



Rydoo Single-Sign-On

SUPPORT



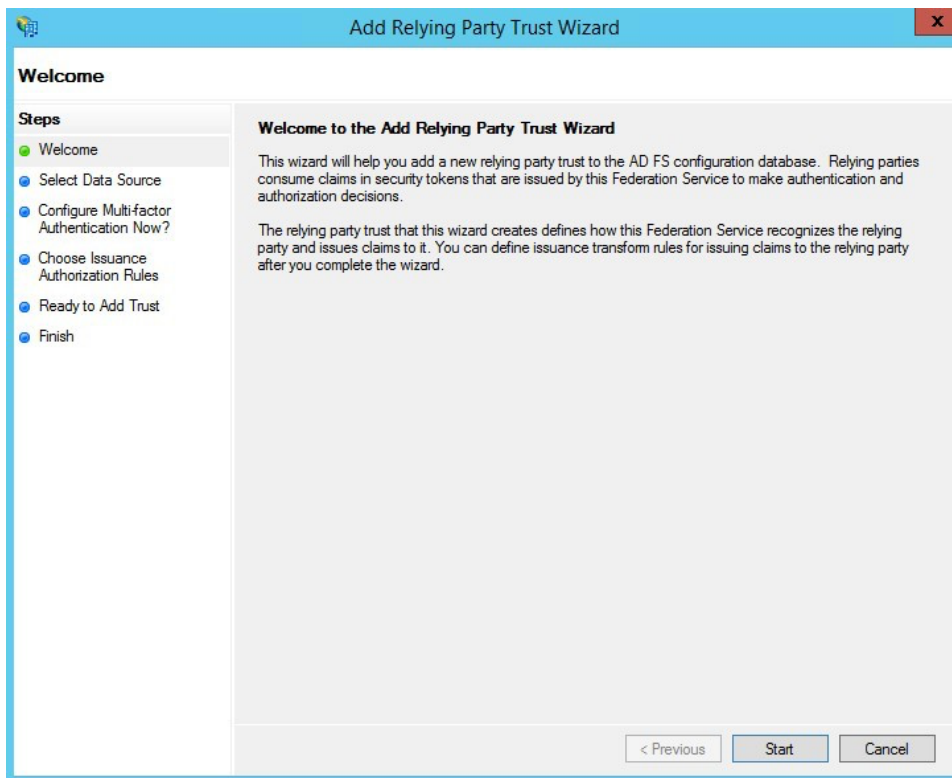
Configure Rydoo Single Sign-On (SSO) with ADFS 3.0

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.

Add Relying Party Trust Wizard

Select Data Source

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
- Finish

Select an option that this wizard will use to obtain data about this relying party:

☐ Import data about the relying party published online or on a local network

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.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

☐ Import data about the relying party from a file

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.

Federation metadata file location:

Browse...

☒ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

< Previous Next > Cancel

3. Enter a display name (for example, "Rydoos SSO Login"). The Notes field is optional.

Add Relying Party Trust Wizard

Specify Display Name

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
- Finish

Enter the display name and any optional notes for this relying party.

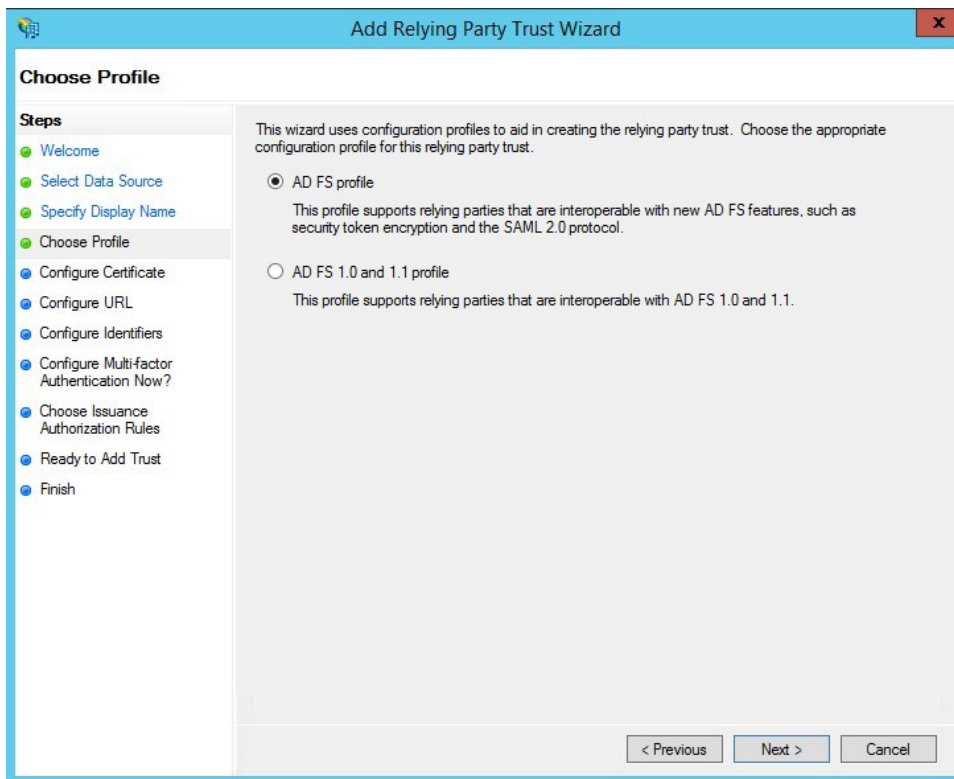
Display name:

rydoos SSO Login

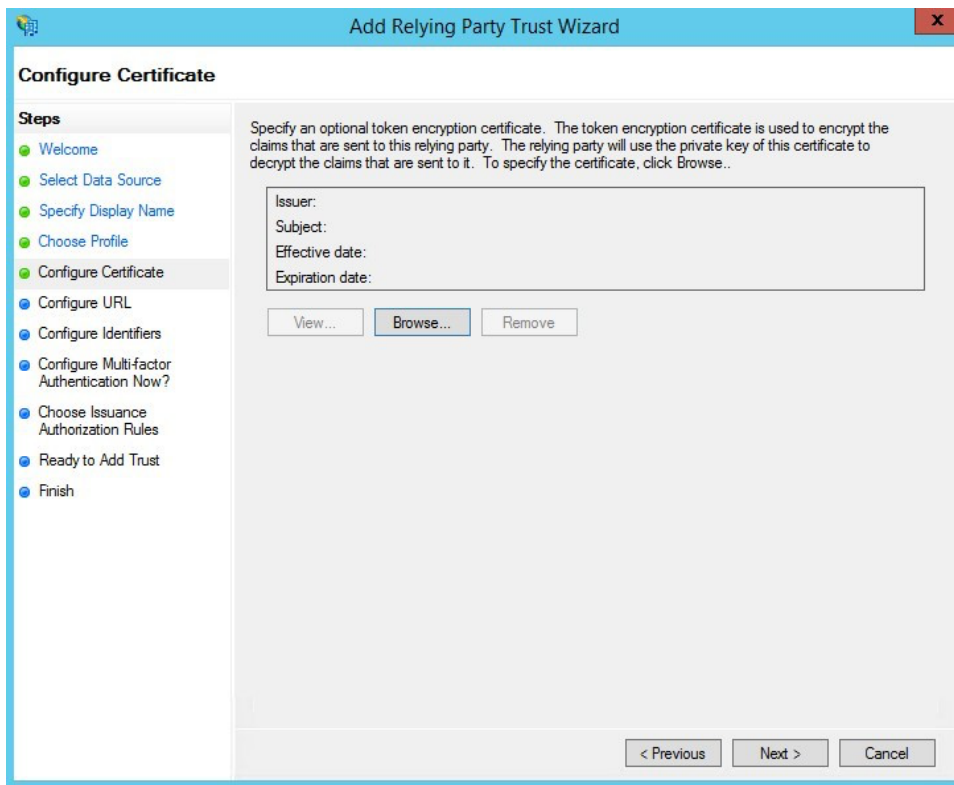
Notes:

< Previous Next > Cancel

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>

Add Relying Party Trust Wizard

Configure Identifiers

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
- Finish

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for party trust.

Relying party trust identifier:

Example: <https://fs.contoso.com/adfs/services/trust>

Relying party trust identifiers:

< Previous Next > Cancel

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

Add Relying Party Trust Wizard

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.

Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

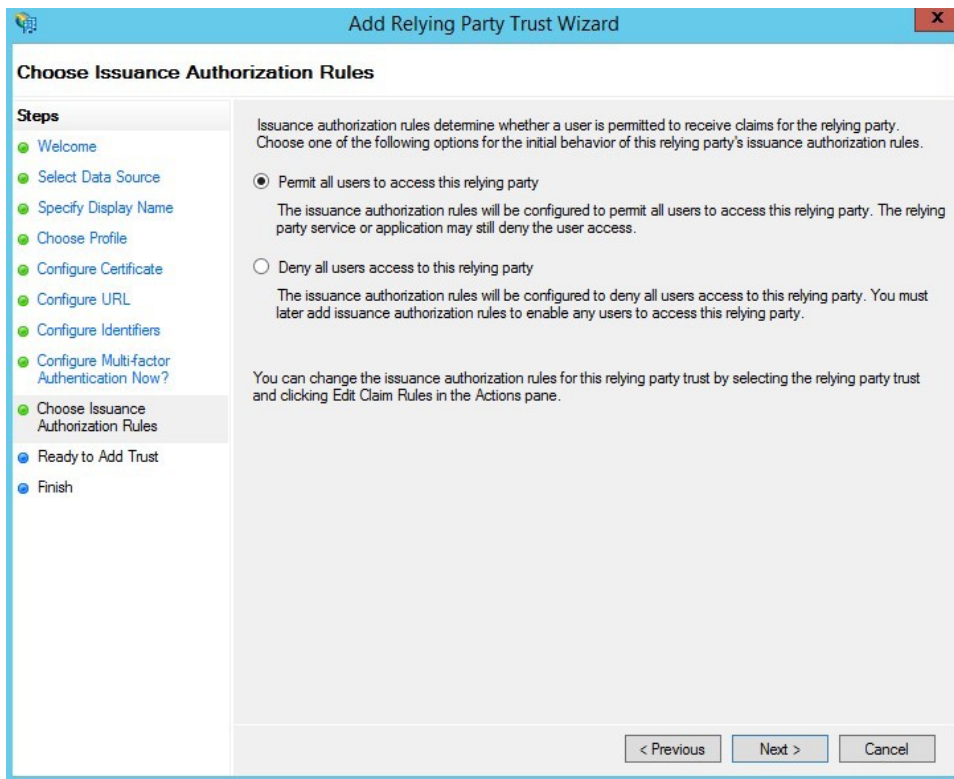
☒ I do not want to configure multi-factor authentication settings for this relying party trust at this time.

☐ Configure multi-factor authentication settings for this relying party trust.

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](#).

< Previous Next > Cancel

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.

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

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.

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

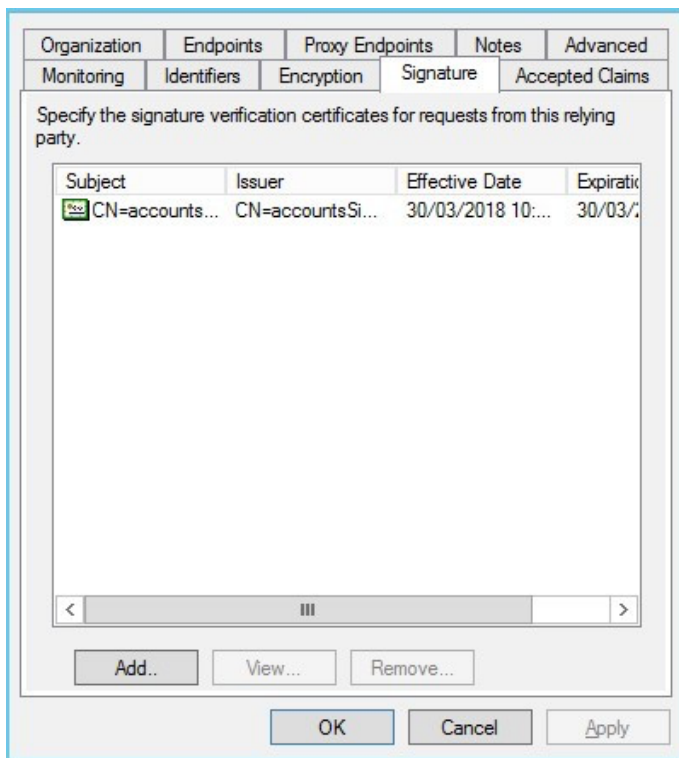
New e-mail suffix:

Example: fabrikam.com

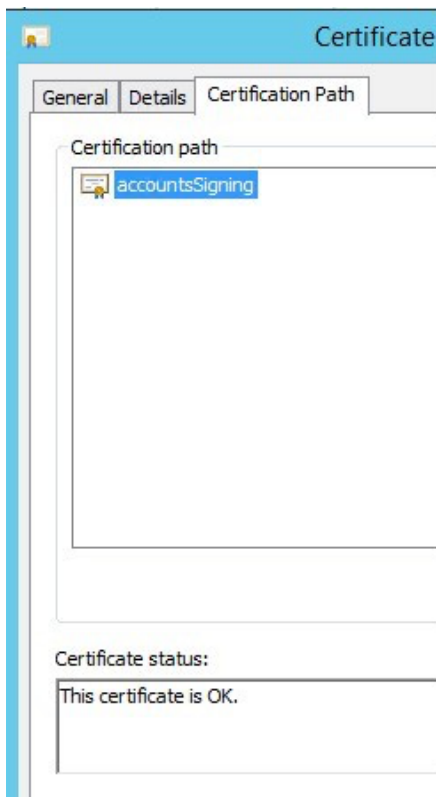
8. Click Apply to save the claim rules.

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>

Endpoint type:
SAML Logout

Binding:
POST

☐ Set the trusted URL as default

Index: 0

Trusted URL:
https://accounts.rydoo.com/saml/Logout
Example: https://sts.contoso.com/adfs/ls

Response URL:
Example: https://sts.contoso.com/logout

OK Cancel

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