

SSO against Active Directory Federation Services (AD FS)

This article describes how to configure your Active Directory Federation Services (ADFS) to enable Imagicle users to login to web portal, gadgets and Attendant Console with Single Sign-on based on SAML protocol.

This procedure has been tested with ADFS 3.0.

Prerequisites

In order to successfully configure your ADFS, you should have the following data:

- **User Pool ID**
- **Redirect URI**

More details are available [here](#).

Procedure

1. Connect to the Windows Server instance where you have installed ADFS as an Administrator via RDP
2. Open the ADFS console
3. Go to **"Trust Relationships" > "Relying Party Trusts" > "Add relying party trusts"**. This will start a wizard
4. On the Welcome tab select **"Claims aware"**, then click **"Next"**
5. On the Data Source tab select **"Enter data about the relying part manually"**, then click **"Next"**
6. On the Display Name tab set **"Imagicle UCS"** as **"Display name"** (or whatever you prefer), then click **"Next"**
7. On the Configure Certificate tab do not configure anything and click **"Next"**
8. On the Configure URL tab select **"Enable support for the SAML 2.0 WebSSO protocol"** and set the **Redirect URI** as a **"Relying party SAML 2.0 SSO service URL"**, then click **"Next"**

Configure URL

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- **Configure URL**
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

Example: https://www.contoso.com/adfs/ls/

< Previous

Next >

Cancel

9. On the Configure Identifiers tab add the **User Pool ID** as a "Relying party trust identifier". It must be in the format **urn:amazon:cognito:sp:<User Pool ID>** (e.g., urn:amazon:cognito:sp:eu-central-1_xxxxxxx). Then click "Next"

Configure Identifiers

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- **Configure Identifiers**
- Choose Access Control Policy
- Ready to Add Trust
- Finish

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

Relying party trust identifier:

Add

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

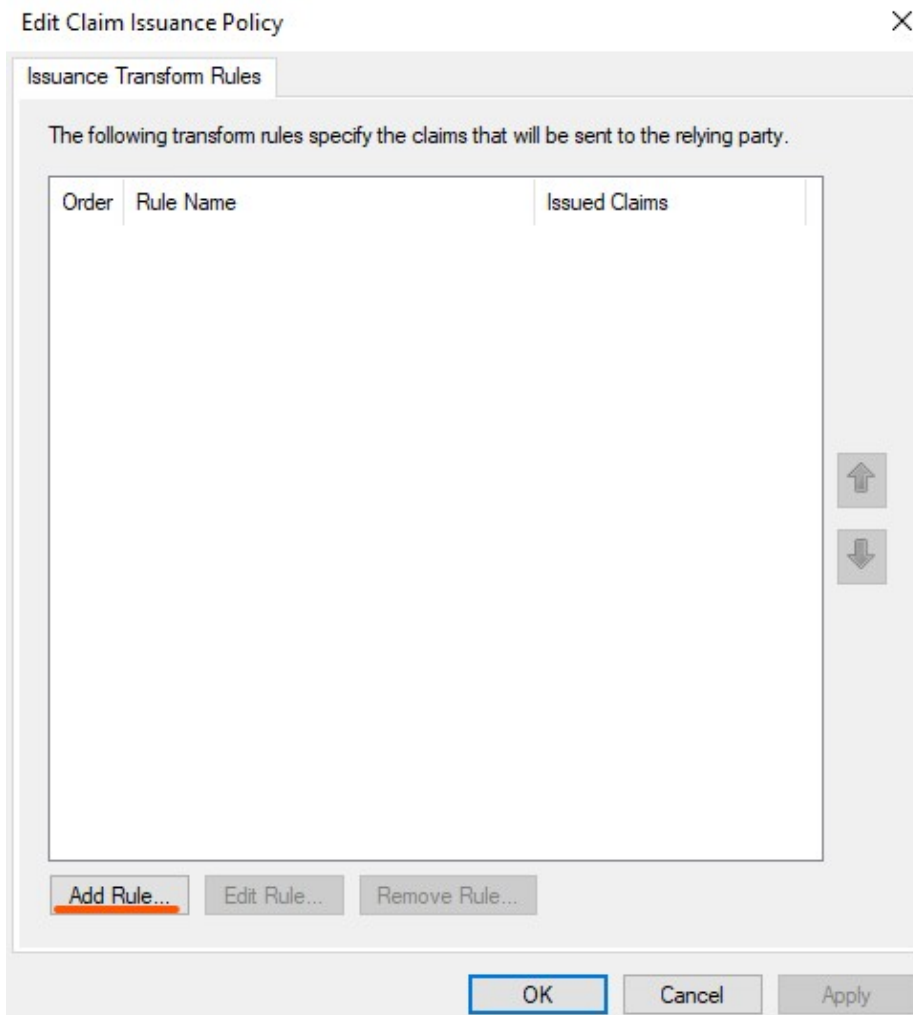
Relying party trust identifiers:

Identifier
https://fs.contoso.com/adfs/services/trust

Remove

< Previous Next > Cancel

10. On the Access Control Policy select **"Permit everyone"**, then click **"Next"**
11. On the Ready to Add Trust do not change anything and click **"Next"**
12. On the Finish tab enable **"Configure claims issuance policy for this application"**, then click **"Close"**
13. On the Edit Claim Issuance Policy click on **"Add Rule"**



14. On the Add Transform Claim Rule Wizard select **"Send LDAP Attributes as Claims"** as a **"Claim rule template"**, then click **"Next"**
15. On the Configure Claim Rule:
 - ◆ set **"Name ID"** as a **"Claim rule name"**
 - ◆ set **"Active Directory"** as an **"Attribute store"**
16. On the Mapping of LDAP attributes:
 - ◆ set **"SAM-Account-Name"** as an **"LDAP Attribute"**
 - ◆ set **"Name ID"** as an **"Outgoing Claim Type"**

Add Transform Claim Rule Wizard X

Configure Rule

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:

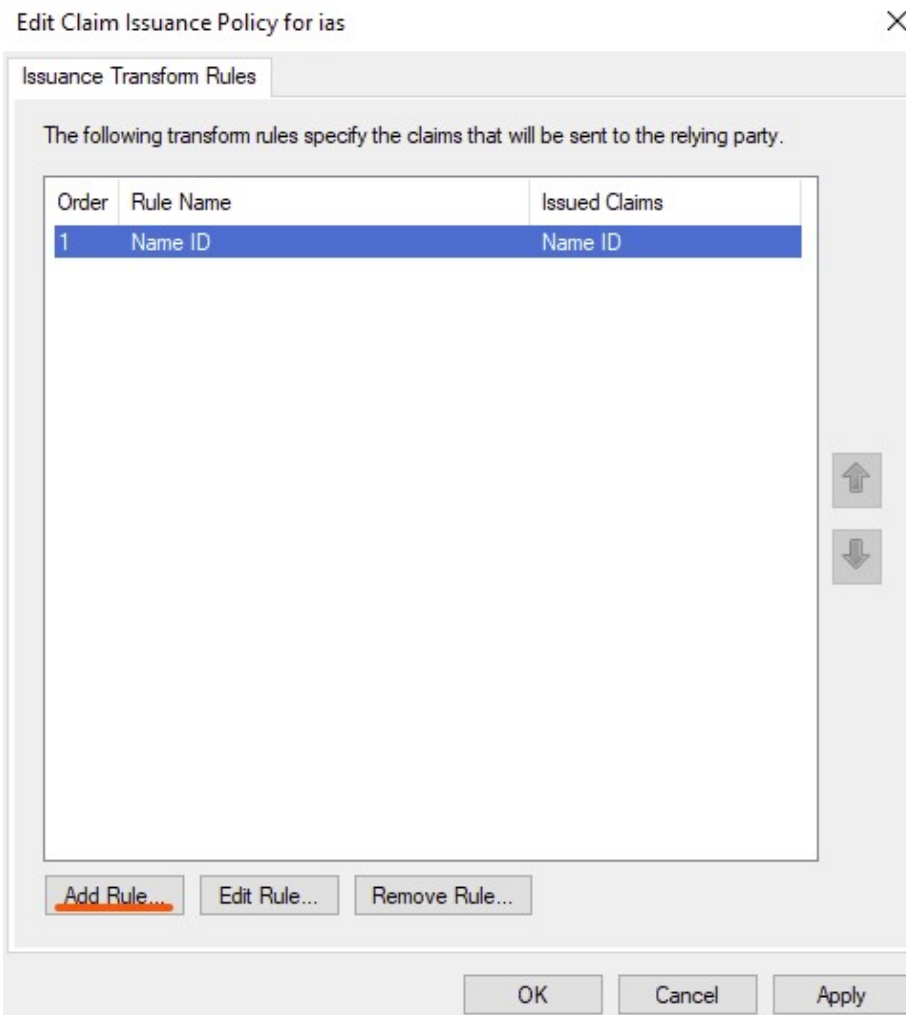
Rule template: Send LDAP Attributes as Claims

Attribute store:

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)
▶	SAM-Account-Name	Name ID
*		

- â
- then click on **"Finish"**
- 17. Click again on **"Add rule"**



18. On the Add Transform Claim Rule Wizard select **"Send LDAP Attributes as Claims"** as a **"Claim rule template"**, then click **"Next"**
19. On the Configure Claim Rule:
 - ◆ set **"E-Mail"** as a **"Claim rule name"**
 - ◆ set **"Active Directory"** as an **"Attribute store"**
20. On the Mapping of LDAP attributes:
 - ◆ set **"E-Mail-Addresses"** as an **"LDAP Attribute"**
 - ◆ set **"E-Mail Address"** as an **"Outgoing Claim Type"**

Add Transform Claim Rule Wizard

Configure Rule

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.

Steps

- Choose Rule Type
- Configure Claim Rule

Claim rule name: E-Mail

Rule template: Send LDAP Attributes as Claims

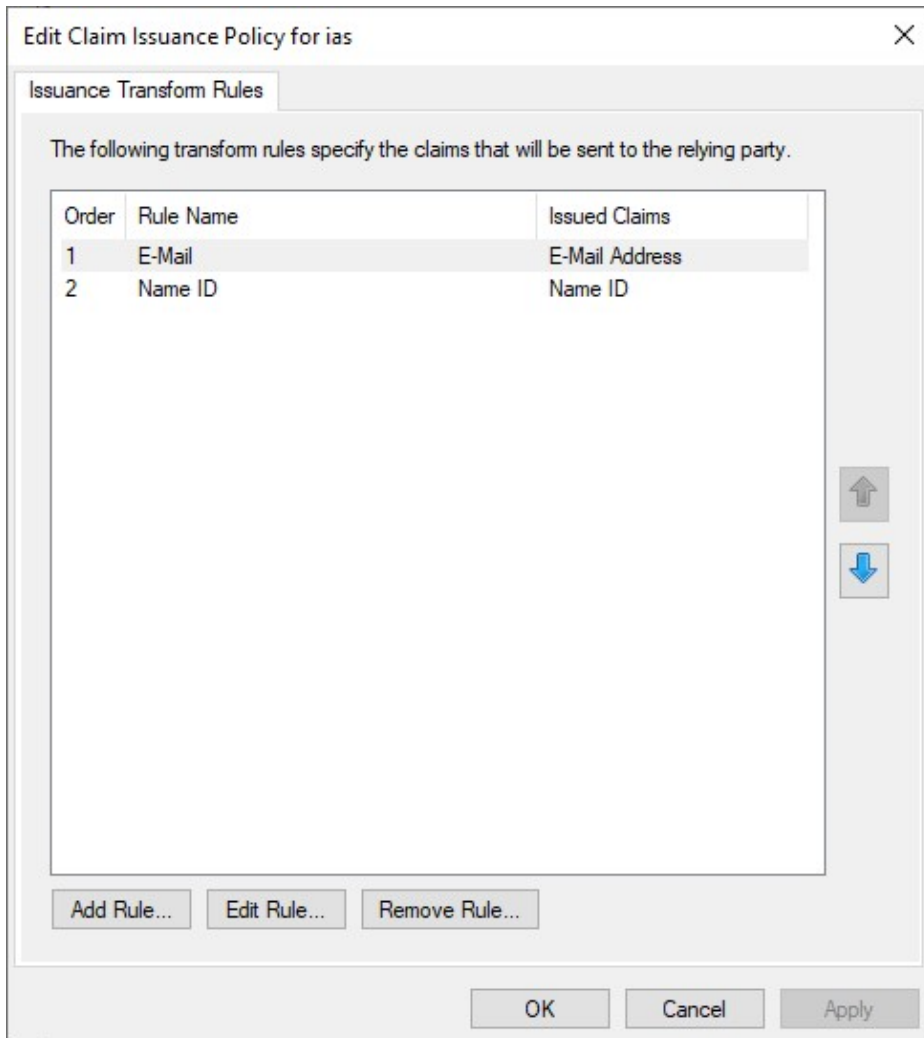
Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

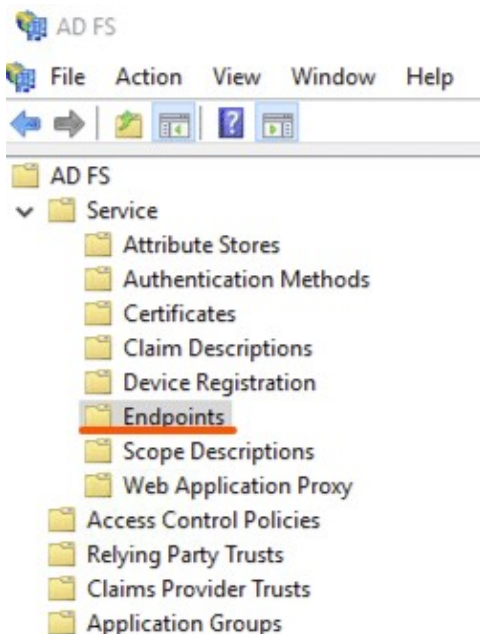
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
*		

< Previous Finish Cancel

- then click on "Finish"
- Click now on "OK" to complete the configuration



22. Last thing to do is download the Federation Metadata xml file. This can be found by clicking on **"AD FS" > "Service" > "Endpoints"** then locate the URL path in the **"Metadata"** section. The path is typically **/FederationMetadata/2007-06/FederationMetadata.xml** as shown



below:

imagicle

23. To download the file, load the URL in the browser on the server (e.g.,
<https://<hostname>/FederationMetadata/2007-06/FederationMetadata.xml>)
24. Please send downloaded file to **Imagicle Team** to complete the SSO federation.