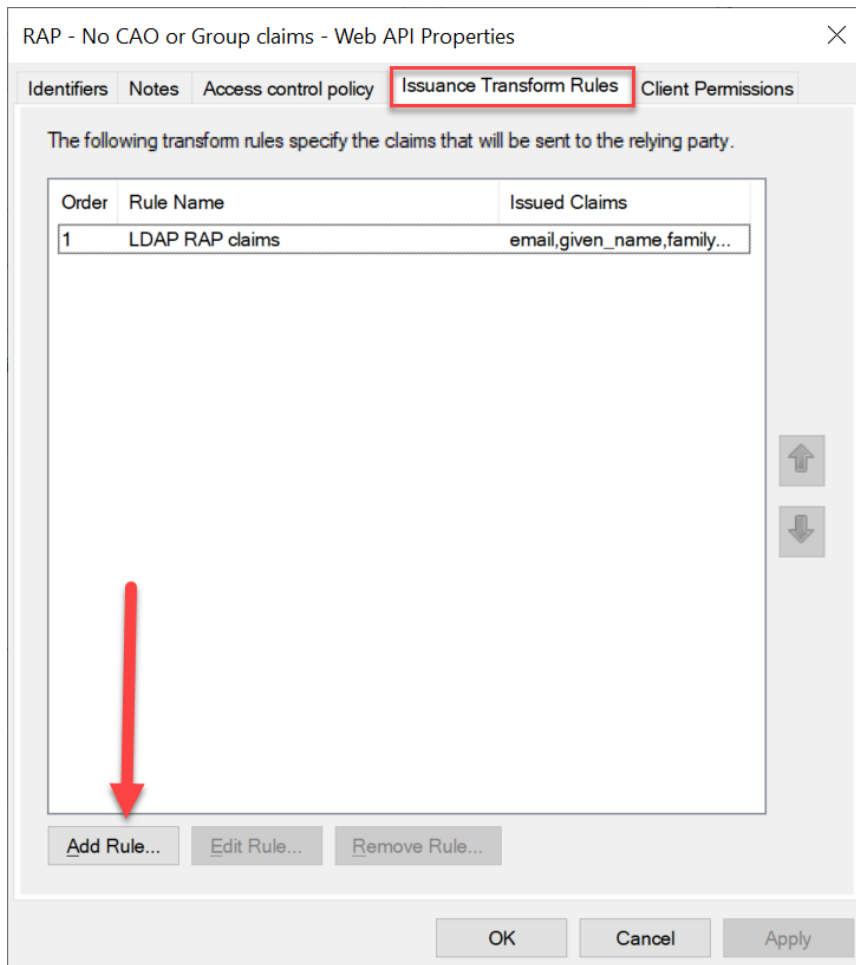
View Rule Language... [OK] [Cancel]

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 'Insurance 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:
[redacted]

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

Add Transform Claim Rule Wizard [Close]

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:

Rule template: Send Group Membership as a Claim

User's group:

Outgoing claim type:

- V2 Template Name
- V1 Template Name
- Thumbprint
- X.509 Version
- Inside Corporate Network
- Password Expiration Time
- Password Expiration Days
- Update Password URL
- Authentication Methods References
- Client Request ID
- Alternate Login ID
- Account Store
- Anchor Claim Type
- OAuth Client Id
- OAuth Client Type
- Device compliance status
- Device Usage Time
- Is Known Device
- Persistent Single Sign On
- Primary Refresh Token
- Scope of access
- Windows device group
- Windows deny-only device group
- Device Trust Type
- User IP
- Authentication Methods Provider
- Token Binding Id
- Multifactor Authentication time stamp
- Ceo
- Groups

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.

