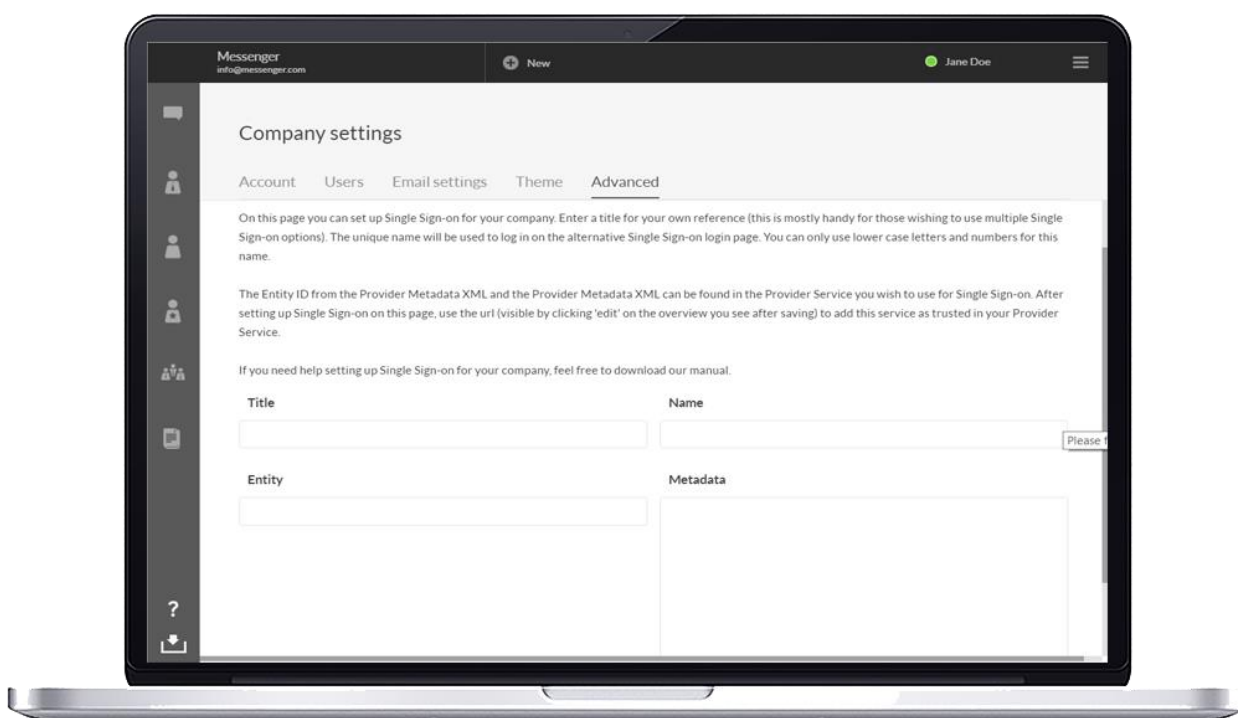


SETTING UP ADFS

A MANUAL



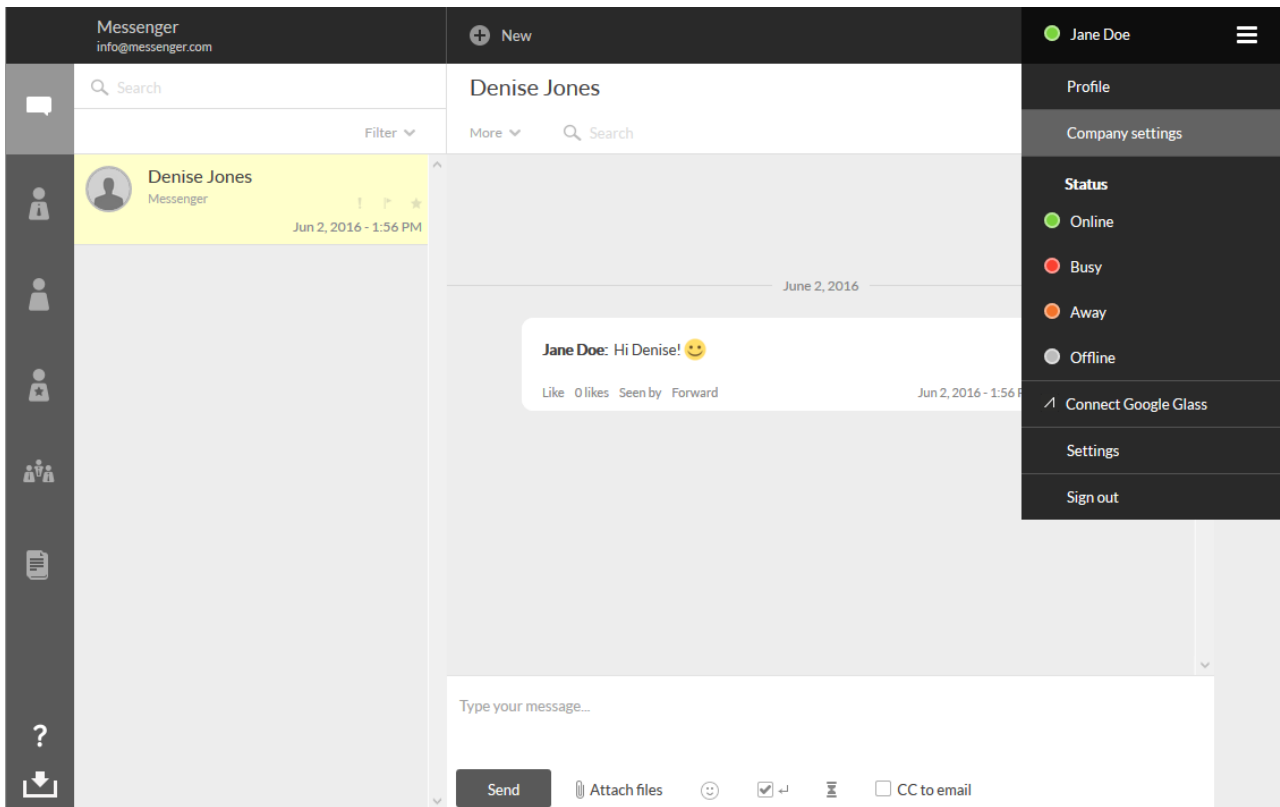
Contents

- Before configuring the settings on the ADFS server 3
- Set up ADFS 6
- Add Relying Party Trust..... 7
- Set the Claim Rules..... 14
 - Rule 1** 17
 - Rule 2** 17
 - Rule 3** 18
- What SSO looks like for messenger users 21

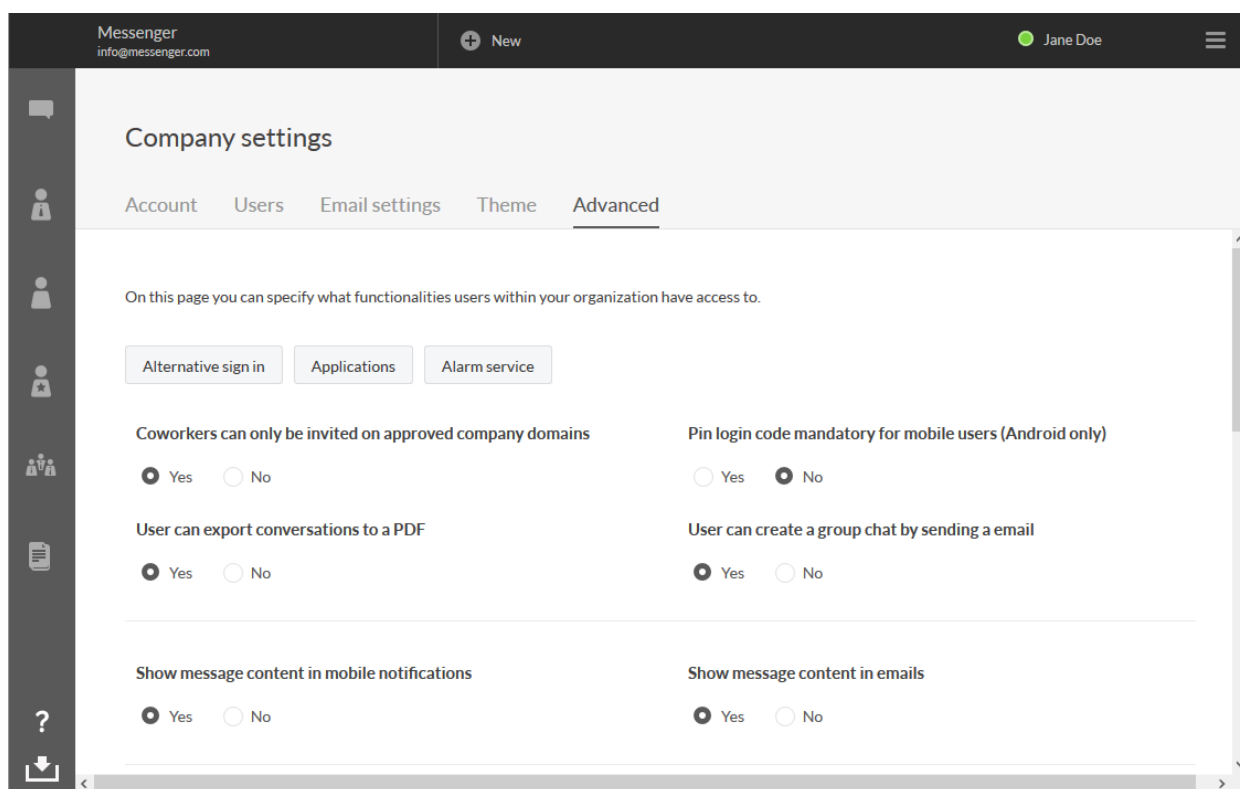
Before configuring the settings on the ADFS server

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.

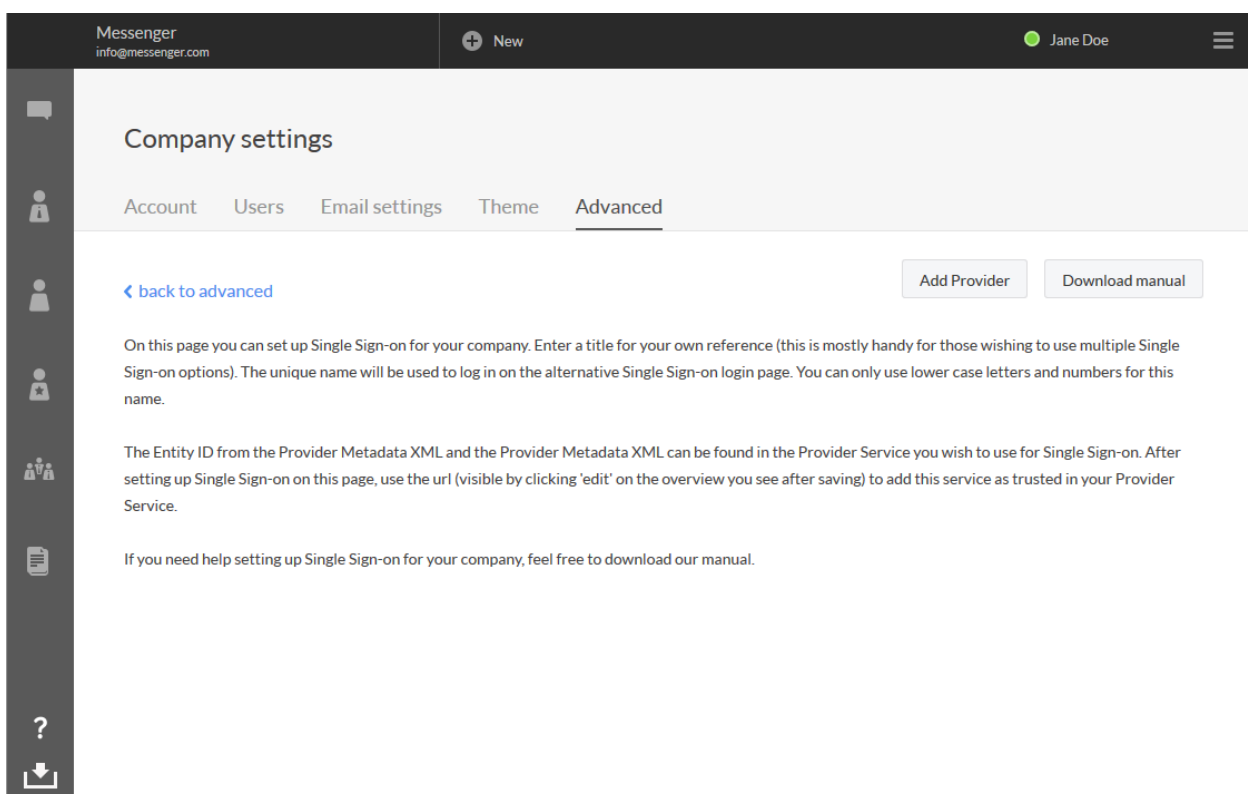
Click on 'Company settings'.



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 configure the ADFS on the ADFS server.

Title

Name

Entity

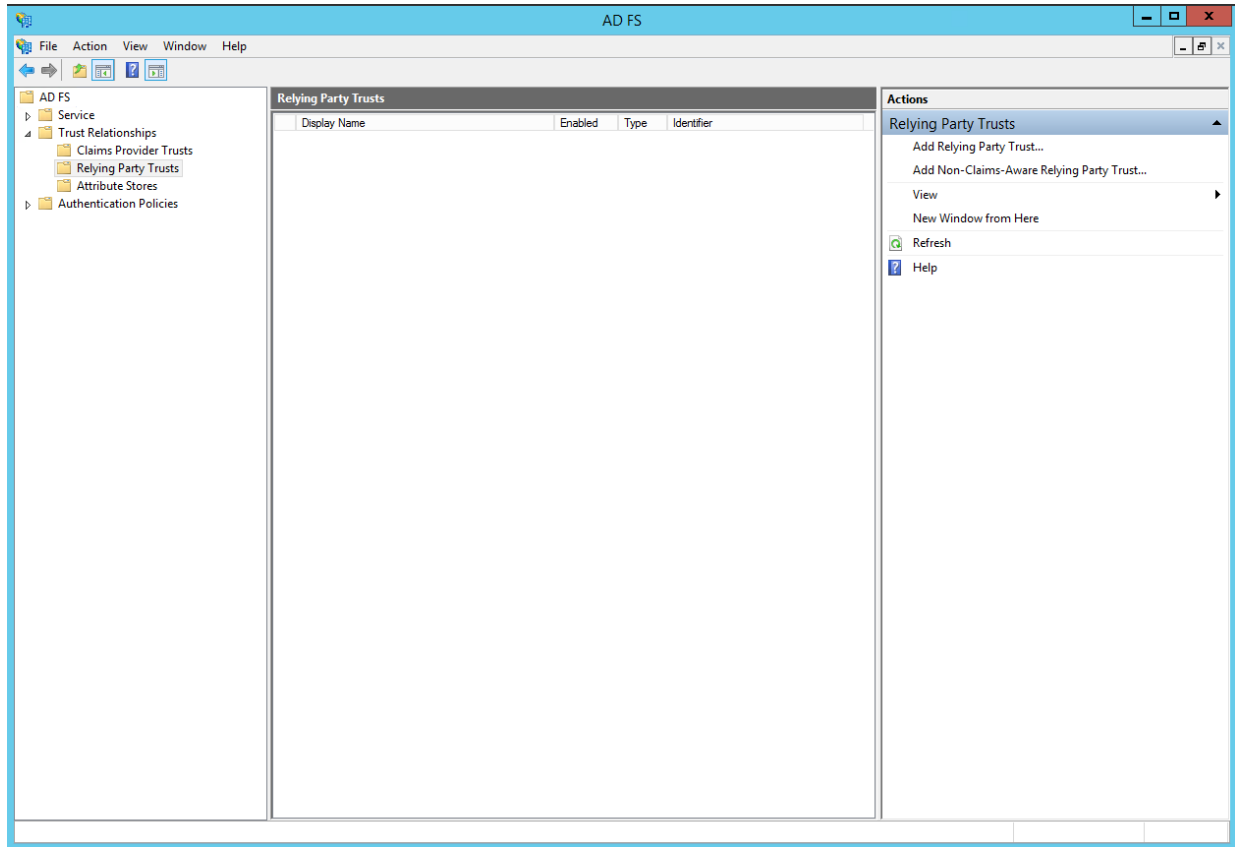
Metadata

Save

Cancel

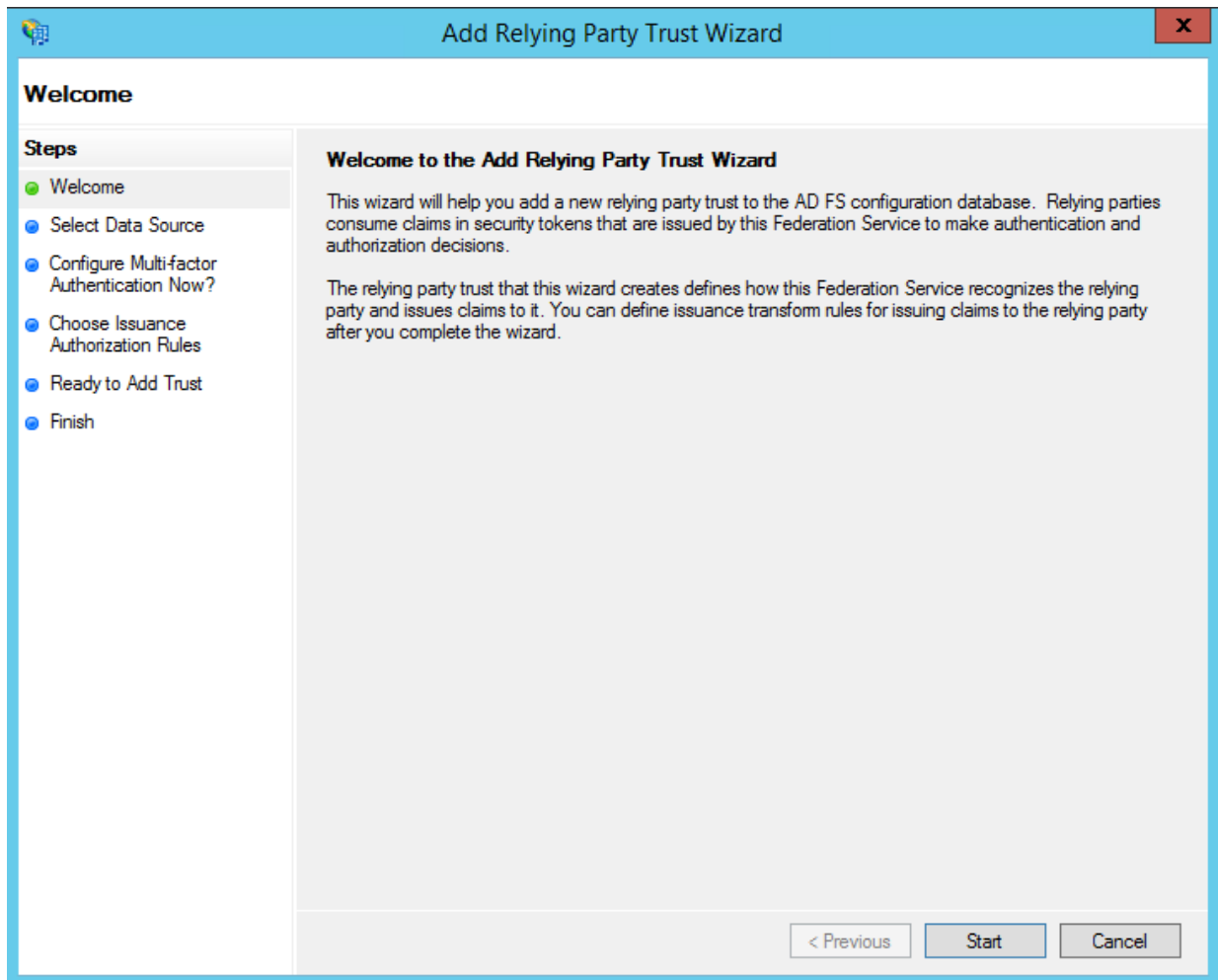
Set up ADFS

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=xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx>

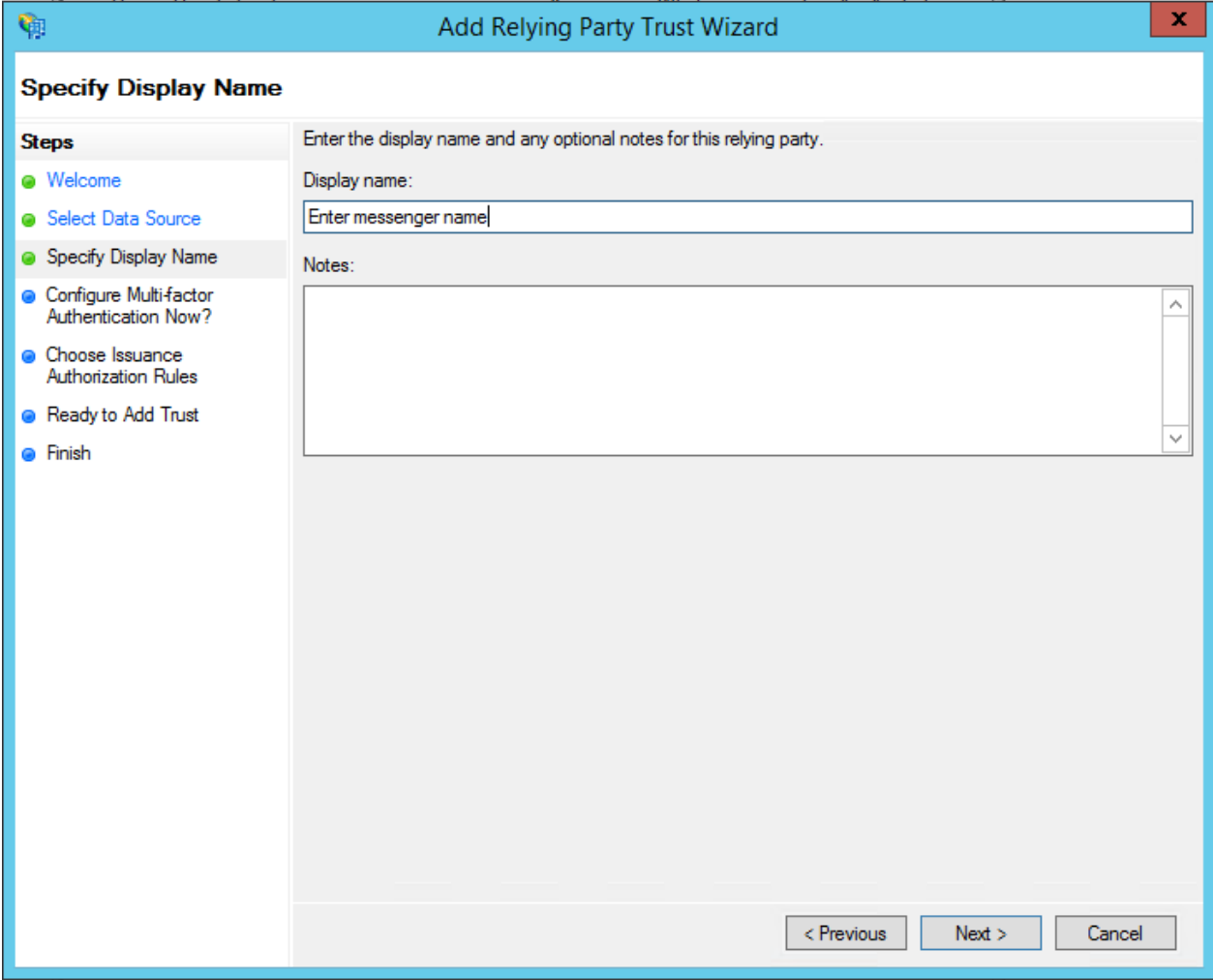
The 'xxxx' key consists of a unique code that is different for each company and can be generated based on the contents of the MetaData field.

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

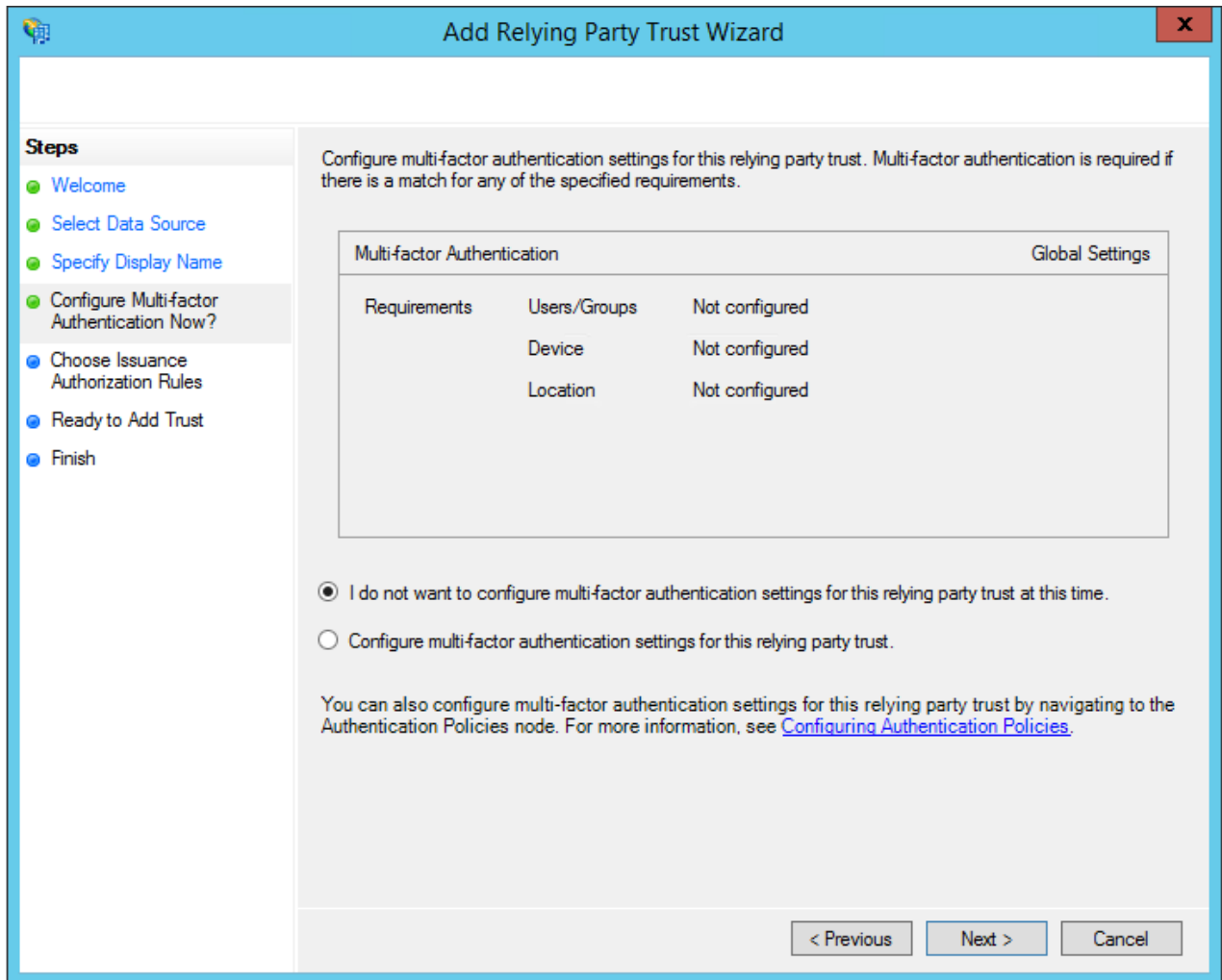
Fill in the Relying Party Trust URL and click 'Next'.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard' with a close button (X) on the right. The main area is titled 'Select Data Source'. On the left, a 'Steps' pane lists: Welcome, Select Data Source (highlighted), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main content area has 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: 'Federation metadata address (host name or URL):' with a text box containing 'https://url-to-messenger/msrv/auth/samlMetadata?UriParam=<xxxxxxx>:xxxx:xxxx:xxxx:xxxxxxxxxxxx'. 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: 'Federation metadata file location:' with a 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'.

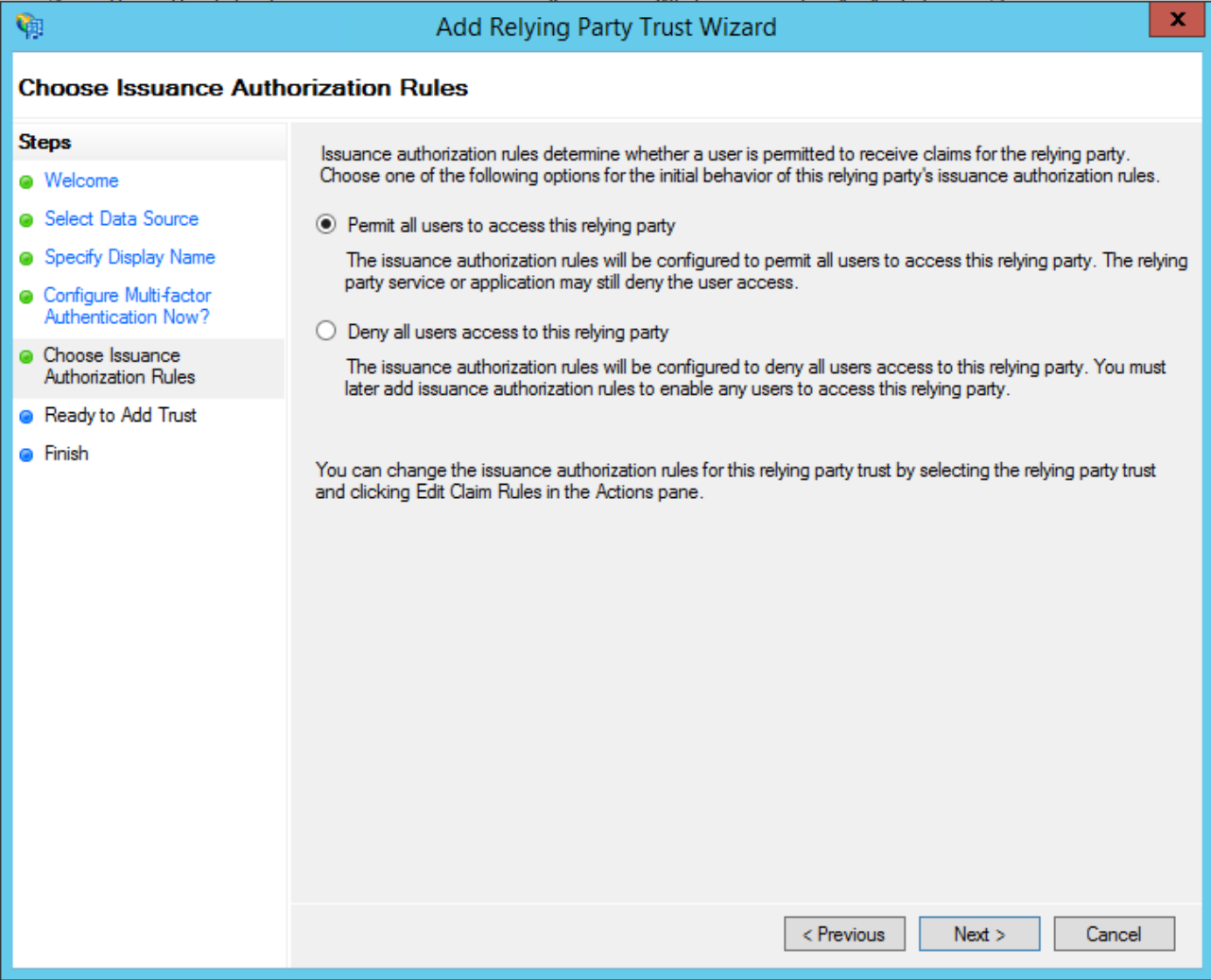
On the next screen you can enter a name and notes according to your own preferences. Click 'Next'.



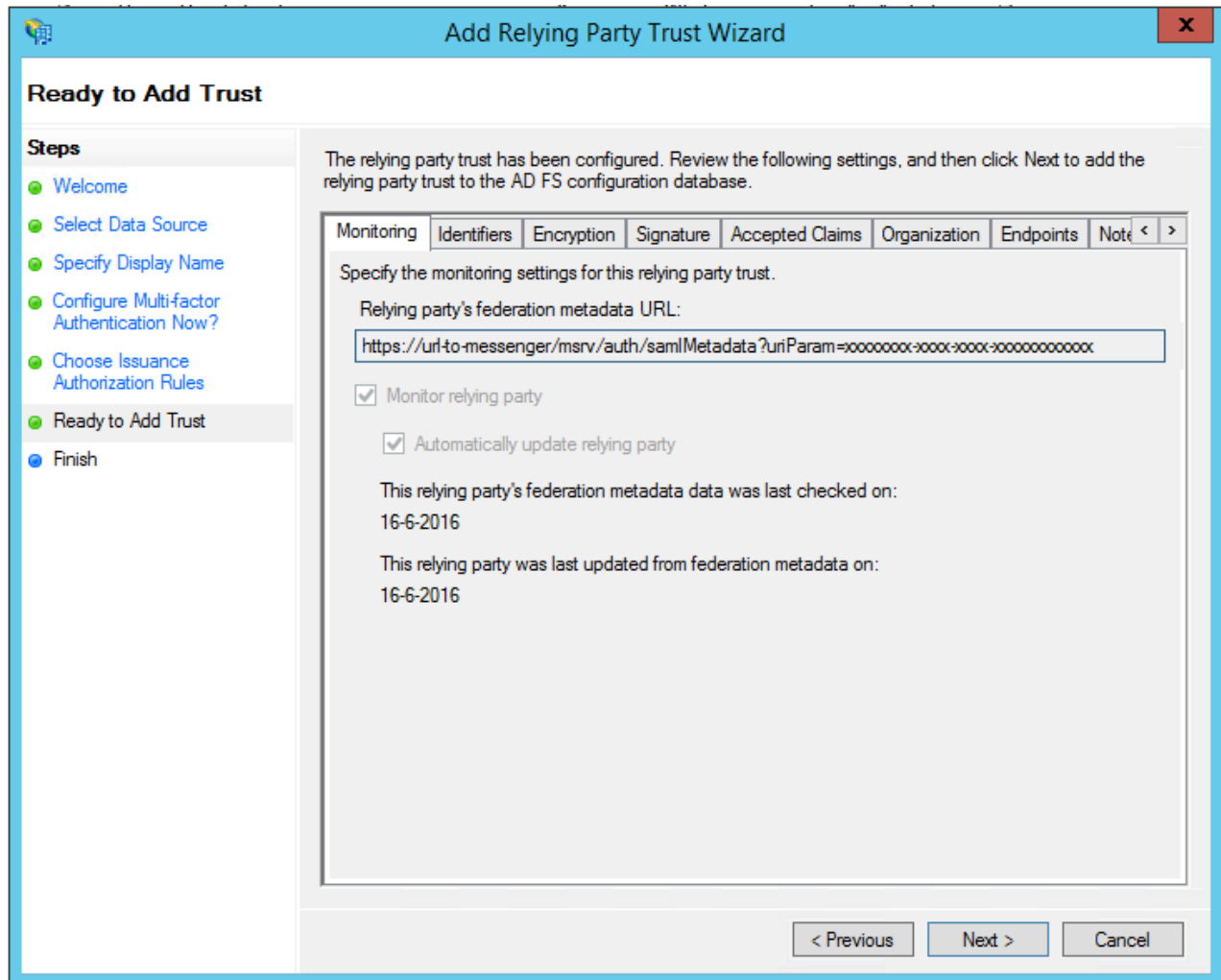
Next you will see the following screen – for our messenger, you can ignore this one. Click 'Next'.



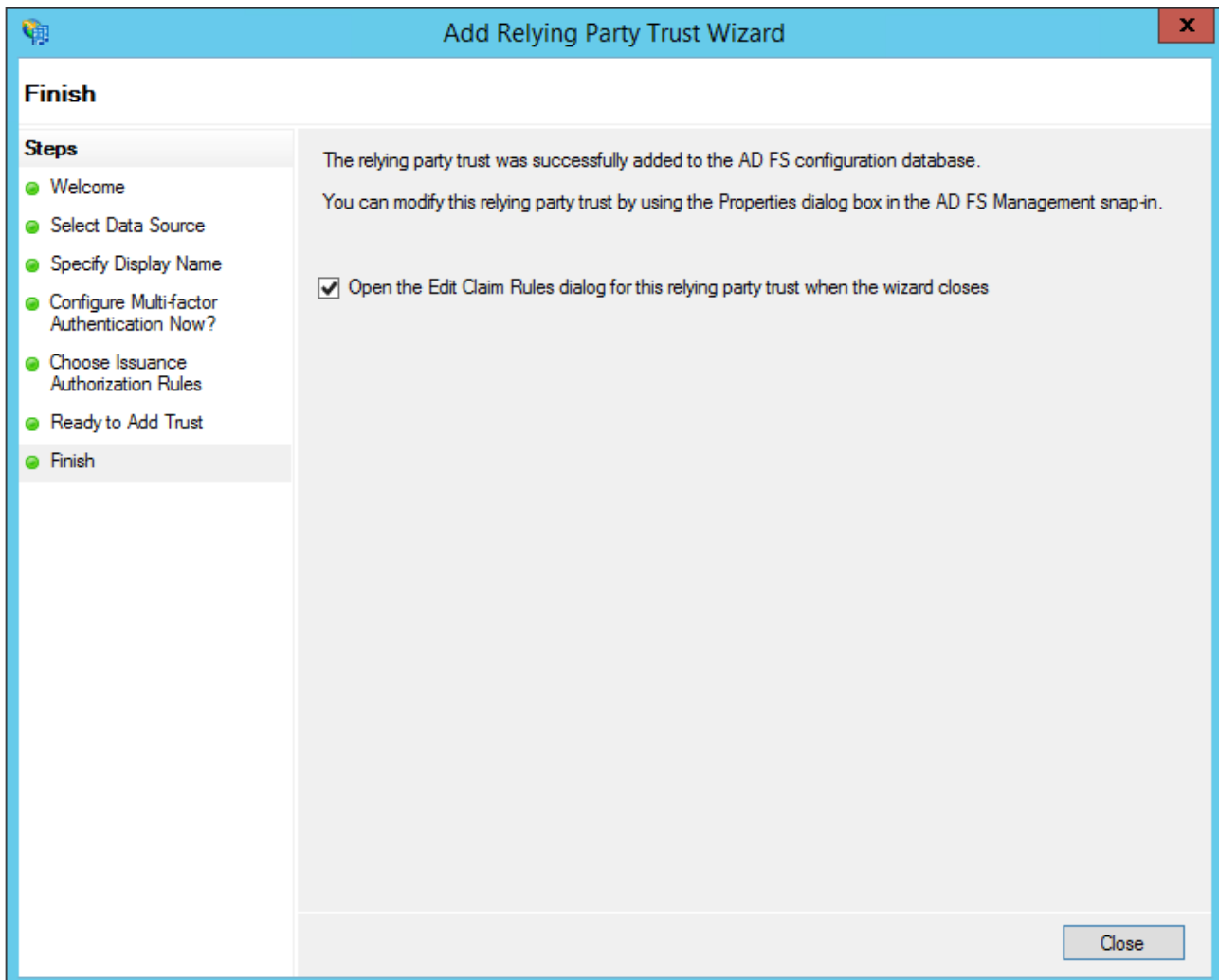
Next you will see the screen below. For our messenger, the default settings are correct. Click 'Next'.



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

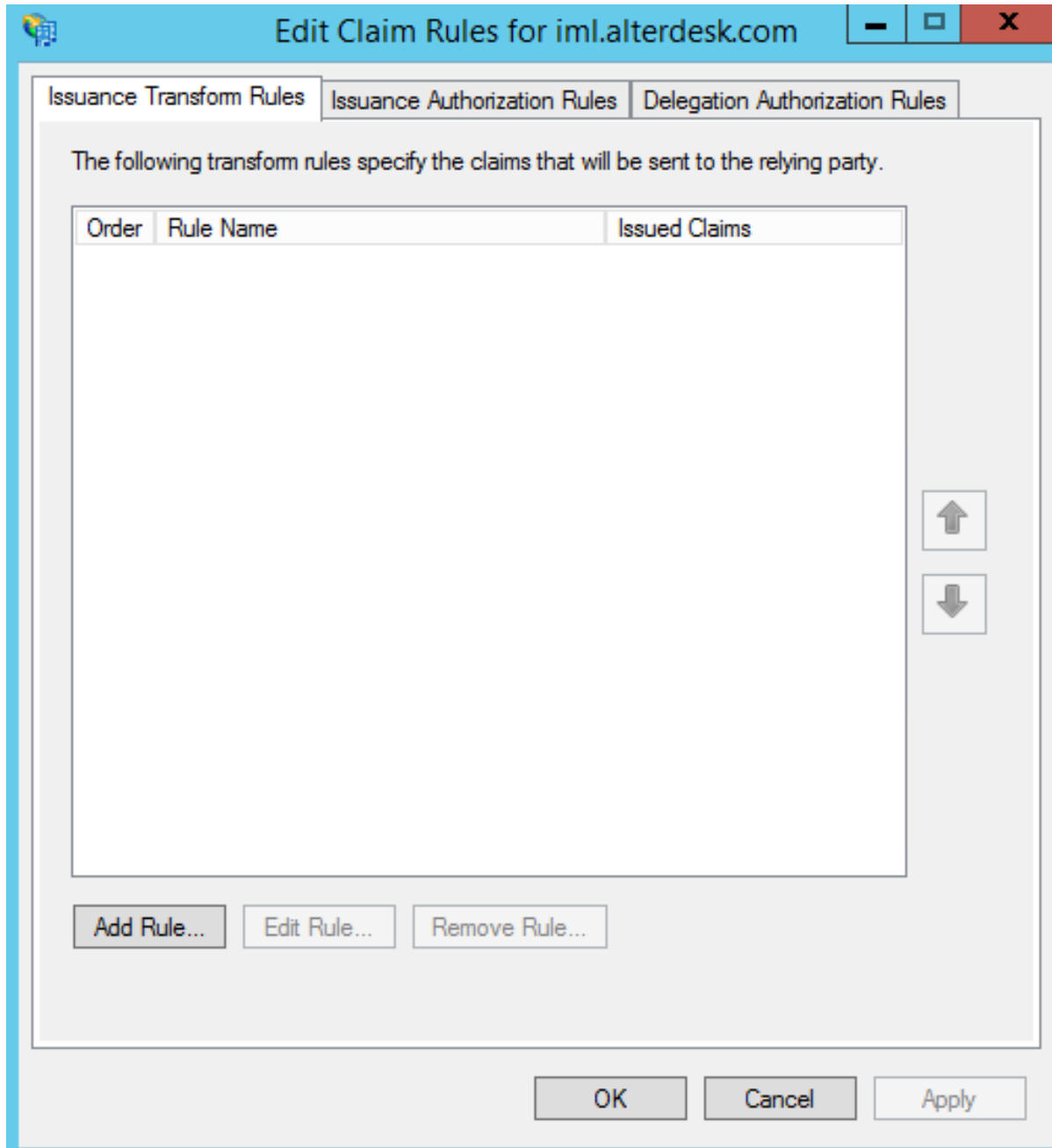


You have now reached the 'Finish' screen. Keep the check mark for 'Edit Claim Rules' on – you will need to configure these next. Click 'Close'.



Set the Claim Rules

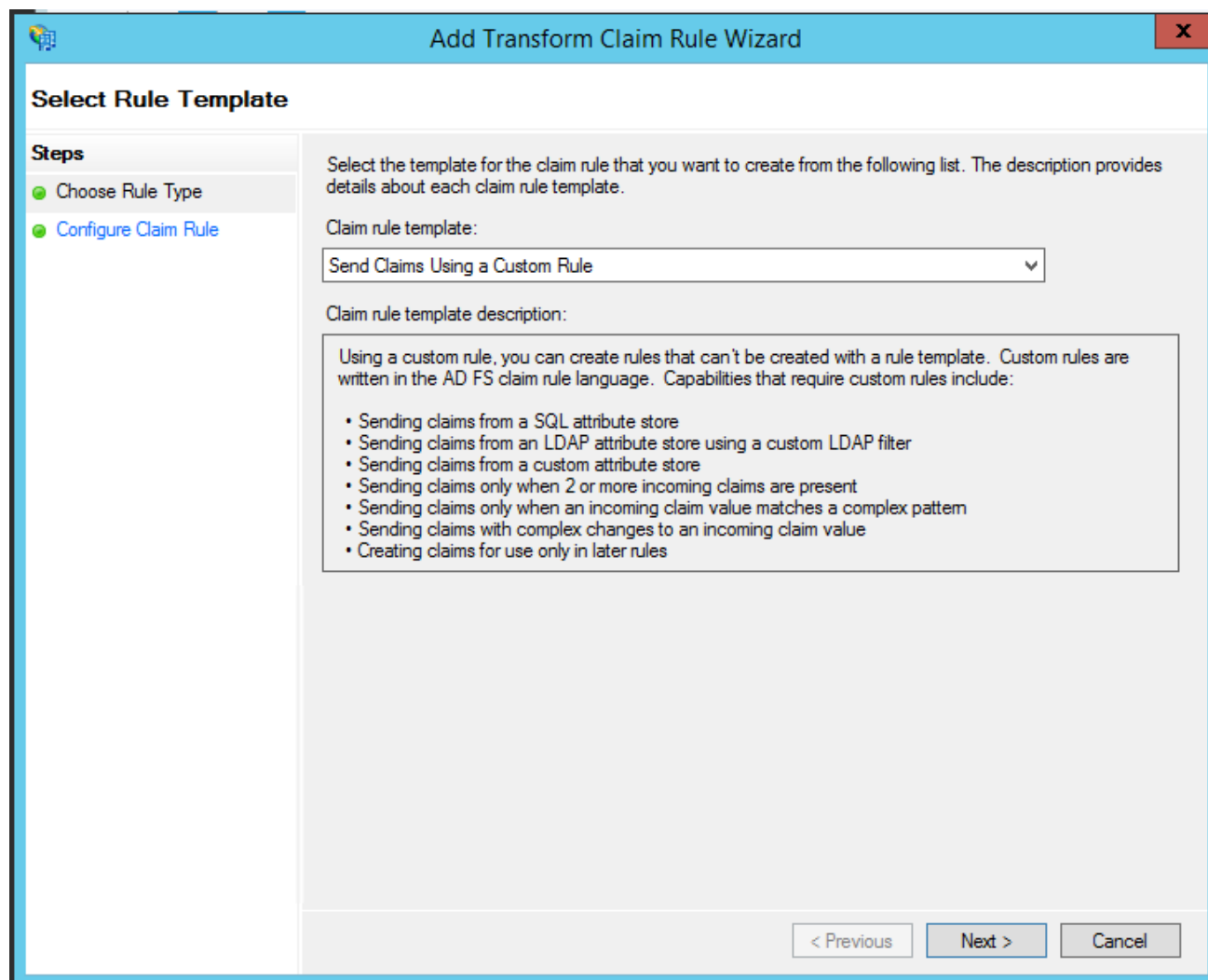
The 'Edit Claim Rules' screen will be opened after you close the previous screen.



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.

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 "Configure Rule". On the left, a "Steps" pane shows two steps: "Choose Rule Type" (highlighted with a green dot) and "Configure Claim Rule" (with a green dot). 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 is a text box labeled "Claim rule name:" which is currently empty. Underneath is the text "Rule template: Send Claims Using a Custom Rule". Below that is a large text area labeled "Custom rule:" which is also empty. At the bottom right of the dialog are three buttons: "< Previous", "Finish", and "Cancel".

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

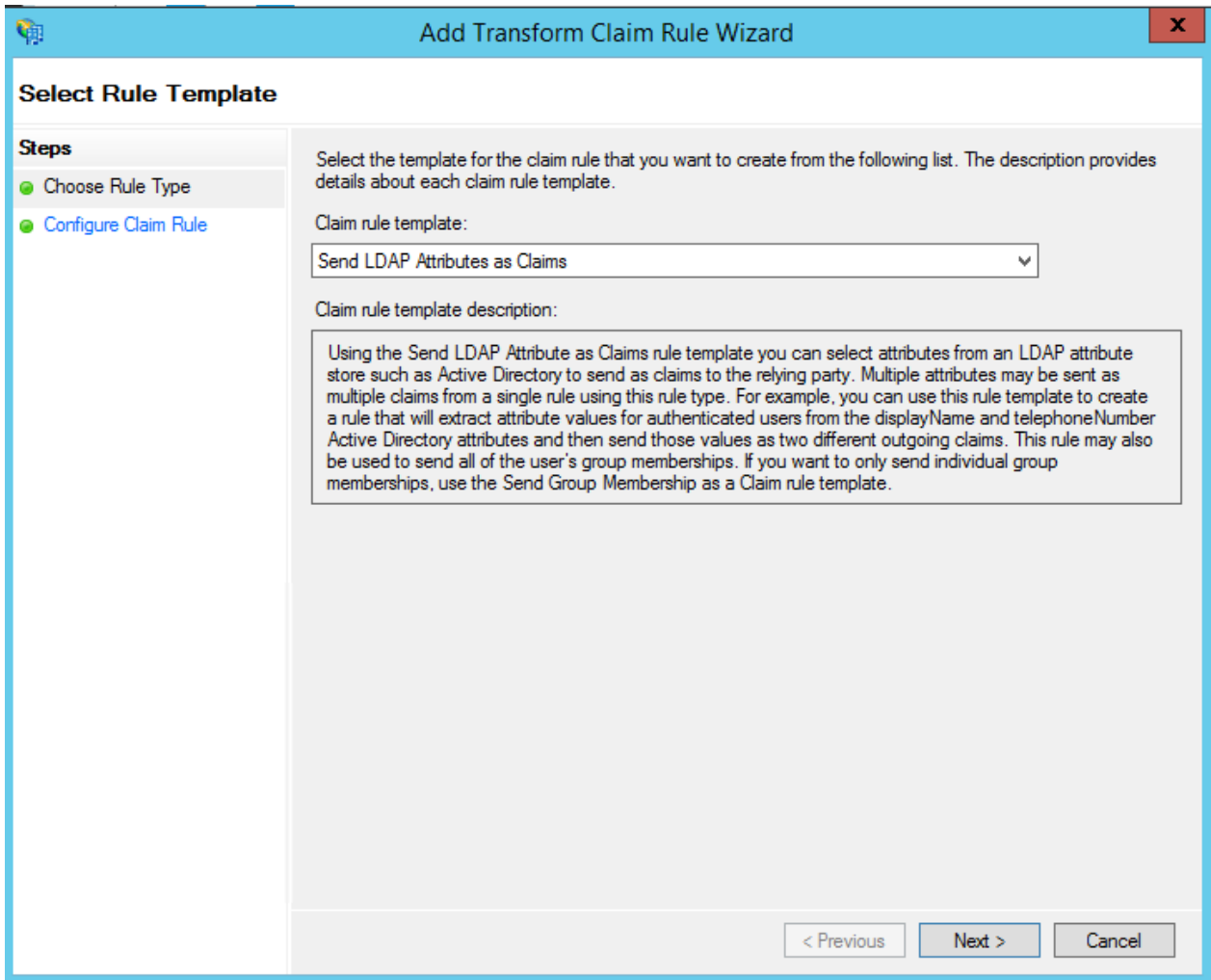
Rule 2 consists of the following 'Custom Rule':

```
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'.



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" (indicated by a green dot) and "Configure Claim Rule" (indicated by 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:

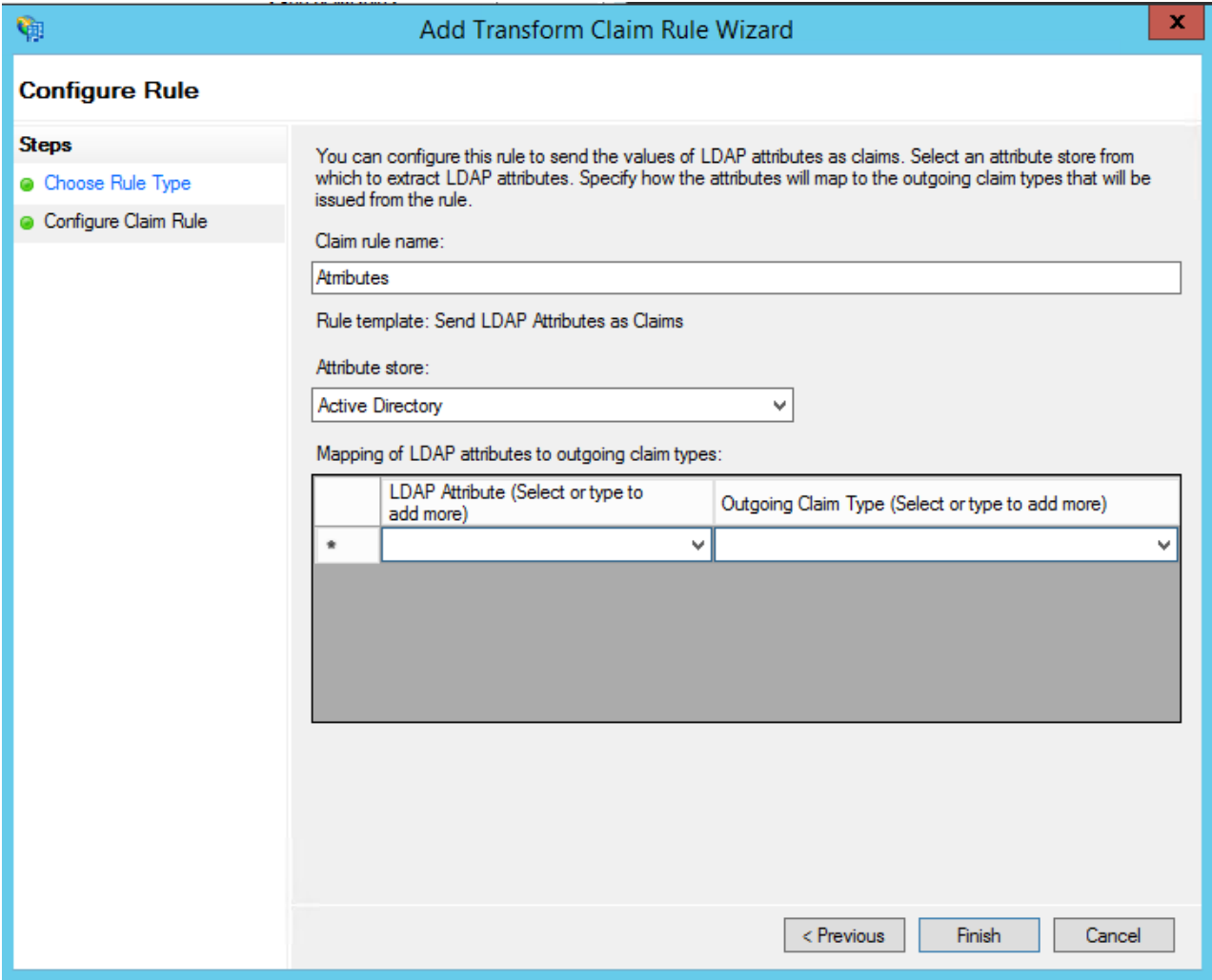
Send LDAP Attributes as Claims

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 >" (highlighted in blue), and "Cancel".

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.

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

View Rule Language... OK Cancel

What SSO looks like for messenger users

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

USERNAME / EMAIL ADDRESS

PASSWORD

Sign in

Forgot password?
No account yet?

Sign in Alternative sign in

You will then see this screen:

Alternative sign in

PROVIDER

Sign in

Sign in Alternative sign in

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.

