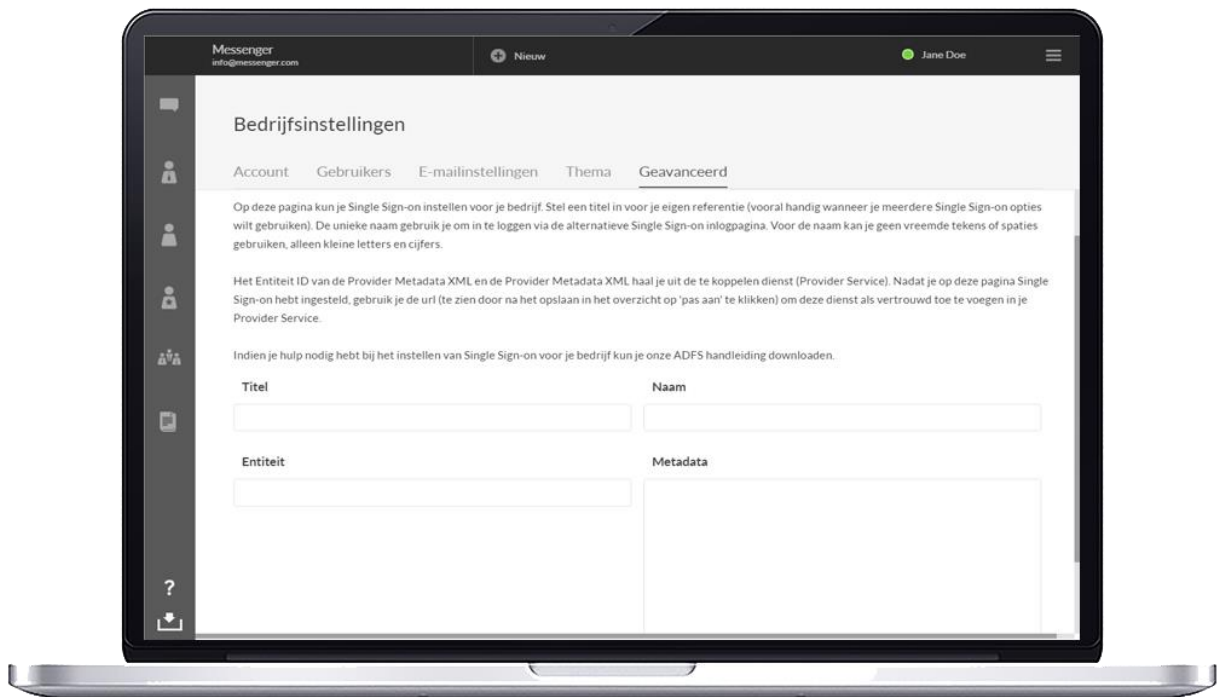


# ADFS INSTELLEN

## EEN HANDLEIDING



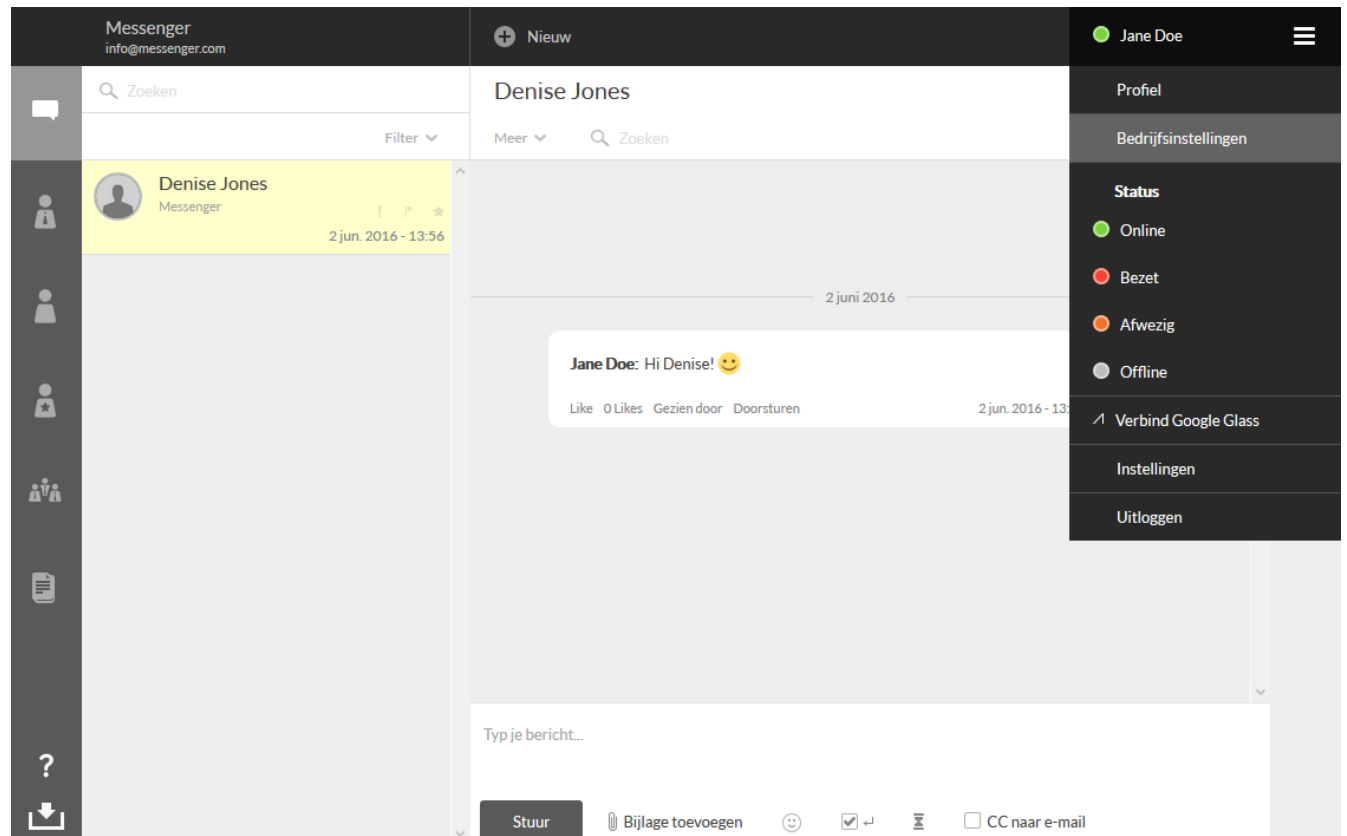
# Inhoud

Voor je op de ADFS server de instellingen aanpast .....	3
ADFS instellen.....	6
Relying Party Trust toevoegen .....	7
Claim Rules instellen.....	14
<b>Rule 1</b> .....	17
<b>Rule 2</b> .....	17
<b>Rule 3</b> .....	18
Hoe SSO er uitziet vanuit messenger-gebruikers.....	21

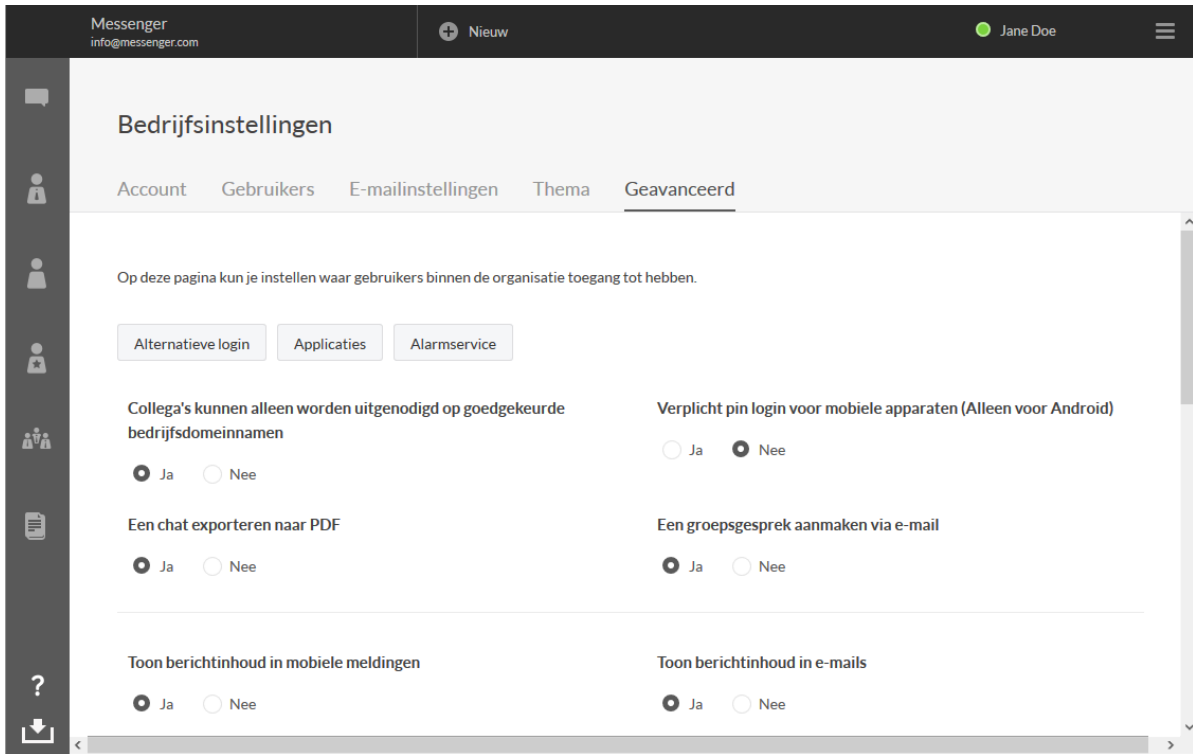
## Voor je op de ADFS server de instellingen aanpast

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'.

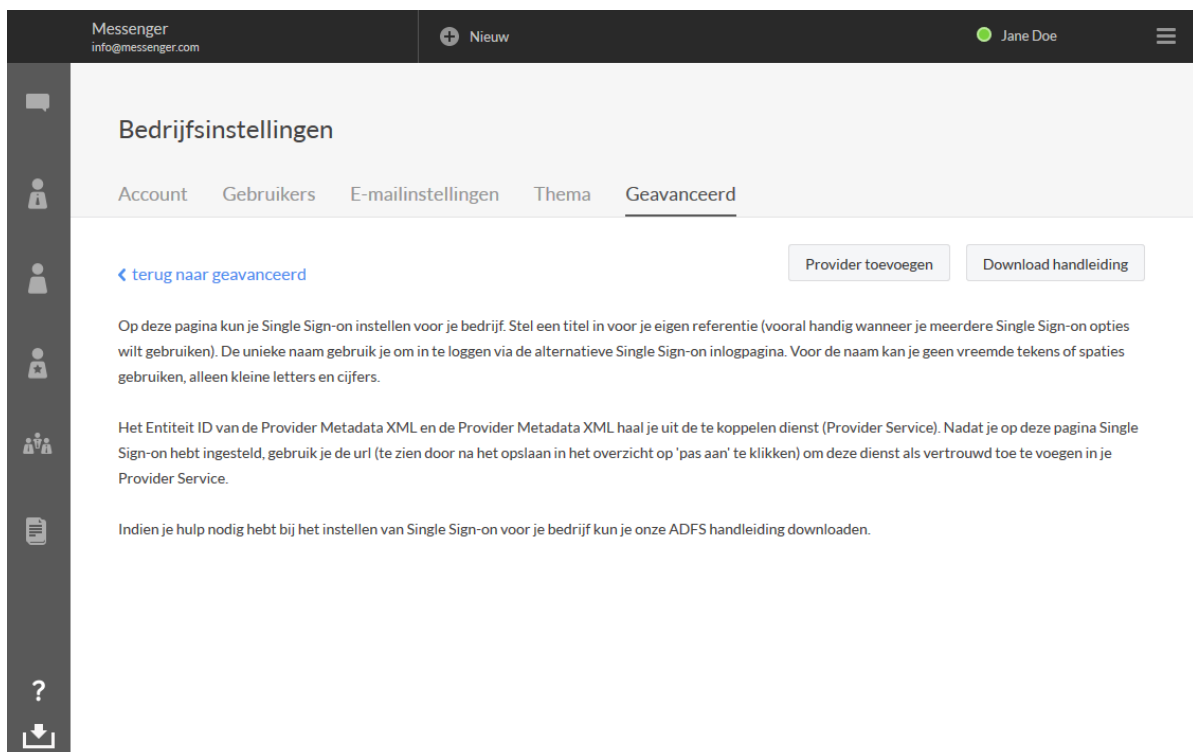
Klik op 'Bedrijfsinstellingen'.



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.

Titel

Naam

Entiteit

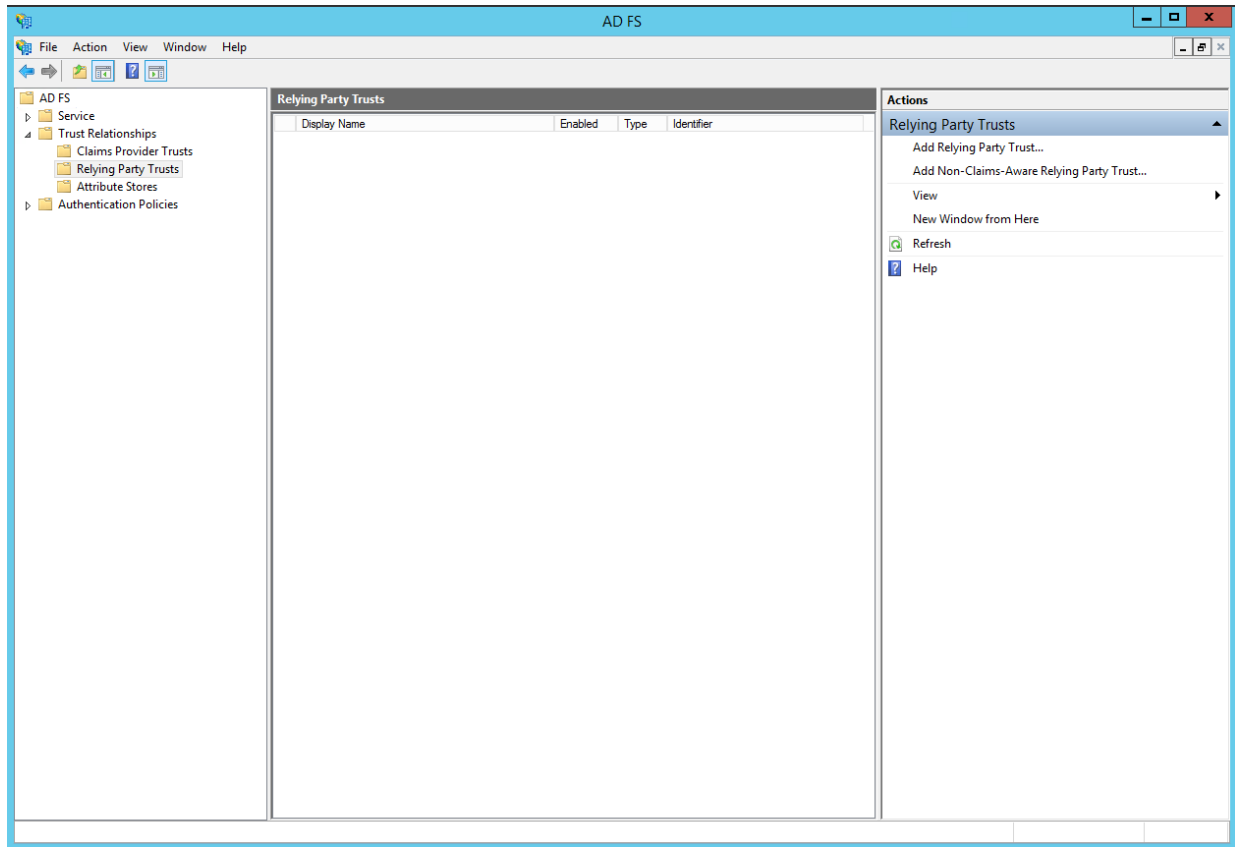
Metadata

Opslaan

Annuleren

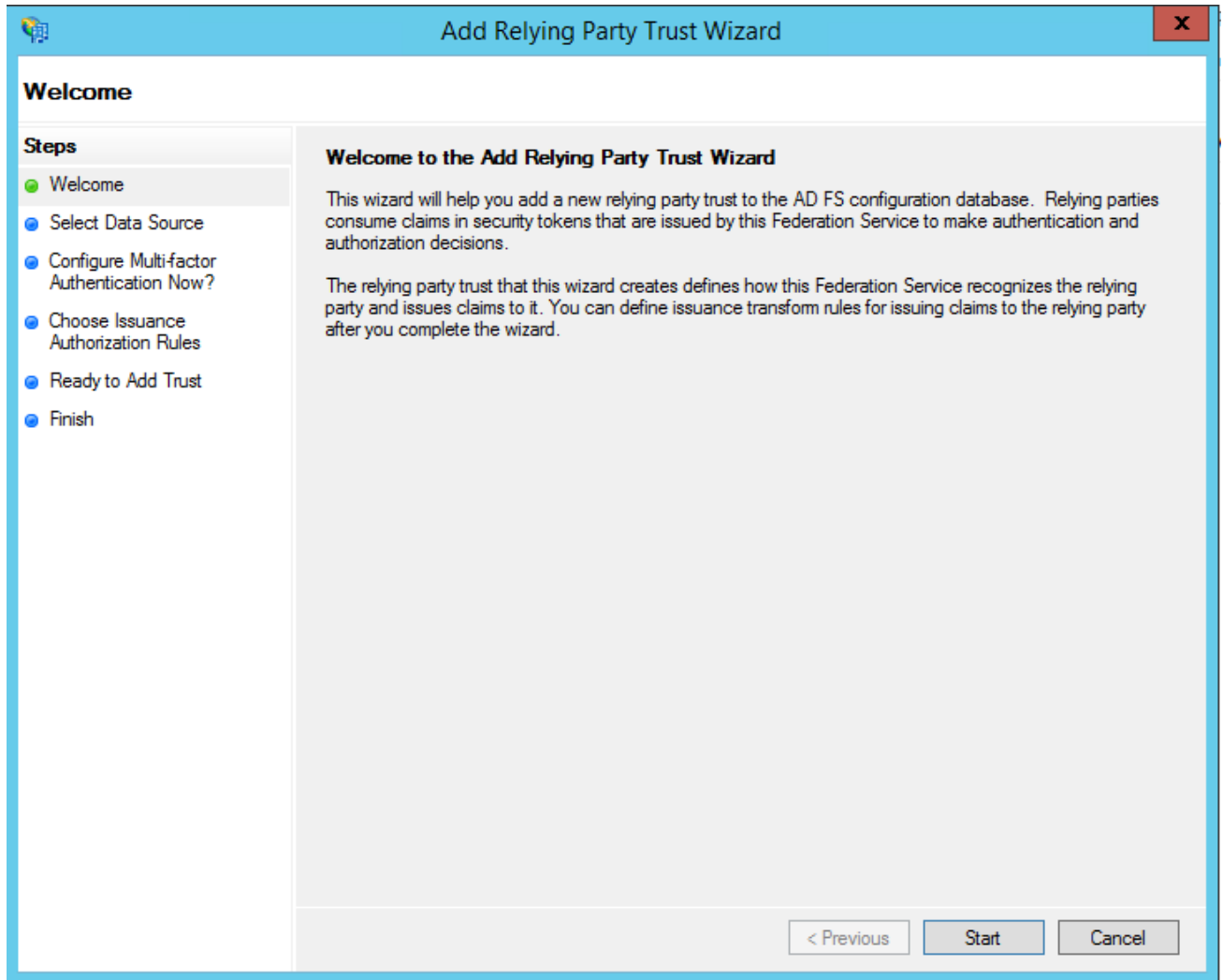
# ADFS instellen

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=xxxxxxx-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'.

The screenshot shows a Windows-style dialog box titled "Add Relying Party Trust Wizard" with a close button (X) in the top right corner. The main area is titled "Select Data Source". On the left, a "Steps" pane lists the following steps: Welcome (completed), Select Data Source (current step), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main content area contains the instruction: "Select an option that this wizard will use to obtain data about this relying party:". There are three radio button options: 1. "Import data about the relying party published online or on a local network" (selected). Description: "Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network." Input field: "Federation metadata address (host name or URL):" with the value "https://url-to-messenger/msrv/auth/samlMetadata?uriParam=>xxxxxxx>xxxx>xxxx>xxxx>xxxxxxxxxxxxx". Example: "fs.contoso.com or https://www.contoso.com/app". 2. "Import data about the relying party from a file". Description: "Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file." Input field: "Federation metadata file location:" with an empty text box and a "Browse..." button. 3. "Enter data about the relying party manually". Description: "Use this option to manually input the necessary data about this relying party organization." At the bottom right, there are three buttons: "< Previous", "Next >", and "Cancel".



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

The screenshot shows a Windows-style dialog box titled "Add Relying Party Trust Wizard" with a close button (X) in the top right corner. The main area is titled "Specify Display Name". On the left, a "Steps" pane lists the following steps: "Welcome", "Select Data Source", "Specify Display Name" (which is the current step and highlighted), "Configure Multi-factor Authentication Now?", "Choose Issuance Authorization Rules", "Ready to Add Trust", and "Finish". The main content area contains the instruction "Enter the display name and any optional notes for this relying party." Below this, there is a "Display name:" label followed by a text input field containing the placeholder text "Enter messenger name". Underneath the input field is a "Notes:" label followed by a large, empty text area with a vertical scrollbar on the right side. At the bottom right of the dialog, there are three buttons: "< Previous", "Next >", and "Cancel".

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

**Add Relying Party Trust Wizard**

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Configure Multi-factor Authentication Now?**
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

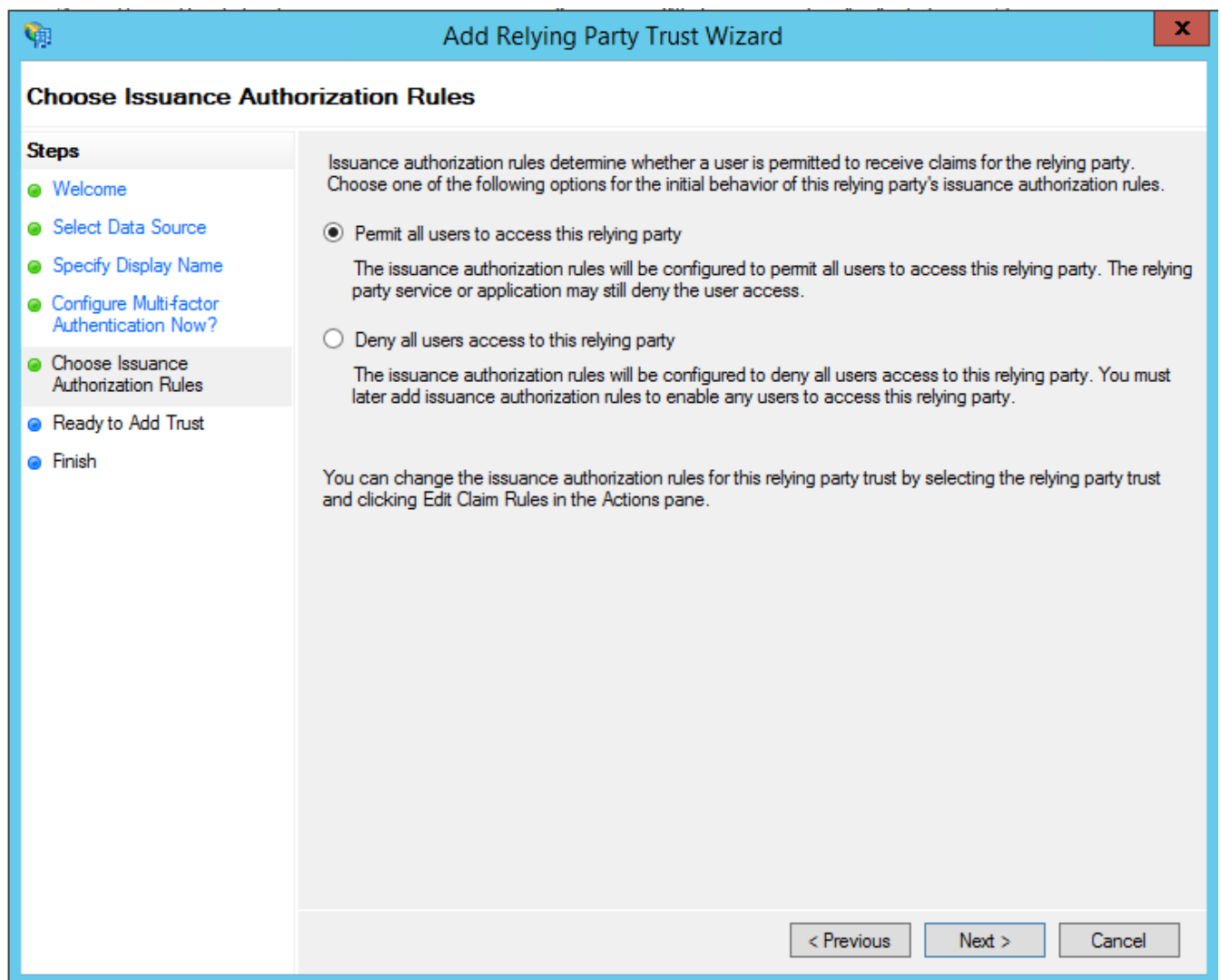
I do not want to configure multi-factor authentication settings for this relying party trust at this time.

Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).

< Previous    Next >    Cancel

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



The screenshot shows a Windows-style dialog box titled "Add Relying Party Trust Wizard" with a close button (X) in the top right corner. The main content area is titled "Choose Issuance Authorization Rules". On the left, there is a "Steps" pane with a list of steps: "Welcome", "Select Data Source", "Specify Display Name", "Configure Multi-factor Authentication Now?", "Choose Issuance Authorization Rules" (which is highlighted in grey), "Ready to Add Trust", and "Finish". The main area contains the following text: "Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules." Below this are two radio button options: "Permit all users to access this relying party" (which is selected) and "Deny all users access to this relying party". Each option has a descriptive paragraph. At the bottom right, there are three buttons: "< Previous", "Next >", and "Cancel".

**Add Relying Party Trust Wizard**

### Choose Issuance Authorization Rules

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules**
- Ready to Add Trust
- Finish

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

Permit all users to access this relying party

The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

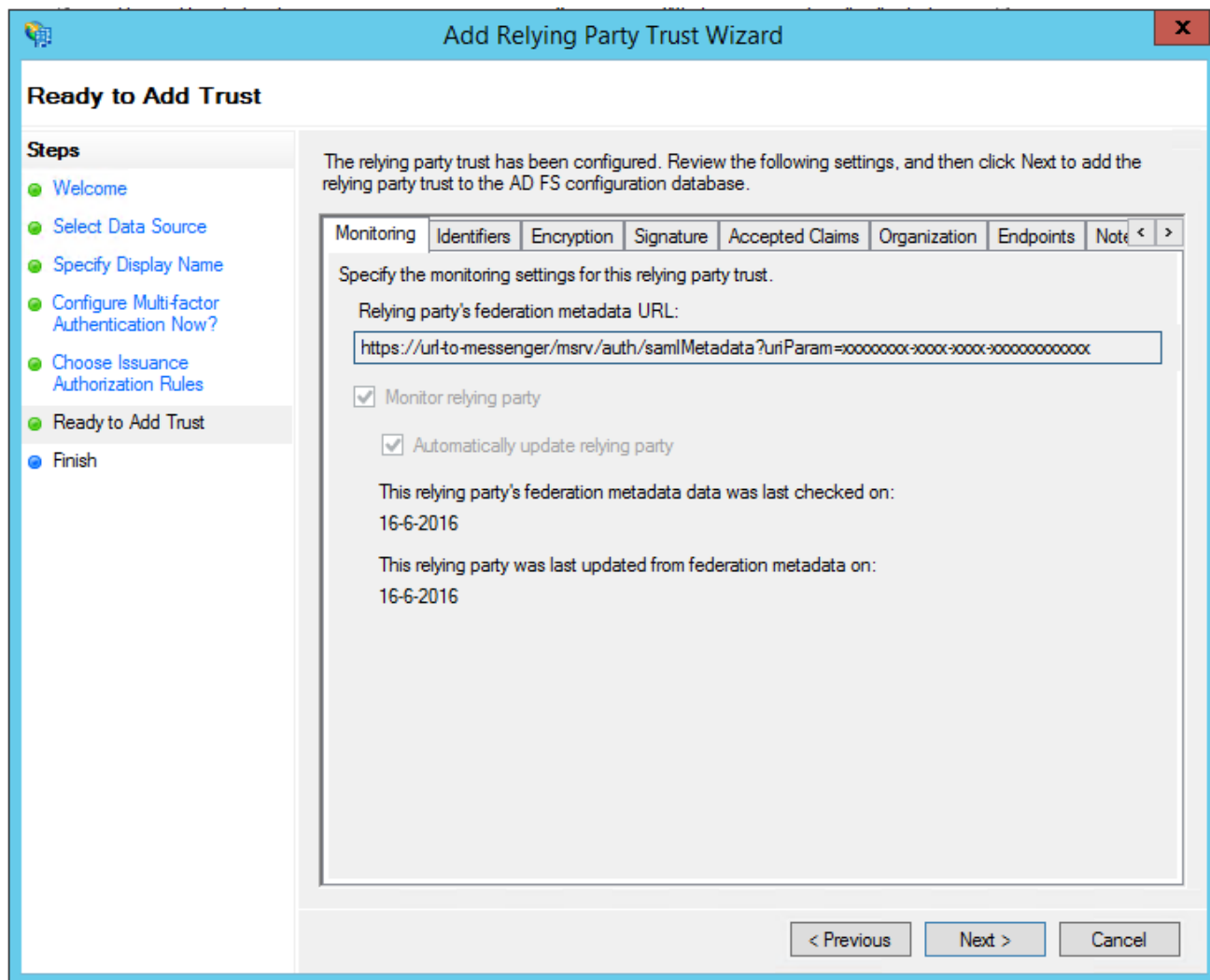
Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

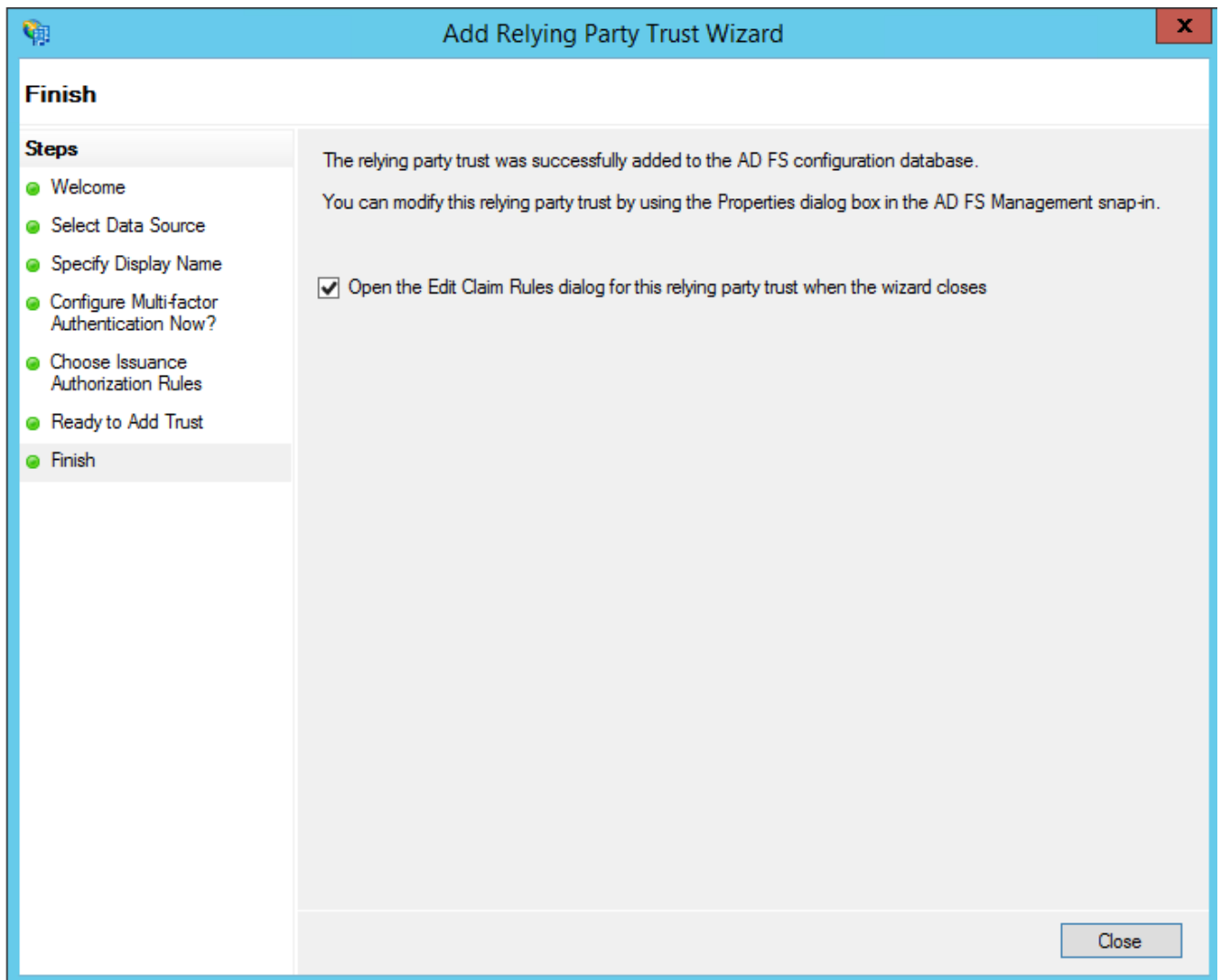
You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

< Previous    Next >    Cancel

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

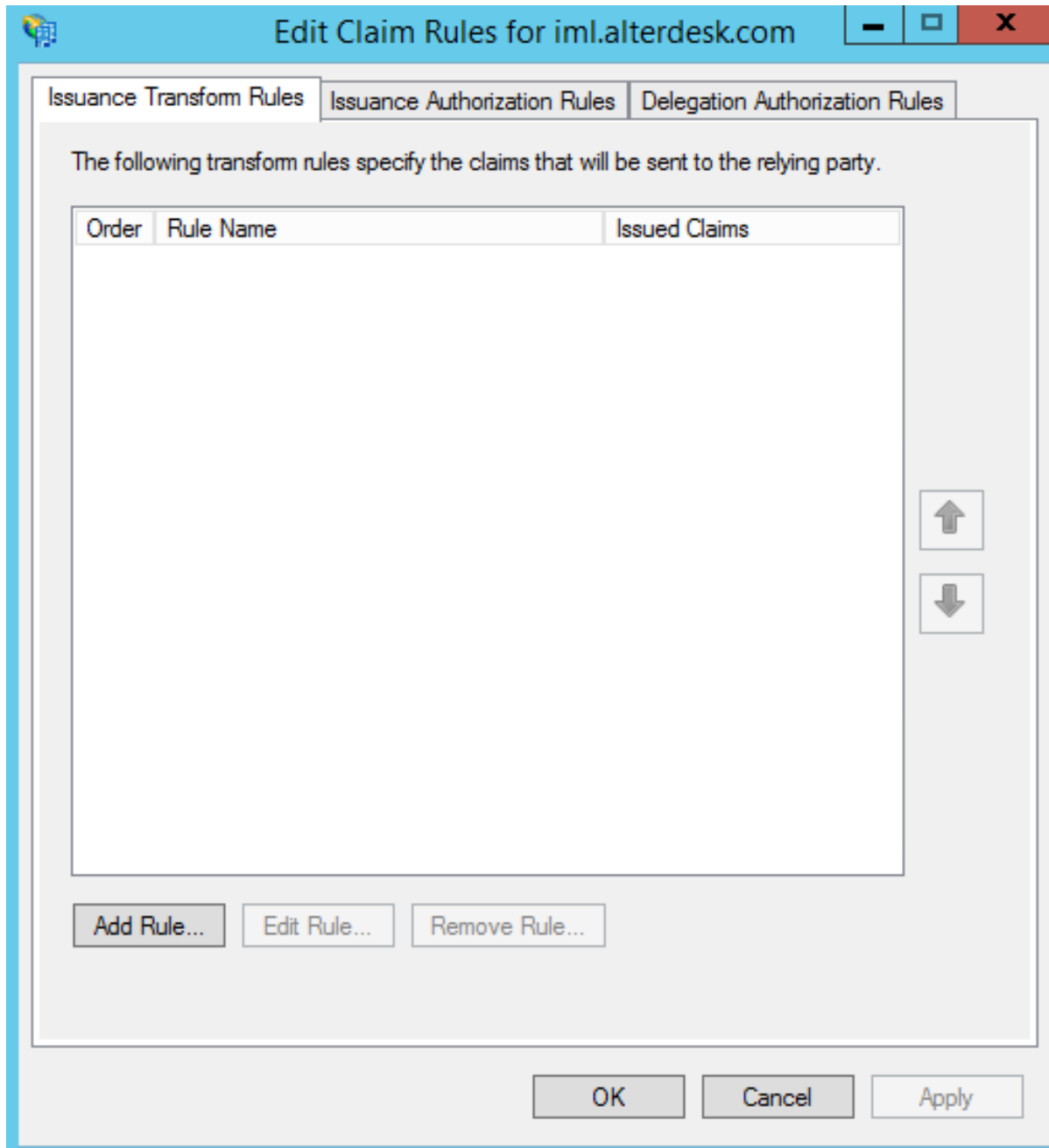


Uiteindelijk kom je op een Finish scherm. Het vinkje voor de Claim Rules kan aanblijven, want deze moeten ook worden geconfigureerd. Klik op 'Close'.



## Claim Rules instellen

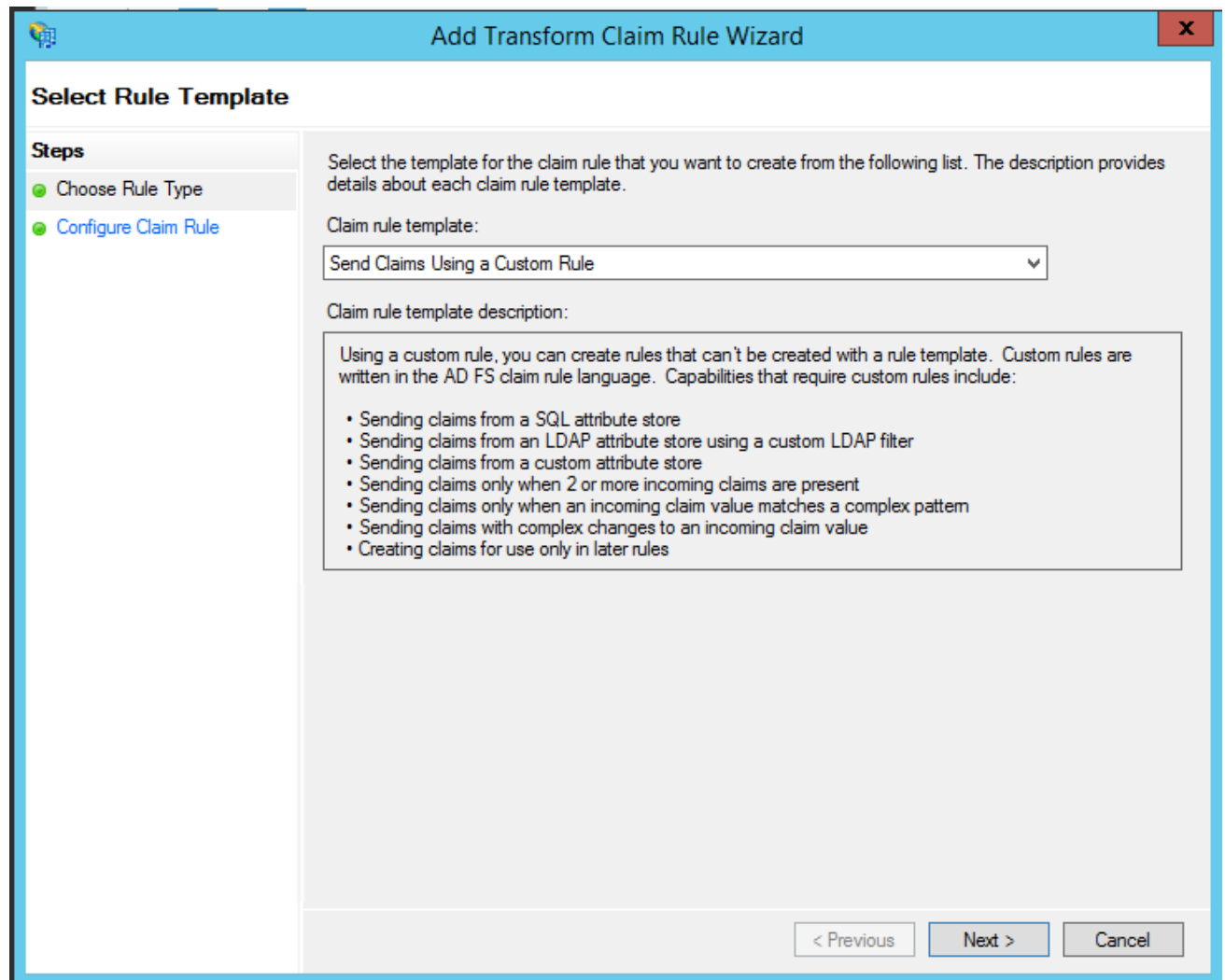
Vervolgens wordt het 'Edit Claim Rules' scherm geopend.



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.

The screenshot shows a Windows-style dialog box titled "Add Transform Claim Rule Wizard". The main area is titled "Configure Rule". On the left, there is a "Steps" pane with two items: "Choose Rule Type" (highlighted in blue) and "Configure Claim Rule" (highlighted in green). The main content area contains the following text: "You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language." Below this text is a text box labeled "Claim rule name:". Underneath that is the text "Rule template: Send Claims Using a Custom Rule". Below that is a text box labeled "Custom rule:". At the bottom right of the dialog are three buttons: "< Previous", "Finish", and "Cancel".

**Add Transform Claim Rule Wizard**

### Configure Rule

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

Rule template: Send Claims Using a Custom Rule

Custom rule:

< Previous   Finish   Cancel



## 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

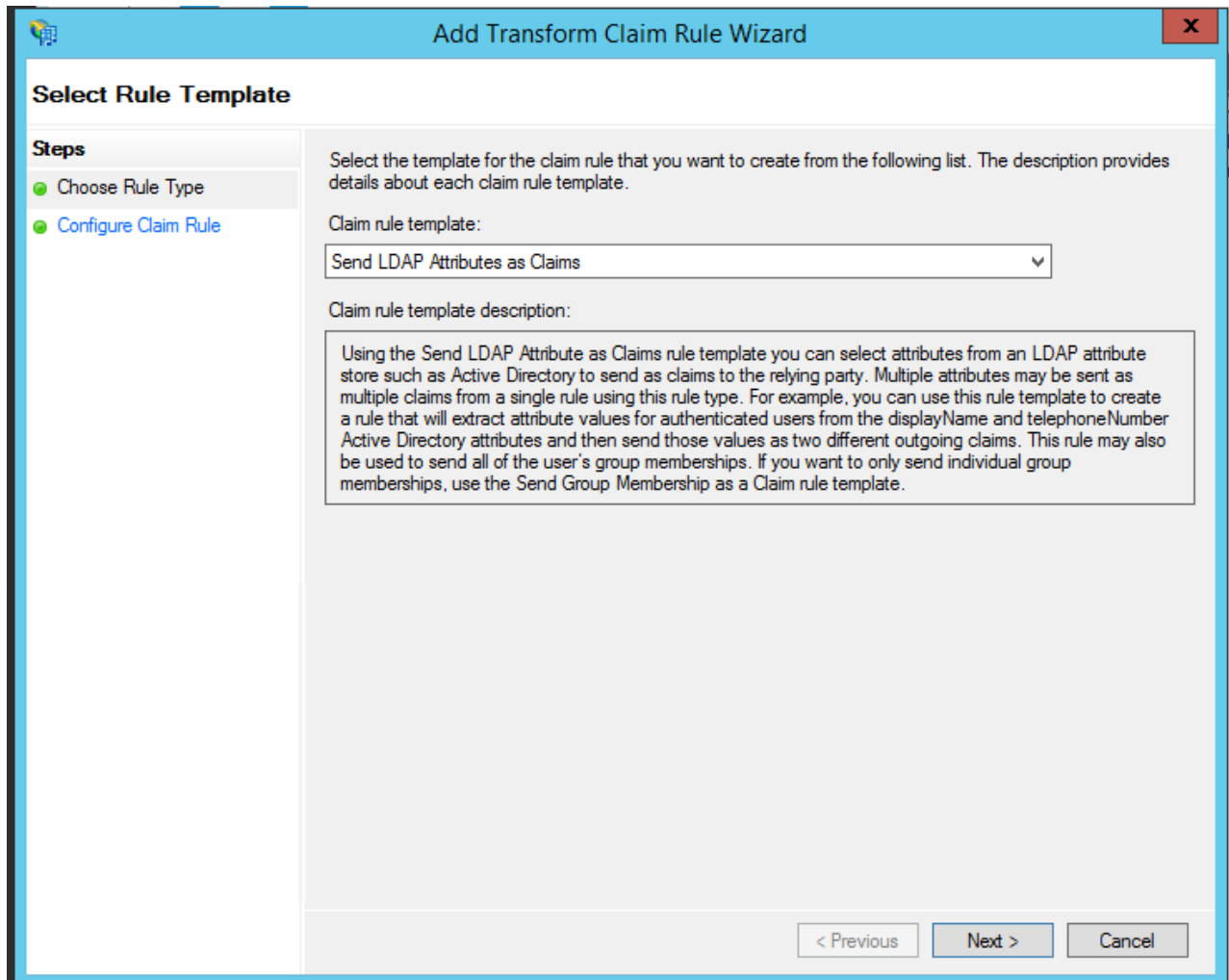
Rule 2 bevat de volgende 'Custom Rule':

```
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'.



The screenshot shows a Windows-style dialog box titled "Add Transform Claim Rule Wizard" with a close button (X) in the top right corner. The main area is titled "Select Rule Template". On the left, there is a "Steps" sidebar with two items: "Choose Rule Type" (selected with a green dot) and "Configure Claim Rule" (with a blue dot). The main content area contains the following text:

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 LDAP Attributes as Claims

Claim rule template description:  
Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

At the bottom right, there are three buttons: "< Previous", "Next >", and "Cancel".

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

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, specifically the 'Configure Rule' step. The title bar reads 'Add Transform Claim Rule Wizard' with a close button (X) on the right. The main area is titled 'Configure Rule' and contains the following elements:

- Steps:** A list on the left with two items: 'Choose Rule Type' (highlighted in blue) and 'Configure Claim Rule' (highlighted in grey).
- Instructional Text:** '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:** A text input field containing 'Atributes'.
- Rule template:** A label 'Rule template: Send LDAP Attributes as Claims'.
- Attribute store:** A dropdown menu showing 'Active Directory'.
- Mapping of LDAP attributes to outgoing claim types:** A table with two columns: 'LDAP Attribute (Select or type to add more)' and 'Outgoing Claim Type (Select or type to add more)'. The first row has an asterisk (\*) in the first column and dropdown arrows in both columns. Below this is a large grey rectangular area.
- Navigation Buttons:** '< Previous', 'Finish', and 'Cancel' buttons at the bottom right.

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.

**Edit Rule - Attributes**

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)
▶	E-Mail-Addresses	E-Mail Address
	Given-Name	Given Name
	Surname	Surname
	Display-Name	Display Name
	objectGUID	objectGUID

# Hoe SSO er uitziet vanuit messenger-gebruikers

Klik in het inlogscherm op 'Andere inlogdienst'.

Change language ▾



[Inloggen](#) [Andere inlogdienst](#)

GEBRUIKERSNAAM / E-MAILADRES



WACHTWOORD

Inloggen

[Nog geen account?](#)

[Wachtwoord vergeten?](#)

Vervolgens zie je dit:

Change language ▾



Inloggen

Andere inlogdienst

PROVIDER



Inloggen

[Nog geen account?](#)

[Wachtwoord vergeten?](#)

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).