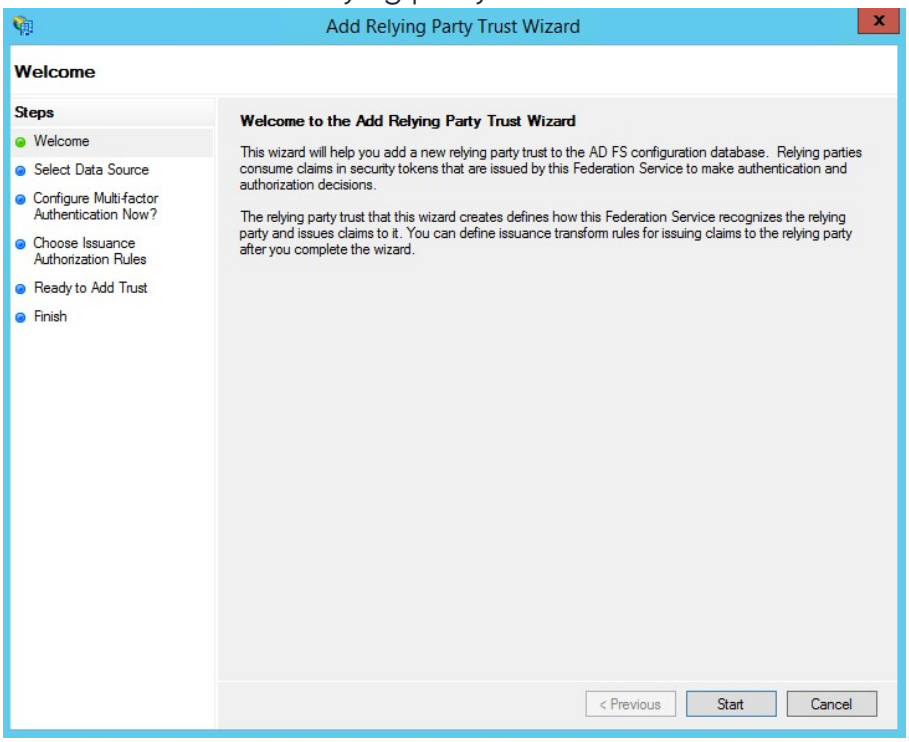
rydoo

Rydoo
Single-Sign-On

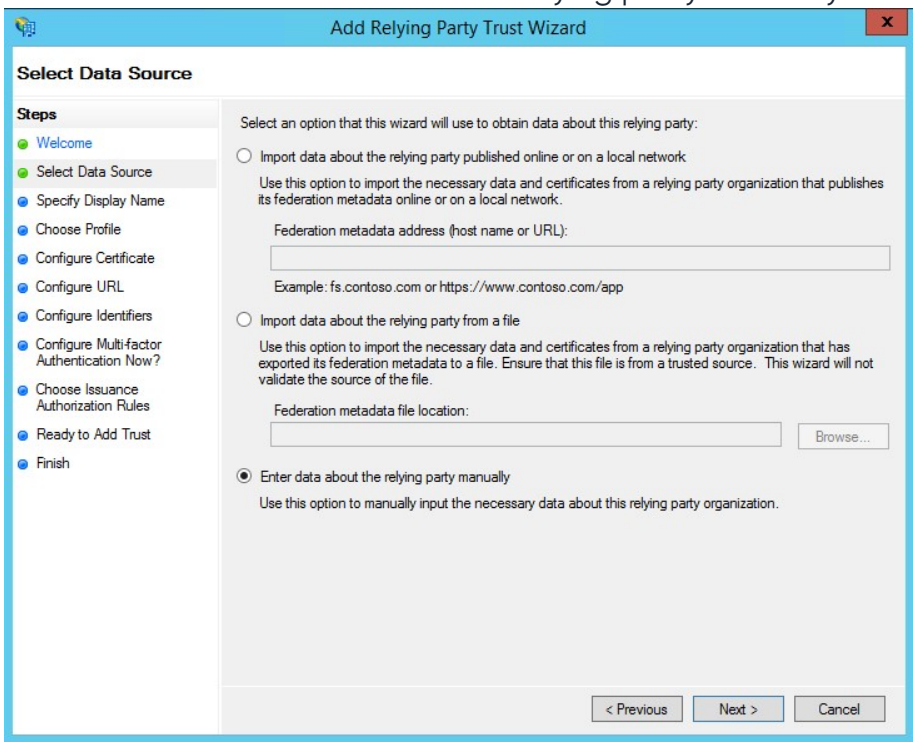
SUPPORT

Configure Rydoo Single Sign-On using ADFS 3.0

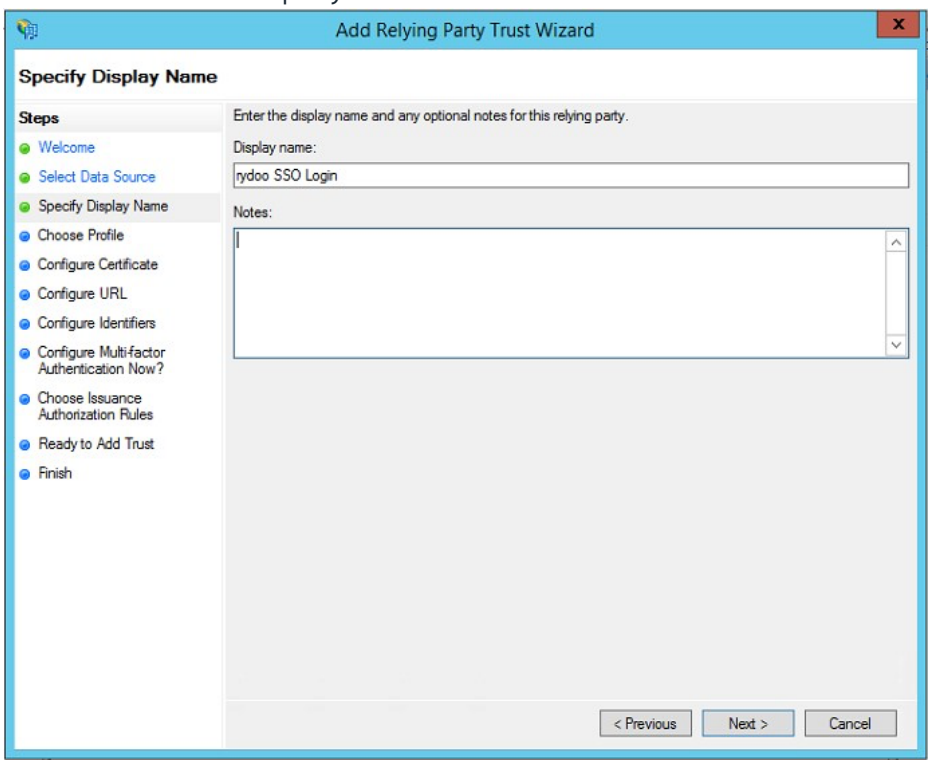
1. Create a new relying party trust.



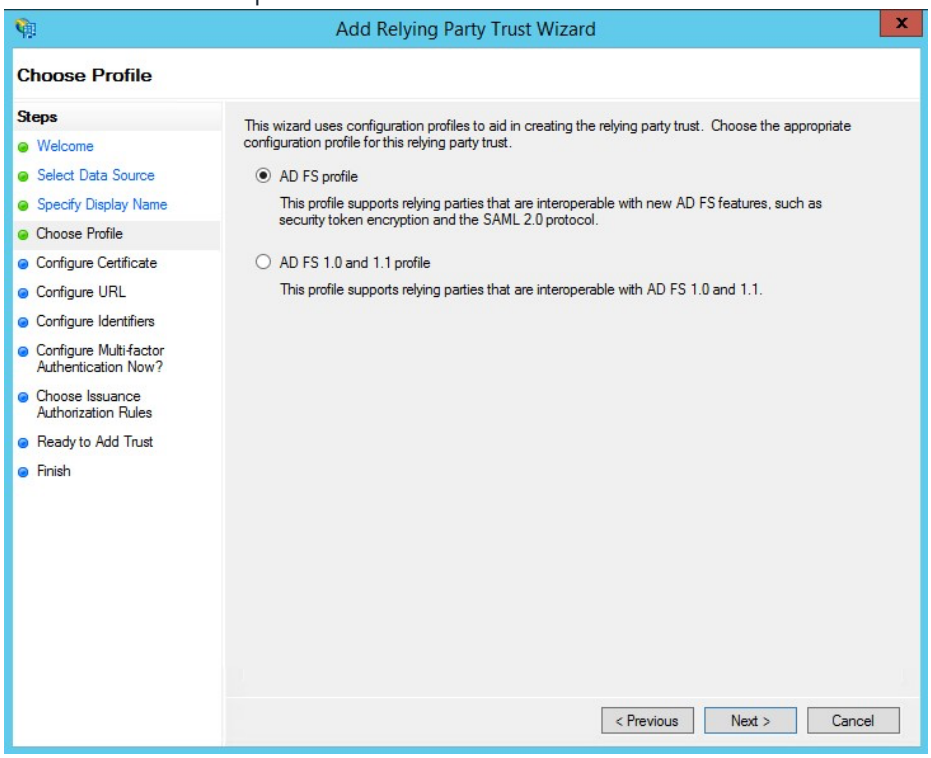
2. Select Enter data about the relying party manually.



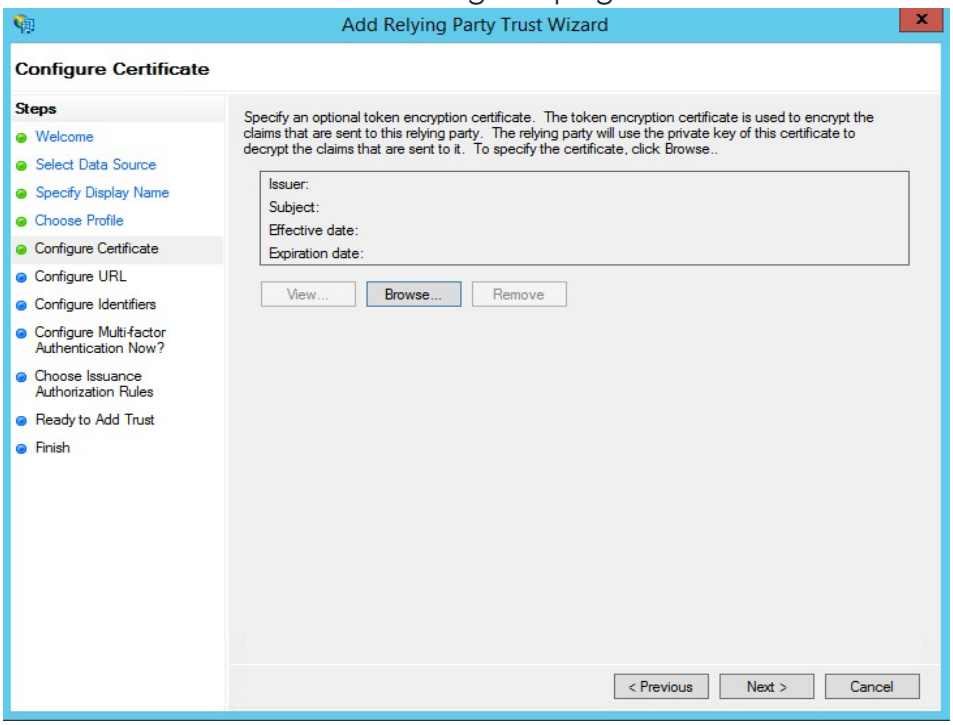
3. Enter the Display name and Notes as shown below.



4. Use AD FS profile.

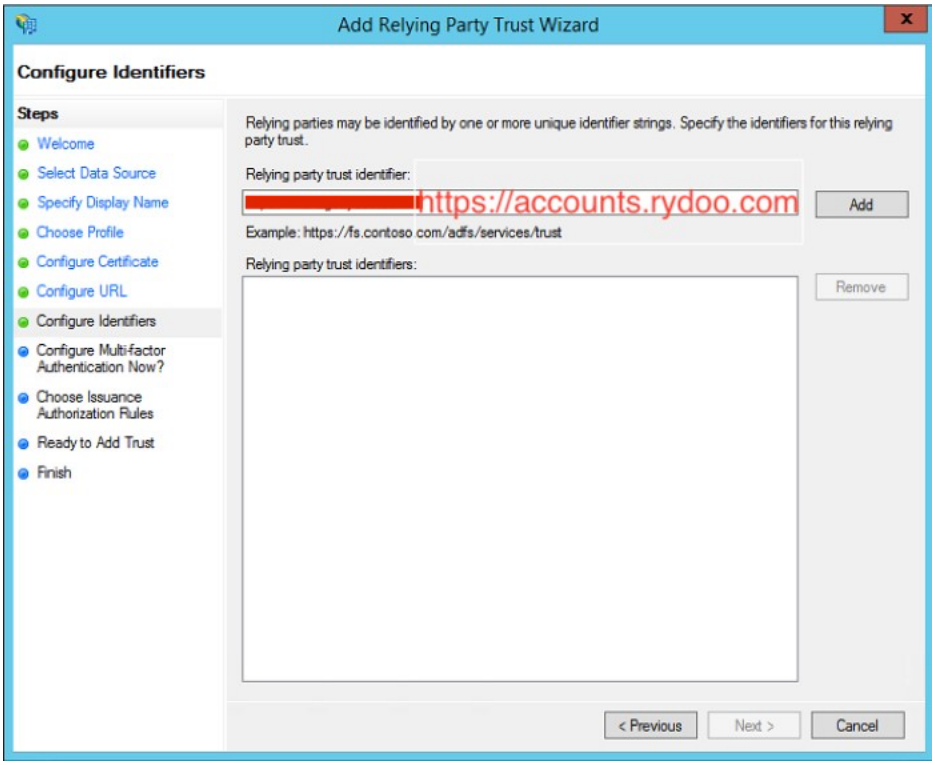


5. Click Next without altering this page



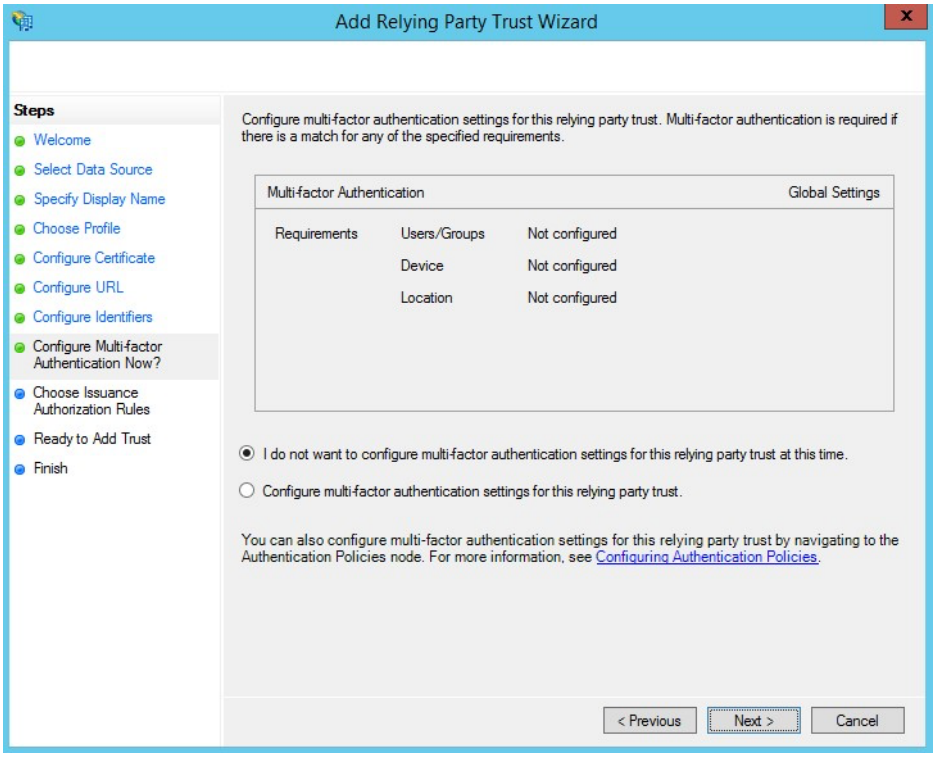
6. Choose SAML 2.0 and set the service URL:
https://accounts.rydoo.com/saml/CompanyName/Acs

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

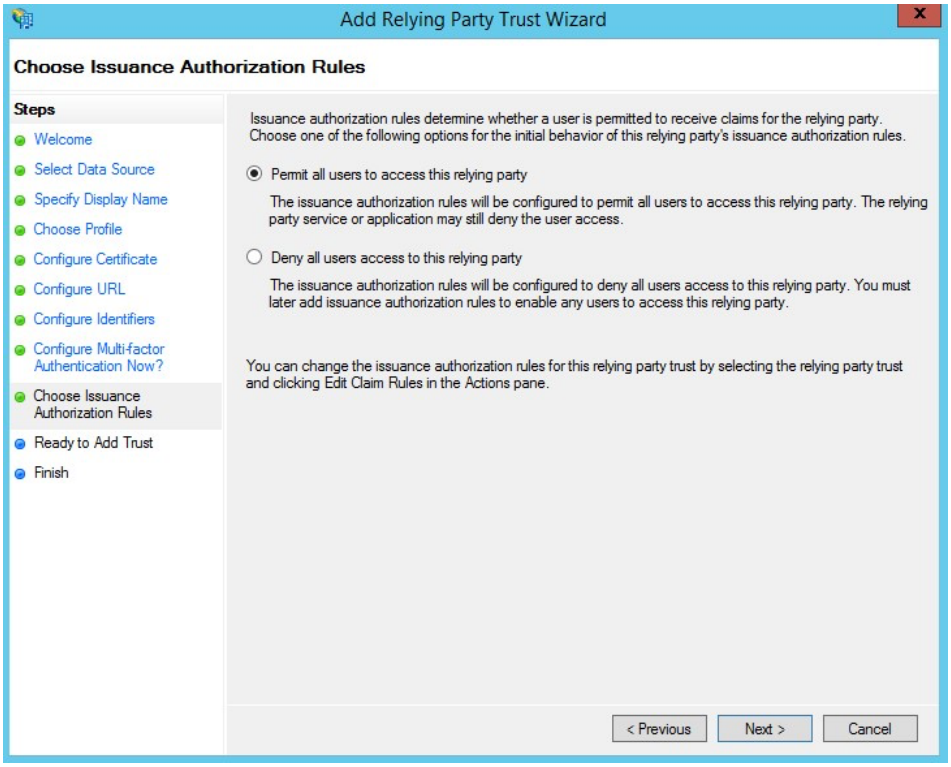


8. Set the relying party identifier to Rydoo: https://accounts.rydoo.com

9. Leave Multifactor Authentication at default.



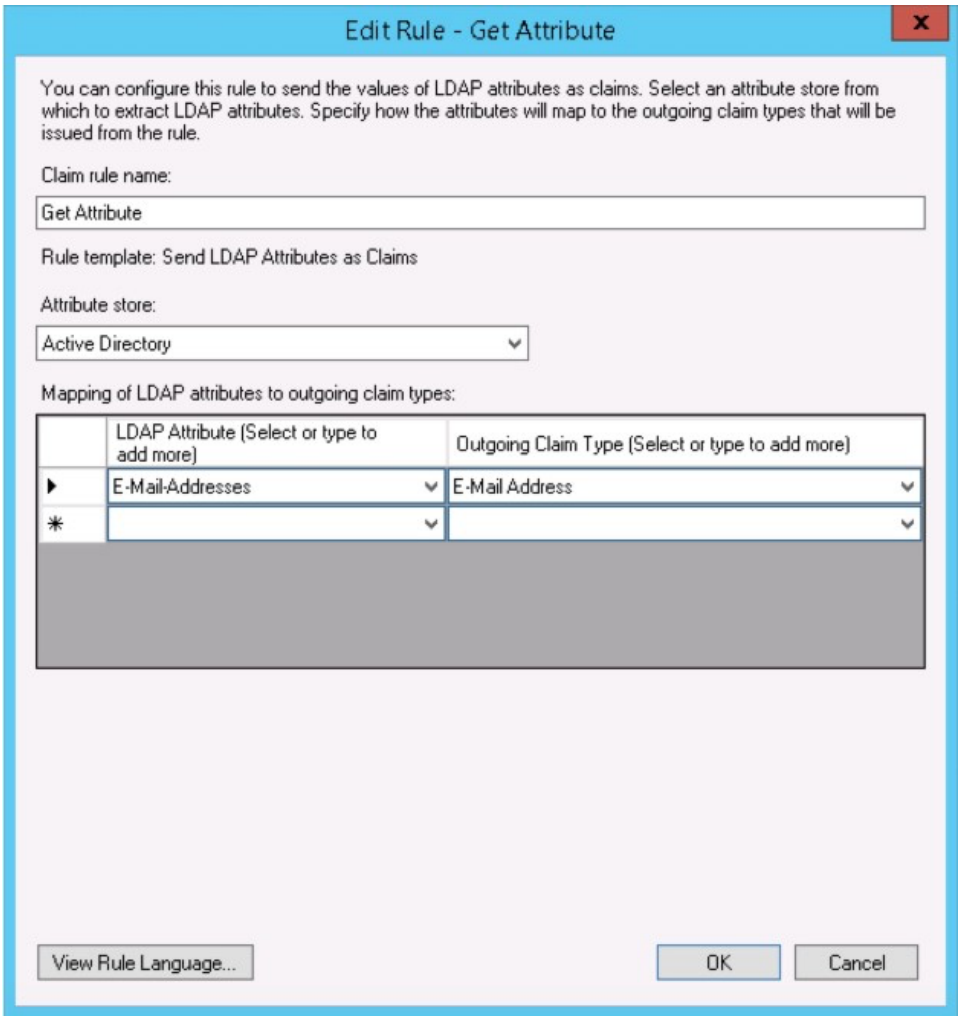
10. On the next screen, select the Permit all users to access this relying party



11. Click Next to add the relying party trust.
12. Close the wizard.

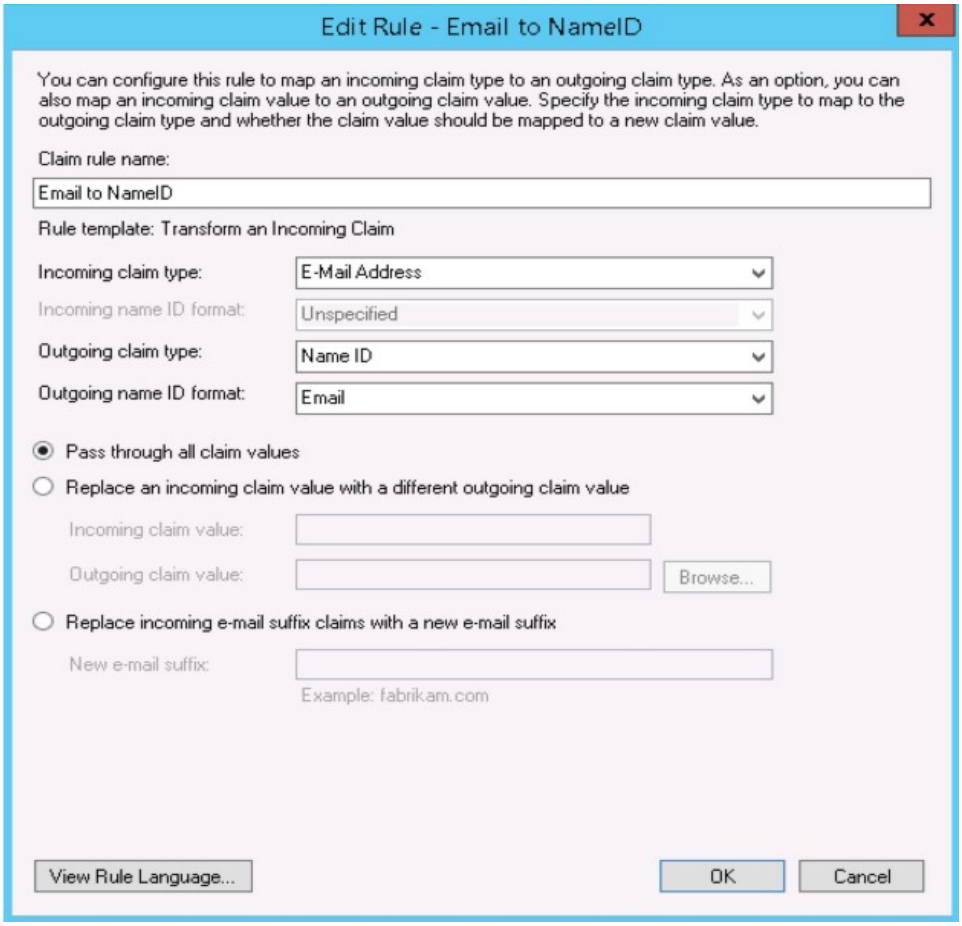
CLAIM RULES

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.



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.

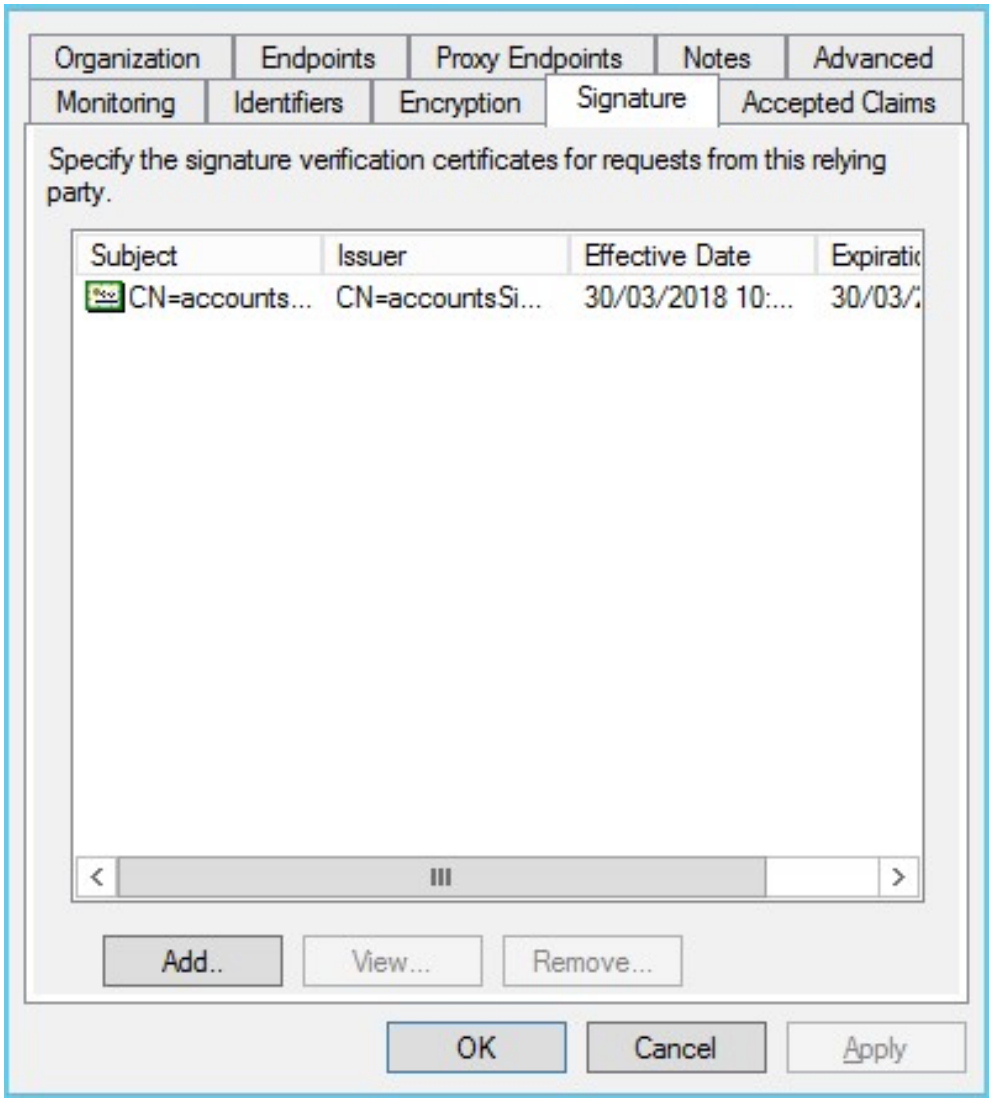
12. Set the Outgoing claim type to Name ID and the Outgoing name ID format to Email.
13. Note: These values must match the Name ID policy you define during SAML 2.0 configuration.
14. Select Pass through all claim values.
15. Click on Finish.



16. Apply rules.

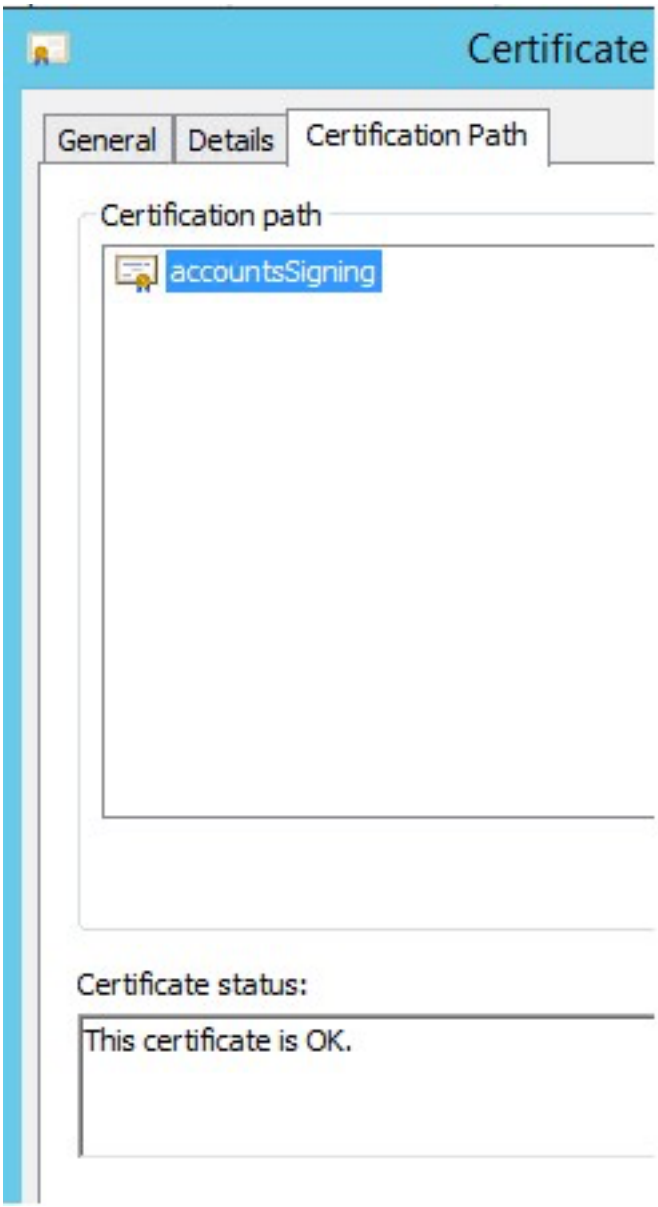
Logout certificate configuration

17. 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.

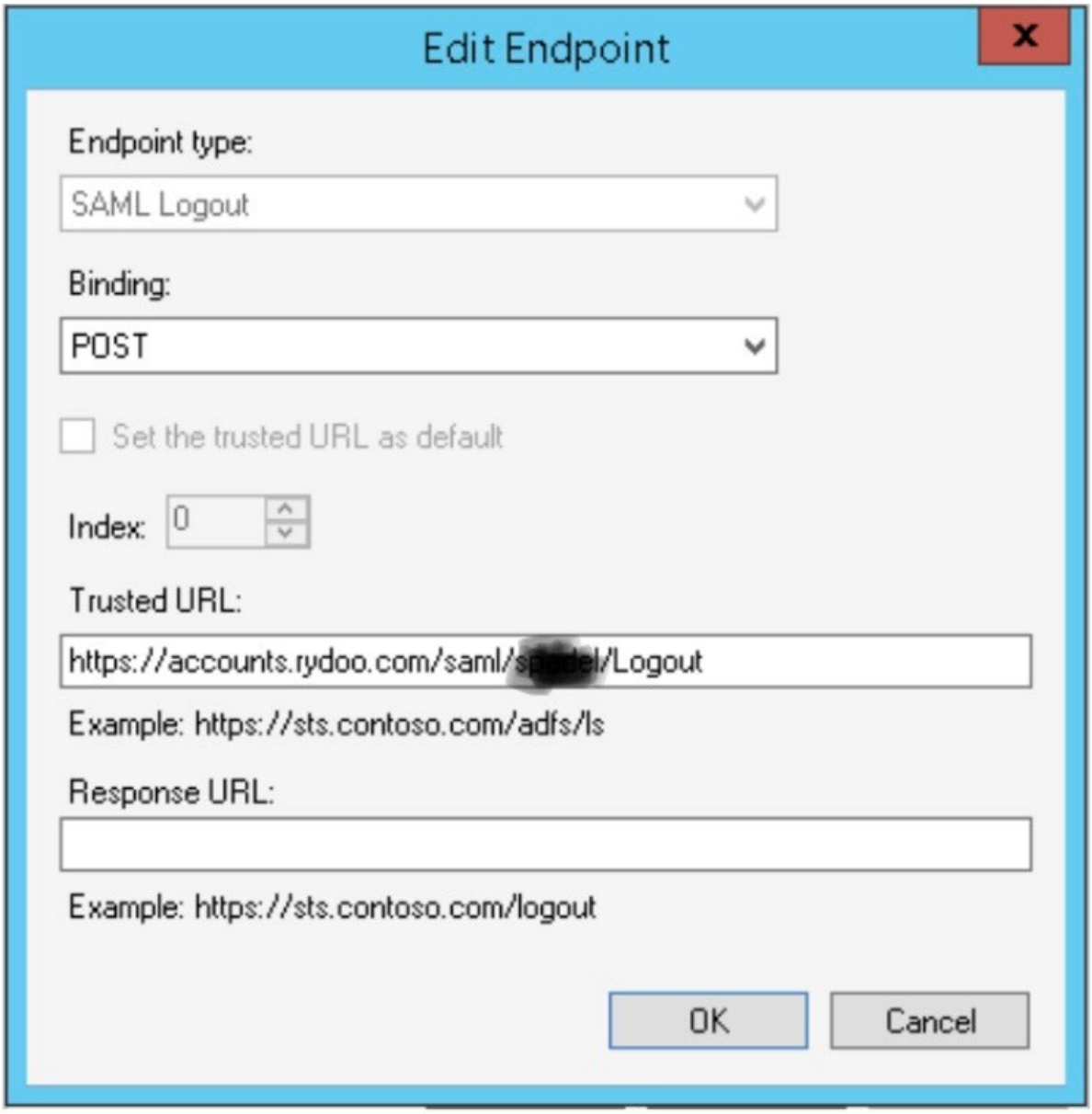


18. Then you double click on the certificate, and install it in the local machine Trusted root certification authorities store, this needs to be done on all the ADFS servers, it's a local reference that the certificate is valid. Otherwise it's possible that this will show an error, something like "not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

Note: it's also possible to the 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



+ Request ADFS certificate from your CSM or send a message to connect@rydoo.com.