



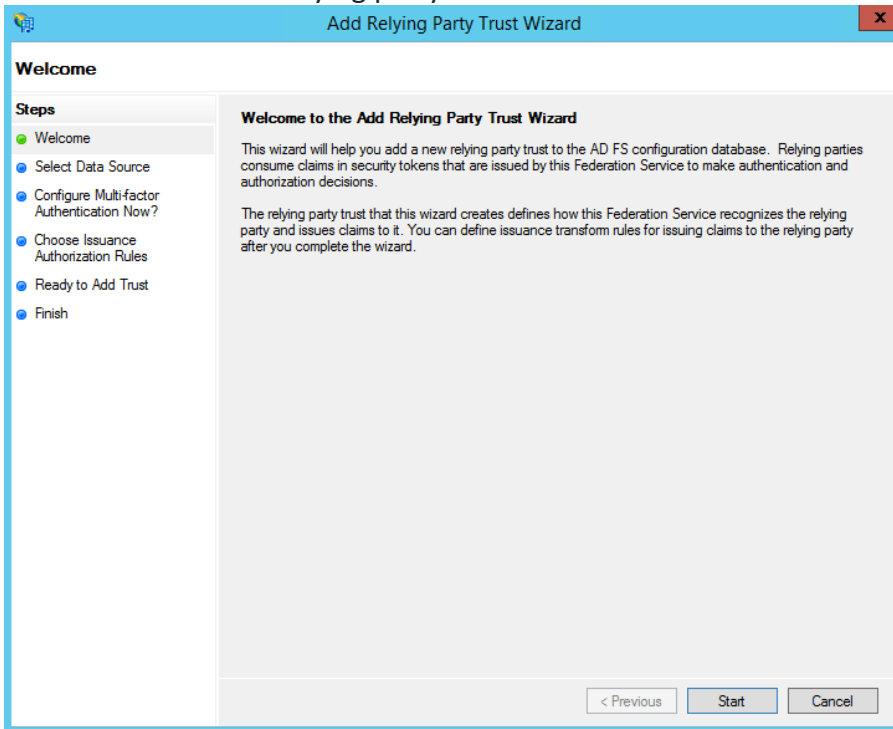
# Rydoo Single-Sign-On

Support



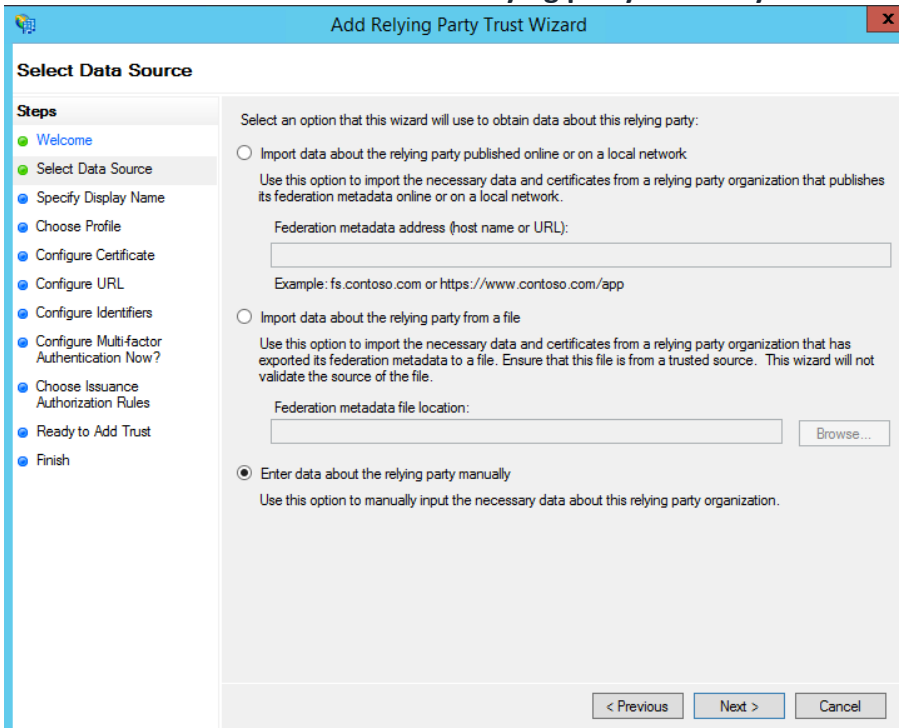
# Connect Rydoo to AD FS 3.0 for SSO

## 1. Create a new relying party trust.



The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with the text 'Add Relying Party Trust Wizard' and a close button. The window is divided into two main sections. On the left, under the heading 'Welcome', there is a 'Steps' list with the following items: 'Welcome' (selected with a green dot), 'Select Data Source', 'Configure Multi-factor Authentication Now?', 'Choose Issuance Authorization Rules', 'Ready to Add Trust', and 'Finish'. The main area on the right is titled 'Welcome to the Add Relying Party Trust Wizard'. It contains two paragraphs of text: 'This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.' and 'The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.' At the bottom right, there are three buttons: '< Previous', 'Start', and 'Cancel'.

## 2. Select Enter data about the relying party manually.



The screenshot shows the 'Add Relying Party Trust Wizard' window at the 'Select Data Source' step. The title bar is blue with the text 'Add Relying Party Trust Wizard' and a close button. The window is divided into two main sections. On the left, under the heading 'Select Data Source', there is a 'Steps' list with the following items: 'Welcome', 'Select Data Source' (selected with a green dot), 'Specify Display Name', 'Choose Profile', 'Configure Certificate', 'Configure URL', 'Configure Identifiers', 'Configure Multi-factor Authentication Now?', 'Choose Issuance Authorization Rules', 'Ready to Add Trust', and 'Finish'. The main area on the right is titled 'Select an option that this wizard will use to obtain data about this relying party:'. It contains three radio button options: 'Import data about the relying party published online or on a local network' (unselected), 'Import data about the relying party from a file' (unselected), and 'Enter data about the relying party manually' (selected with a green dot). The first option has a text box for 'Federation metadata address (host name or URL):' with the example 'fs.contoso.com or https://www.contoso.com/app'. The second option has a text box for 'Federation metadata file location:' with a 'Browse...' button. The third option has a 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'.

3. Enter the Display name and Notes as shown below.

The screenshot shows the 'Specify Display Name' step of the 'Add Relying Party Trust Wizard'. The window title is 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name (current), Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area is titled 'Specify Display Name' and 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 box containing 'rydoo SSO Login'. Below that is a 'Notes:' label followed by a large text area. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

4. Use AD FS profile.

The screenshot shows the 'Choose Profile' step of the 'Add Relying Party Trust Wizard'. The window title is 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile (current), Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area is titled 'Choose Profile' and contains the instruction 'This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.' Below this, there are two radio button options. The first option is 'AD FS profile', which is selected, and it has a description: 'This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.' The second option is 'AD FS 1.0 and 1.1 profile', which is not selected, and it has a description: 'This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.' At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

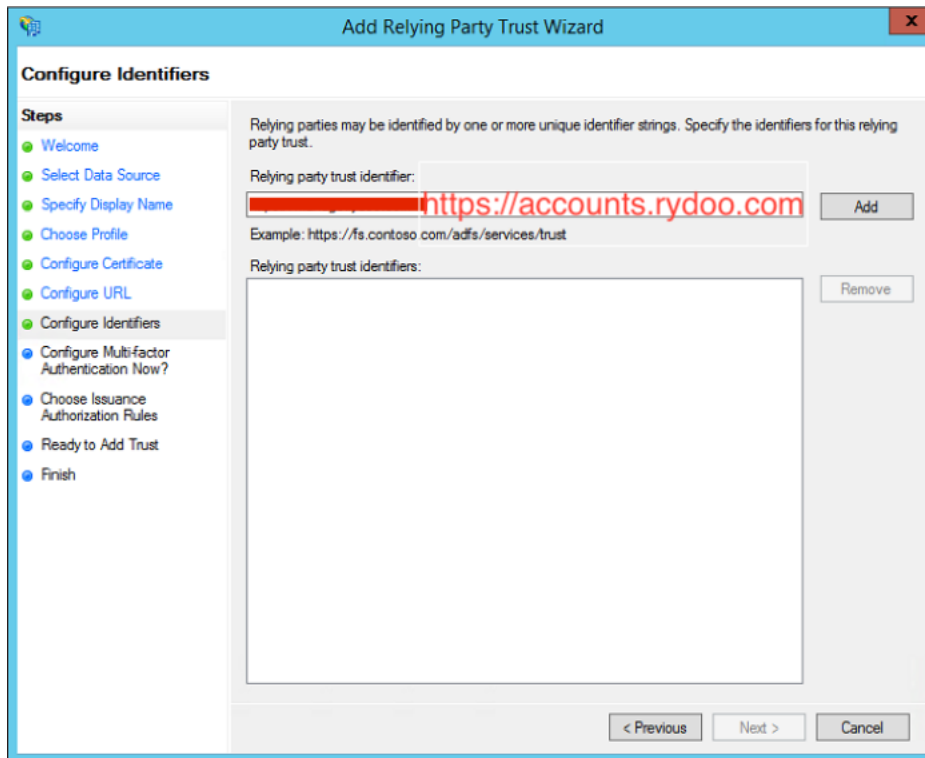
5. Click **Next** without altering this page

The screenshot shows a Windows-style window titled "Add Relying Party Trust Wizard" with a close button (X) in the top right corner. The window is divided into two main sections. On the left is a "Steps" sidebar with a list of steps: "Welcome", "Select Data Source", "Specify Display Name", "Choose Profile", "Configure Certificate" (which is highlighted with a green dot and a blue selection bar), "Configure URL", "Configure Identifiers", "Configure Multi-factor Authentication Now?", "Choose Issuance Authorization Rules", "Ready to Add Trust", and "Finish". The main area on the right is titled "Configure Certificate" and contains the following text: "Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click: Browse...". Below this text is a form with four labels: "Issuer:", "Subject:", "Effective date:", and "Expiration date:". Below the form are three buttons: "View...", "Browse..." (which is highlighted with a blue border), and "Remove". At the bottom right of the window are three buttons: "< Previous", "Next >", and "Cancel".

6. Choose SAML 2.0 and set the service URL:

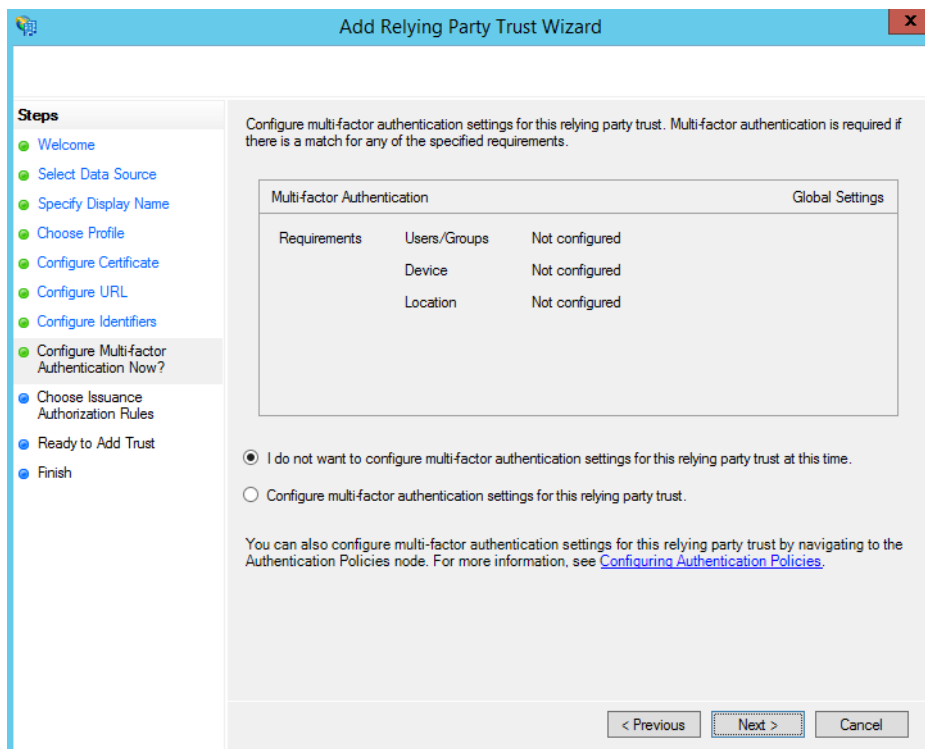
<https://accounts.rydoo.com/saml/CompanyName/Acs>

7. On the next screen, add a **Relying party trust identifier**: <https://accounts.rydoo.com>

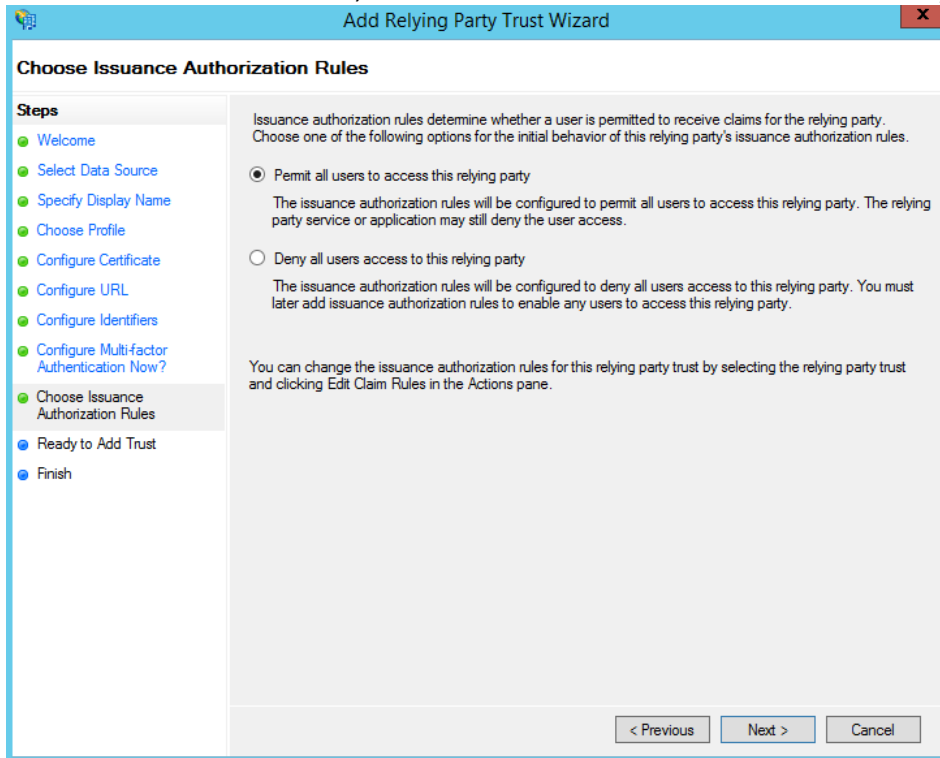


8. Set the relying party identifier to **Rydoo**: <https://accounts.rydoo.com>

9. Leave Multifactor Authentication at default.



10. On the next screen, select the **Permit all users to access this relying party**



11. Click **Next** to add the relying party trust.

12. Close the wizard.

### **CLAIM RULES**

1. Log into the ADFS server and open the management console.
2. Right-click the relying party trust and select **Edit Claim Rules**.
3. Click the **Issuance Transform Rules** tab.
4. Select **Add Rules**.
5. Select **Send LDAP Attribute as Claims** as the claim rule template to use.
6. Give the claim a name such as Get LDAP Attributes.
7. Set the **Attribute store** to Active Directory, the **LDAP Attribute** to E-Mail-Addresses, and the **Outgoing Claim Type** to E-mail Address.

Edit Rule - Get Attribute

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
*		

8. Select **Add Rules**.
9. Select **Transform an Incoming Claim** as the claim rule template to use.
10. Give the Claim a name such as Email to Name ID.
11. Set the **Incoming claim type** to the **Outgoing Claim Type** in the previous rule. For example, E-Mail Address.
12. Set the **Outgoing claim type** to Name ID and the **Outgoing name ID format** to Email.
13. **Note:** These values must match the [Name ID policy](#) you define during SAML 2.0 configuration.
14. Select **Pass through all claim values**.
15. Click on Finish.

Edit Rule - Email to NameID

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

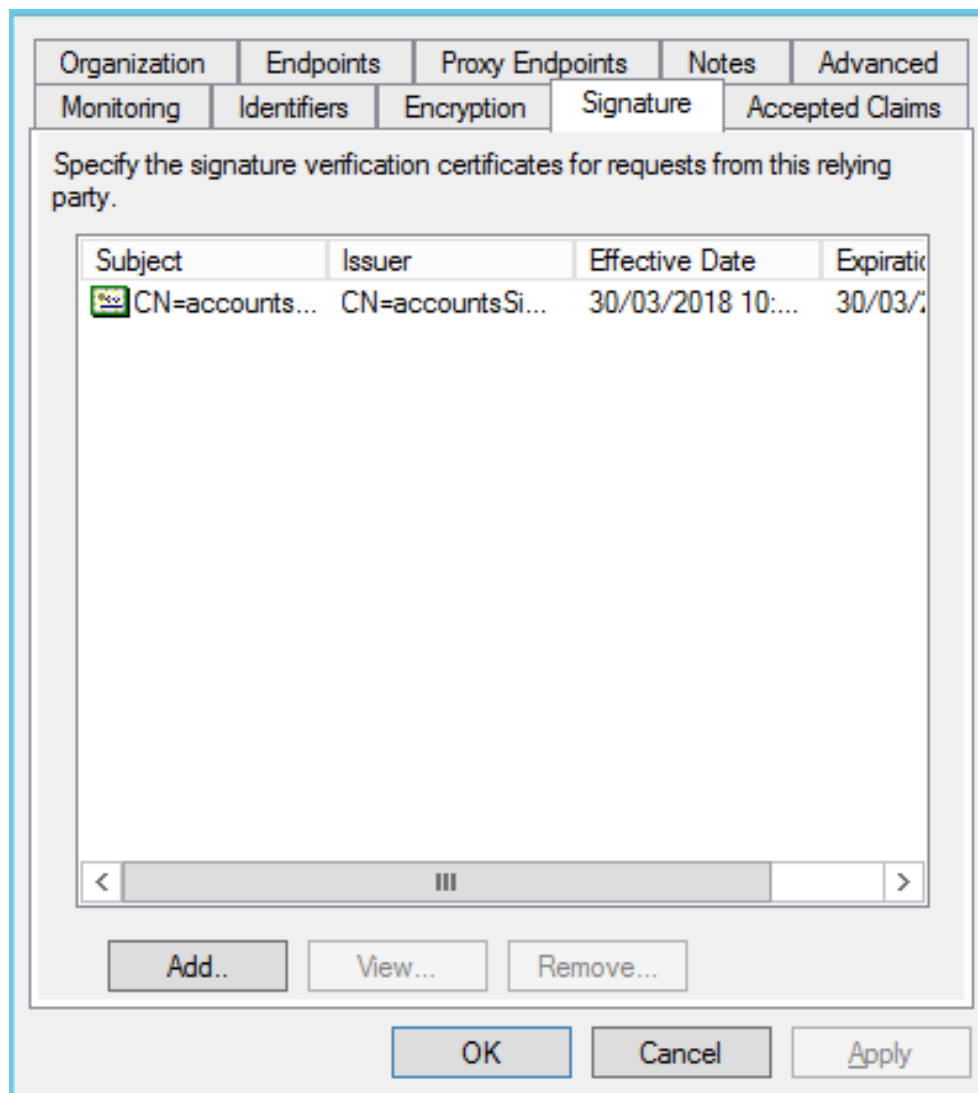
☒ Pass through all claim values  
☐ Replace an incoming claim value with a different outgoing claim value  
     Incoming claim value:   
     Outgoing claim value:    
☐ Replace incoming e-mail suffix claims with a new e-mail suffix  
     New e-mail suffix:   
     Example: fabrikam.com

16. Apply rules.

### Logout certificate configuration

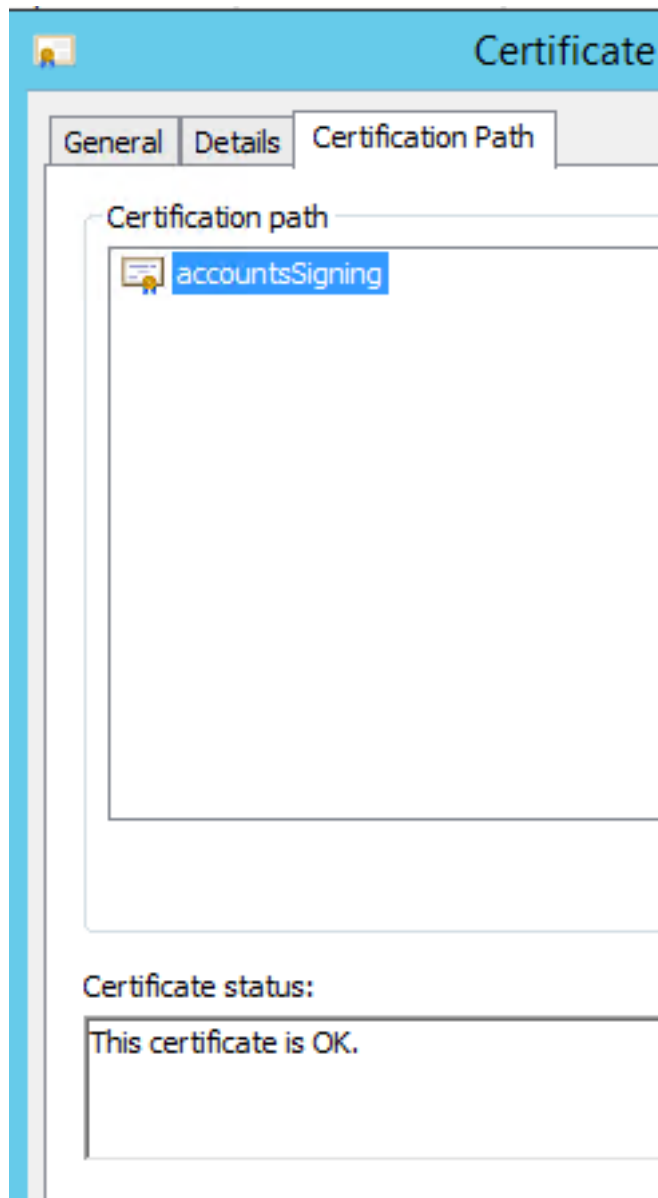
17. you open the relying party trust, go to tab Signature, you click Add, then go to the location of where you saved the .cer and install it.





18. Then you double click on the certificate, and install it in the local machine Trusted root certification authorities store, this needs to be done on all the ADFS servers, it's a local reference that the certificate is valid. Otherwise it's possible that this will show an error, something like "not possible to validate the root CA".

Note: it's also possible to use an encryption certificate, this can be the same as the signature.



19. Under SAML Logout (TrustedURL) should be configured as follows:  
<https://accounts.rydoo.com/saml/CompanyName/Logout>

## Edit Endpoint



Endpoint type:

SAML Logout

Binding:

POST

☐ Set the trusted URL as default

Index: 0

Trusted URL:

<https://accounts.rydoo.com/saml/sp/dest/Logout>

Example: <https://sts.contoso.com/adfs/ls>

Response URL:

Example: <https://sts.contoso.com/logout>

OK

Cancel