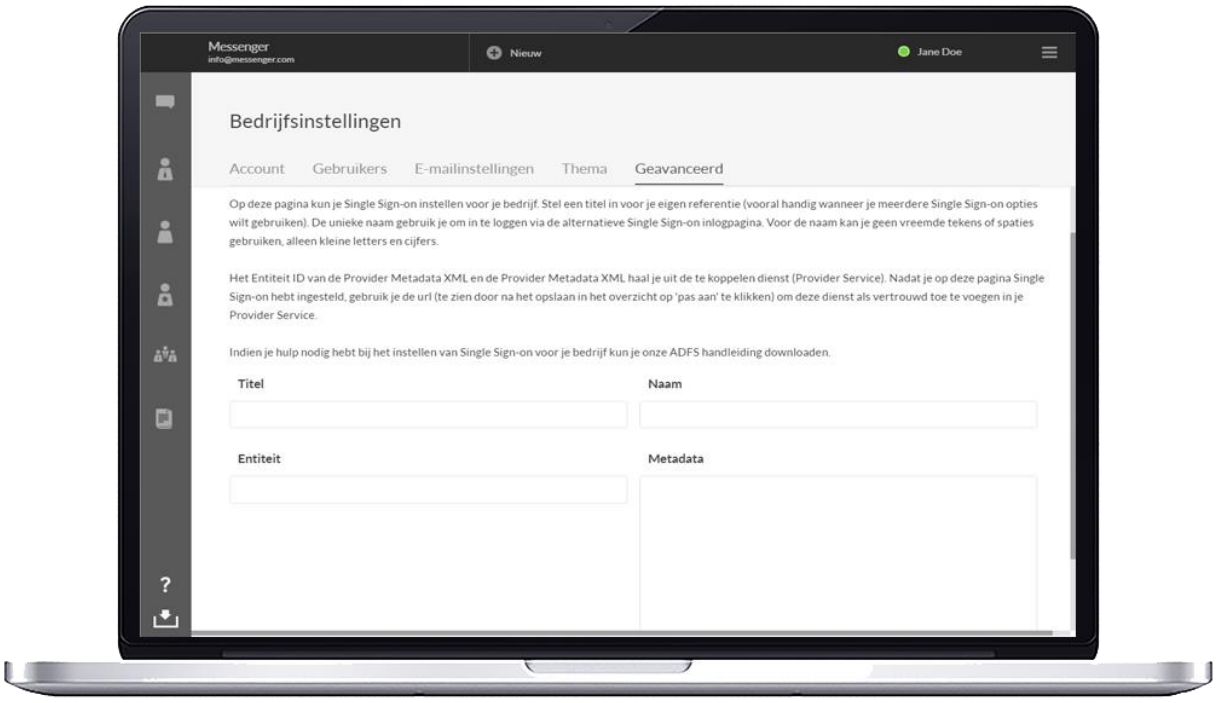
ADFS INSTELLEN

EEN HANDLEIDING



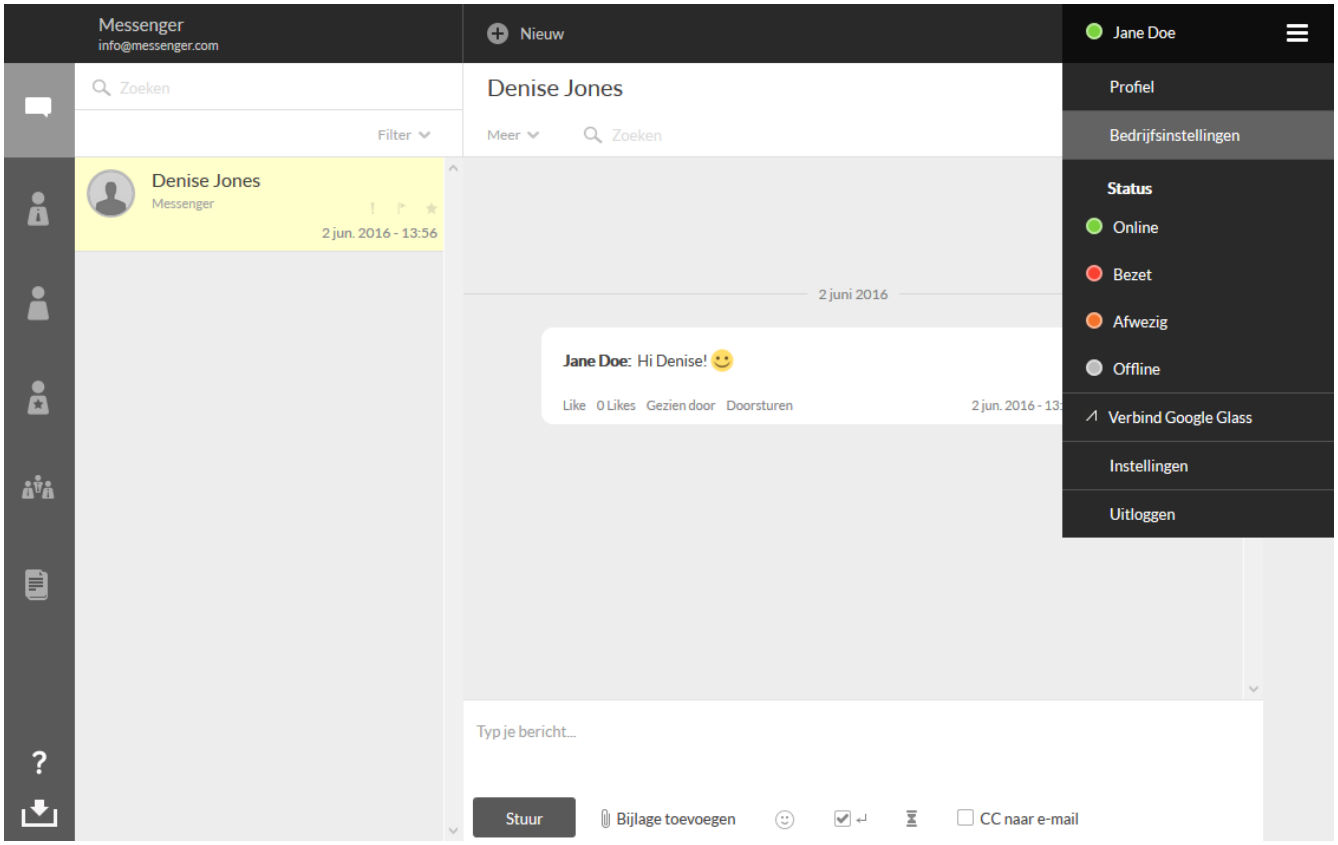
ZAURUS

Inhoud

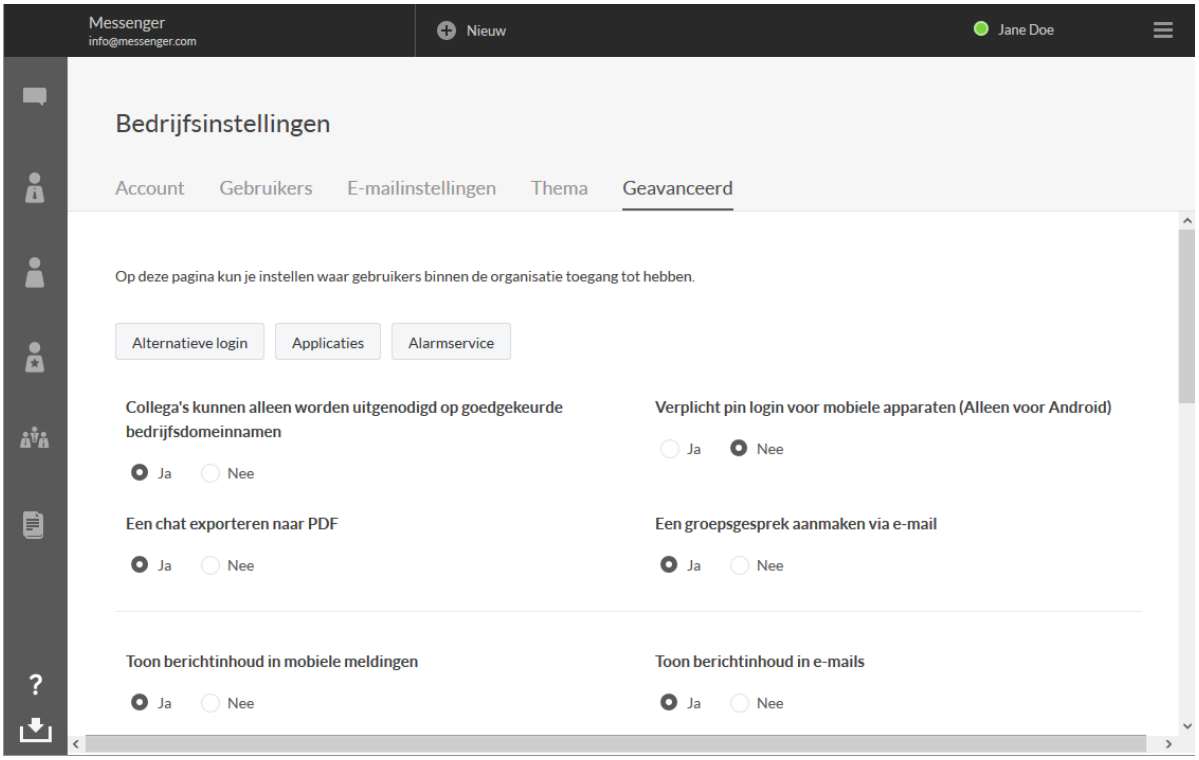
Voor je op de ADFS server de instellingen aanpast

Log in bij de messenger met een account met administrator rechten – je vindt dan op de webversie rechts bovenin onder de dropdown de optie ‘Bedrijfsinstellingen’.

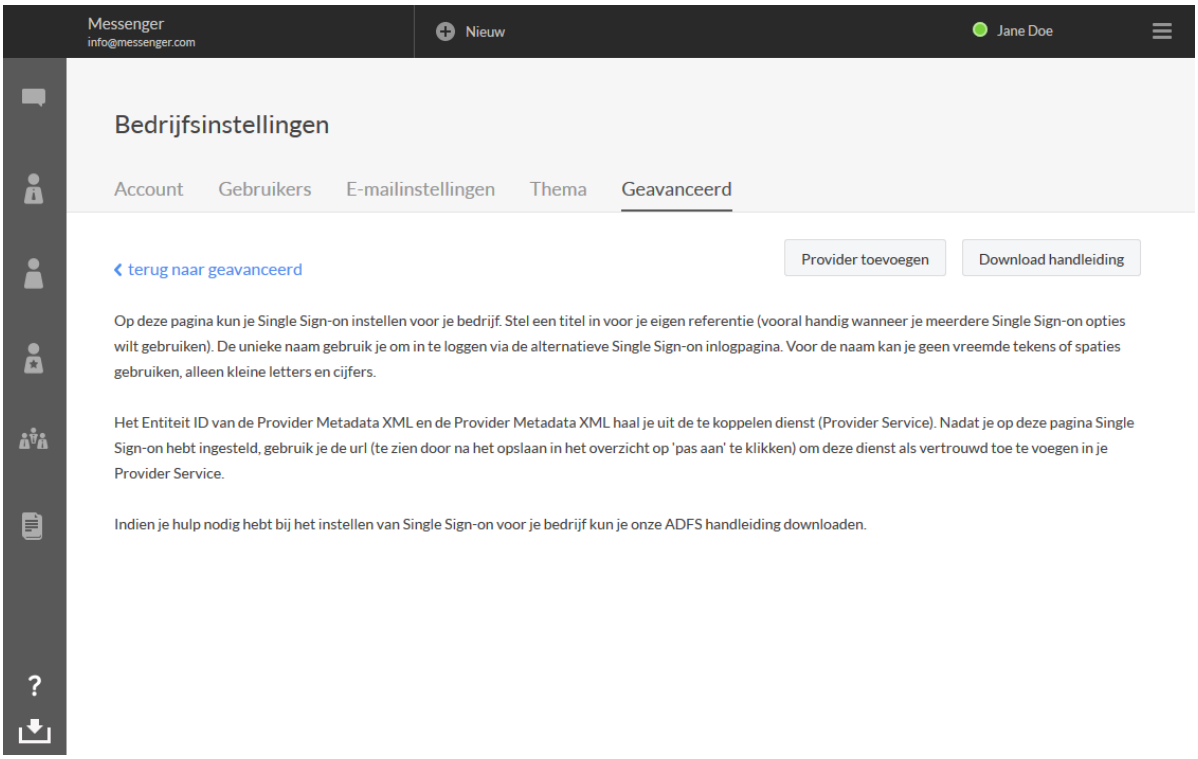
Klik op ‘Bedrijfsinstellingen’.



Vervolgens klik je op de meest rechter tab: ‘Geavanceerd’.



Hier zie je bovenin drie buttons. Kies de meest linker: ‘Alternatieve login’. Rechts bovenin zie je hier de optie ‘Provider toevoegen’. Klik hierop om de benodigde invoervelden te tonen.



Voer vervolgens e.e.a. als volgt in:

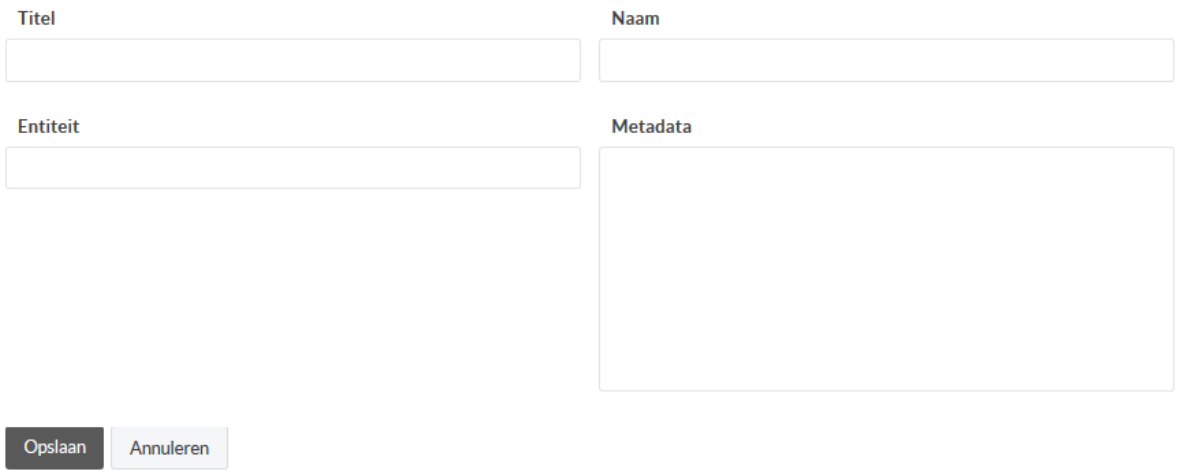
Titel: Dit zie je terug als Administrator – kies dus een titel die voor jouzelf helder is.

Naam: Dit is de naam waarmee je eindgebruikers verbinding maken met de ADFS infrastructuur.

Entiteit: Dit is de URL van de ADFS server, bijvoorbeeld https://adfs.COMPANY.com/adfs/services/trust

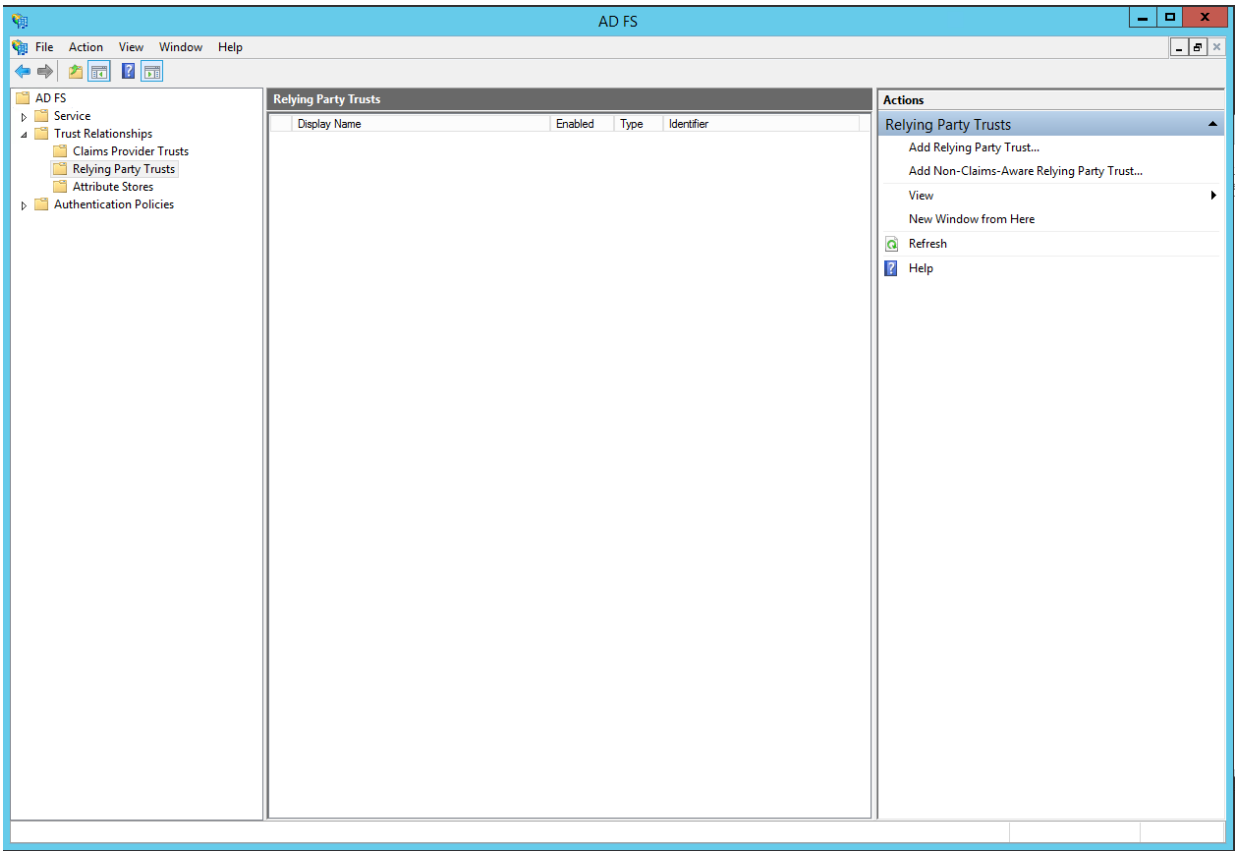
Metadata: Plak hier de informatie uit de federationmetadata.xml die je hebt opgehaald van de ADFS server. De directe URL heeft dit format: https://adfs.COMPANY.com/federationmetadata/2007-06/federationmetadata.xml

Na het opslaan van deze instellingen genereert de messenger een URL voor je, die je moet gebruiken voor de configuratie van de ADFS op de ADFS server.



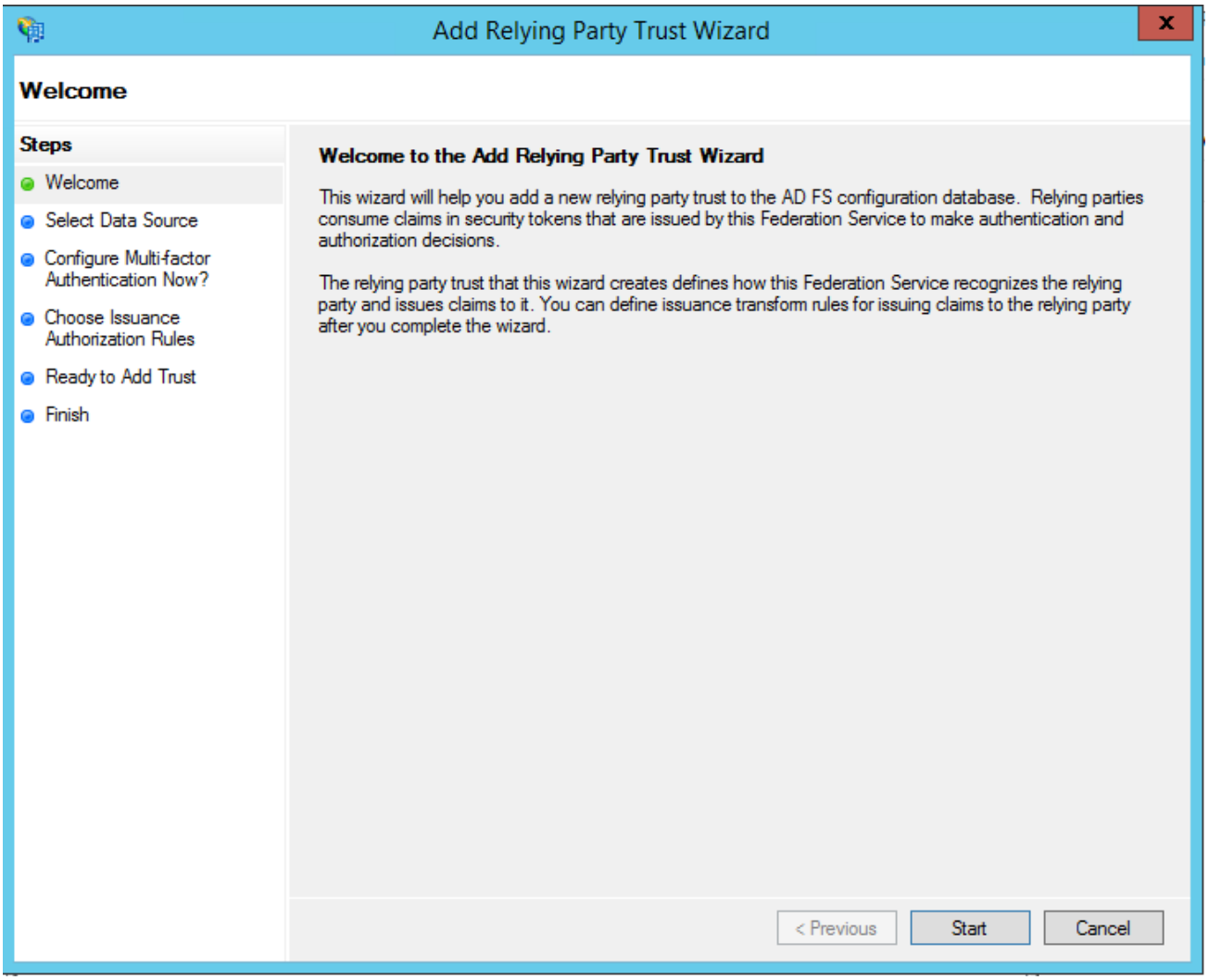
ADFS instellen

Open de ADFS management console op de ADFS server.



Relying Party Trust toevoegen

Klik op ‘Add Relying Party Trust’ in de rechter kolom. Het volgende introscherm verschijnt – klik op ‘Start’.

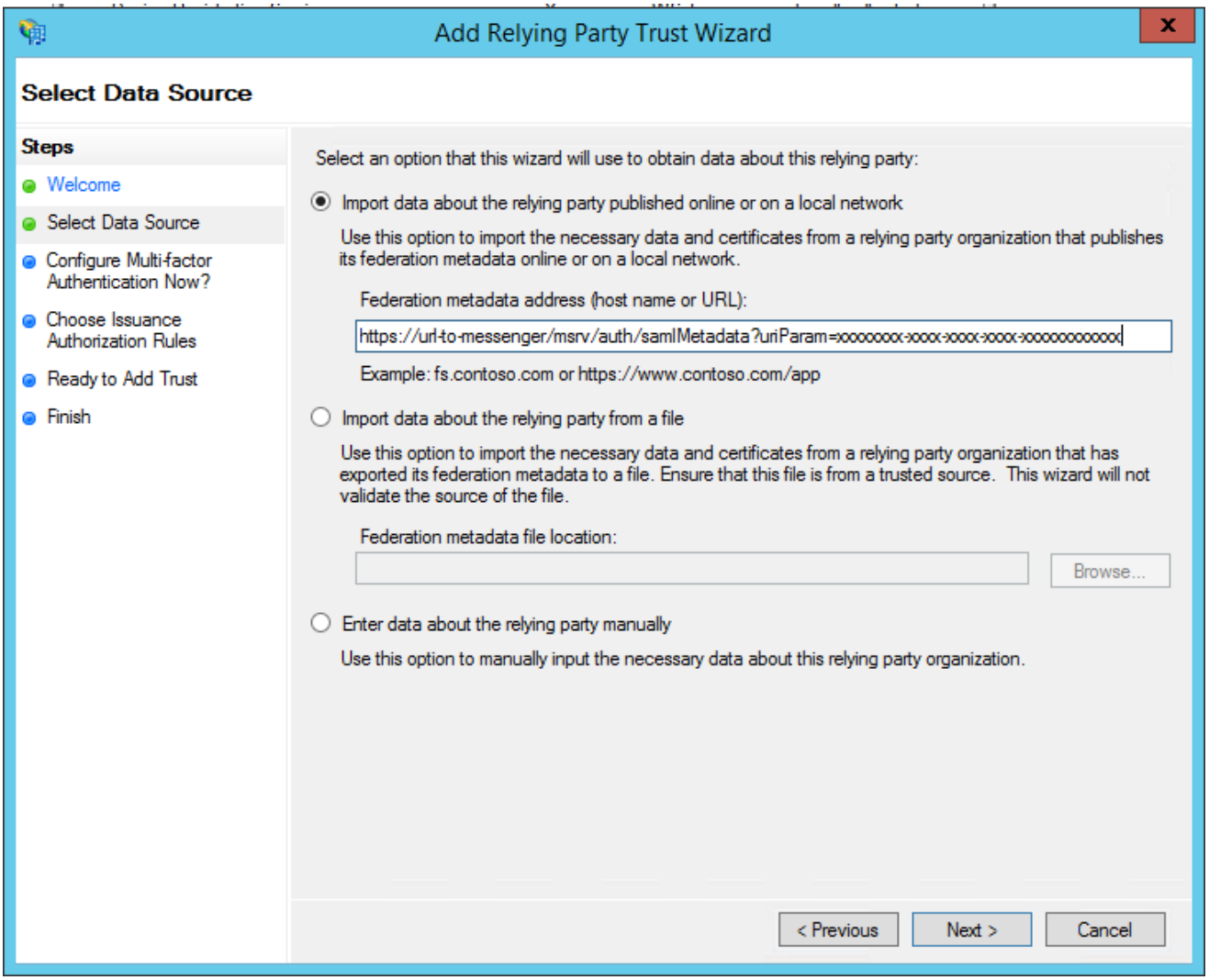


Vervolgens verschijnt het scherm om de federation metadata op te geven. Deze heeft een format gelijk aan: https://url-to-messenger/msrv/auth/samlMetadata?uriParam=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

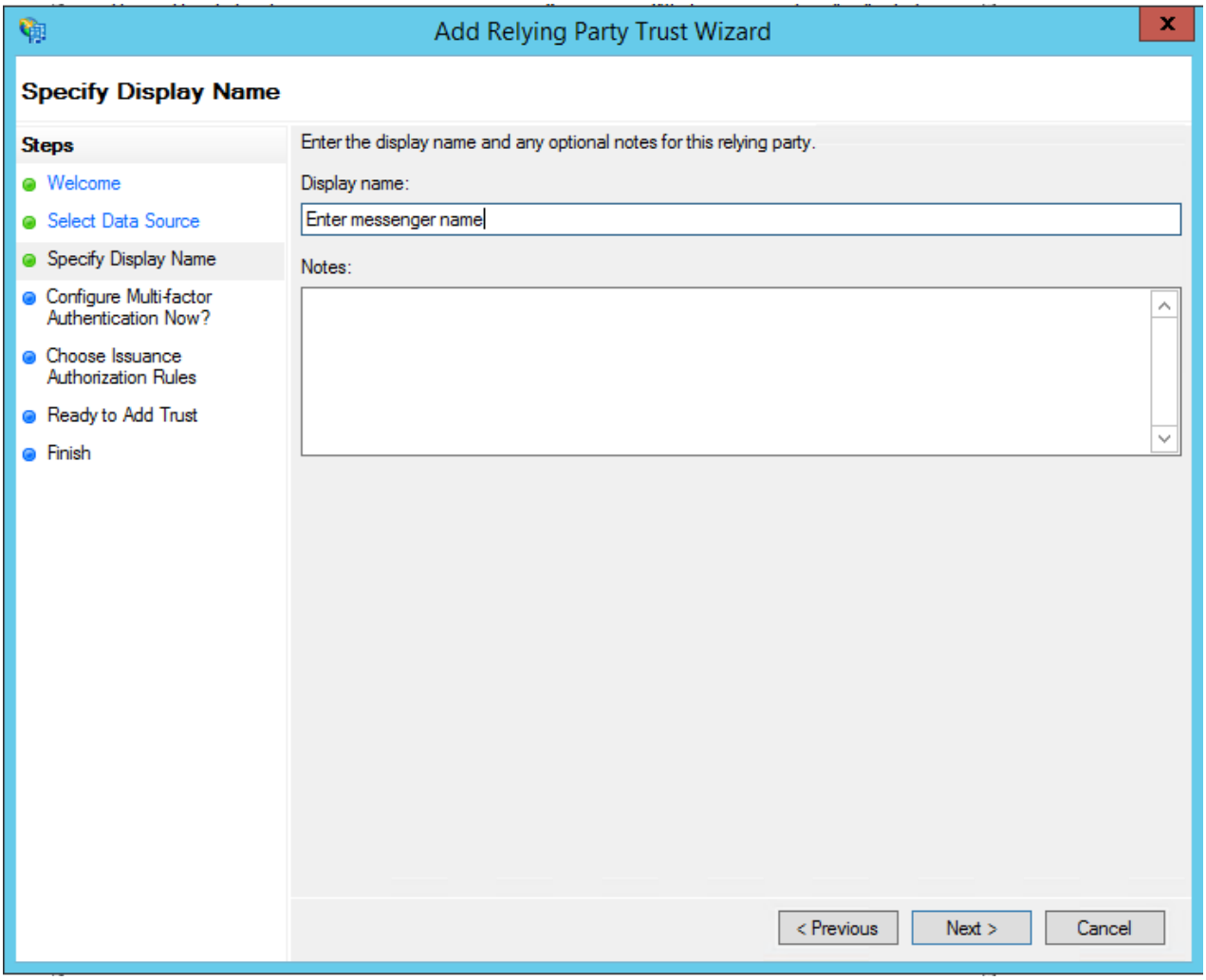
De ‘xxxx’ key bestaat uit een unieke code die voor ieder bedrijf anders is en wordt gegenereerd op basis van de inhoud van het MetaData veld.

Deze URL heb je als het goed is gegenereerd door de eerste stappen van deze handleiding te doorlopen.

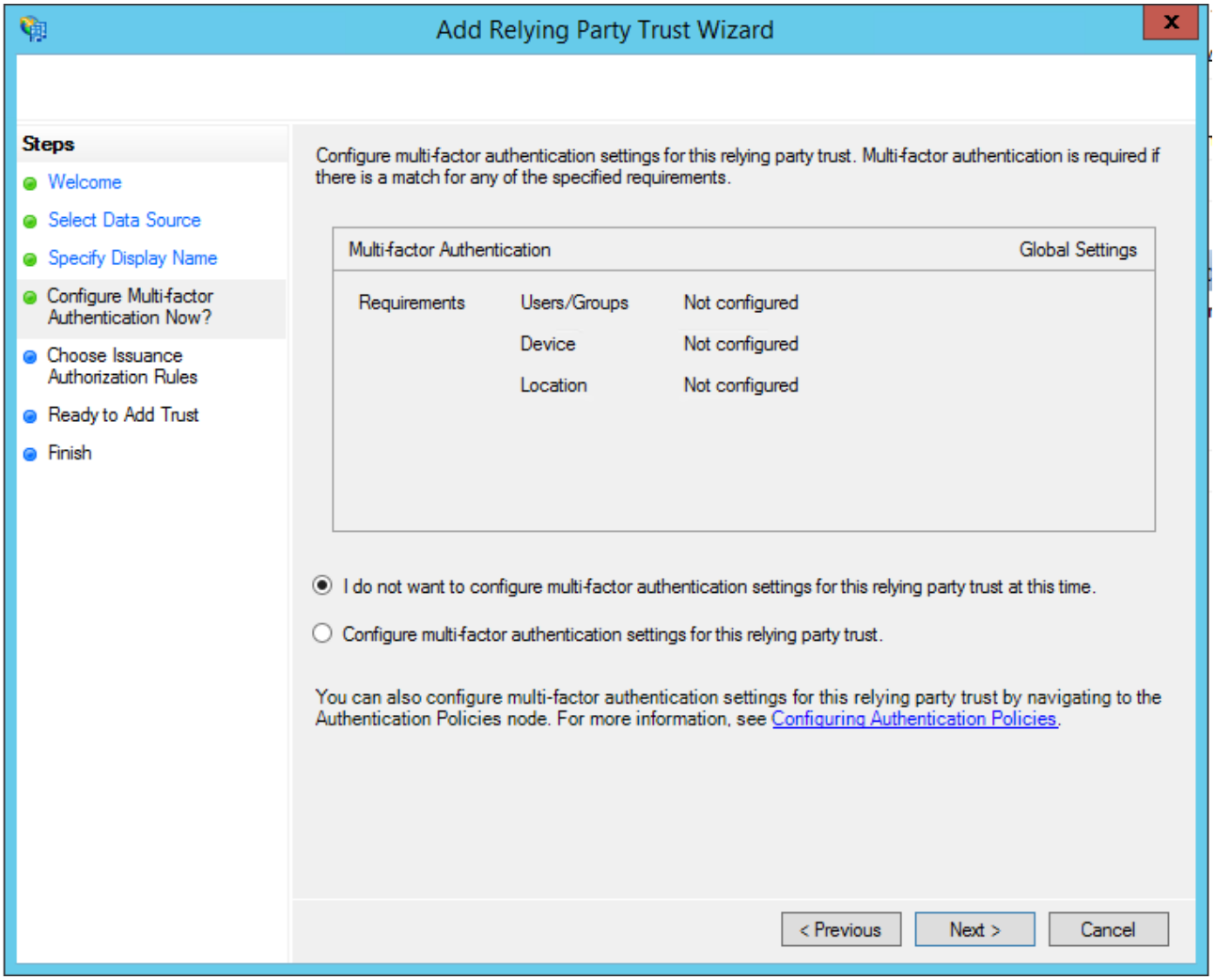
Vul de Relying Party Trust URL in en klik op ‘Next’.



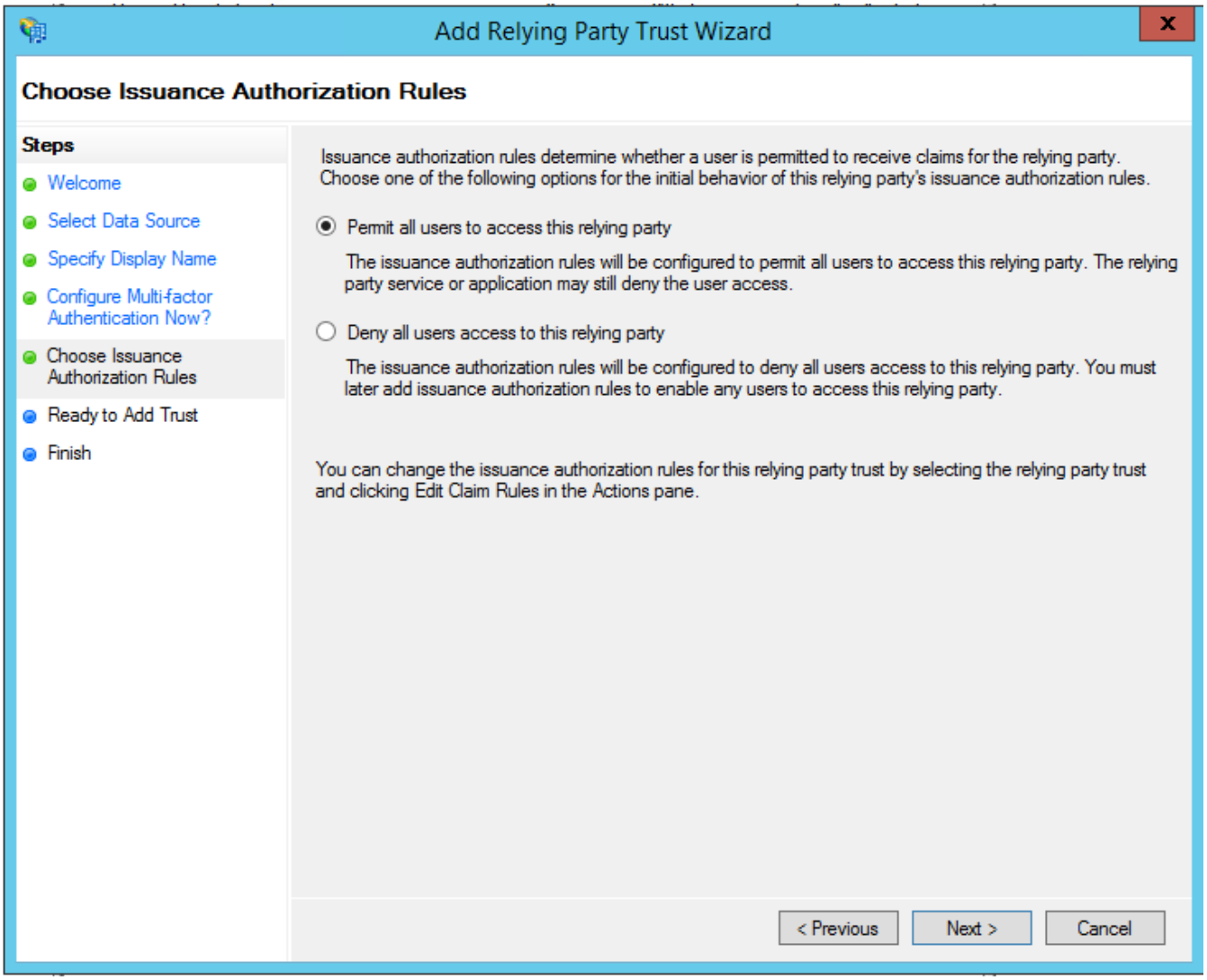
Het volgende scherm is naar wens in te vullen. Klik daarna op ‘Next’.



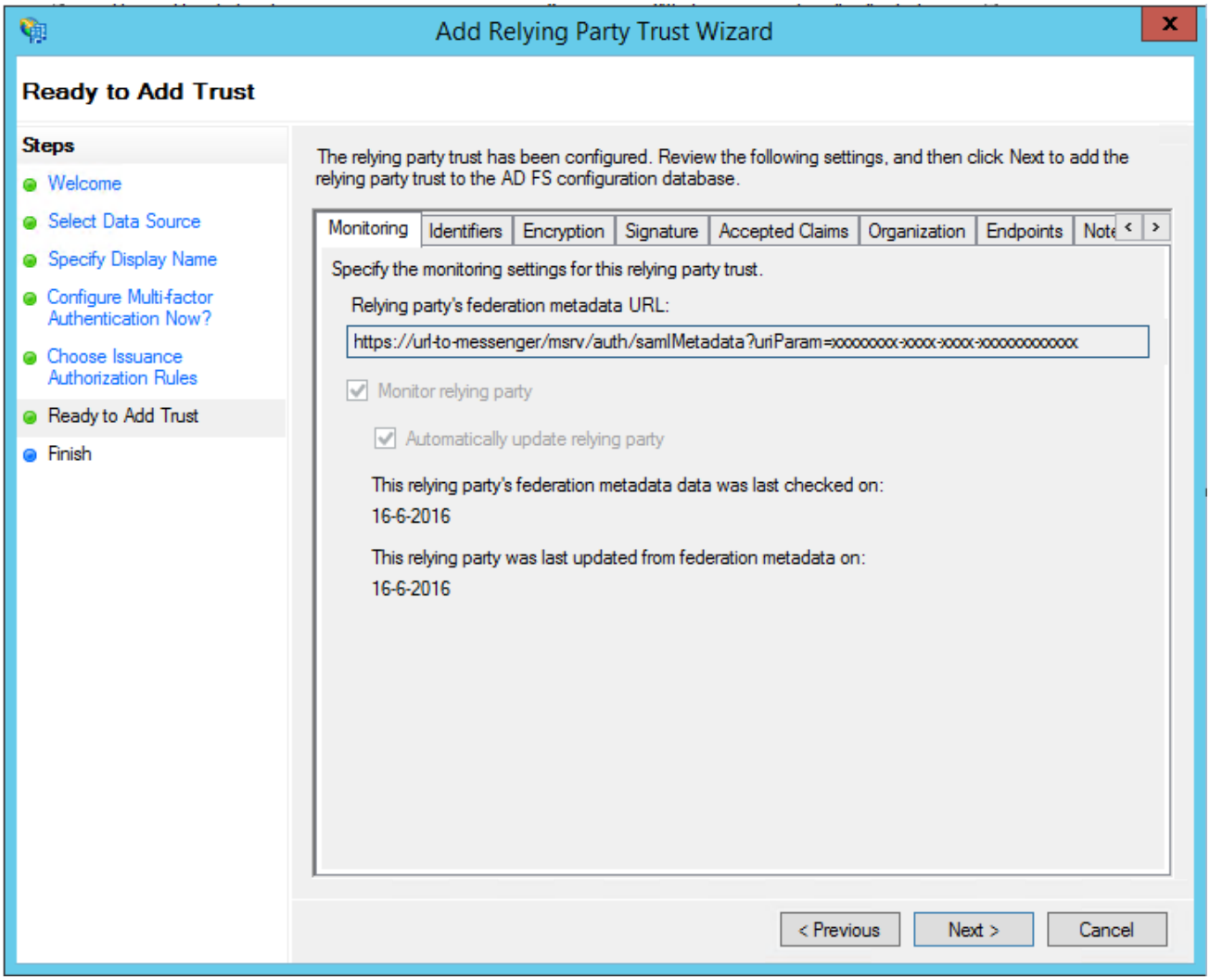
Dan verschijnt het volgende scherm, voor de messenger kun je dit negeren – klik dus op ‘Next’.



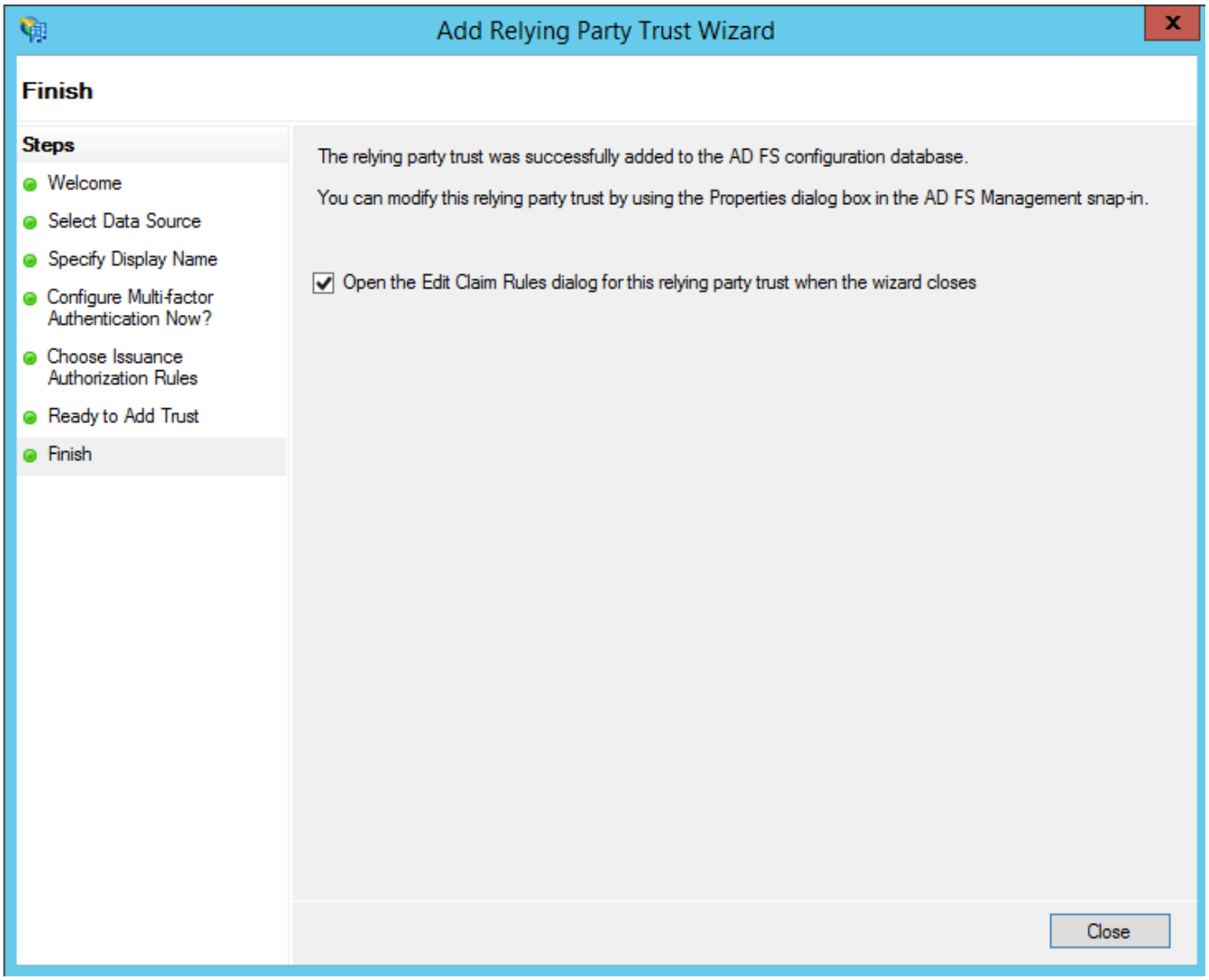
Dan verschijnt het volgende, voor onze messenger zijn de standaard instellingen goed. Klik op ‘Next’.



Vervolgens verschijnt er nog een samenvatting, klik wederom op ‘Next’.

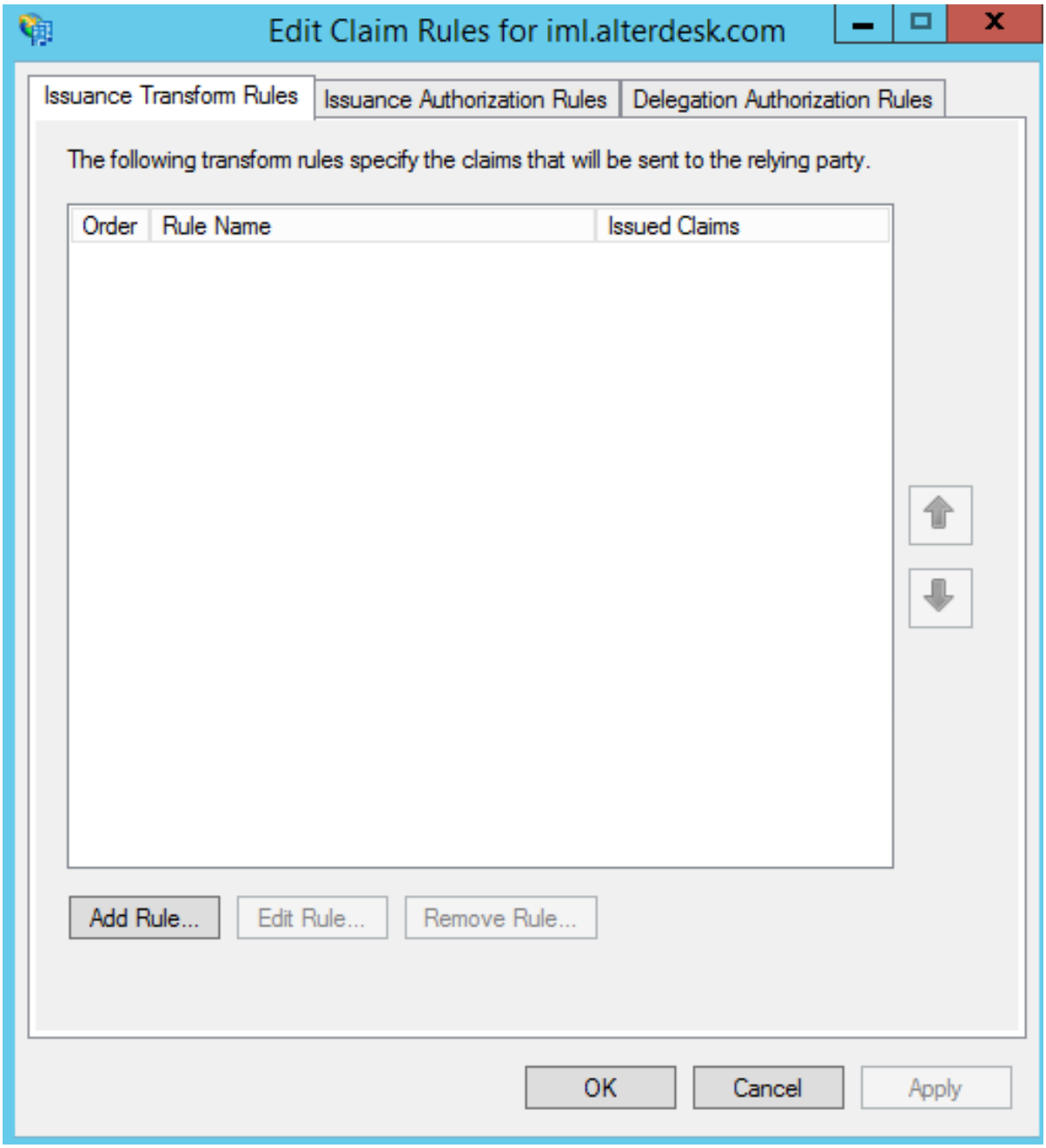


Uiteindelijk kom je op een Finish scherm. Het vinkje voor de Claim Rules kan aanblijven, want deze moeten ook worden geconfigureerd. Klik op ‘Close’.



Claim Rules instellen

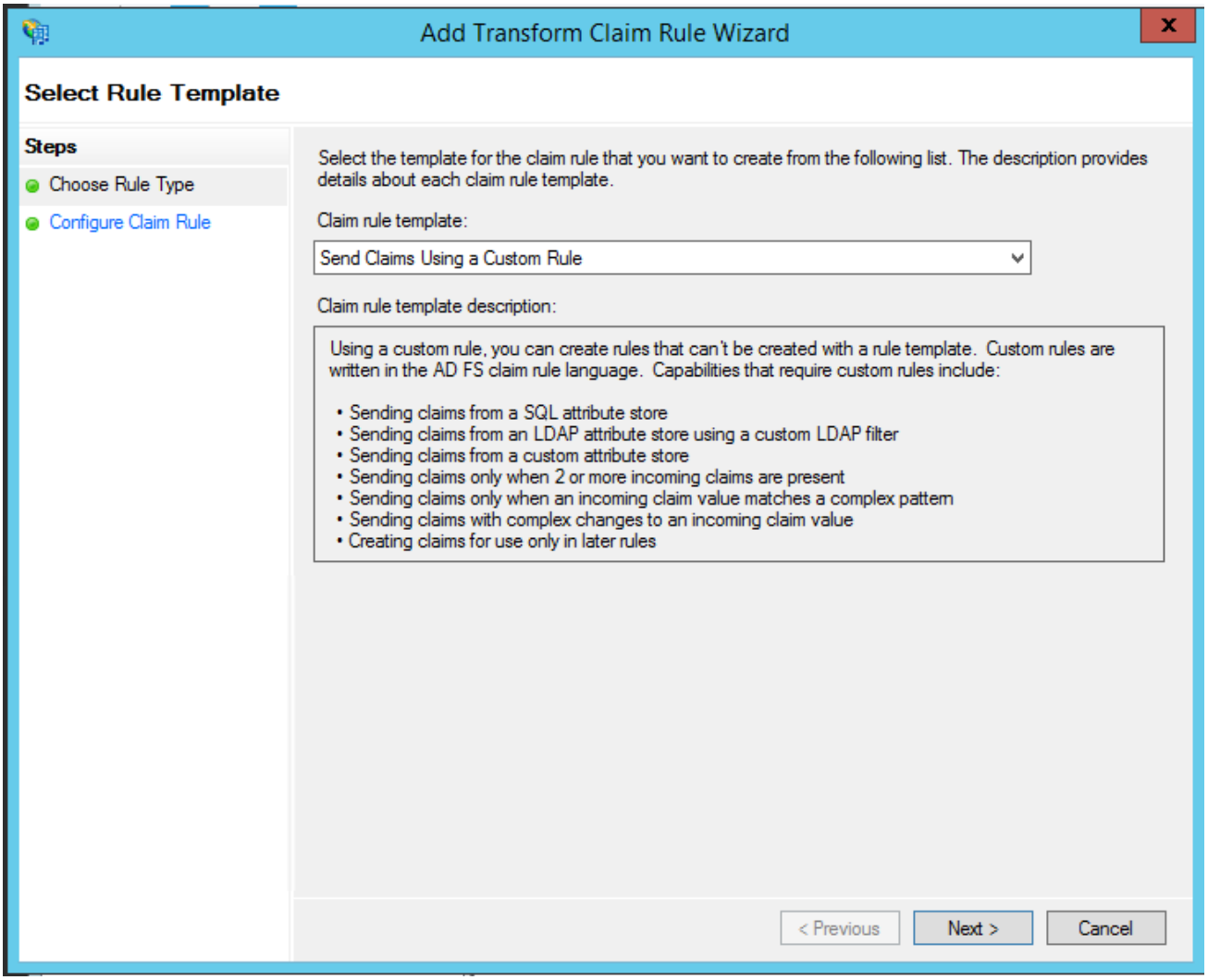
Vervolgens wordt het ‘Edit Claim Rules’ scherm geopend.



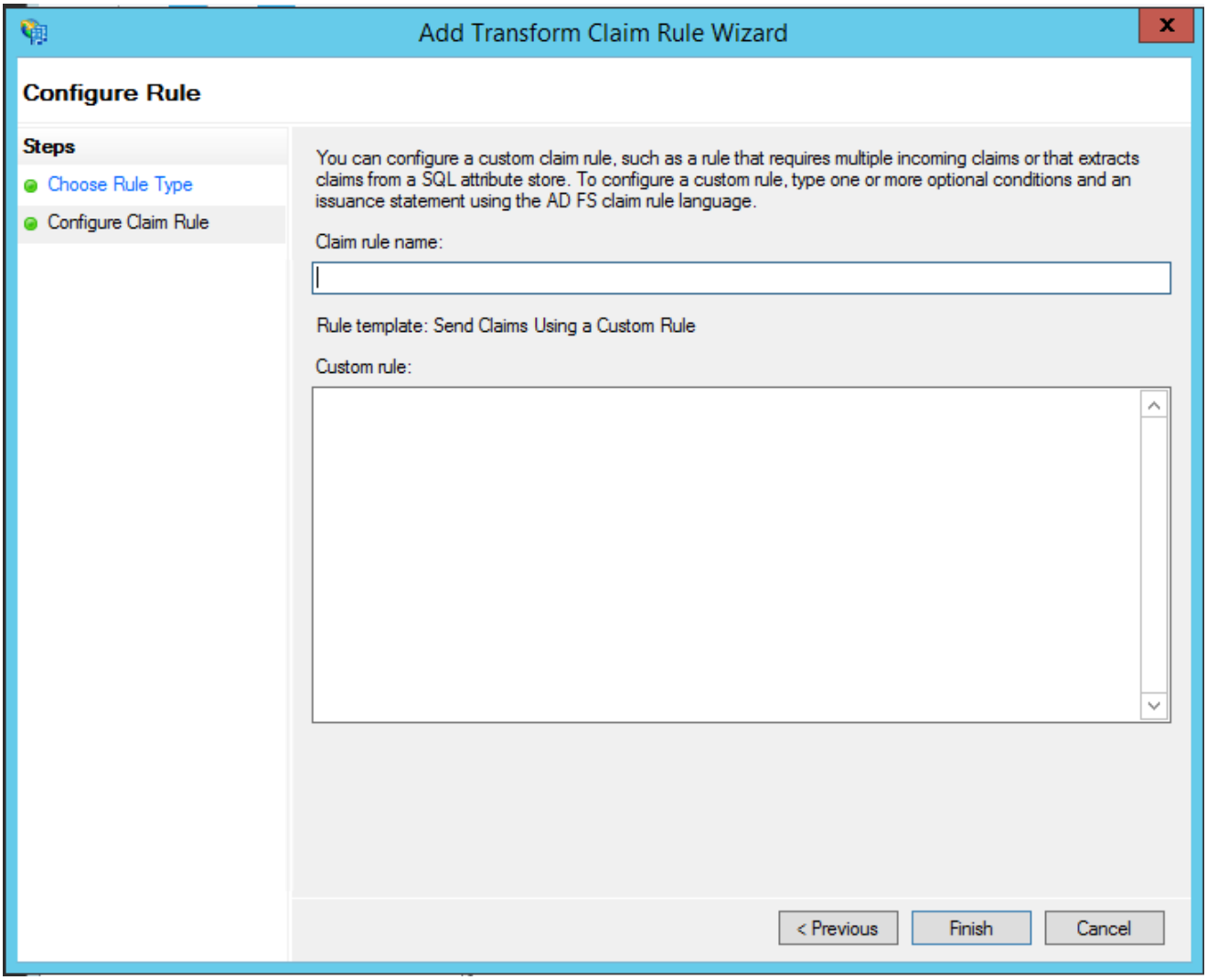
In de ‘Claim Rules settings’ moeten 3 rules worden aangemaakt.

De eerste 2 zijn ervoor om de unieke accountnaam van de gebruiker om te zetten naar een voor de messenger bruikbaar formaat. Kies voor Regel 1 en Regel 2 voor ‘Add Rule’.

Kies voor ‘Send Claims Using a Custom Rule’ en klik op ‘Next’.



Vervolgens zie je onderstaand scherm, waarin je je Custom Rules kunt invoeren. Deze staan op de volgende pagina.



Rule 1

Rule 1 bevat de volgende ‘Custom Rule’:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"]
 => issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/windowsaccountname"), query =
";samaccountname;{0}", param = c.Value);
```

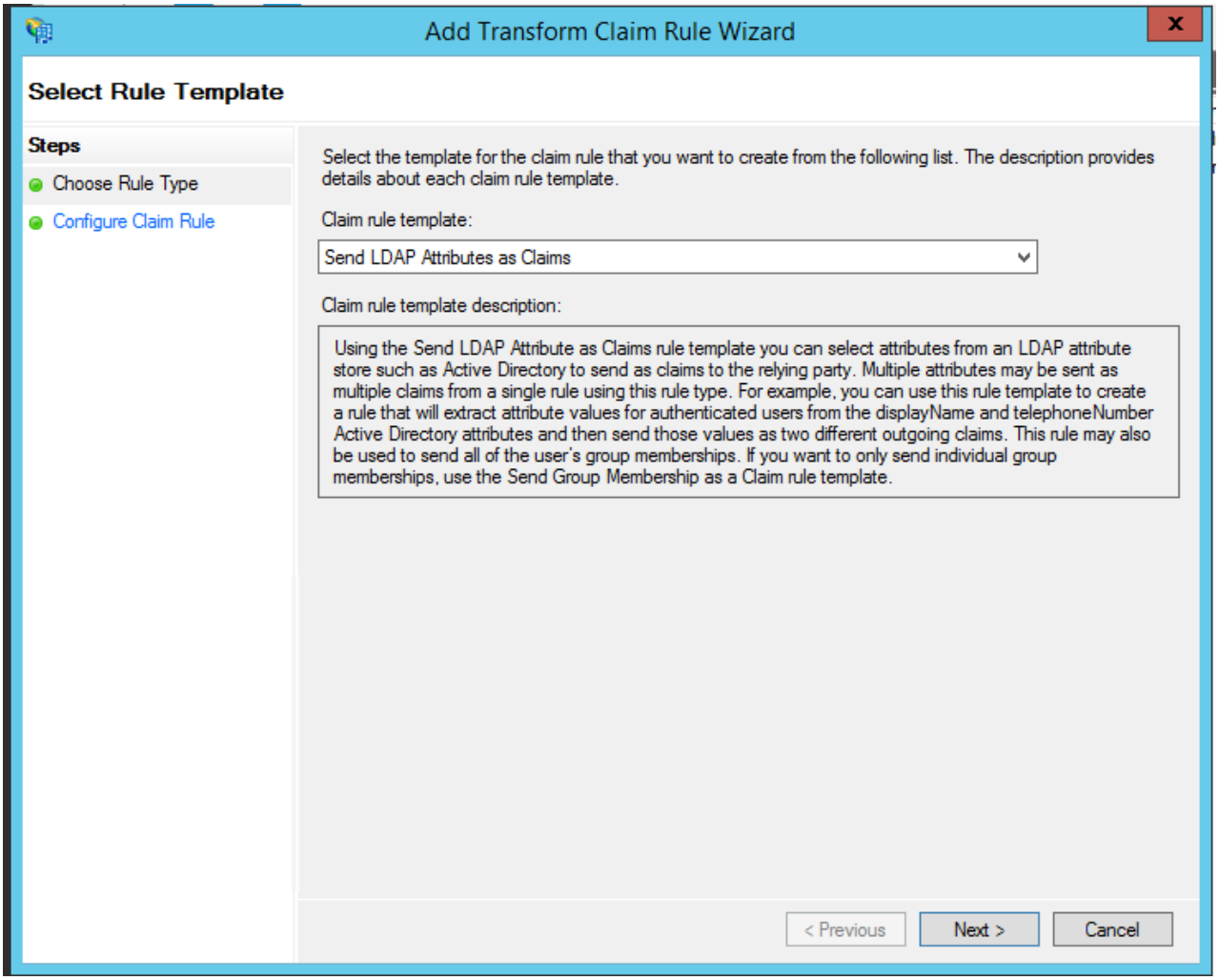
Rule 2

Rule 2 bevat de volgende ‘Custom Rule’:

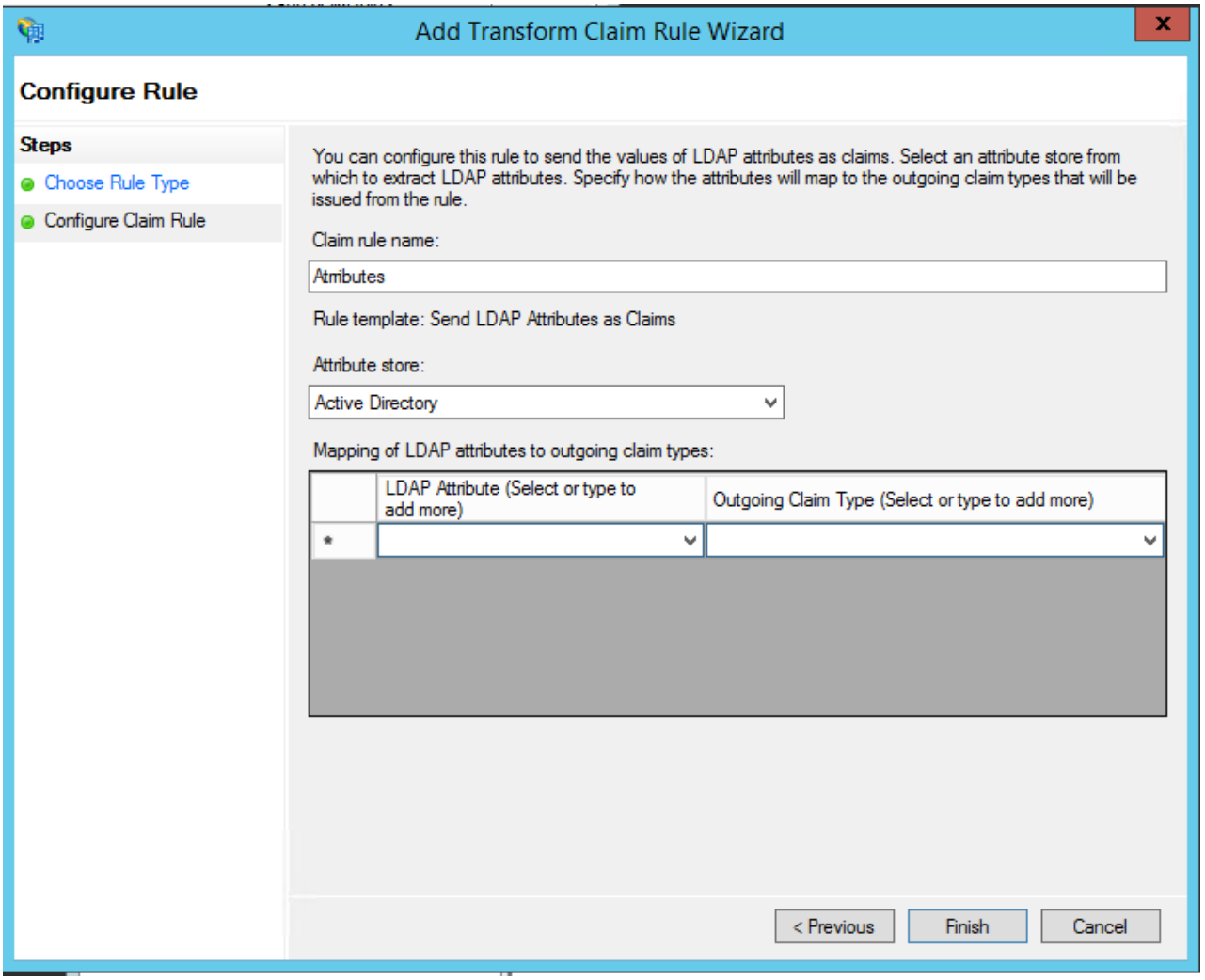
```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/windowsaccountname"]

 => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient");
```

Rule 3

Kies voor Regel 3 ‘Add Rule’.
Kies vervolgens voor ‘Send LDAP Attributes as Claims’ en klik op ‘Next’.



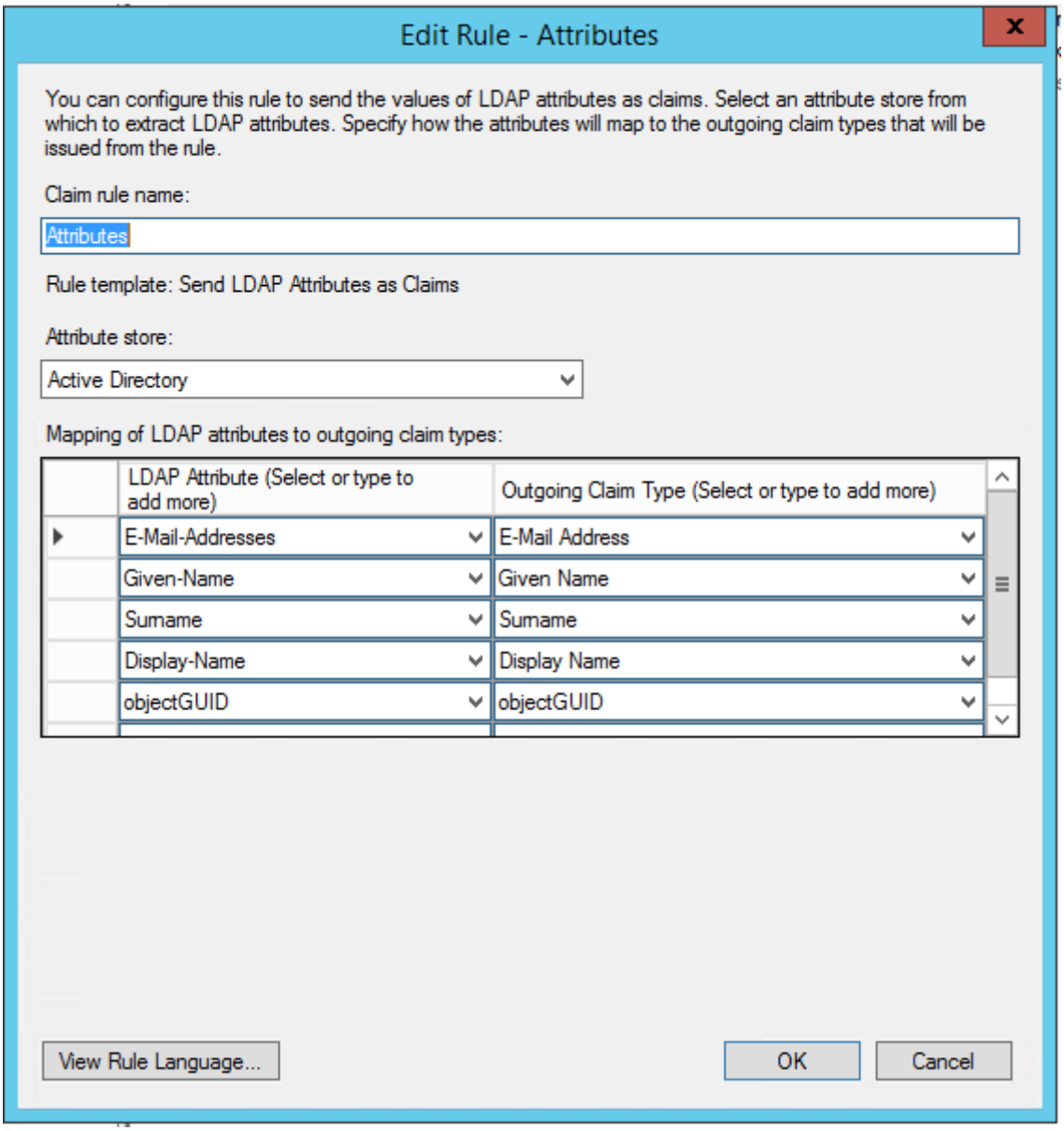
Geef de regel een naam. In het voorbeeld is ‘Attributes’ gebruikt. Kies als Attribute store ‘Active Directory’.



Stel deze in naar het voorbeeld in onderstaande schermprint:

E-Mail-Addresses	E-Mail Address
Given-Name	Given Name
Surname	Surname
Display-Name	Display Name
objectGUID*	objectGUID

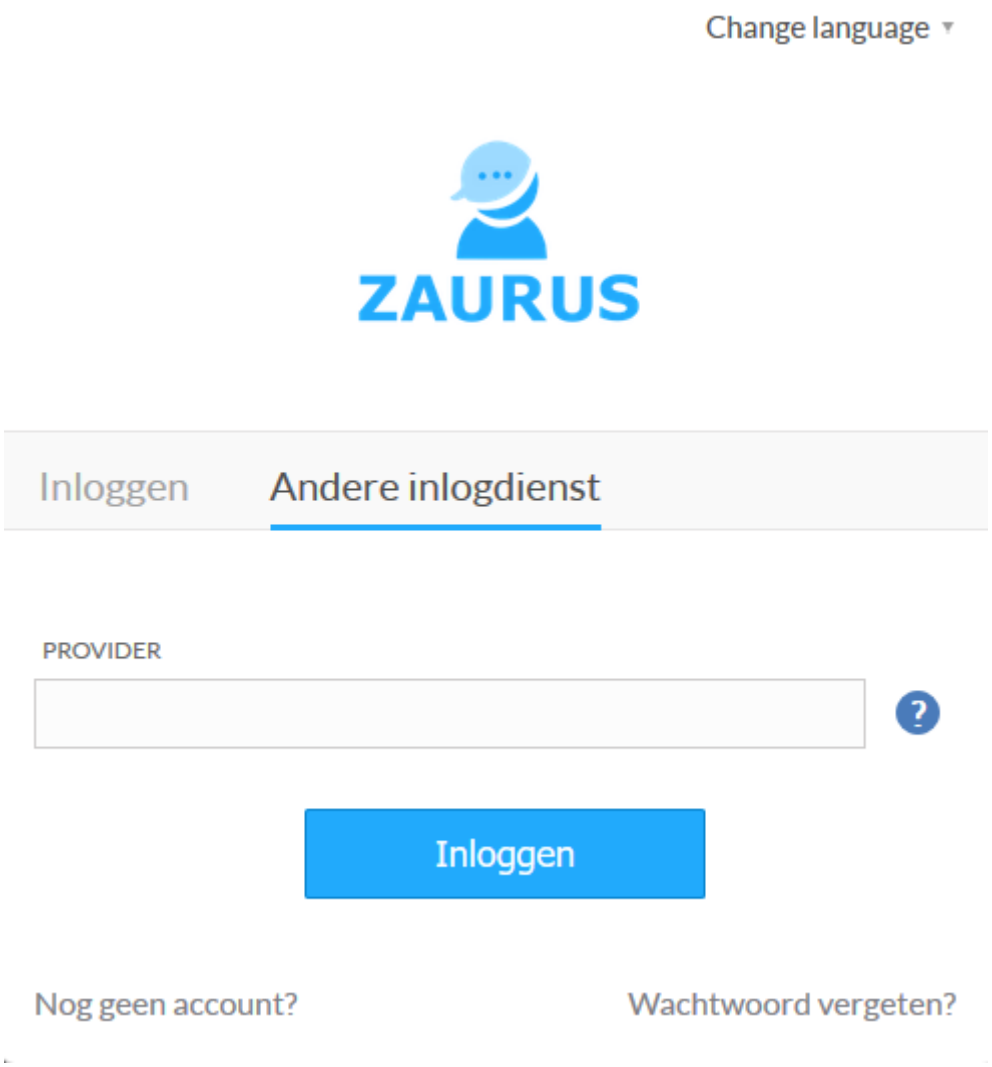
*Voor objectGUID zal deze waarschijnlijk handmatig ingevoerd moeten worden, aangezien deze niet selecteerbaar is. Soms verdwijnt de invoer weer, maar bij een tweede keer invoeren in hetzelfde veld lukt het wel.



Hoe SSO er uitziet vanuit messenger-gebruikers

Klik in het inlogscherm op ‘Andere inlogdienst’.

Vervolgens zie je dit:



Als provider geef je je ingestelde Providernaam in (dit zal veelal de bedrijfsnaam zijn). Deze is ingesteld in de bedrijfsinstellingen van de messenger (onder de 'Geavanceerd' tab).