rydoo

Rydoo
Single-Sign-On

SUPPORT

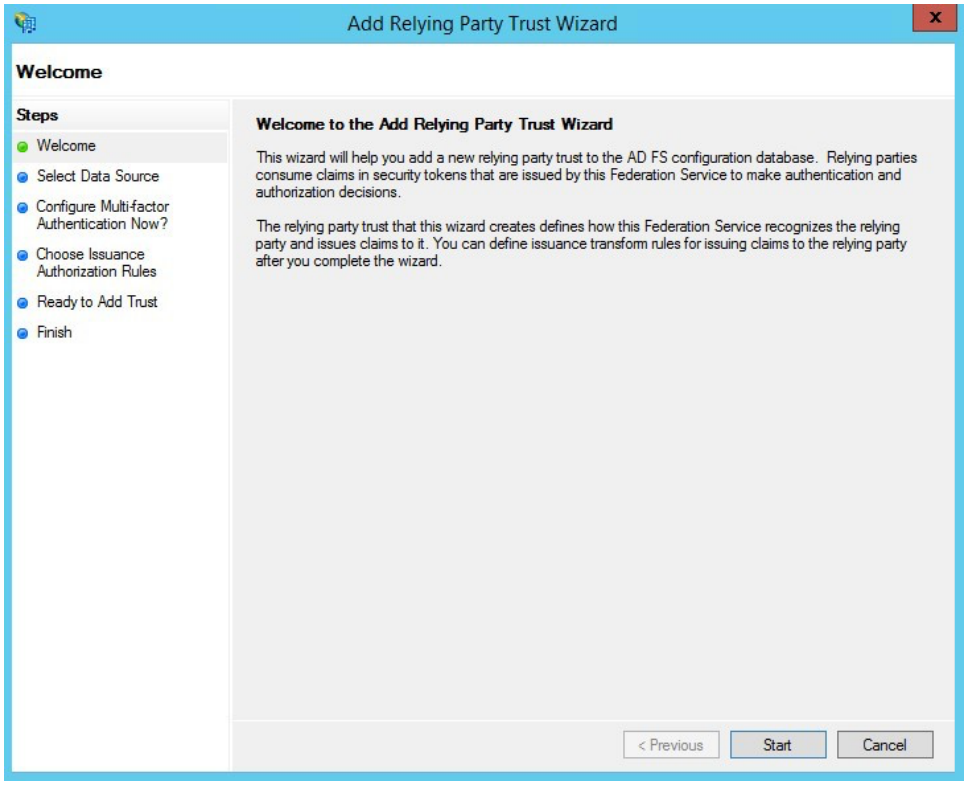
Configure Rydoo Single Sign-On (SSO) with ADFS 3.0

This guide walks you through setting up SAML-based Single Sign-On (SSO) between Active Directory Federation Services (AD FS) 3.0 and Rydoo.

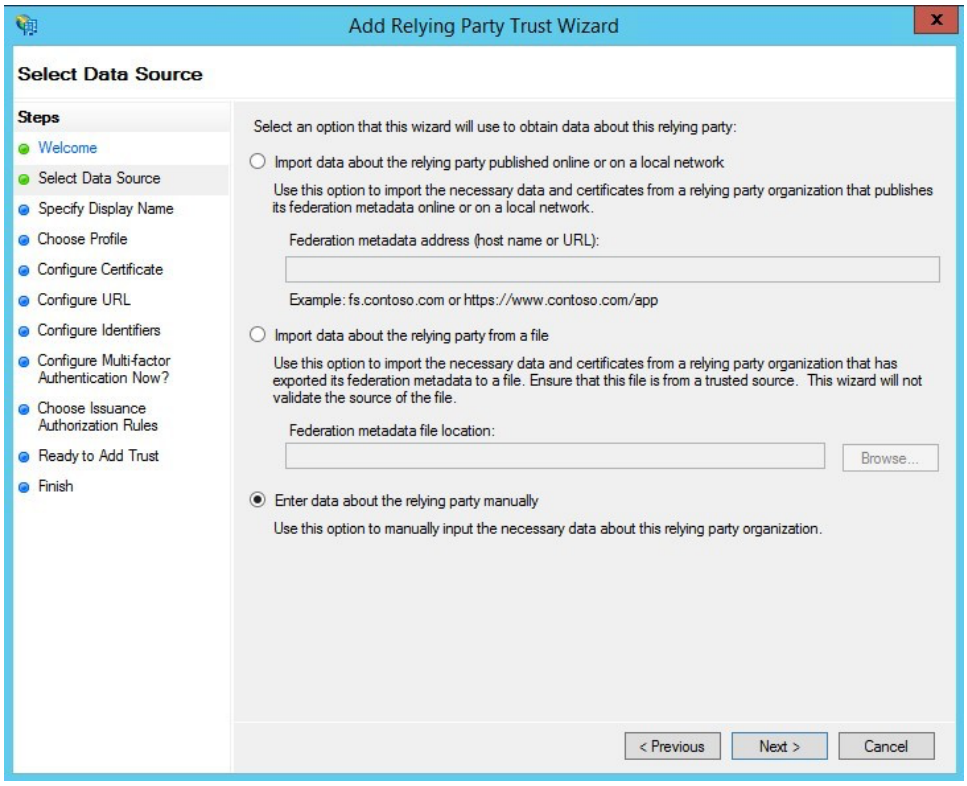
In SAML terms, AD FS is your Identity Provider (IdP) and Rydoo is the Service Provider (SP). You'll create a relying party trust for Rydoo, configure the claim rules that tell AD FS what user information to send, and install the certificate that secures the connection.

1. Create the relying party trust

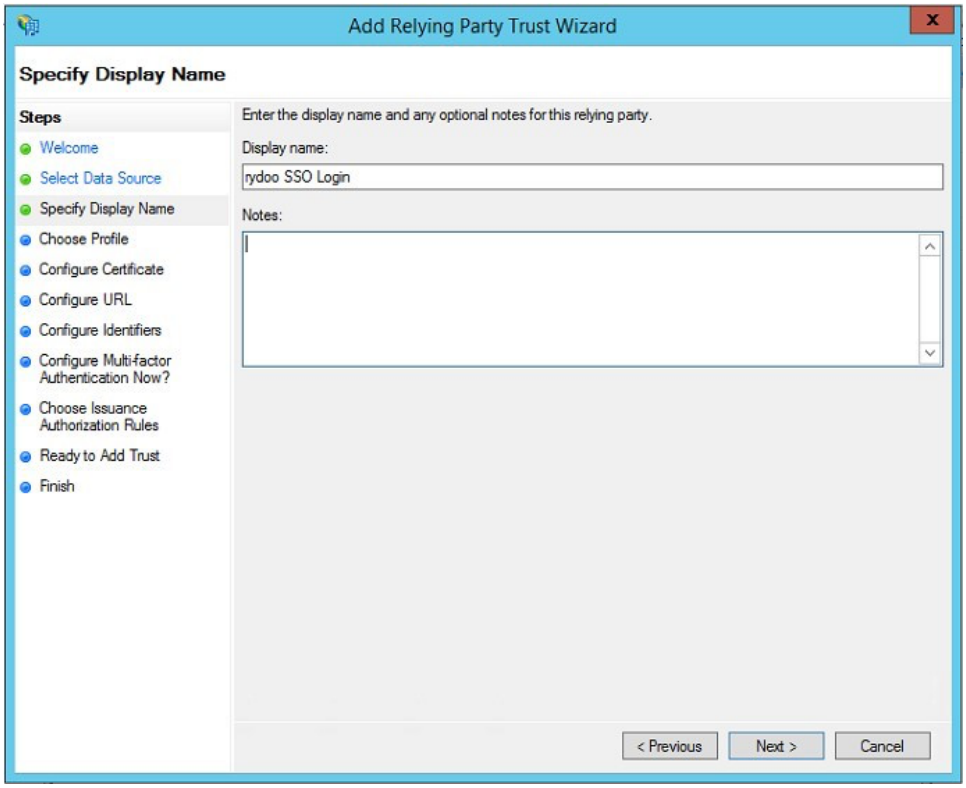
1. In the AD FS management console, start the Add Relying Party Trust wizard.



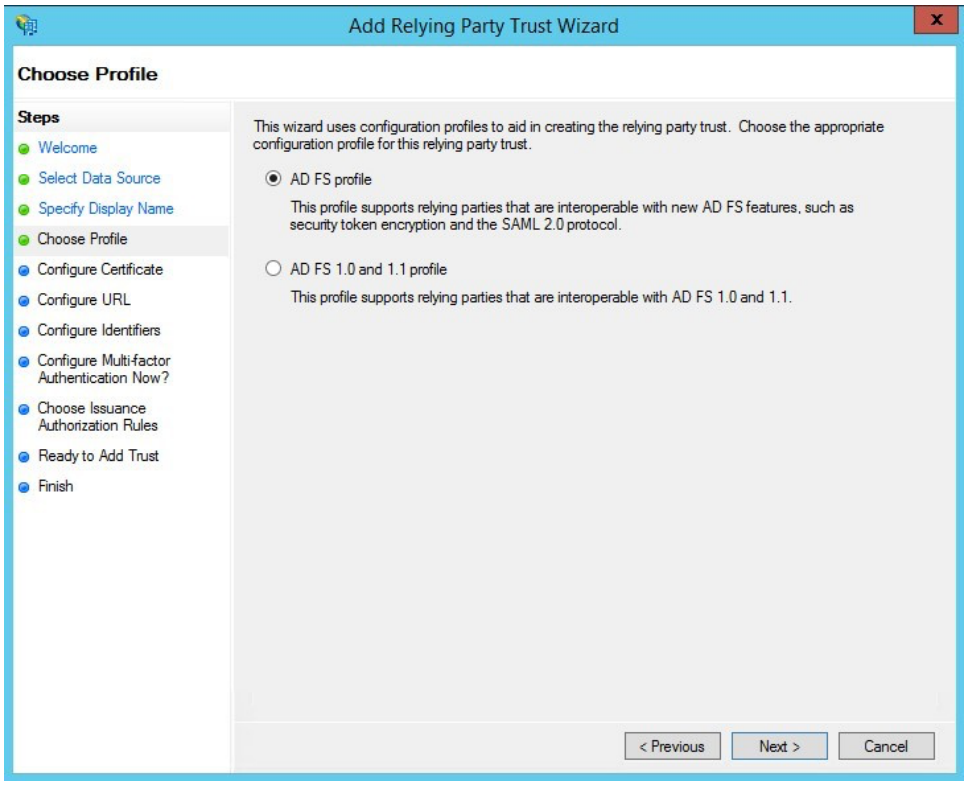
2. Select Enter data about the relying party manually, then click Next.



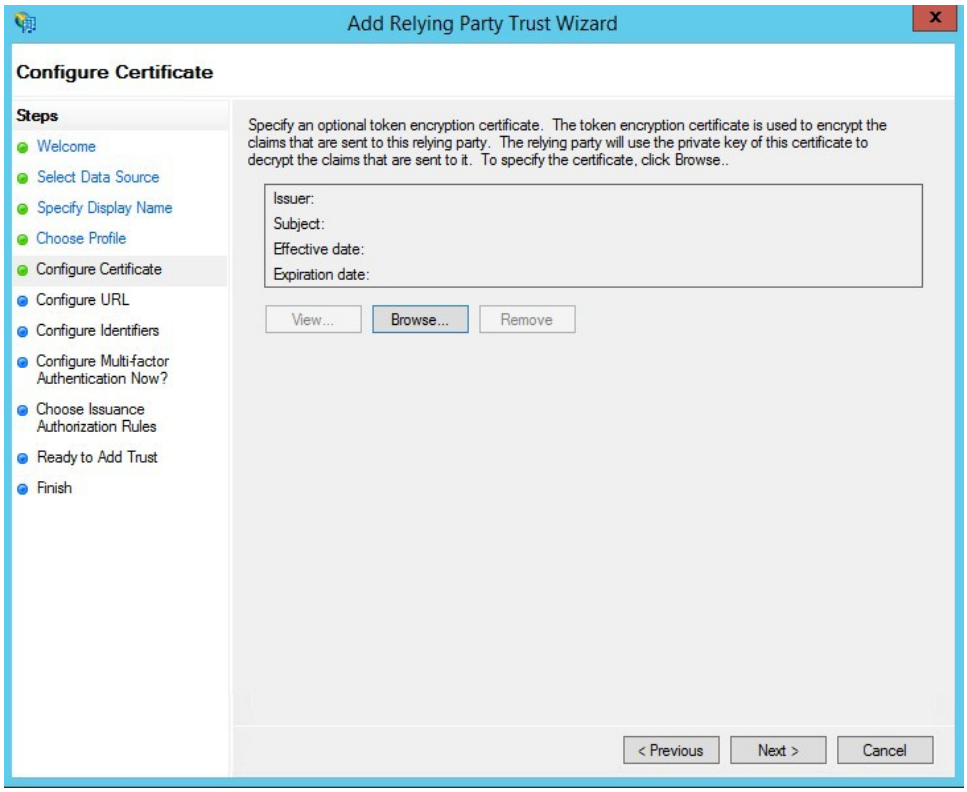
3. Enter a display name (for example, “Rydoo SSO Login”). The Notes field is optional.



4. Choose the AD FS profile, then click Next.



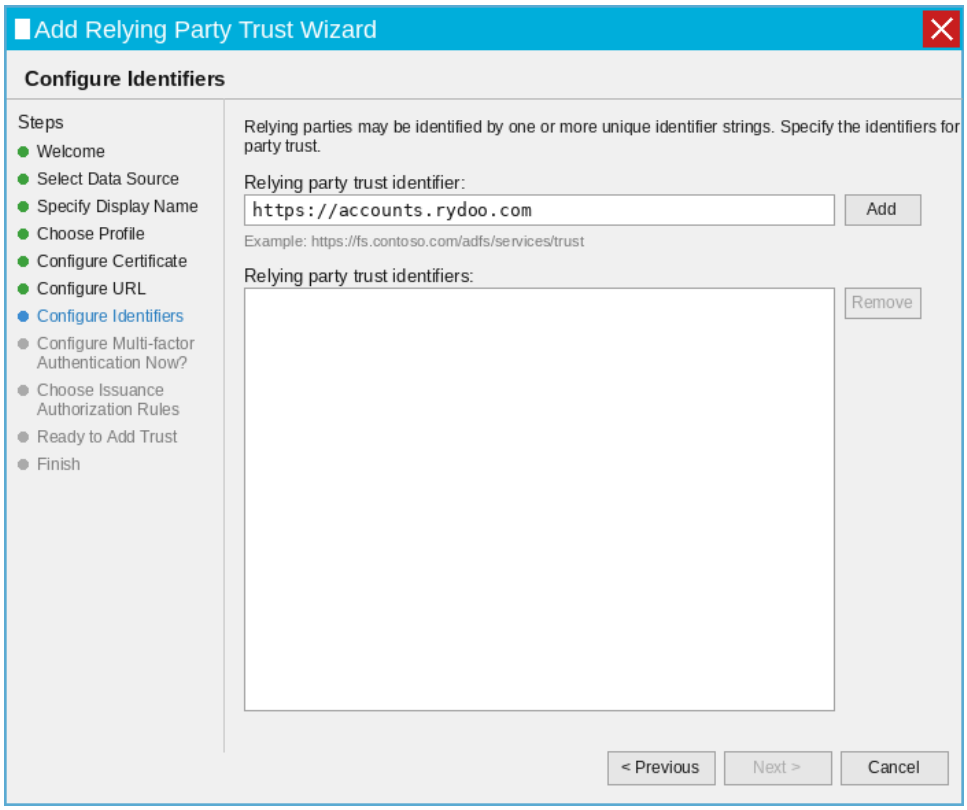
5. On the Configure Certificate screen, leave the default settings and click Next.



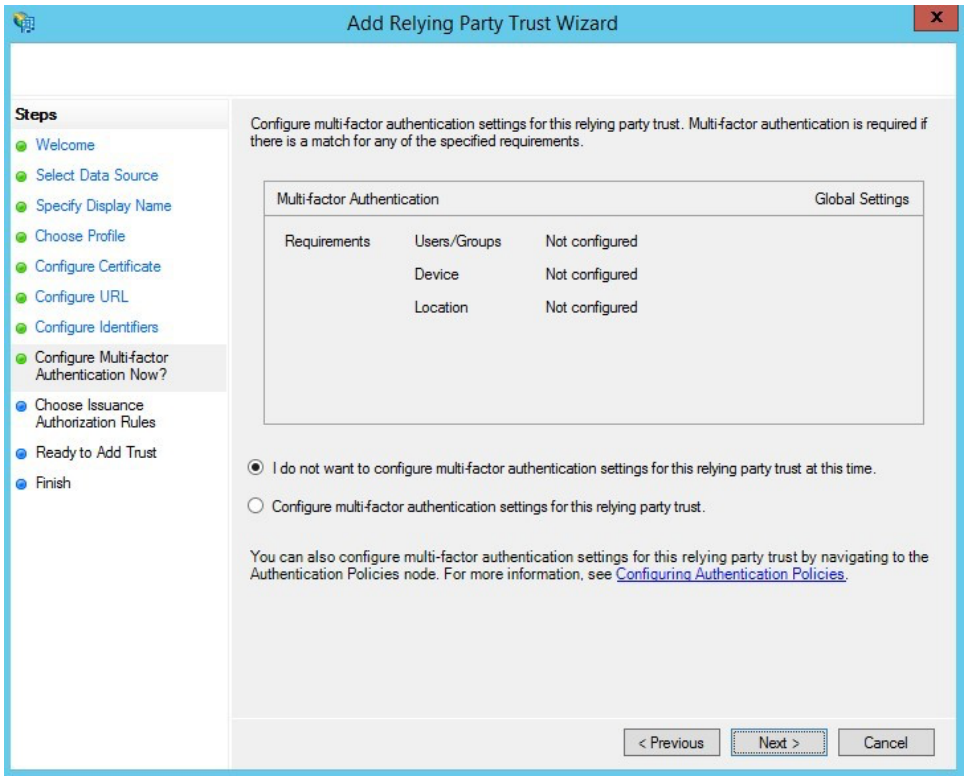
6. On the Configure URL screen, enable support for the SAML 2.0 WebSSO protocol and set the relying party SAML 2.0 SSO service URL to:

`https://accounts.rydoo.com/saml/Acs`

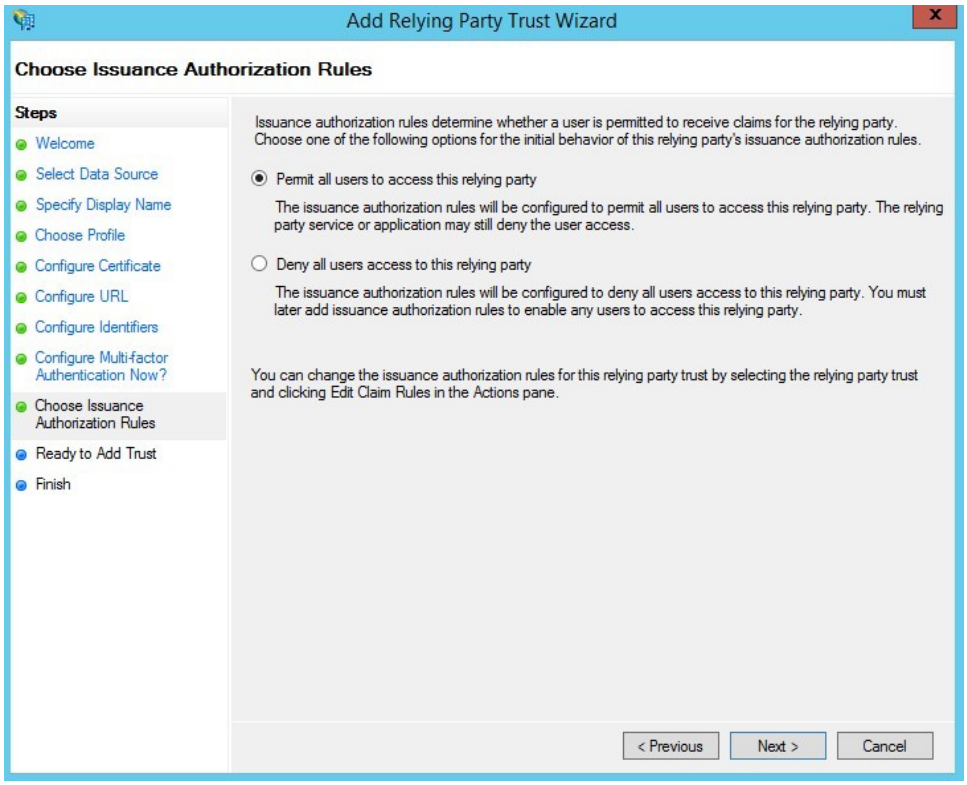
7. On the Configure Identifiers screen, enter the following as the relying party trust identifier and click Add: https://accounts.rydoo.com



8. Leave multi-factor authentication at its default (not configured), then click Next.



9. On the Choose Issuance Authorization Rules screen, select Permit all users to access this relying party.



10. Click Next to add the relying party trust, then close the wizard.

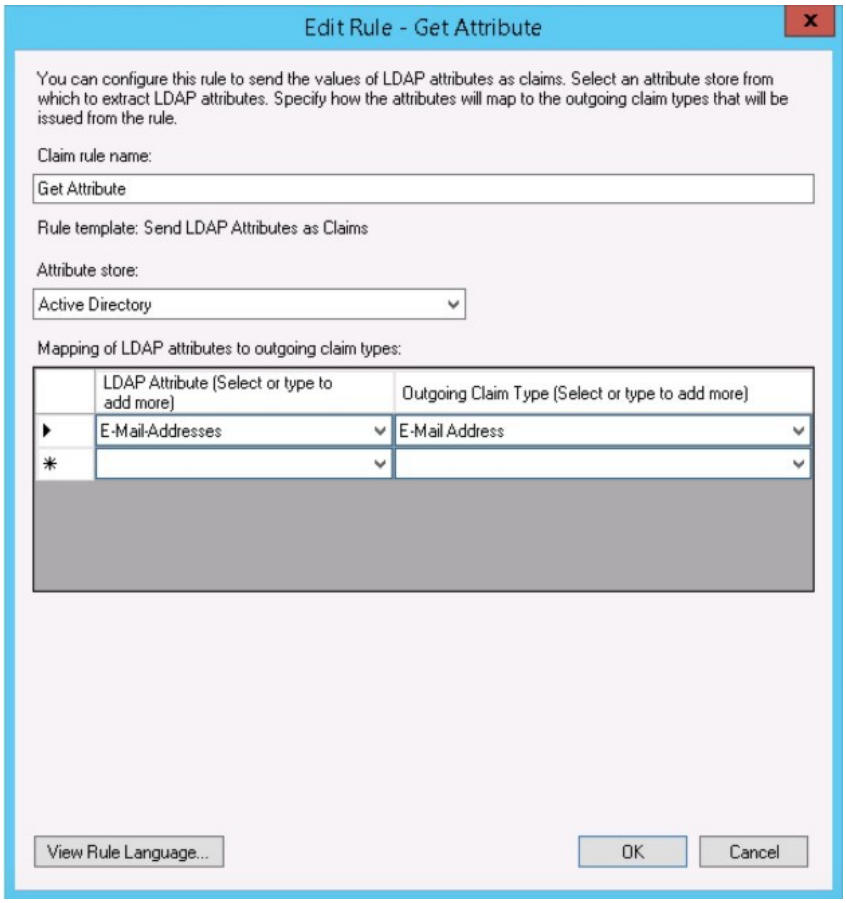
2. Configure the claim rules

1. In the AD FS management console, right-click the relying party trust and select Edit Claim Rules.

2. On the Issuance Transform Rules tab, click Add Rule.

3. Select Send LDAP Attributes as Claims as the claim rule template, then click Next.

4. Give the rule a name (for example, “Get Attribute”). Set the attribute store to Active Directory, map the LDAP attribute E-Mail-Addresses to the outgoing claim type E-Mail Address, then click Finish.

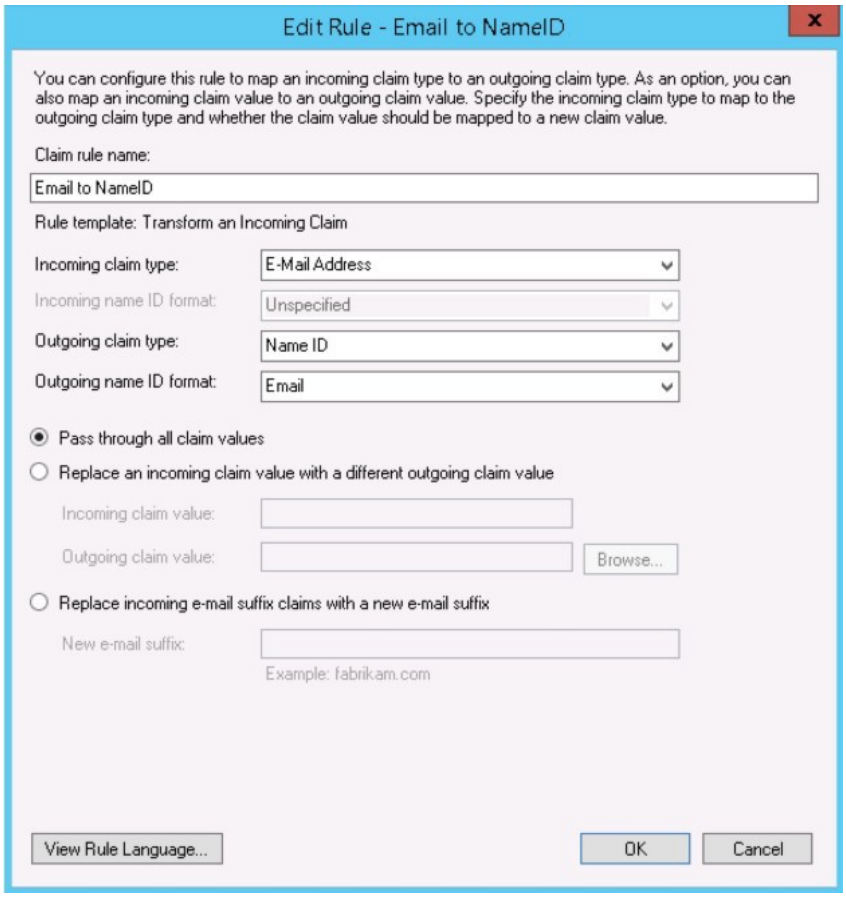


5. Click Add Rule again, this time selecting Transform an Incoming Claim as the template.

6. Give the rule a name (for example, “Email to Name ID”). Set the incoming claim type to E-Mail Address (the outgoing claim type from the previous rule), the outgoing claim type to Name ID, and the outgoing name ID format to Email.

> **Note:** These values must match the Name ID policy configured during the SAML 2.0 setup above.

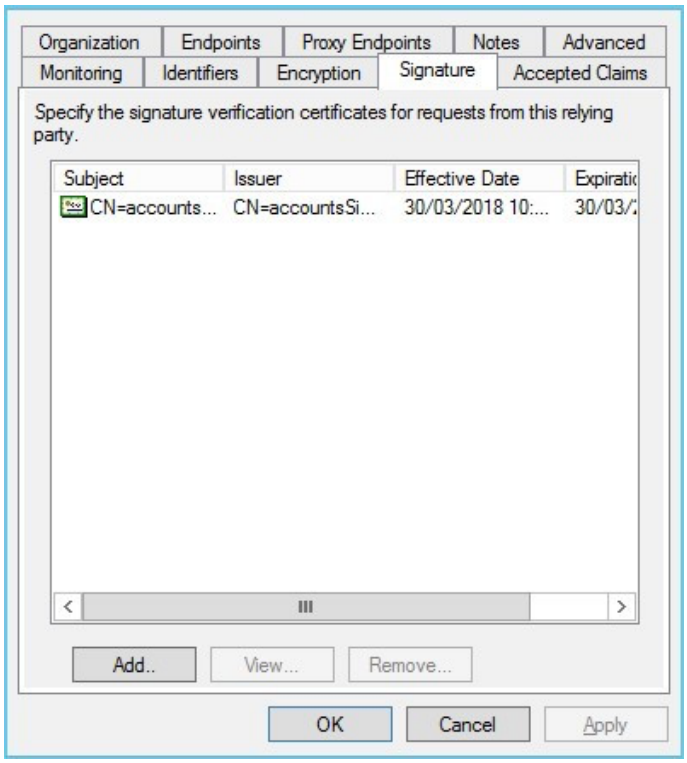
7. Select Pass through all claim values, then click Finish.



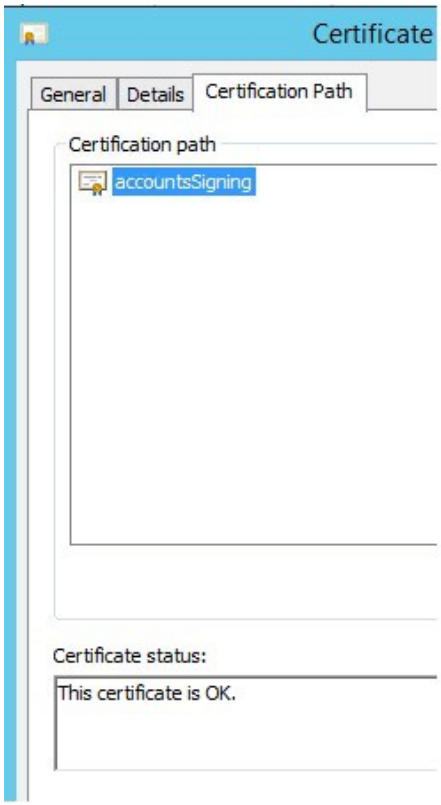
8. Click Apply to save the claim rules.

3. Install the logout certificate

1. Open the relying party trust properties, go to the Signature tab, click Add, and select the .cer file you received from Rydoo.

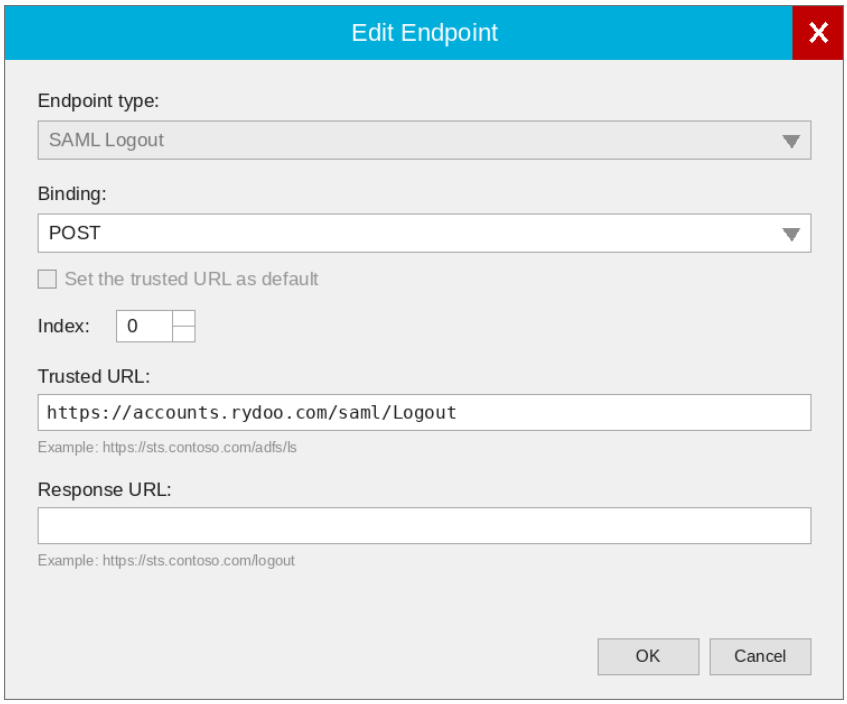


2. Double-click the certificate and install it in the local machine's Trusted Root Certification Authorities store. Do this on every AD FS server — it's a local reference that confirms the certificate is valid. Skipping this step on any server can cause a “not possible to validate the root CA” error.



Note: You can also use an encryption certificate here — it can be the same certificate as the signature.

3. Open the relying party trust's Endpoints tab, edit the SAML Logout endpoint, and set the Trusted URL to: https://accounts.rydoo.com/saml/Logout



Need an AD FS certificate? Request one from your Customer Success Manager, or email *connect@rydoo.com*.