



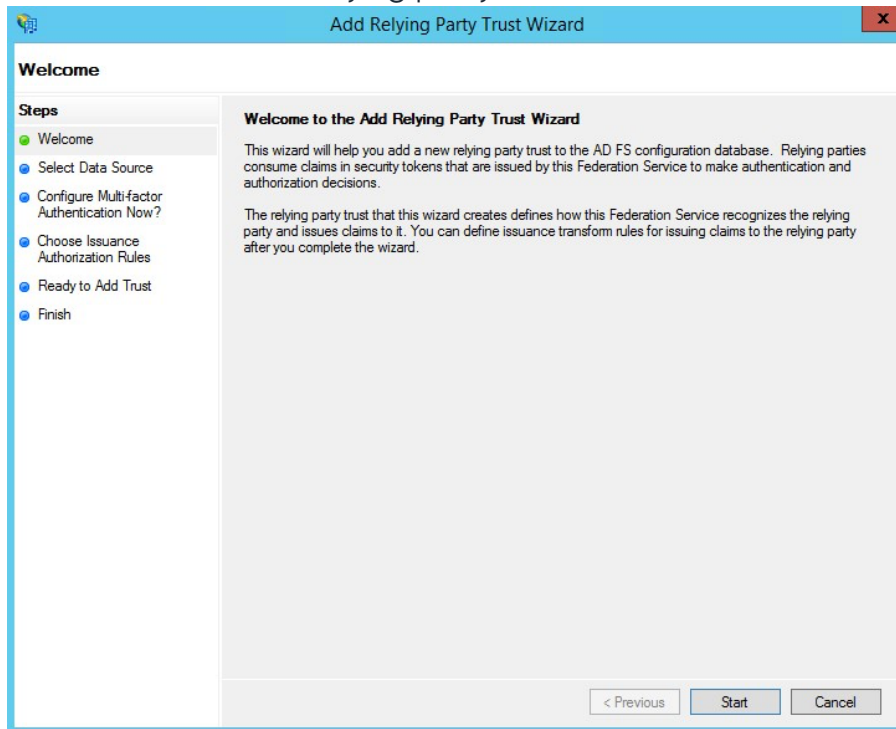
Rydoo Single-Sign-On

SUPPORT

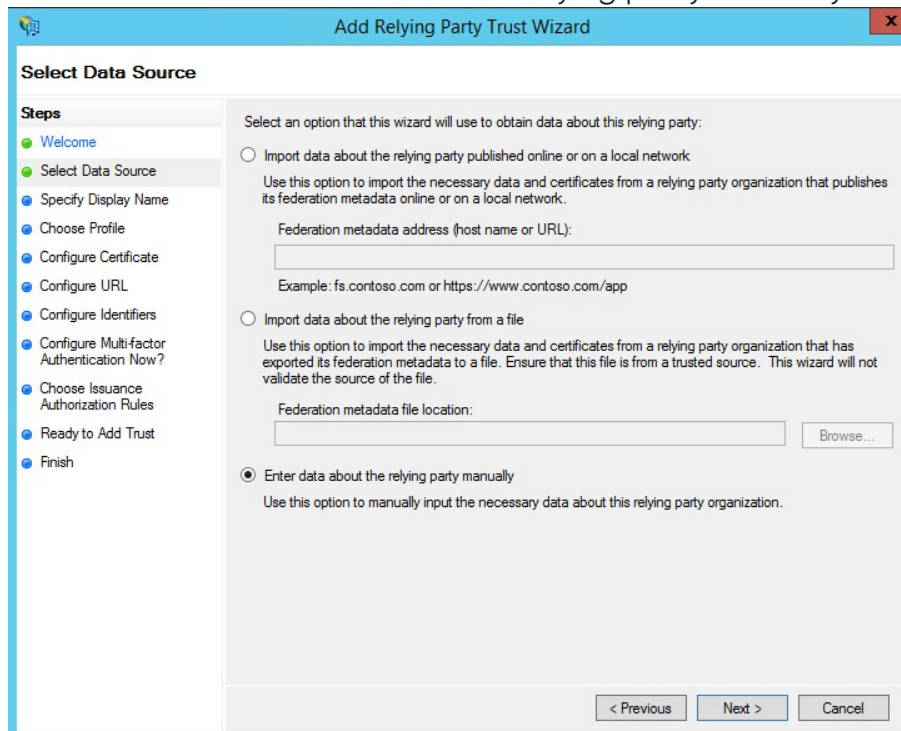


Configure Rydoo Single Sign-On using ADFS 3.0

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.

The screenshot shows the 'Add Relying Party Trust Wizard' window at the 'Specify Display Name' step. The window has a blue title bar with the text 'Add Relying Party Trust Wizard' and a close button. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name (highlighted), 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 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 the text box 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 'Add Relying Party Trust Wizard' window at the 'Choose Profile' step. The window has a blue title bar with the text 'Add Relying Party Trust Wizard' and a close button. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile (highlighted), Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area 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 the 'Add Relying Party Trust Wizard' at the 'Configure Certificate' step. The left sidebar lists the steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate (highlighted), Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains instructions: '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 are input fields for Issuer, Subject, Effective date, and Expiration date, with 'Browse...' and 'Remove' buttons. At the bottom are '< Previous', 'Next >', and 'Cancel' buttons.

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>

The screenshot shows the 'Add Relying Party Trust Wizard' at the 'Configure Identifiers' step. The left sidebar lists the steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers (highlighted), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains instructions: 'Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.' Below this is a text input field for 'Relying party trust identifier:' with the value 'https://accounts.rydoo.com' entered and highlighted in red. An 'Add' button is to the right. Below the input field is an 'Example: https://fs.contoso.com/adfs/services/trust'. Below that is a list box for 'Relying party trust identifiers:' and a 'Remove' button. At the bottom are '< Previous', 'Next >', and 'Cancel' buttons.

8. Set the relying party identifier to Rydoo: <https://accounts.rydoo.com>
9. Leave Multifactor Authentication at default.

The screenshot shows the 'Add Relying Party Trust Wizard' window. The 'Steps' pane on the left lists the following steps: Welcome, Select Data Source, 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 content area has the title 'Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.' Below this is a table with the heading 'Multi-factor Authentication' and a sub-header 'Global Settings'.

Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

Below the table are two radio button options:

- ☒ I do not want to configure multi-factor authentication settings for this relying party trust at this time.
- ☐ Configure multi-factor authentication settings for this relying party trust.

Below the radio buttons is a note: 'You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).'

At the bottom are three buttons: '< Previous', 'Next >', and 'Cancel'.

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

The screenshot shows the 'Add Relying Party Trust Wizard' window. The 'Steps' pane on the left lists the following steps: Welcome, Select Data Source, 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 content area has the title 'Choose Issuance Authorization Rules' and the text: 'Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.'

Below this text are two radio button options:

- ☒ Permit all users to access this relying party
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.
- ☐ Deny all users access to this relying party
The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

Below the radio buttons is a note: 'You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.'

At the bottom are three buttons: '< Previous', 'Next >', and 'Cancel'.

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:
Get Attribute

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

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
*		

View Rule Language... OK Cancel

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:
Email to NameID

Rule template: Transform an Incoming Claim

Incoming claim type: E-Mail Address

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Email

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value: Browse...

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

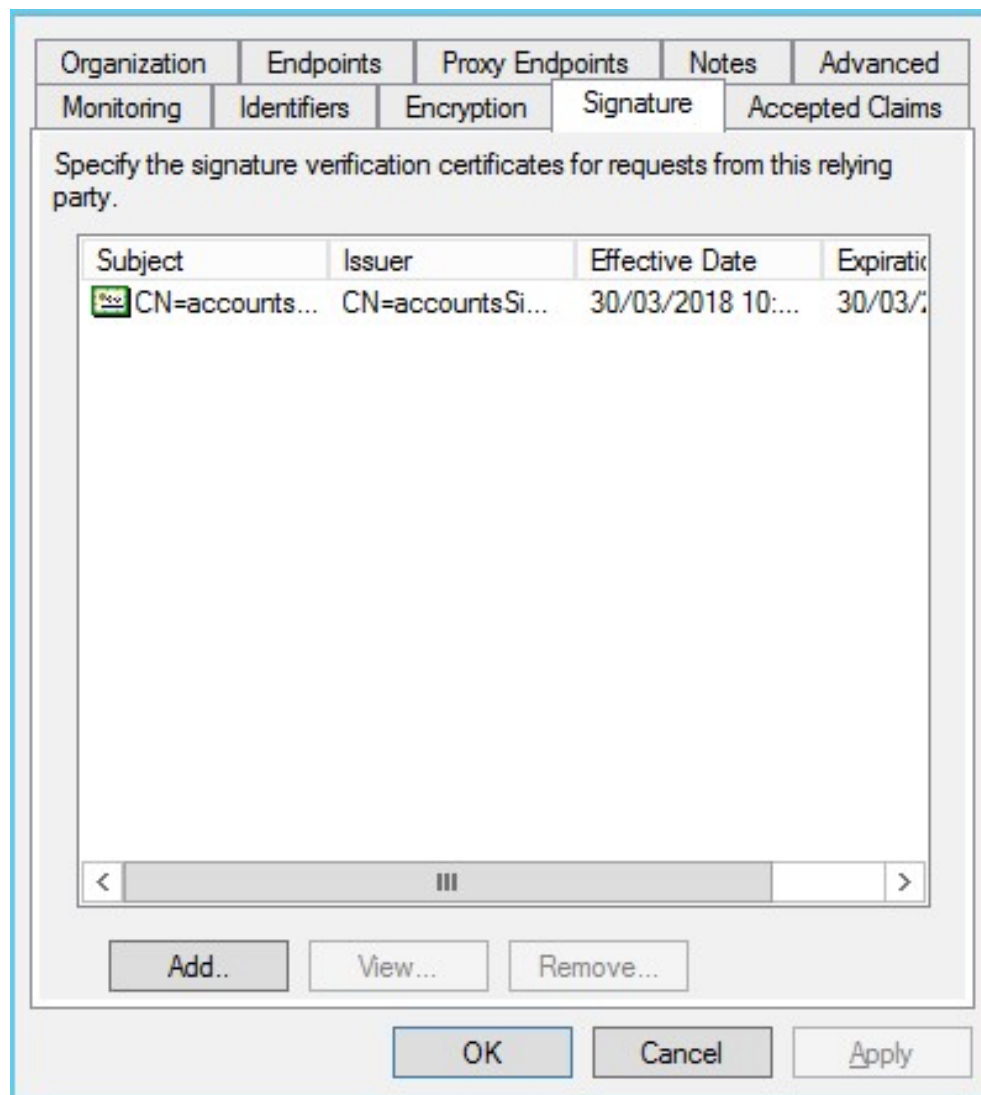
New e-mail suffix:
Example: fabrikam.com

View Rule Language... OK Cancel

16. Apply rules.

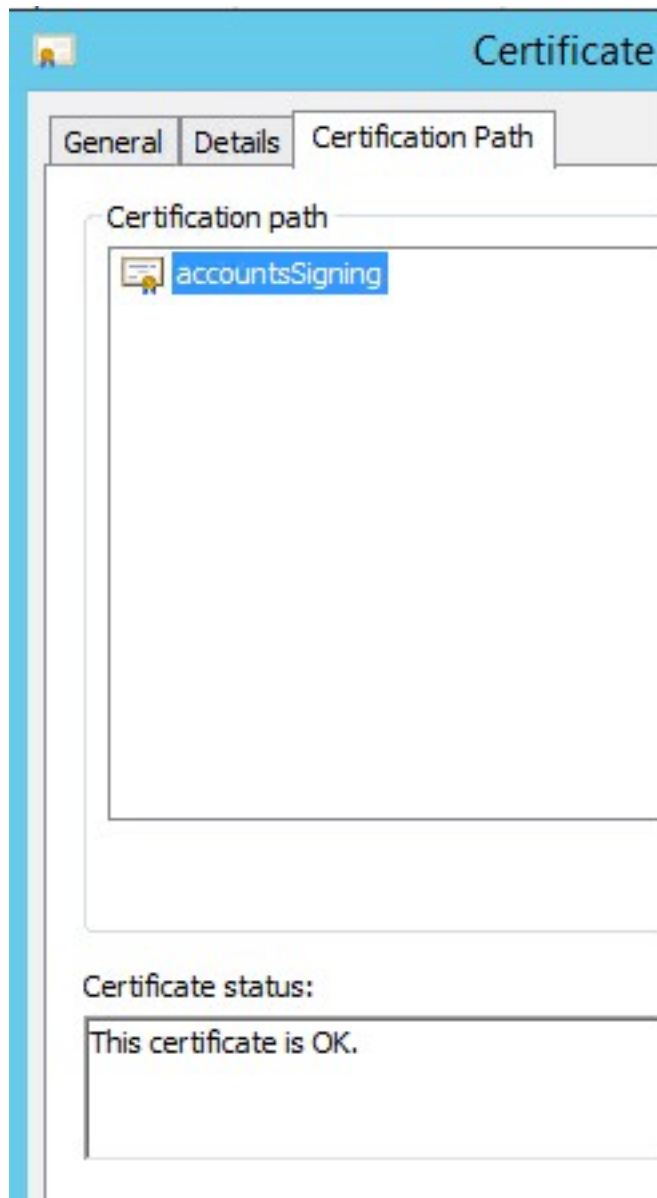
Logout certificate configuration

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 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/IdP/Logout

Example:

https://sts.contoso.com/adfs/ls

Response URL:

Example:

https://sts.contoso.com/logout

OK

Cancel

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