



White Paper

Configuration of Single Sign-On

2019 February Release

Copyright © Fabasoft R&D GmbH, Linz, Austria, 2019.

All rights reserved. All hardware and software names used are registered trade names and/or registered trademarks of the respective manufacturers.

No rights to our software or our professional services, or results of our professional services, or other protected rights can be based on the handing over and presentation of these documents.

Contents

1 Introduction	4
2 Configuration in the Fabasoft Cloud	4
3 Configuration of an Arbitrary SAML 2.0 Identity Provider	4
4 Configuration of Active Directory Federation Services (AD FS)	4
4.1 Prerequisites	4
4.2 Configure Your AD FS	4
4.3 Metadata	10
5 Hints	10

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:

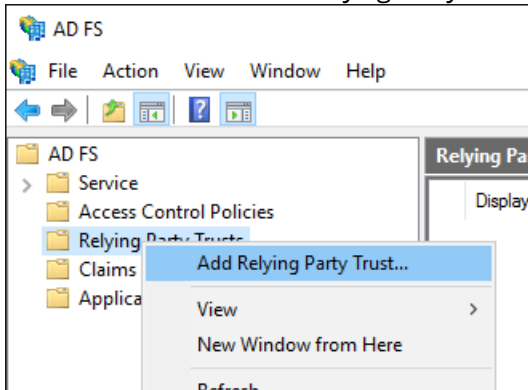
- [Microsoft Active Directory Federation Services 2.0](#)
Note: Microsoft Windows Server 2008 R2 includes AD FS 1.0, which does not support SAML 2.0 - you need to install the [AD FS 2.0 'release to web' \(RTW\) package](#).
- The hotfix <http://support.microsoft.com/kb/2159360/en-us> needs to be installed.
- 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

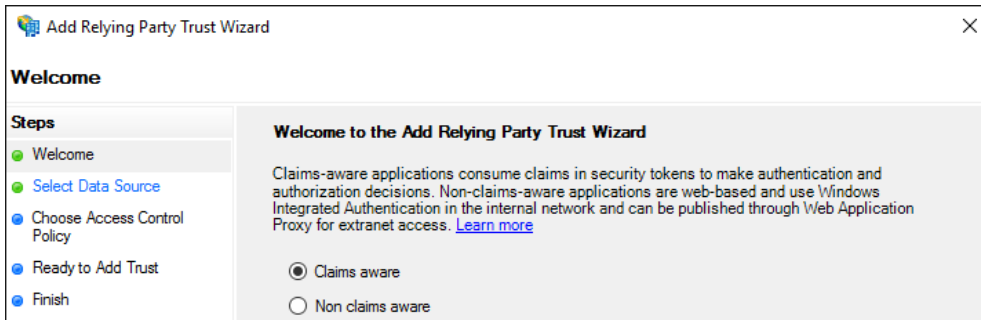
To configure your AD FS for the Fabasoft Cloud, perform the following steps:

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

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

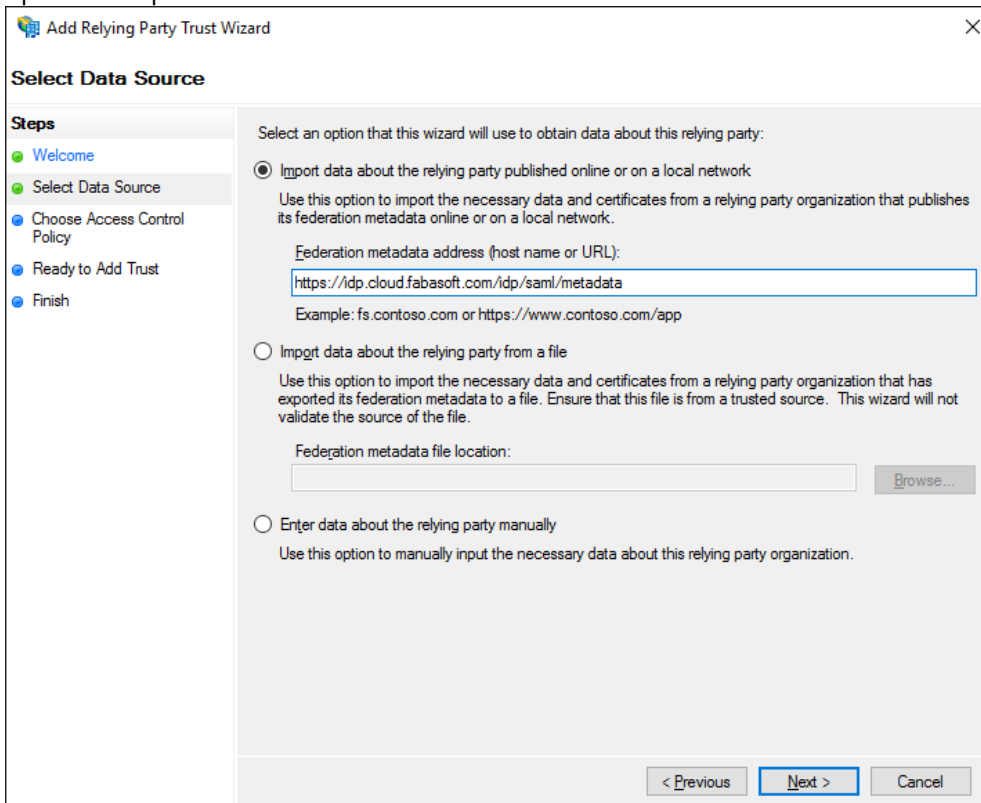


3. Select *Claims aware* and click "Start".



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".

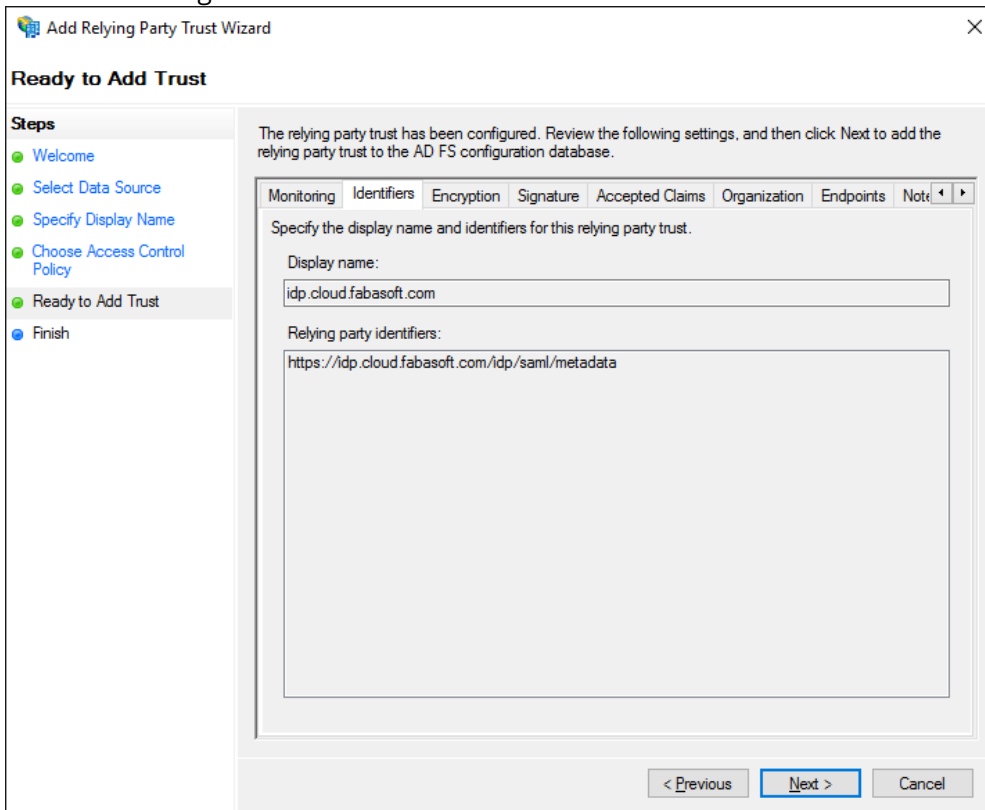
The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Specify Display Name'. On the left, a 'Steps' pane lists: Welcome, Select Data Source, Specify Display Name (highlighted), Choose Access Control Policy, Ready 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:' text box containing 'idp.cloud.fabasoft.com|' and a 'Notes:' text area. At the bottom, there are three buttons: '< Previous', 'Next >' (highlighted), and 'Cancel'.

6. Choose an access control policy and click "Next".

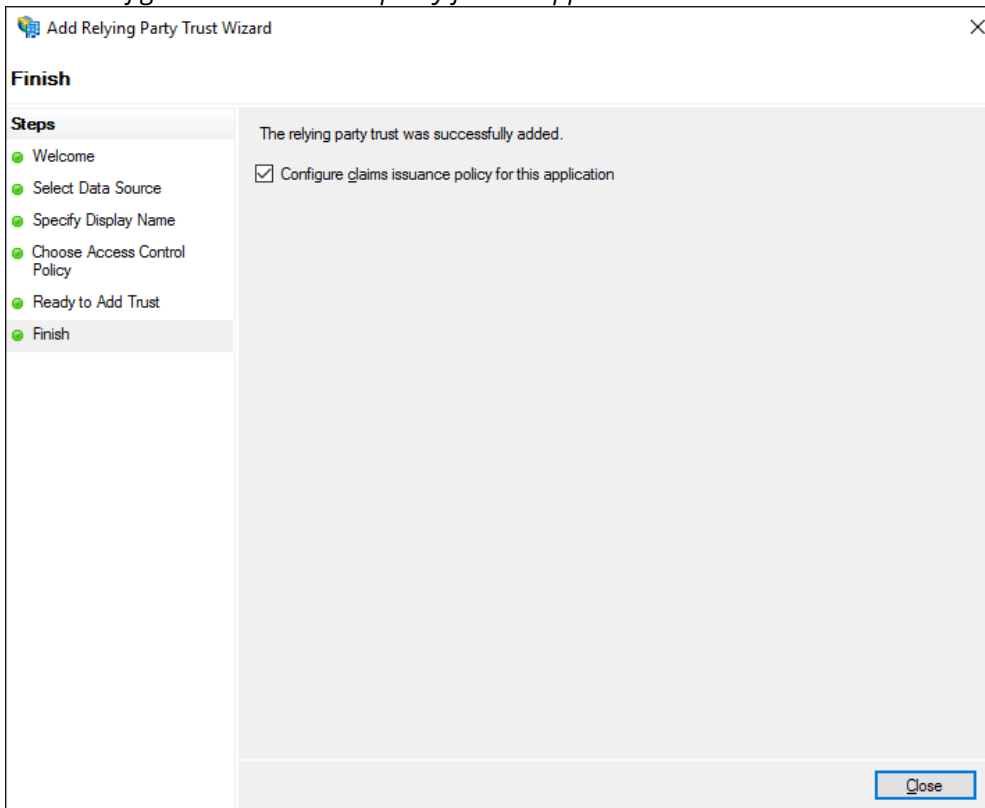
The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Choose Access Control Policy'. On the left, a 'Steps' pane lists: Welcome, Select Data Source, Specify Display Name, Choose Access Control Policy (highlighted), Ready to Add Trust, and Finish. The main area contains the instruction 'Choose an access control policy:'. Below this is a table with two columns: 'Name' and 'Description'. The first row, 'Permit everyone', is selected. Below the table is a 'Policy' text box containing 'Permit everyone'. At the bottom, there is a checkbox with the text 'I do not want to configure access control policies at this time. No user will be permitted access for this application.' and three buttons: '< Previous', 'Next >' (highlighted), and 'Cancel'.

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require MFA.
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA for specific group.
Permit everyone and require MFA from extranet access	Grant access to the intranet users and require MFA from extranet access.
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require MFA from unauthenticated devices.
Permit everyone and require MFA, allow automatic device registration	Grant access to everyone and require MFA, allow automatic device registration.
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more groups.

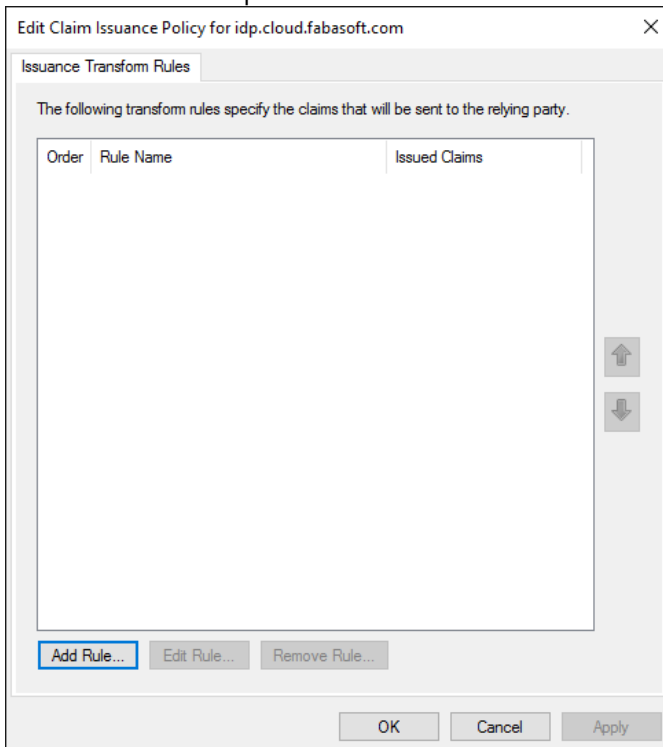
7. Check the settings and click "Next".



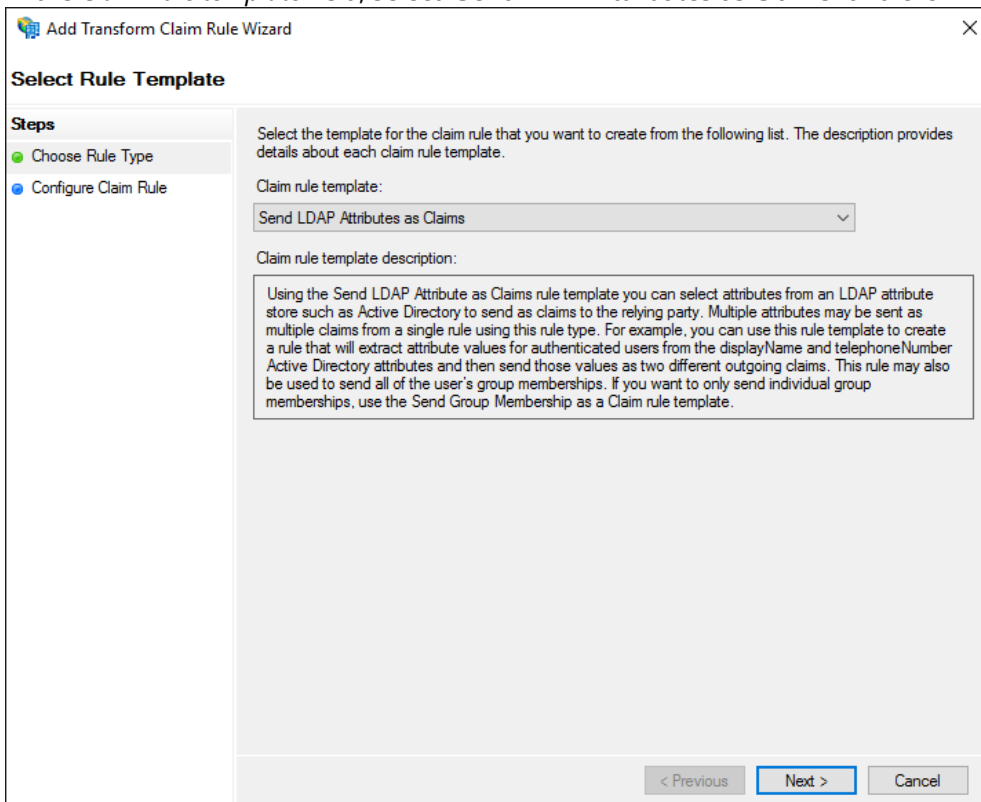
8. Select *Configure claims issuance policy for this application* and click "Close".



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”.

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, specifically the 'Configure Rule' step. The 'Steps' pane on the left shows 'Configure Claim Rule' as the active step. The main area contains the following configuration options:

- Claim rule name:** Fabasoft Cloud
- Rule template:** Send LDAP Attributes as Claims
- Attribute store:** Active Directory
- Mapping of LDAP attributes to outgoing claim types:**

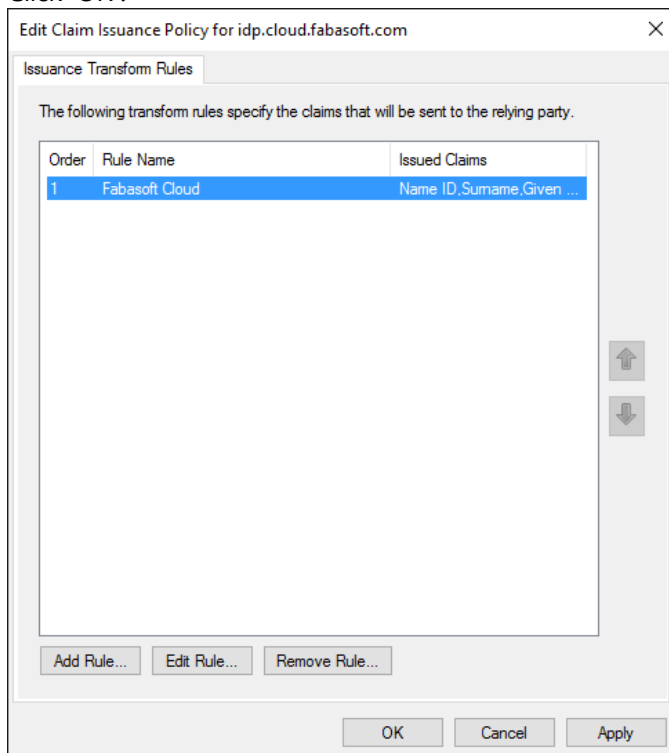
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	User-Principal-Name	Name ID
	Surname	Surname
	Given-Name	Given Name
▶*		

At the bottom of the dialog are three buttons: '< Previous', 'Finish', and 'Cancel'.

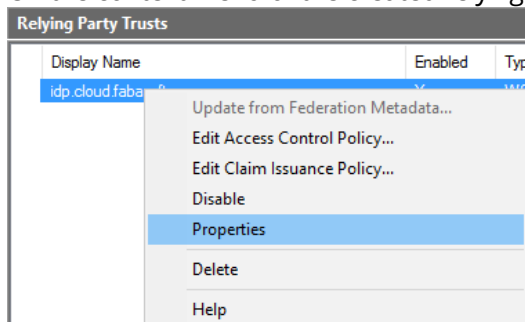
At least the following outgoing claim types must be defined:

- 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

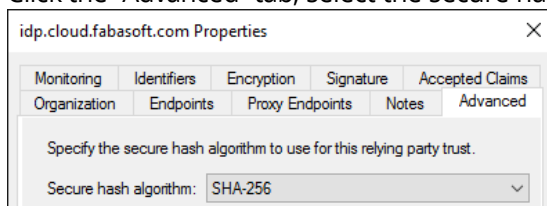
12. Click "OK".



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.