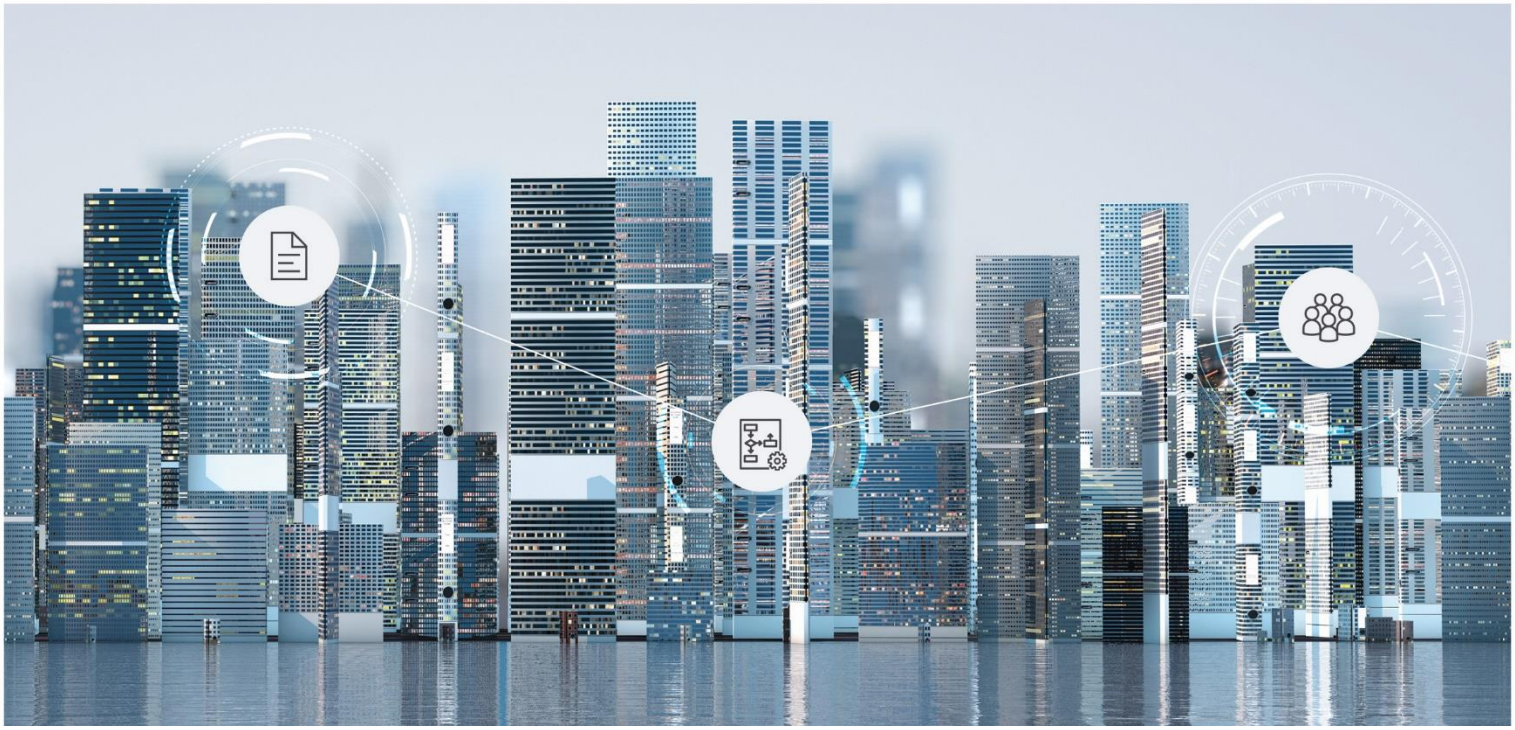
Fabasoft



White Paper

Configuration of Single Sign-On

2019 February Release

Contents

1 Introduction

You can use your own identity provider based on SAML 2.0 for authentication in the Fabasoft Cloud. This document describes how to enable single sign-on for your cloud organization.

2 Configuration in the Fabasoft Cloud

The configuration of your cloud organization is carried out by the Fabasoft Cloud Support. You just have to submit the corresponding data:

- valid e-mail domains
- metadata.xml (exported from your identity provider)

Please send the data to cloudsupport@fabasoft.com.

3 Configuration of an Arbitrary SAML 2.0 Identity Provider

To carry out the necessary configuration steps, please refer to the corresponding third-party documentation.

The metadata of the Fabasoft Cloud identity provider can be found here:

`https://idp.cloud.fabasoft.com/idp/saml/metadata`

The `NameID` must contain the user's e-mail address, which is used for the Fabasoft Cloud log-in.

The following attributes must be provided in the assertion's `AttributeStatement`:

- `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`
- `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`

Assertions must be signed using `SHA-256`.

4 Configuration of Active Directory Federation Services (AD FS)

Active Directory Federation Services can be used as identity provider. The following chapters describe how to configure AD FS for the Fabasoft Cloud.

4.1 Prerequisites

The following prerequisites must be fulfilled:

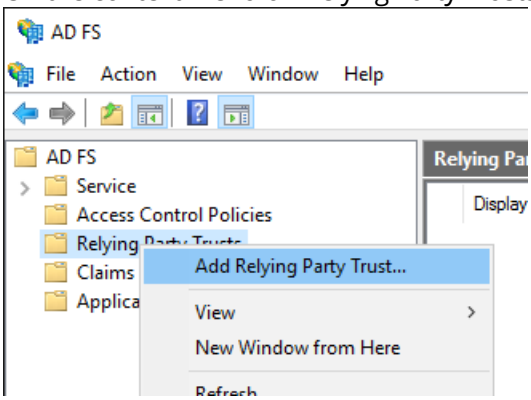
- Microsoft Active Directory Federation Services 2.0
  Note: Microsoft Windows Server 2008 R2 includes AD FS 1.0, which does not support SAML 2.0 - you need to install the AD FS 2.0 'release to web' (RTW) package.
- The hotfix http://support.microsoft.com/kb/2159360/en-us needs to be installed.
- To be able to login via the mobile app you need a valid HTTPS certificate for the AD FS server.

4.2 Configure Your AD FS

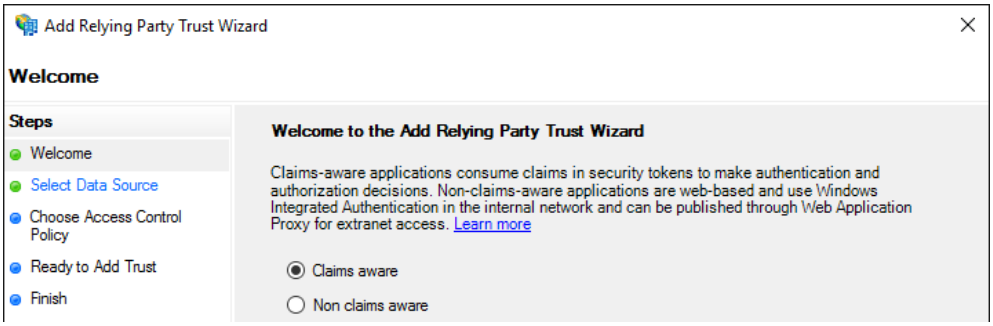
To configure your AD FS for the Fabasoft Cloud, perform the following steps:

1. Start the "AD FS Management" ("Server Manager" > "Tools").

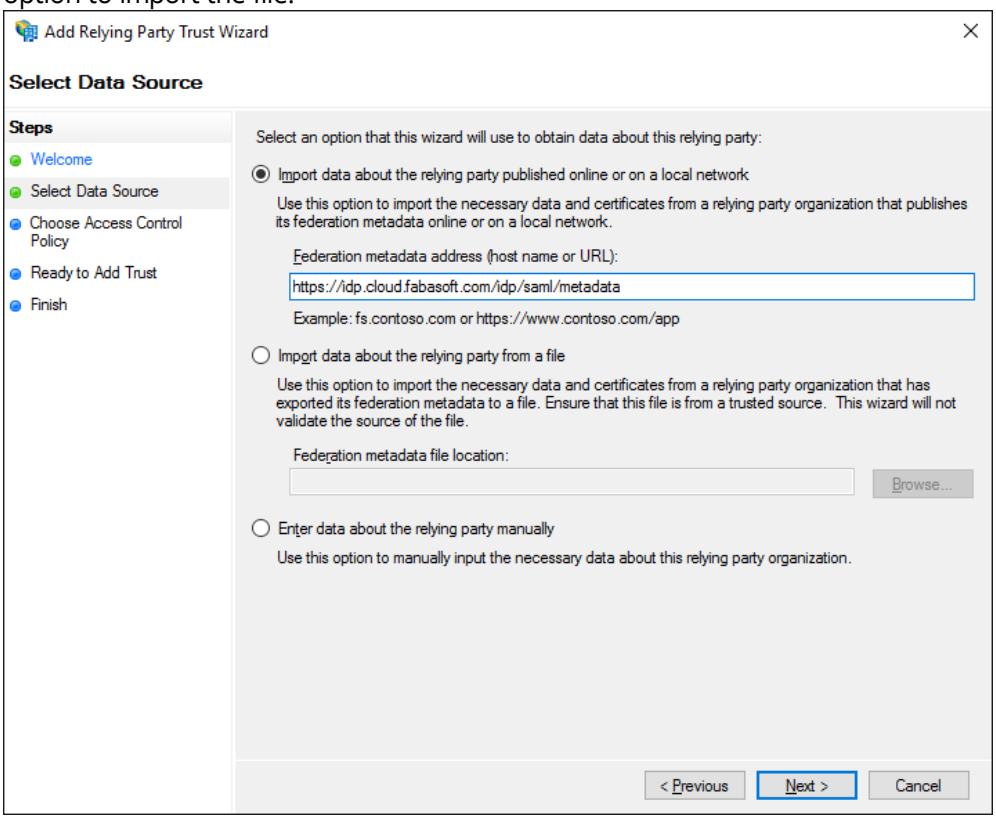
2. On the context menu of “Relying Party Trusts”, click “Add Relying Party Trust”.



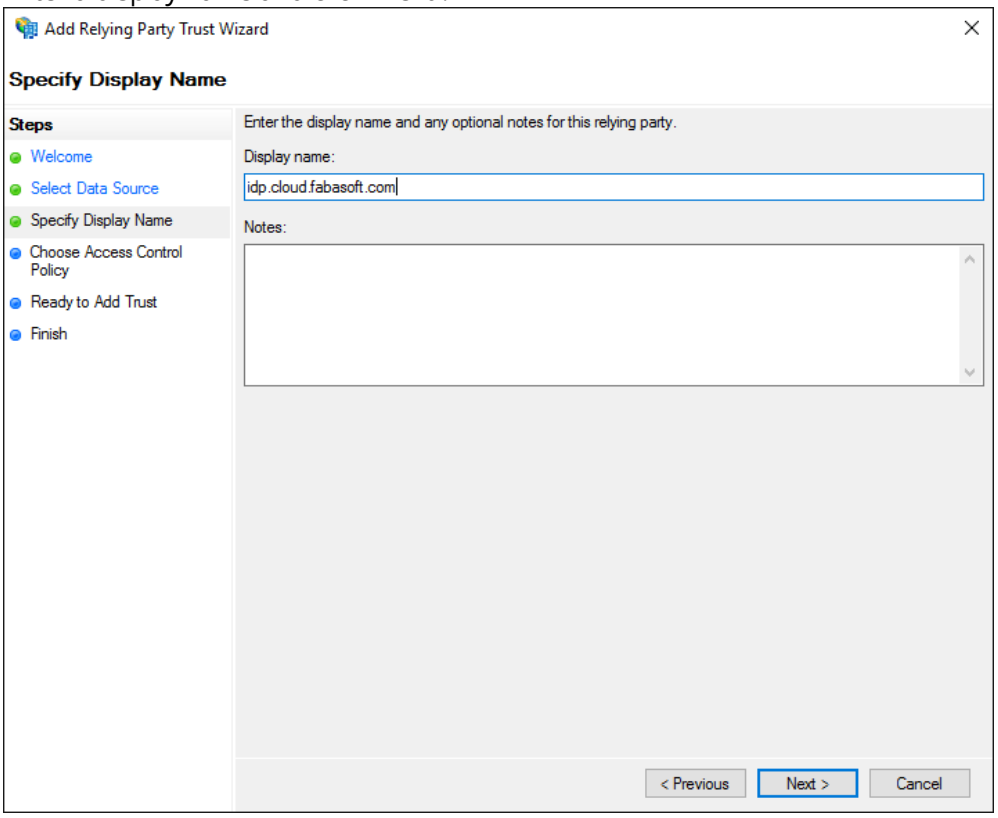
3. Select *Claims aware* and click “Start”.



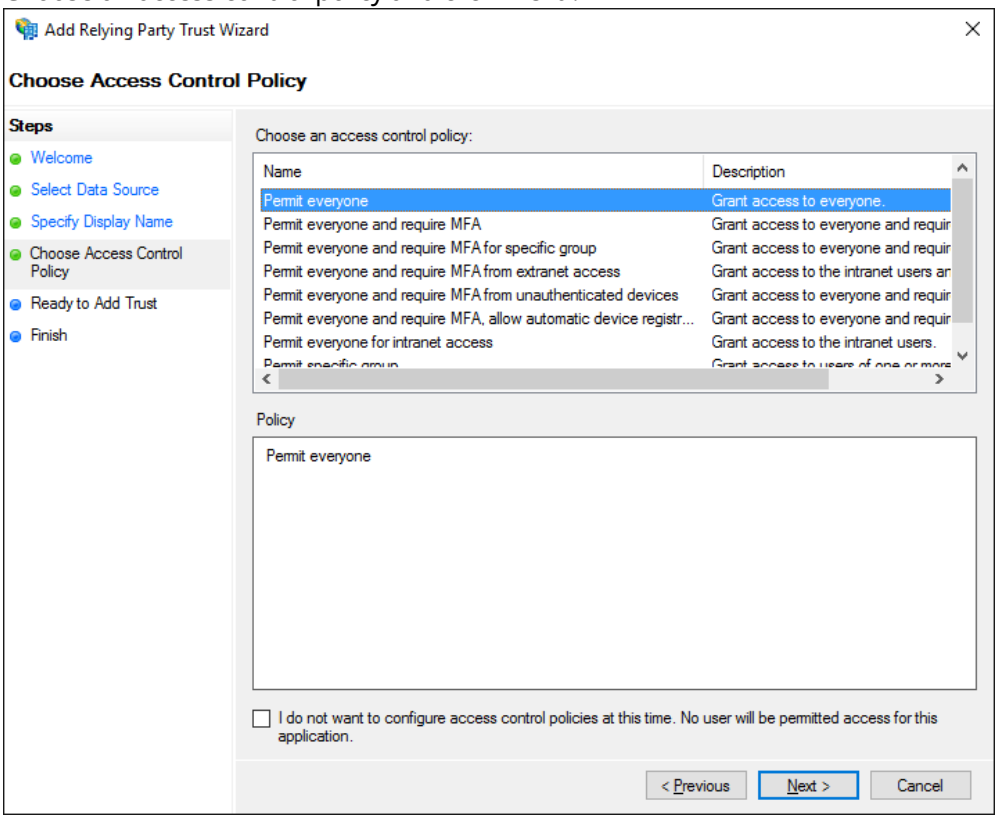
4. Enter the URL `https://idp.cloud.fabasoft.com/idp/saml/metadata` in the *Federation metadata address* field and click “Next”.
Note: Alternatively, you can download the `metadata.xml` from the URL and use the second option to import the file.



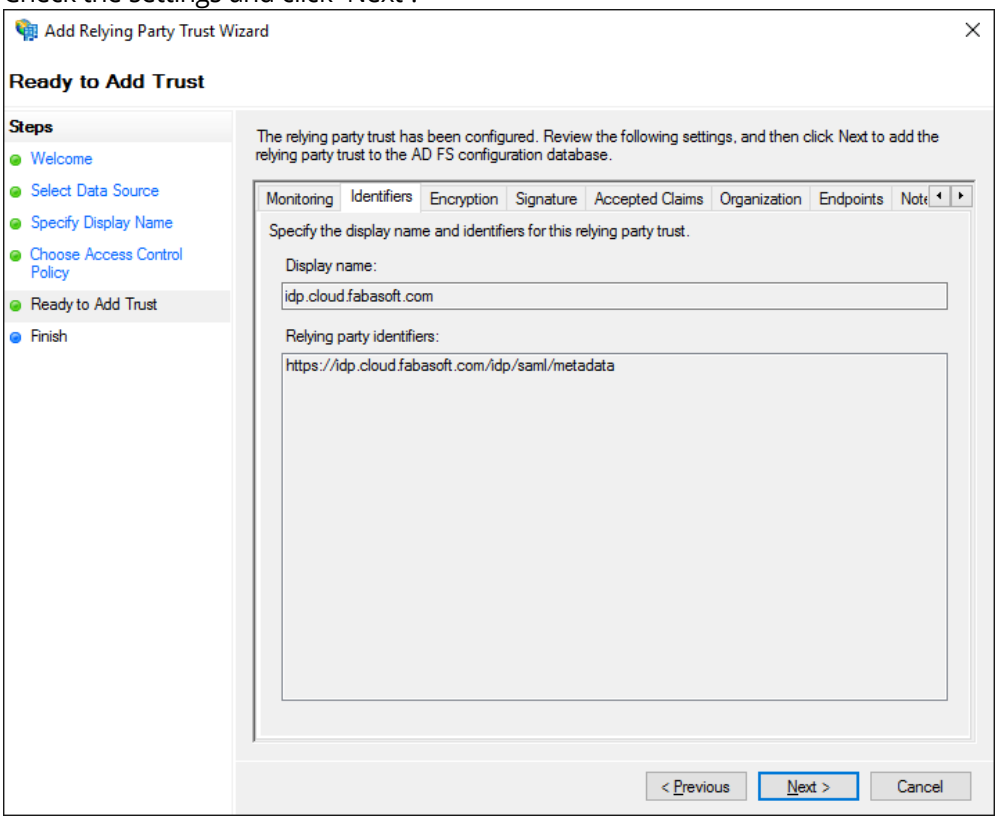
5. Enter a display name and click “Next”.



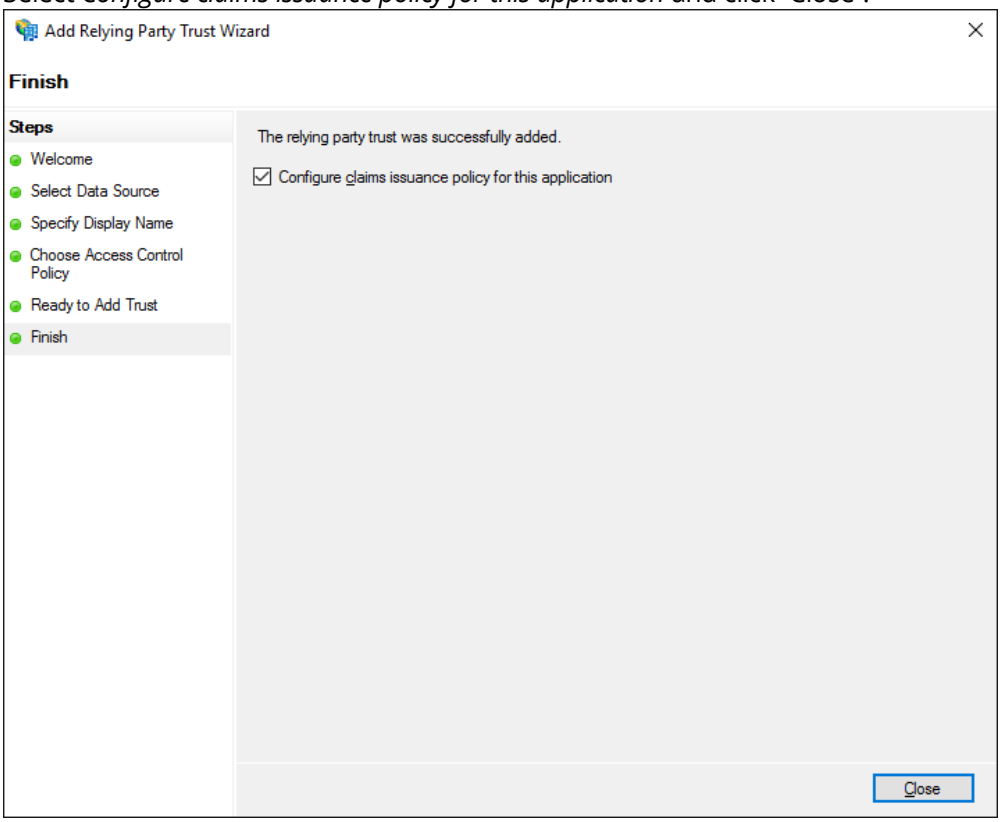
6. Choose an access control policy and click “Next”.



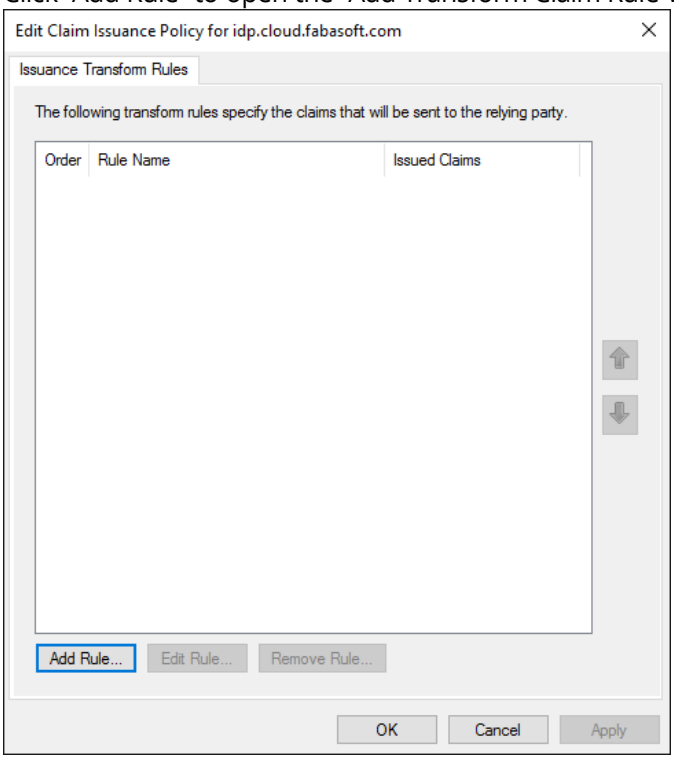
7. Check the settings and click “Next”.



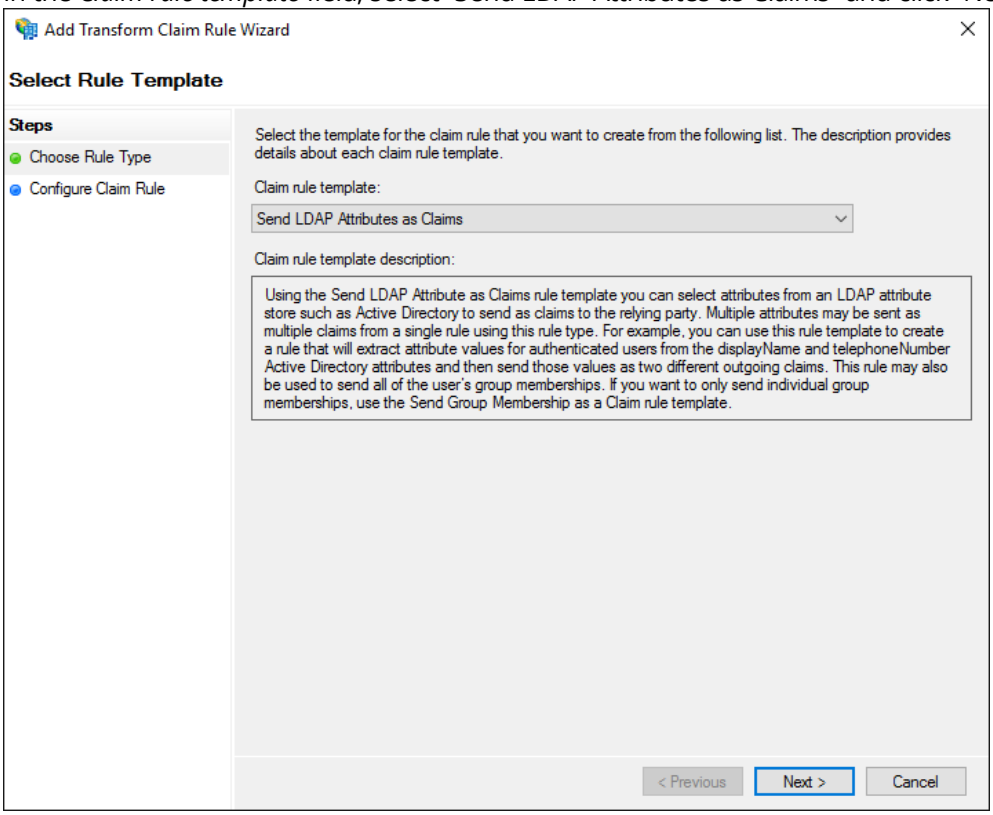
8. Select *Configure claims issuance policy for this application* and click “Close”.



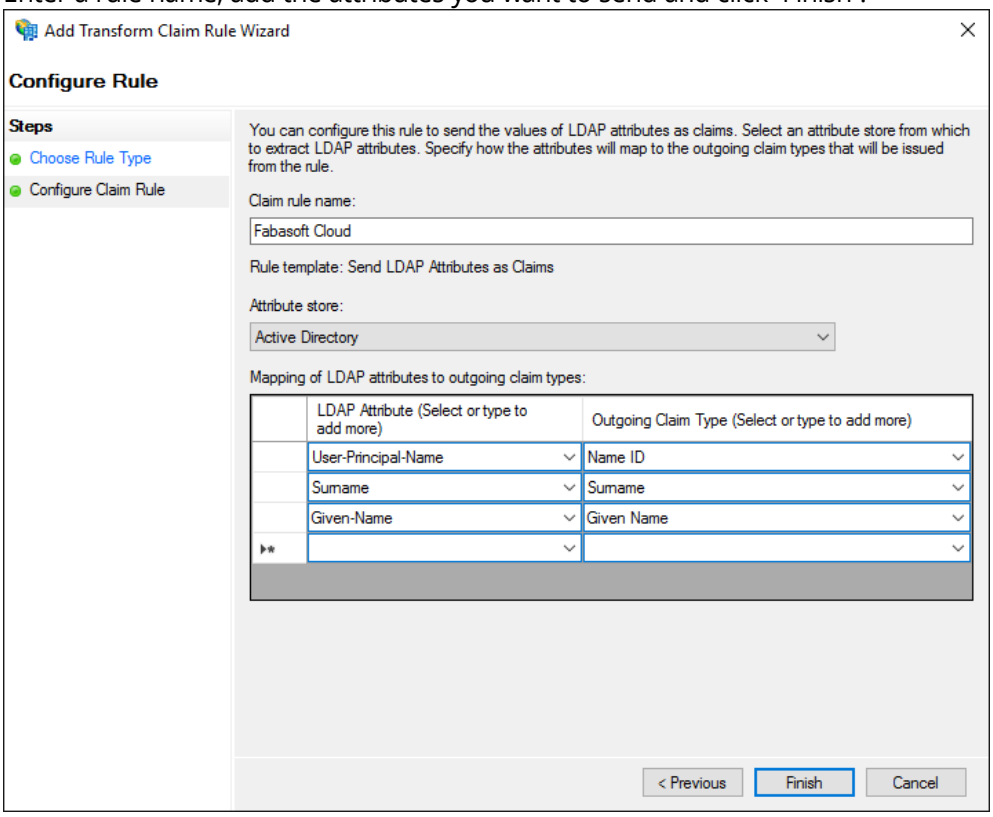
9. Click “Add Rule” to open the “Add Transform Claim Rule Wizard”.



10. In the *Claim rule template* field, select “Send LDAP Attributes as Claims” and click “Next”.



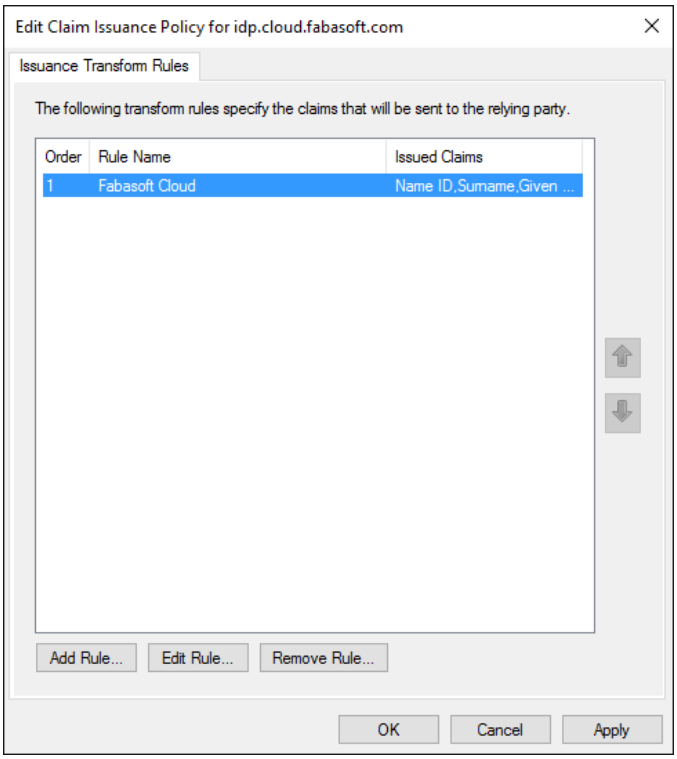
11. Enter a rule name, add the attributes you want to send and click “Finish”.



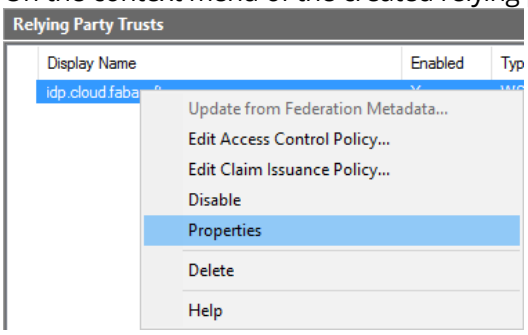
At least the following outgoing claim types must be defined:

- Name ID
  The LDAP attribute that is assigned to the outgoing claim type “Name ID” must contain the user’s e-mail address, which is used for the Fabasoft Cloud log-in.
- Surname
- Given Name

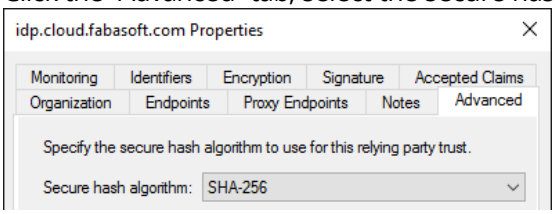
12. Click “OK”.



13. On the context menu of the created relying party trust, click “Properties”.



14. Click the “Advanced” tab, select the secure hash algorithm “SHA-256” and click “OK”.



4.3 Metadata

The `FederationMetadata.xml` metadata file can be opened and saved using the following link:
`https://<your AD FS>/FederationMetadata/2007-06/FederationMetadata.xml`

This file has to be sent to the Fabasoft Cloud Support.

5 Hints

The following hints may be helpful for troubleshooting.

Login With AD FS Fails With Error "SAML Message has wrong signature"

Have a look at http://social.technet.microsoft.com/Forums/en-US/4acc04b7-aac7-43e9-ba50-9570503045f9/msis0038-saml-message-has-wrong-signature.

Login with Google Chrome Fails

Certain client browser software does not support the Extended Protection for Authentication (e.g. Google Chrome). If web browsers that do not support "Extended Protection for Authentication" should be used, you may have to adjust a feature setting in AD FS 2.0.

http://technet.microsoft.com/en-us/library/hh237448%28WS.10%29.aspx

Integrated Authentication With Mozilla Firefox

Integrated authentication with Mozilla Firefox needs further configuration. The information can be found here: https://developer.mozilla.org/en-US/docs/Integrated_Authentication.