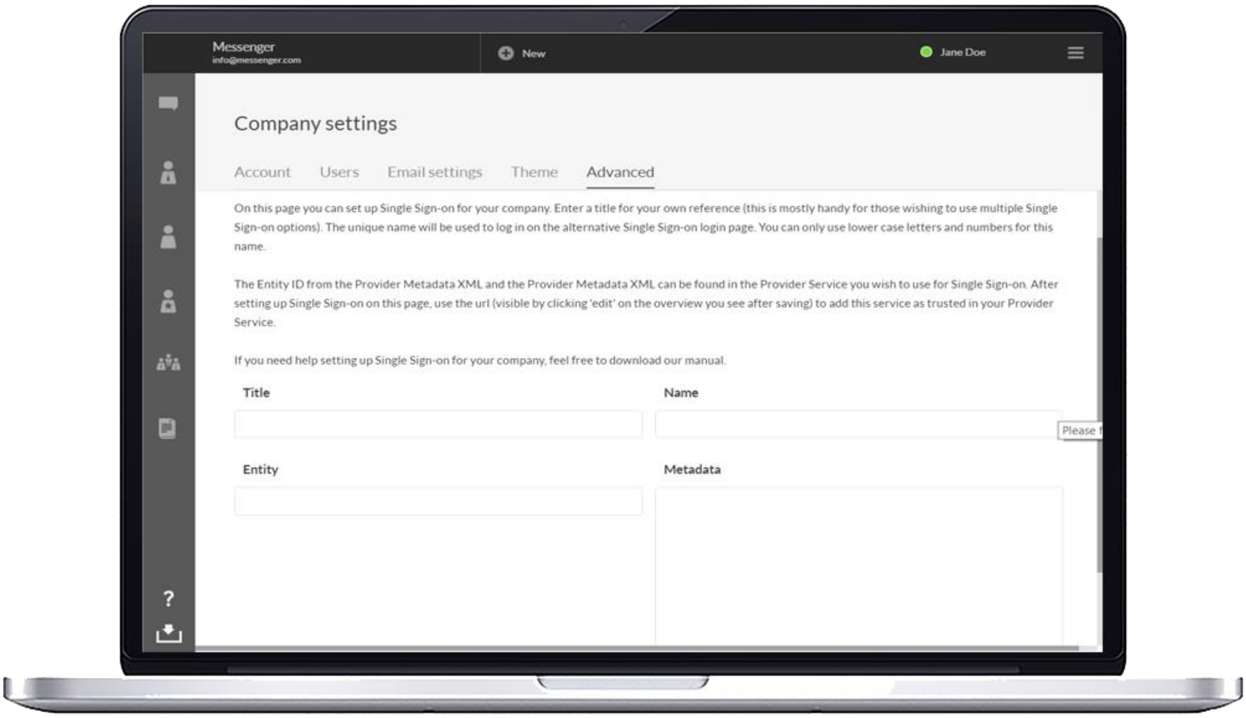
# SETTING UP ADFS

## A MANUAL



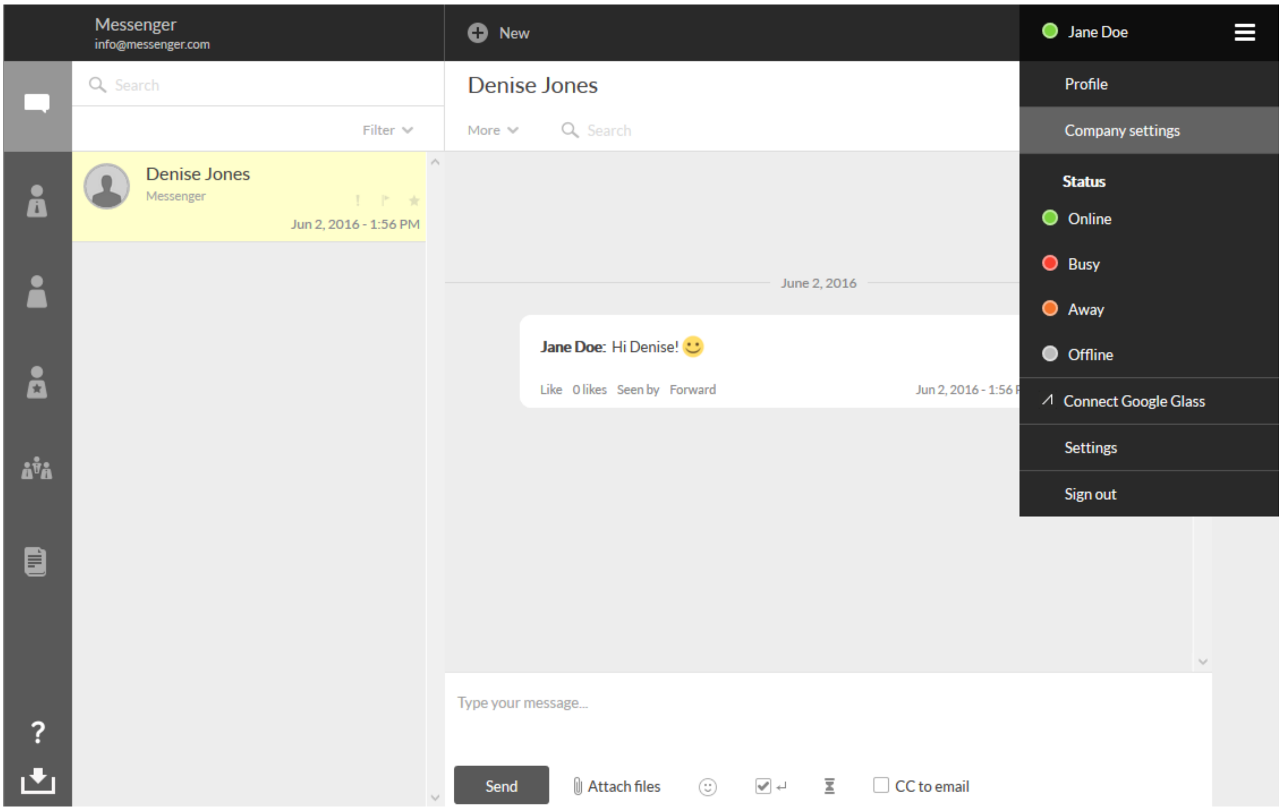

kpn

# Contents

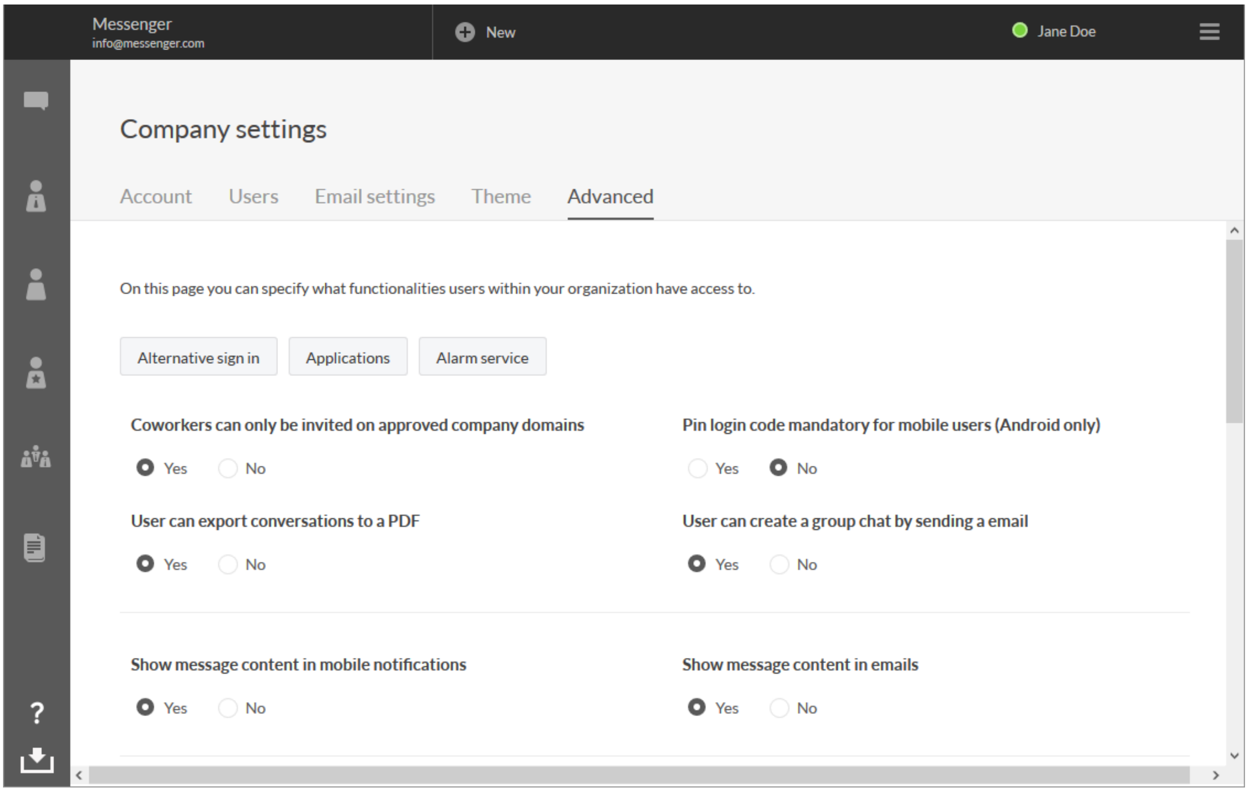
# Before configuring the settings on the ADFS server

Sign in on the messenger with an account with administrator rights. When using the web version, you will find the option 'Company settings' under the dropdown menu at the top right corner of your screen.

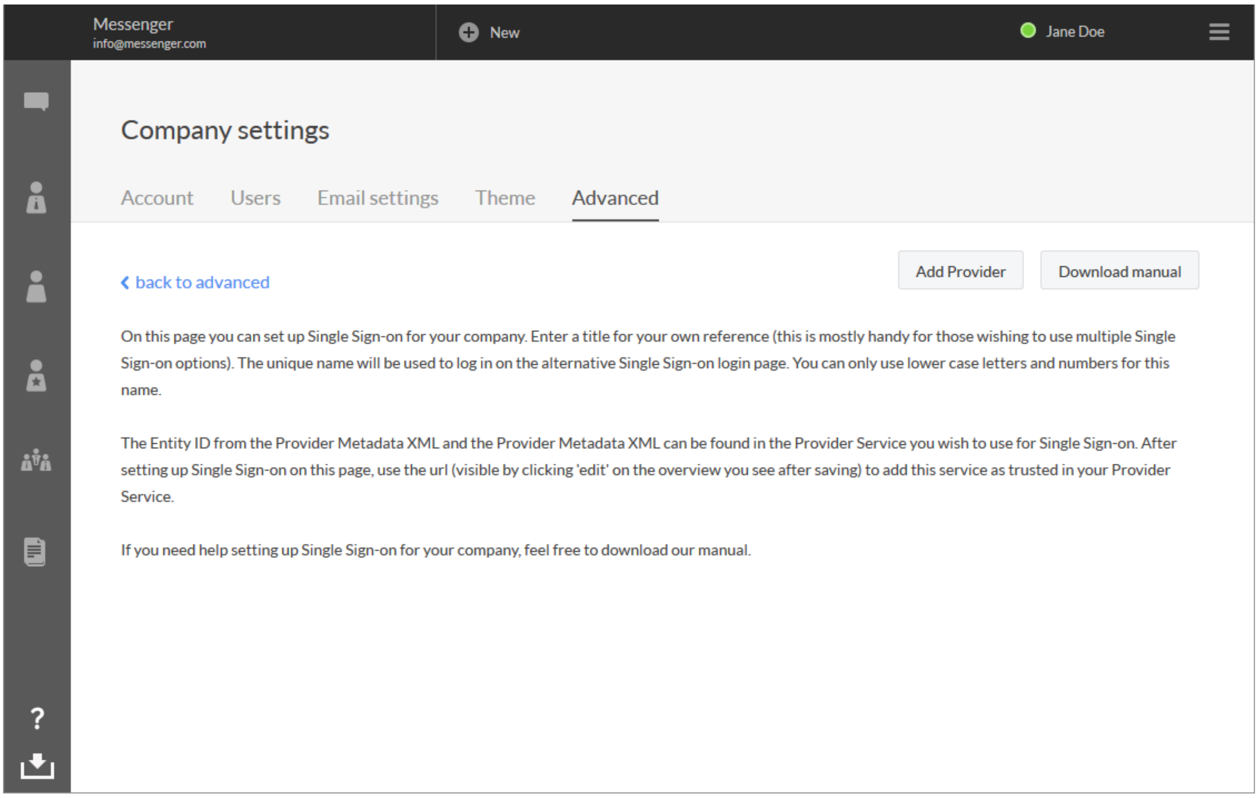
Click on 'Company settings'.



Then click on the tab on the right: 'Advanced'.




Here you will see three buttons at the top of the page. Choose the left one: 'Alternative sign in'. Then you will see the option 'Add Provider' in the top right corner. Click on it to show the fields necessary to start setting up ADFS.



Enter the following information:

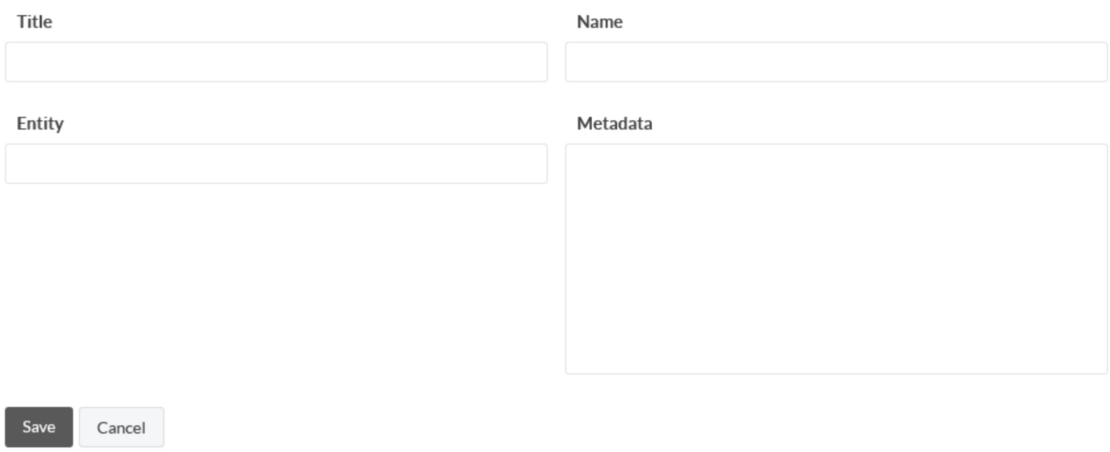
**Title:** This is what you will see as Administrator – choose a title that is clear to you.

**Name:** This is the name end users will use to connect to the ADFS infrastructure.

**Entity:** This is the URL from the ADFS server, for example:
https://adfs.COMPANY.com/adfs/services/trust

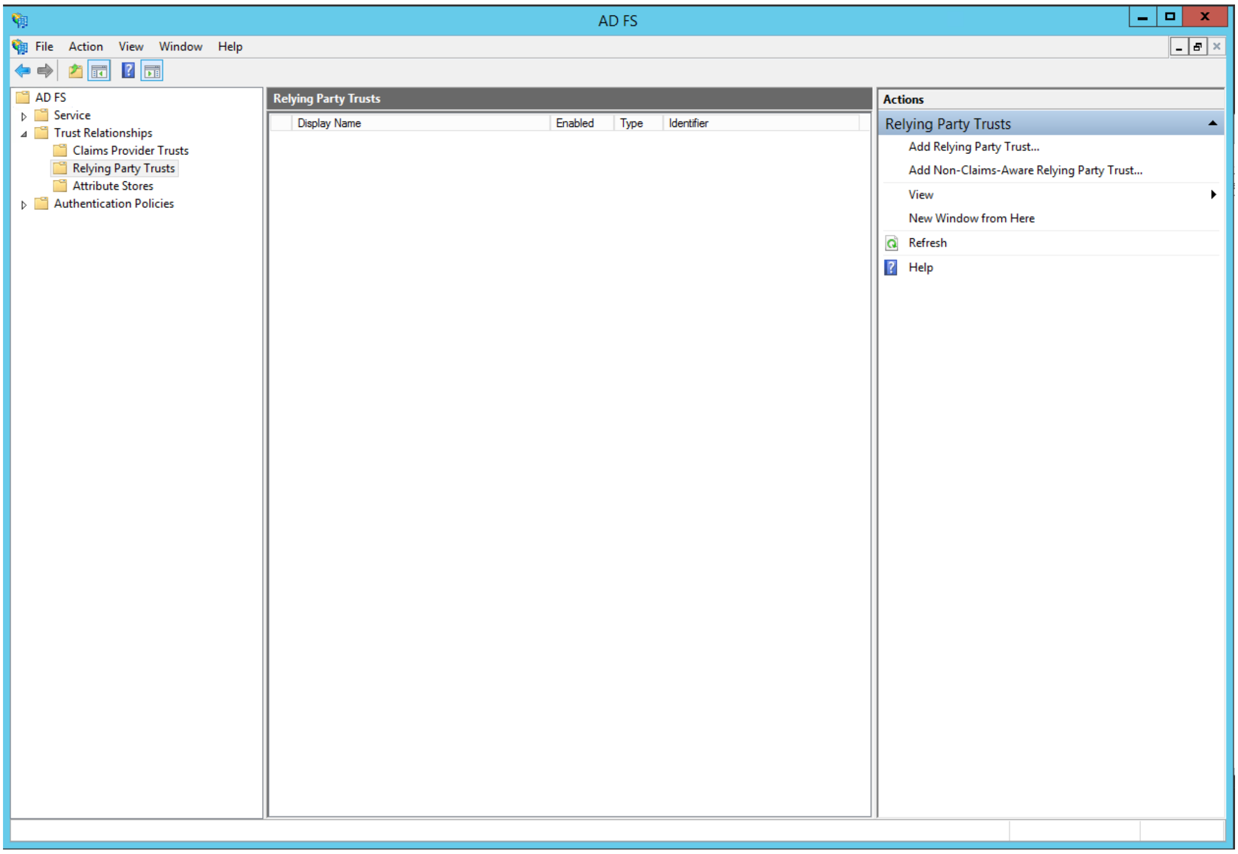
**Metadata:** Here you can paste the information from federationmetadata.xml, retrieved from the ADFS server. The direct URL will have this format:
https://adfs.COMPANY.com/federationmetadata/2007-06/federationmetadata.xml

After saving these settings, the messenger will generate a URL for you, which you can use to configurate the ADFS on the ADFS server.



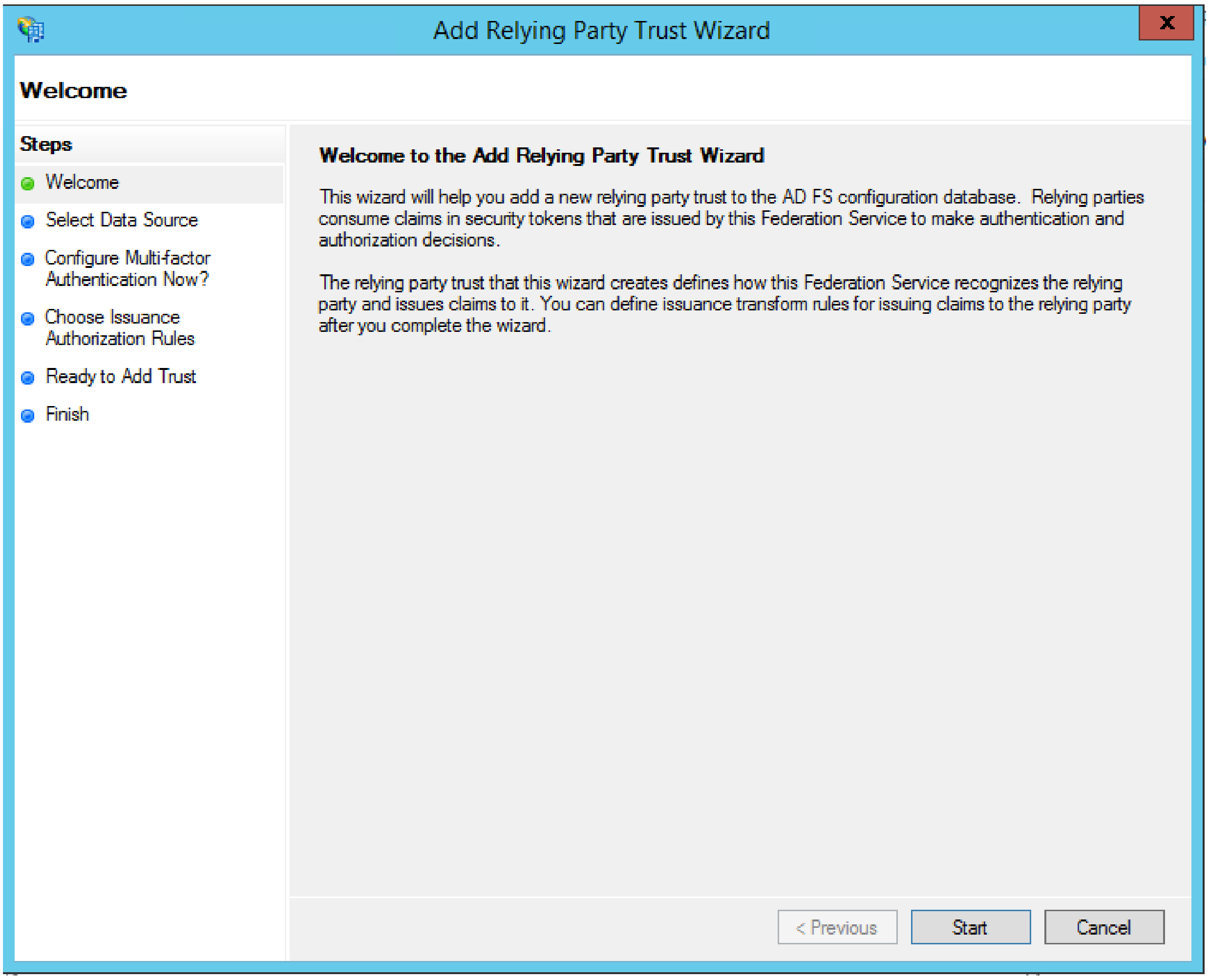
# Set up ADFS

Open the ADFS management console on the ADFS server.



# Add Relying Party Trust

Click on 'Add Relying Party Trust' in the column on the right. You will then see the following intro screen – click 'Start'.

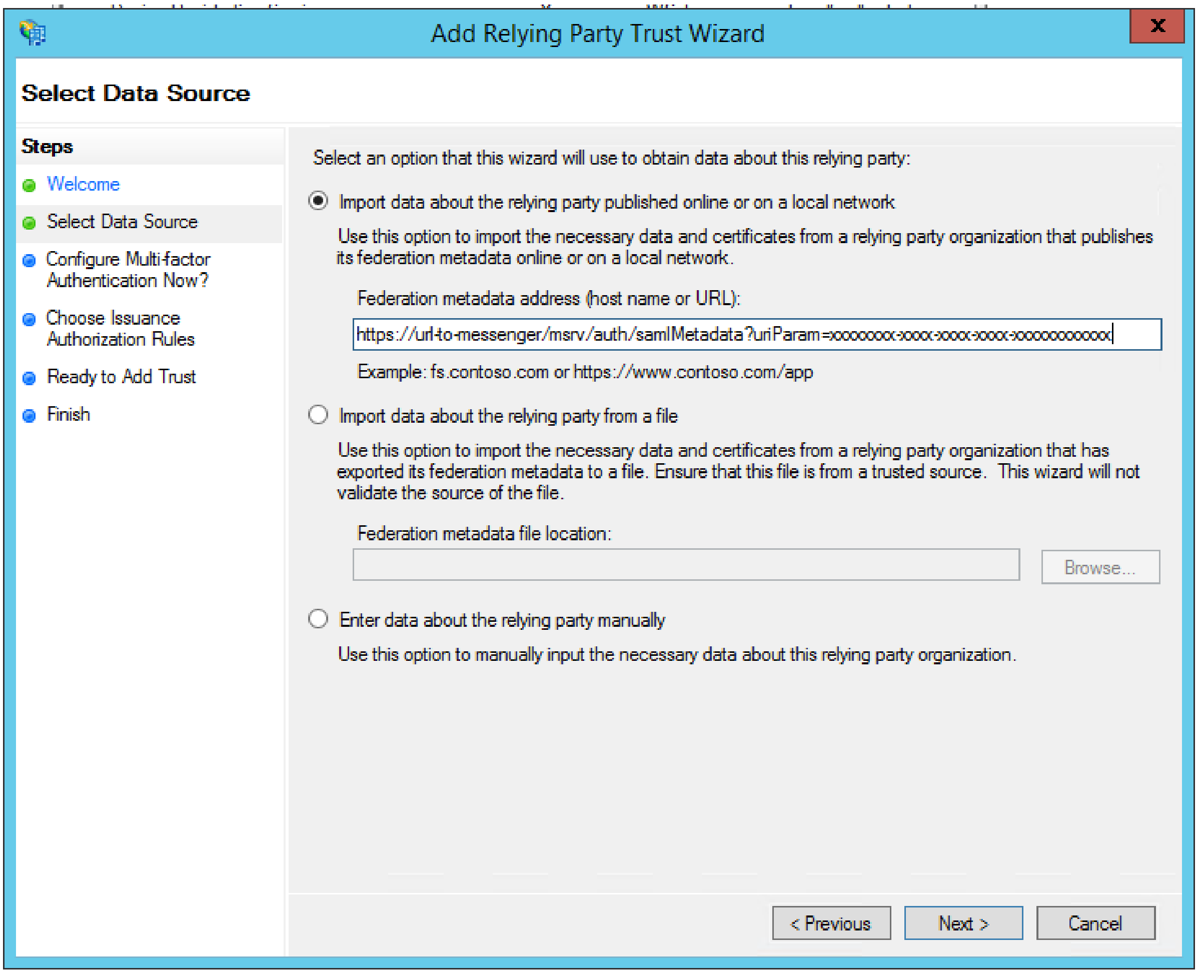



You will then see the screen in which you can enter the federation metadata. This has a format similar to: https://url-to-messenger/msrv/auth/samlMetadata?uriParam=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

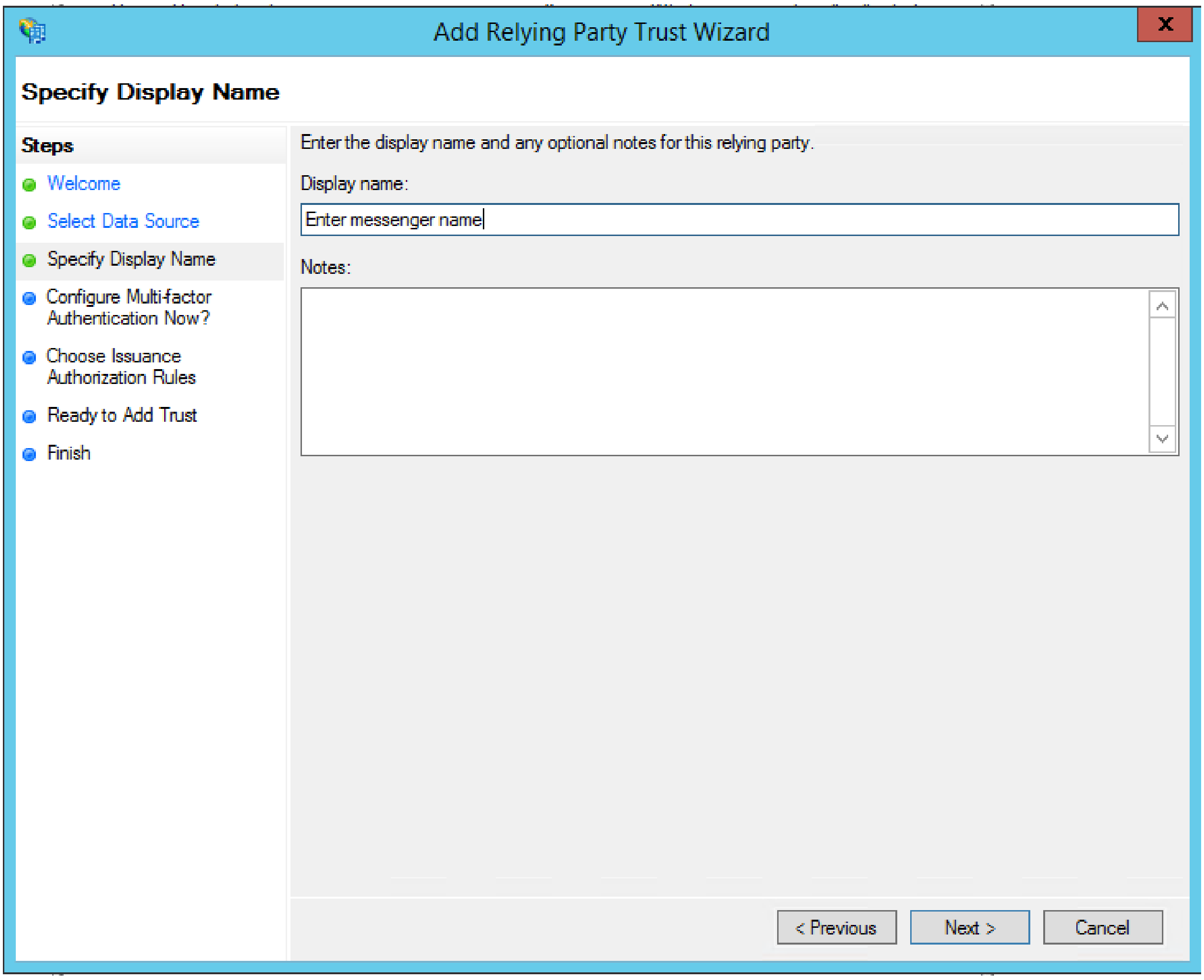
The 'xxxx' key consists of a unique code that is different for each company and can be generated based on the contents of the MetaData field.

If you have followed the first steps of this manual correctly, you will have already generated this URL.

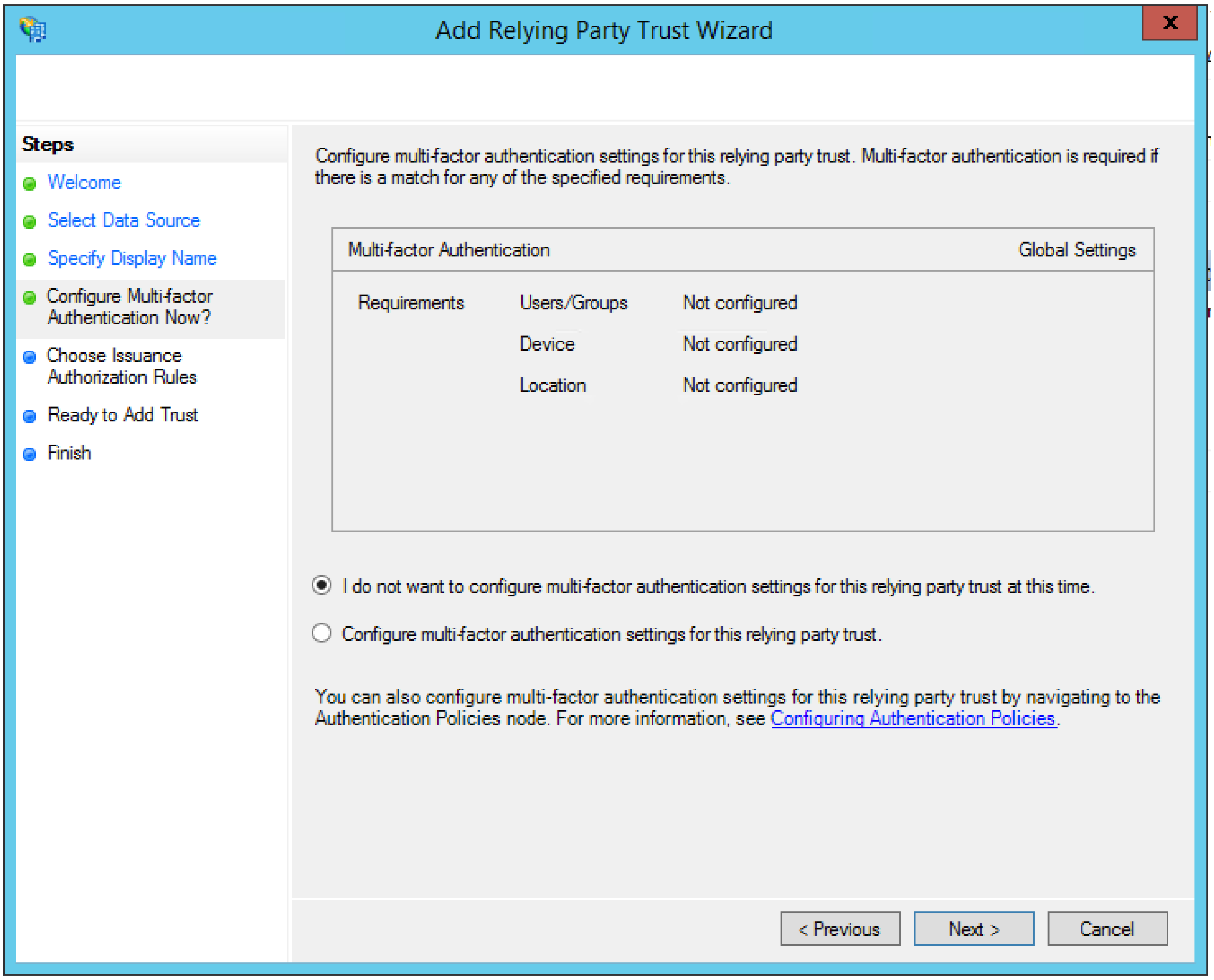
Fill in the Relying Party Trust URL and click ‘Next’.



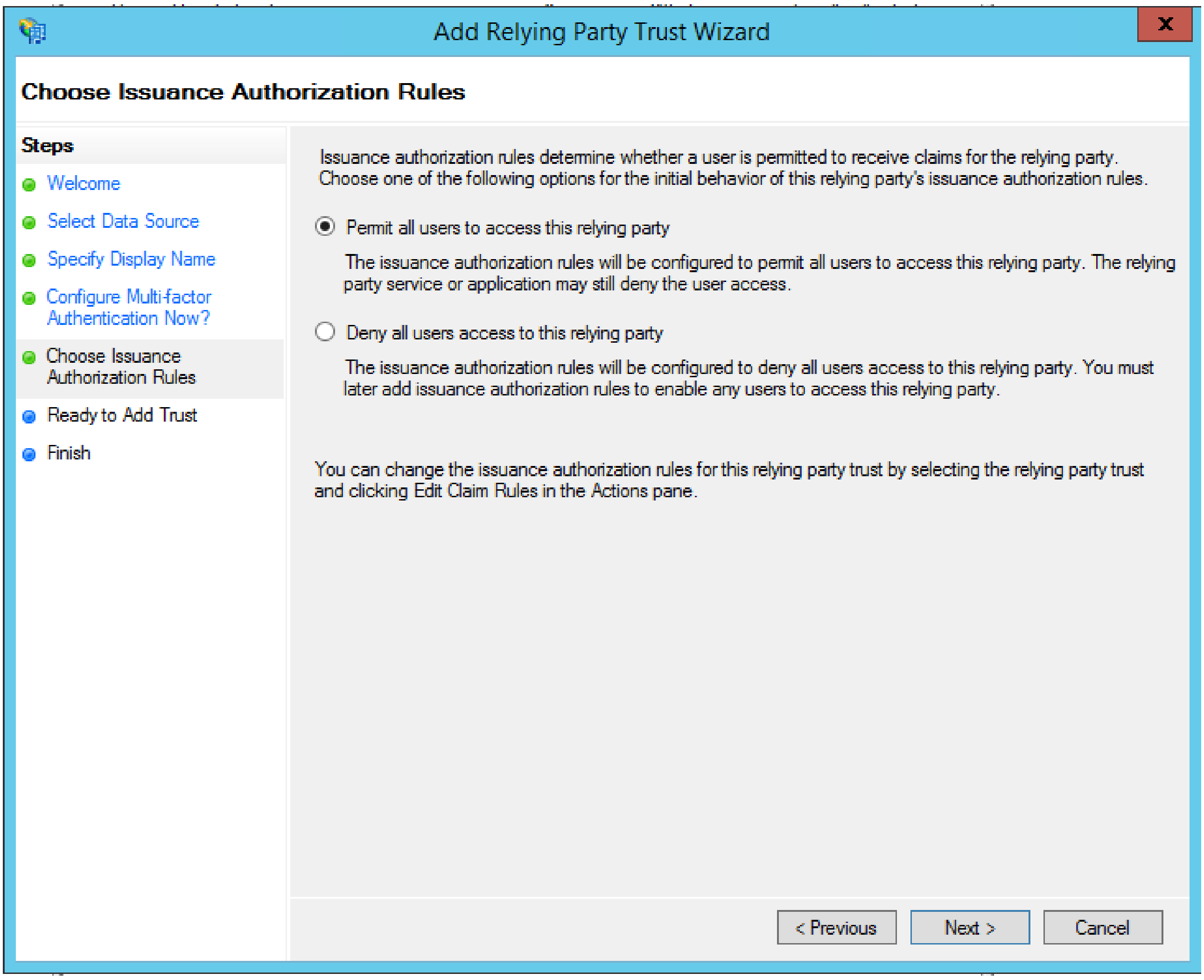
On the next screen you can enter a name and notes according to your own preferences. Click 'Next'.



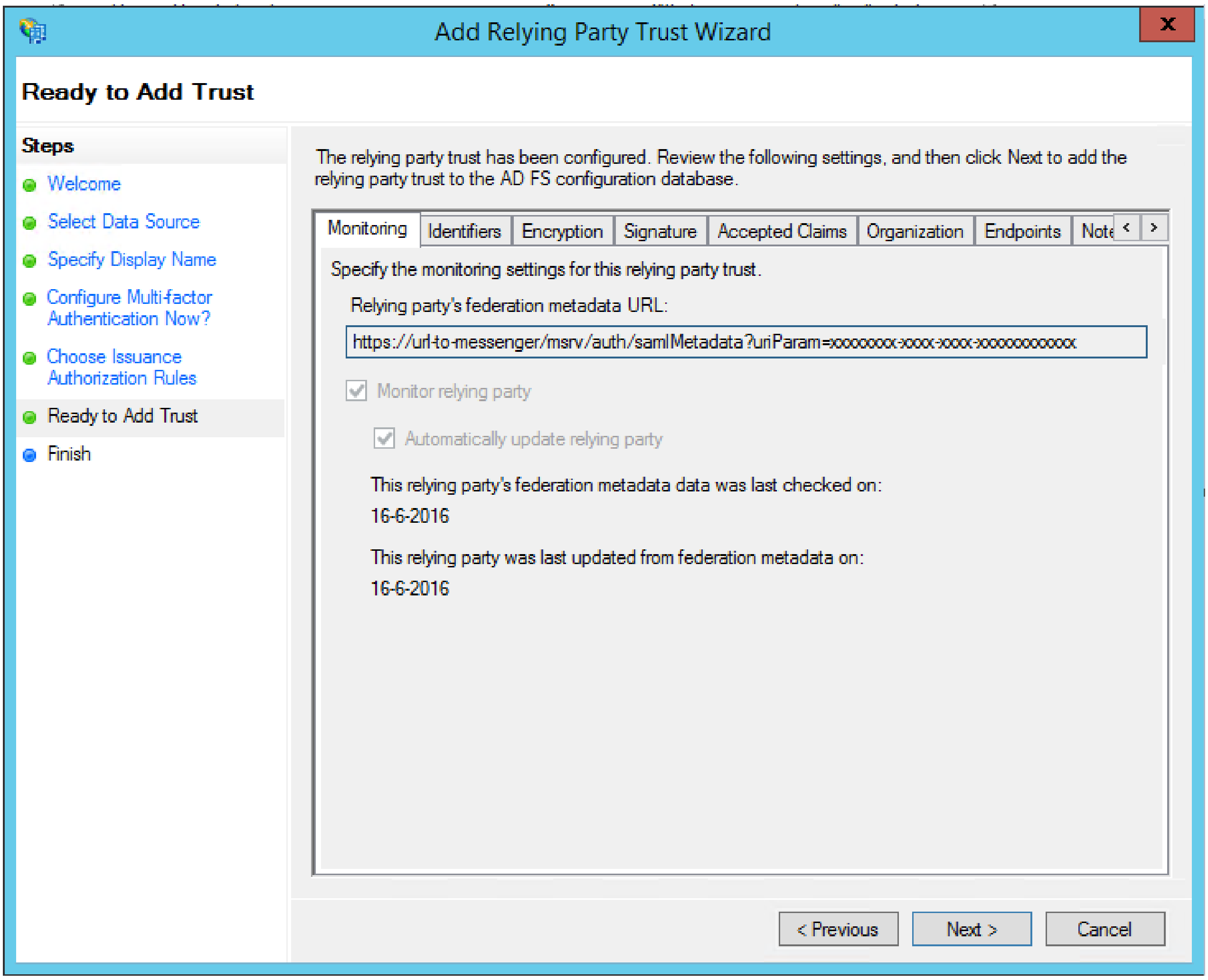
Next you will see the following screen – for our messenger, you can ignore this one. Click 'Next'.



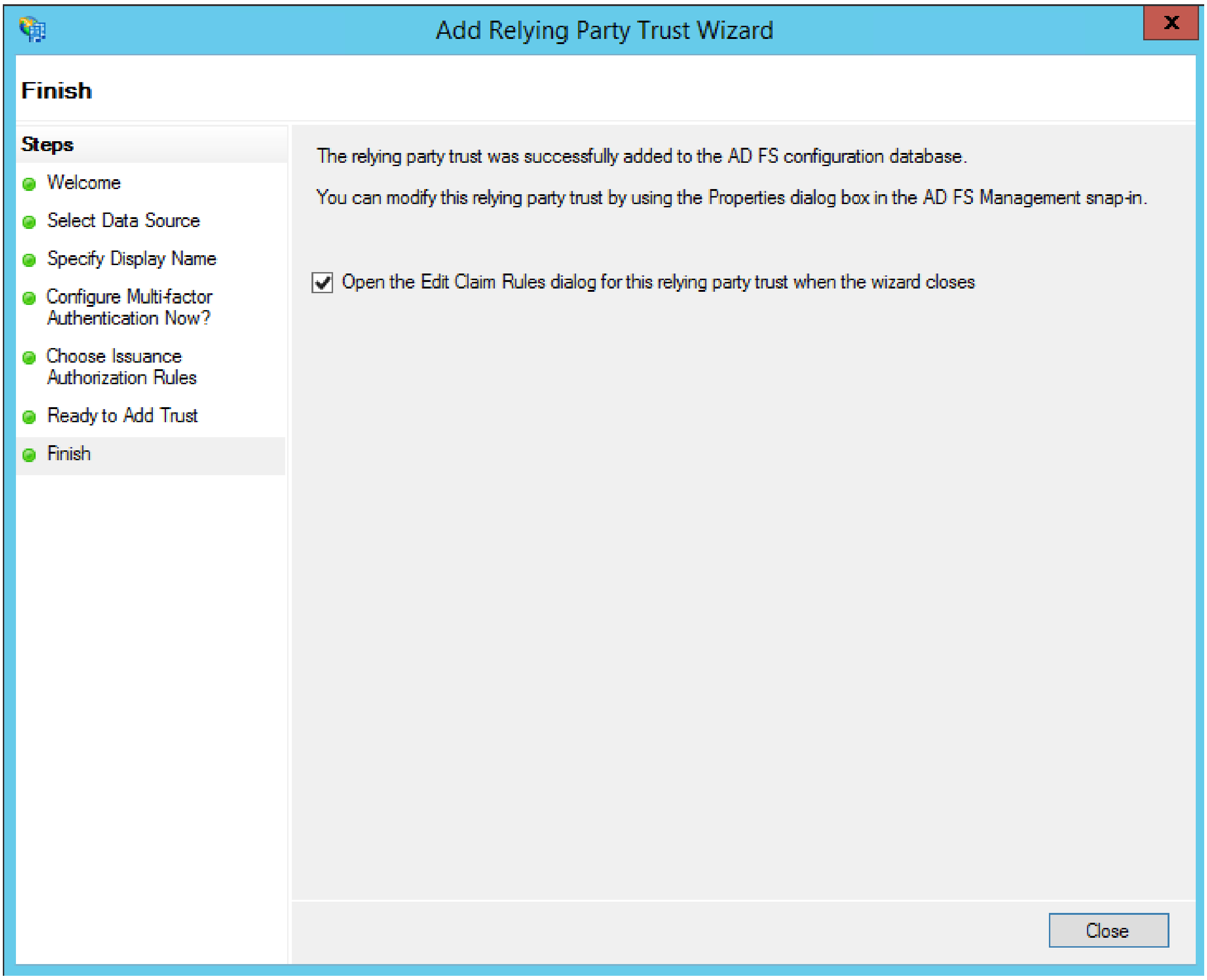
Next you will see the screen below. For our messenger, the default settings are correct. Click ‘Next’.



You will then see a little summary. Click 'Next'.

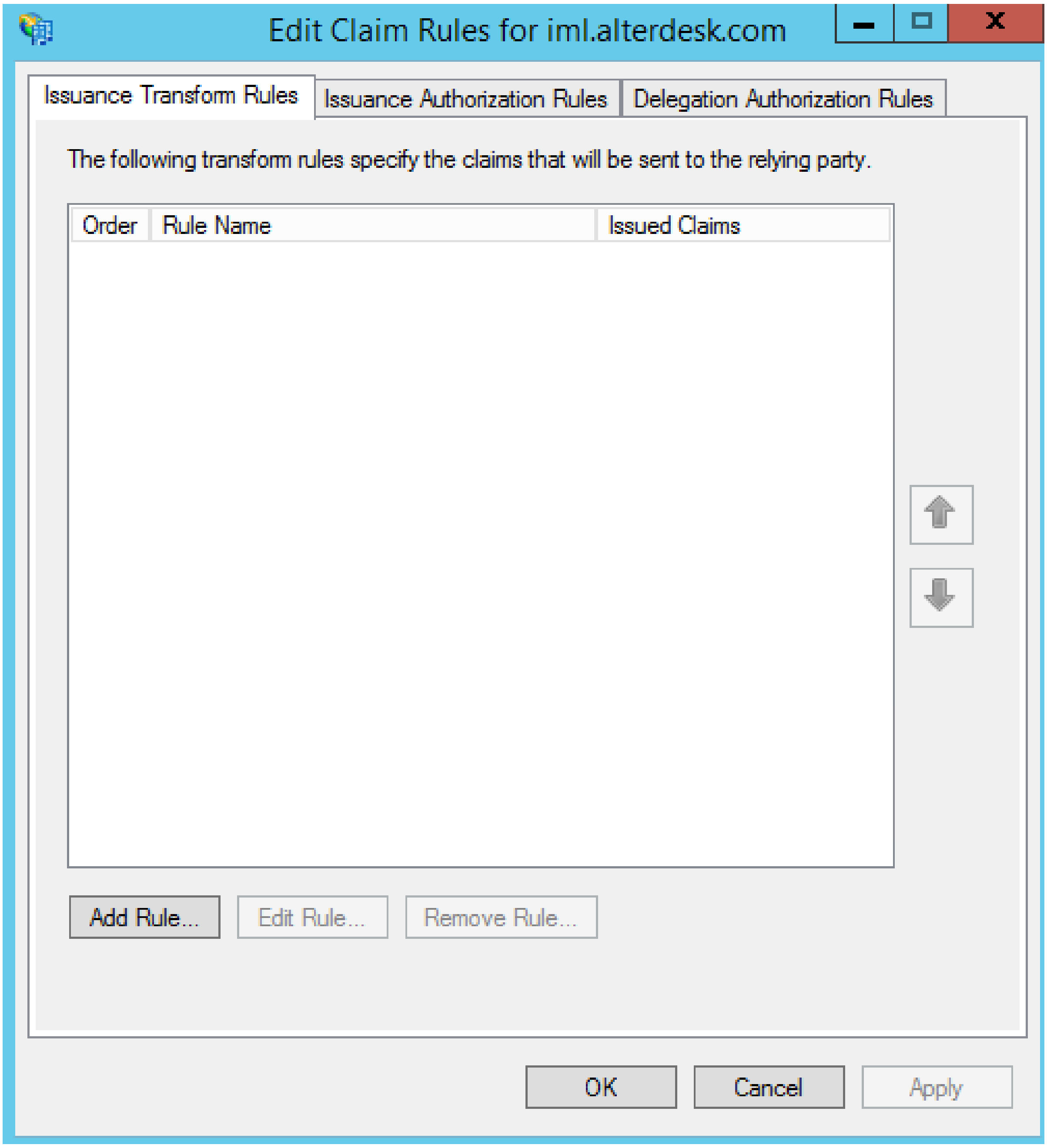


You have now reached the ‘Finish’ screen. Keep the check mark for ‘Edit Claim Rules’ on – you will need to configure these next. Click ‘Close’.



## Set the Claim Rules

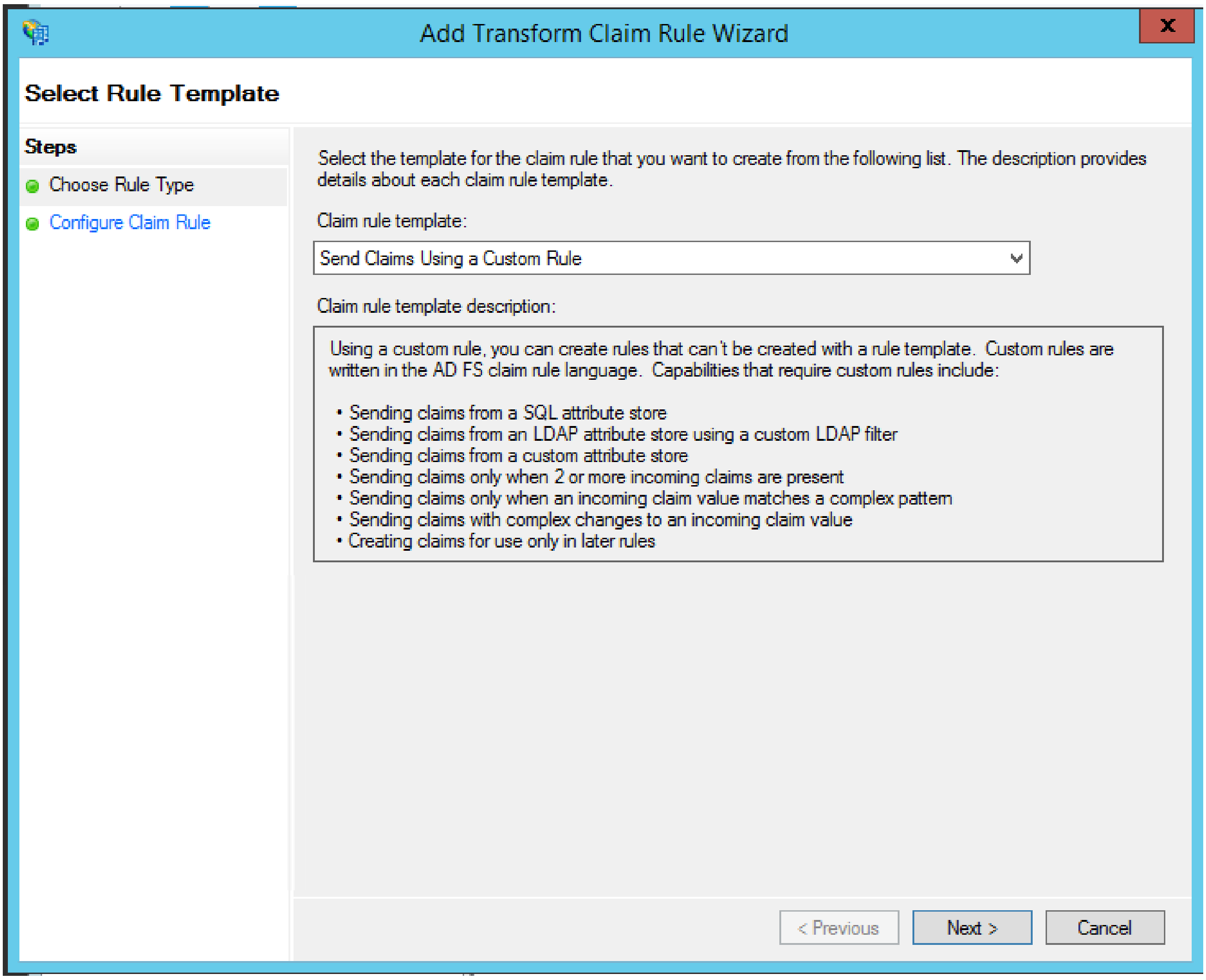
The ‘Edit Claim Rules’ screen will be opened after you close the previous screen.



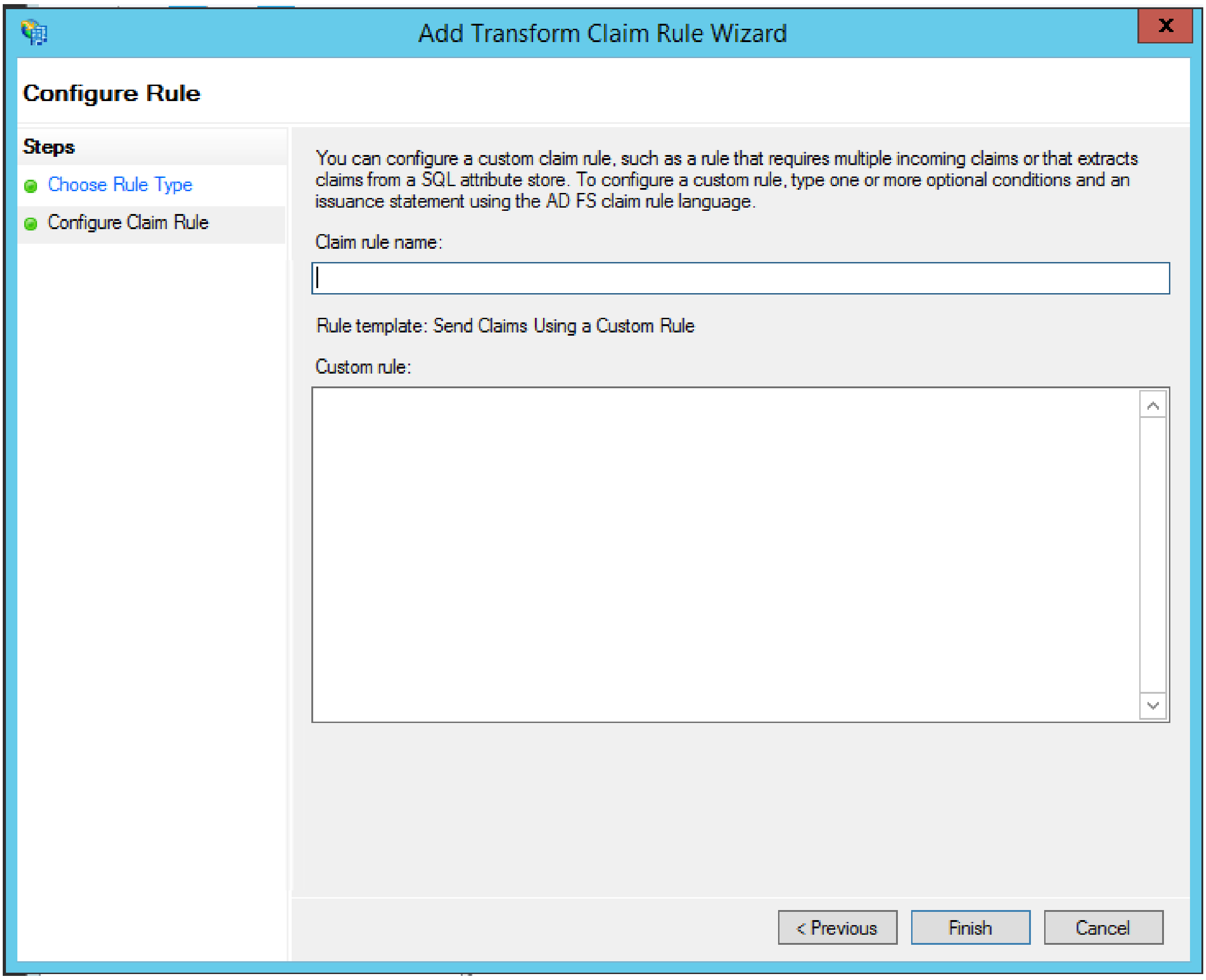

In the ‘Claim Rules settings’, you will need to create three rules.

The first two serve to change the unique account name of the user into a format that can be used by the messenger. Start for both Rule 1 and Rule 2 with ‘Add Rule’.

Select ‘Send Claims Using a Custom Rule’ and click ‘Next’.



Next you will see the screen below, in which you can enter your Custom Rules. You can find these Custom Rules on the next page.



## Rule 1

Rule 1 consists of the following '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);
```

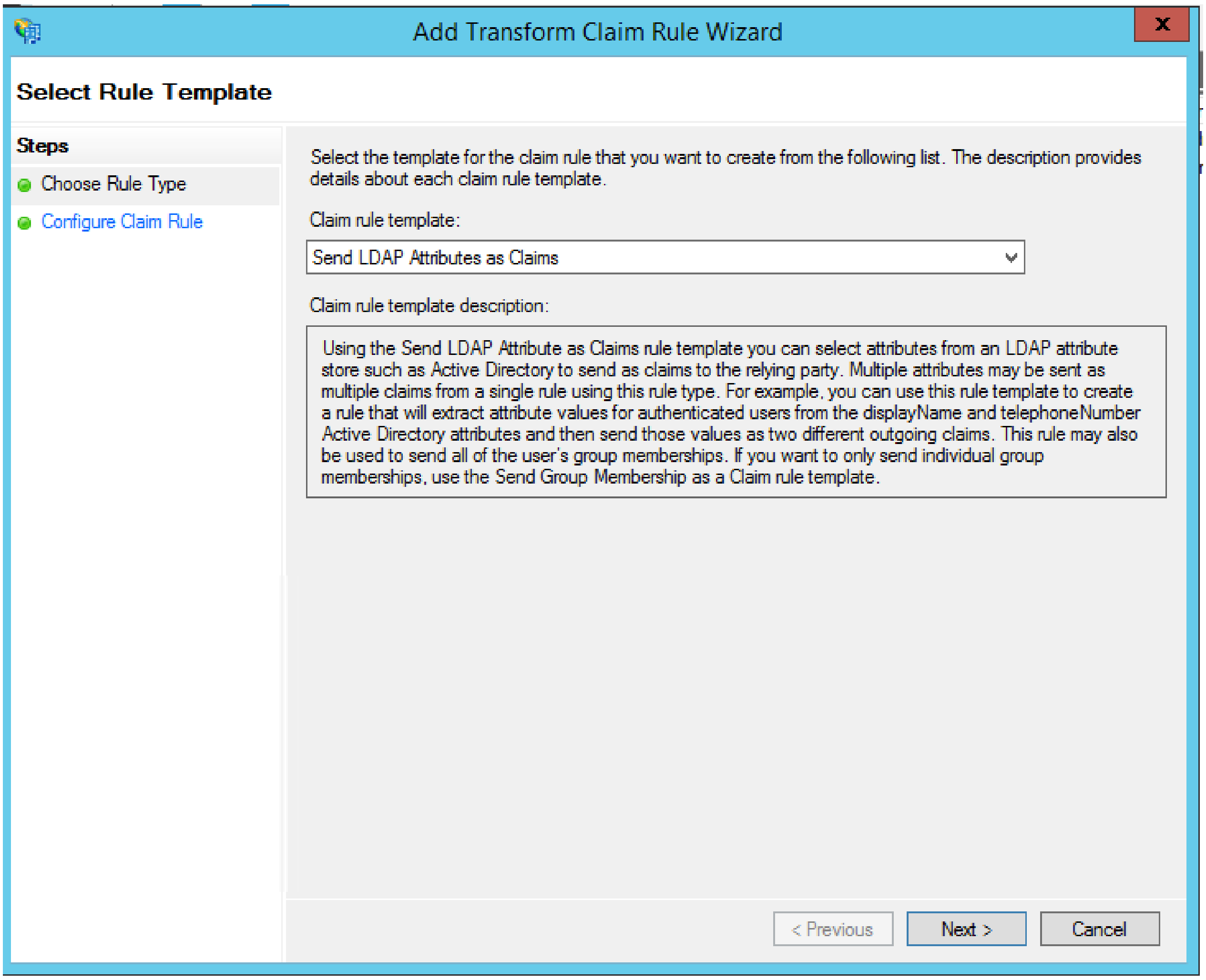
## Rule 2

Rule 2 consists of the following 'Custom Rule':

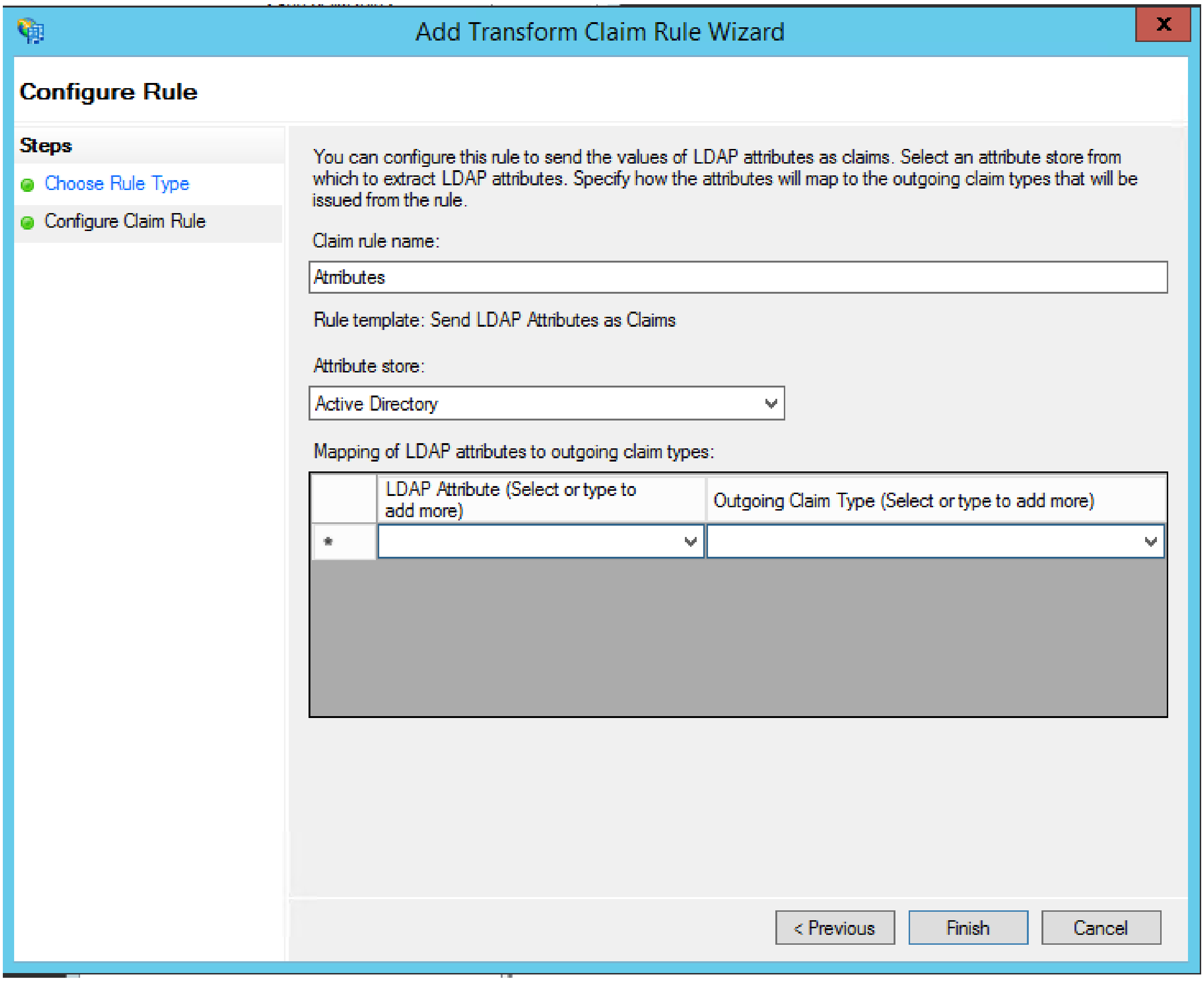
```
c:[Type ==
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/windowsaccountname"]

 => 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

To configure Rule 3, start with ‘Add Rule’.
Then select ‘Send LDAP Attributes as Claims’ and click ‘Next’.



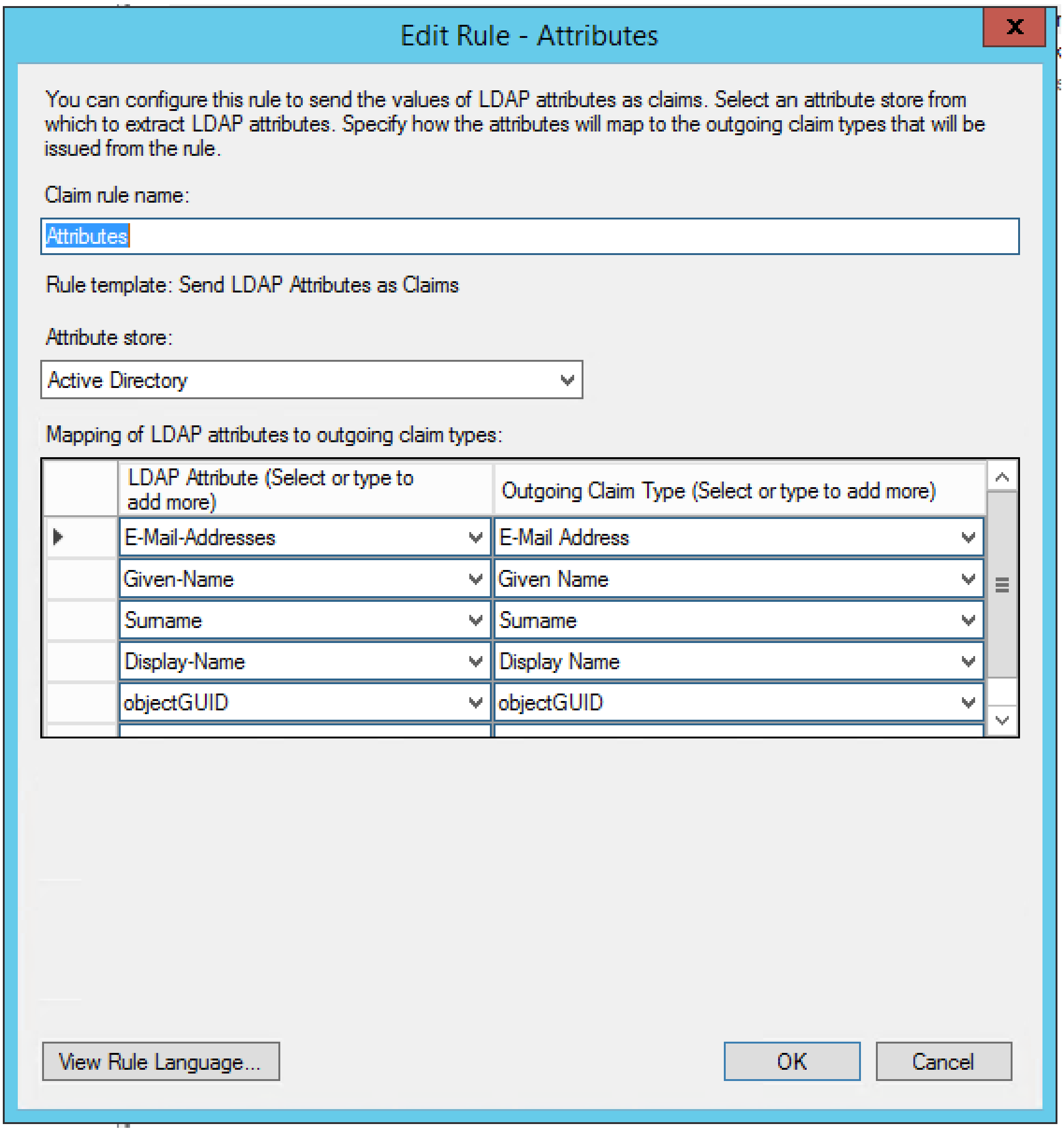
Give the rule a name. In the example we have entered 'Attributes'. Select 'Active Directory' as your Attribute store.



Configure the next screen the same as the example in the screen-print below:

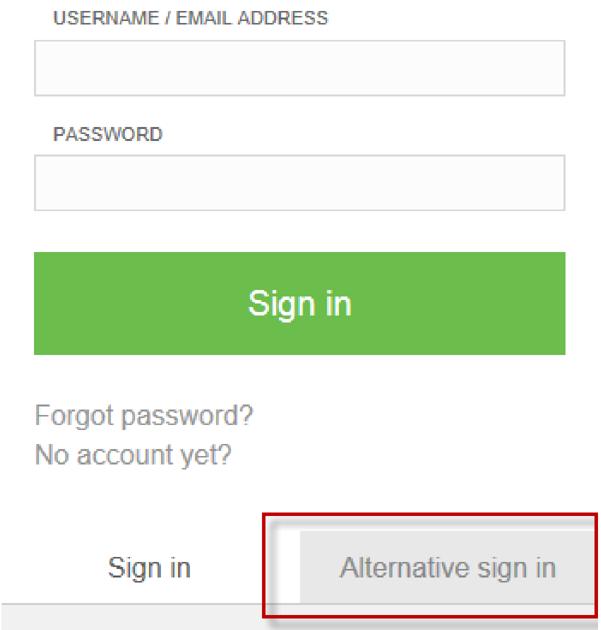
| | |
|---|---|
| E-Mail-Addresses | E-Mail address |
| Given-Name | Given Name |
| Surname | Surname |
| Display-Name | Display Name |
| objectGUID* | objectGUID |

*The objectGUID attribute might need to be entered manually, because it's not selectable by default. Sometimes the manually entered entry disappears, but then it needs to be entered again to make it visible.

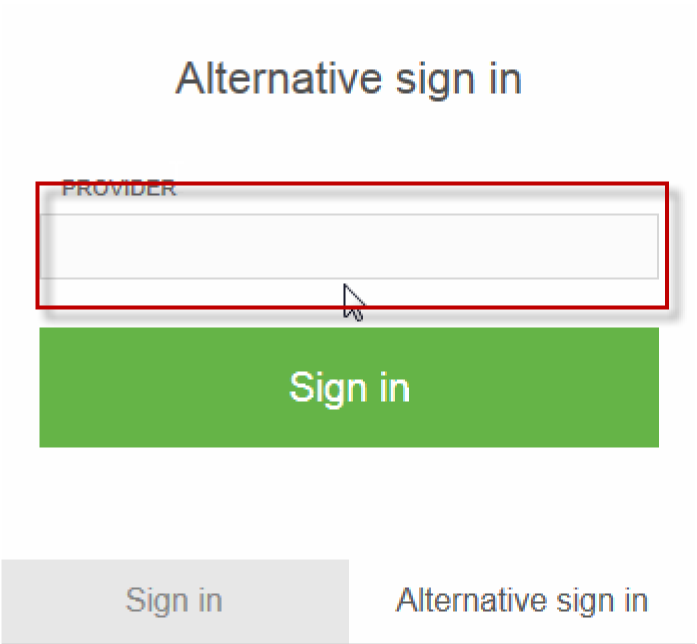


# What SSO looks like for messenger users

At the bottom of the login screen, choose 'Alternative sign in'.




You will then see this screen:




Enter your chosen Provider Name in the 'Provider' field (this will usually be the company name). You have set this in the messenger company settings.