AssetSonar Microsoft ADFS SAML 2.0 configuration instruction

Contents

Configuration short summary: 2
Configure SAML settings on https://{{subdomain}}.assetsonar.com 3
Prerequisites 3
SAML Add On configuration 4
Identity Provider URL: 4
Identity Provider Certificate 6
Login Button Text 6
First Name, Last Name and Email 7
Configure Microsoft AD FS 2.0 8
Create custom claims descriptions 8
Create Relying Party 8
Configure Claim Rules for Relying Party 10
Verify how it works 11
Troubleshooting 12

1. Configuration short summary:

1.1. AssetSonar configuration:

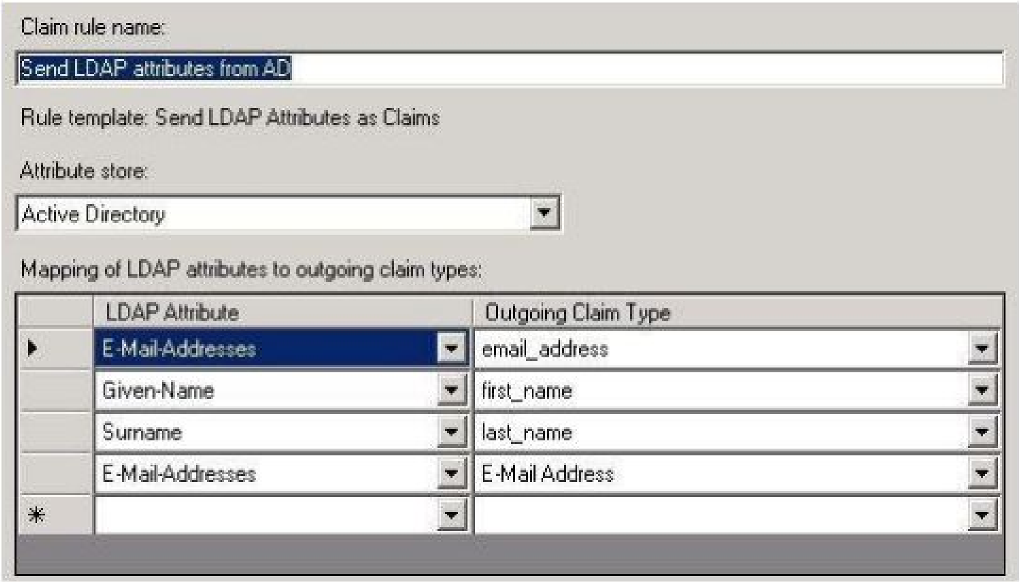
identity provider url	**Microsoft Active Federation Service URL**
IdentityProvider Certificate	**-----BEGIN CERTIFICATE-----** **x509 certificate** **-----END CERTIFICATE-----**
First Name	**first_name(configurable. Using this for setup)**
Last name	**last_name(configurable. Using this for setup)**
Email	**email_address(configurable. Using this for setup)**

1.2. Microsoft AD FS 2.0 configuration

display name	{{subdomain}}.assetsonar.com
relying party identifier	https://ezo.io/assetsonar/
secure hash algorithm	SHA-256
POST endpoint	https://subdomain.assetsonar.com/users/auth/saml/callback

<table>
<tr>
<td><b>Claim rules</b></td>
<td>

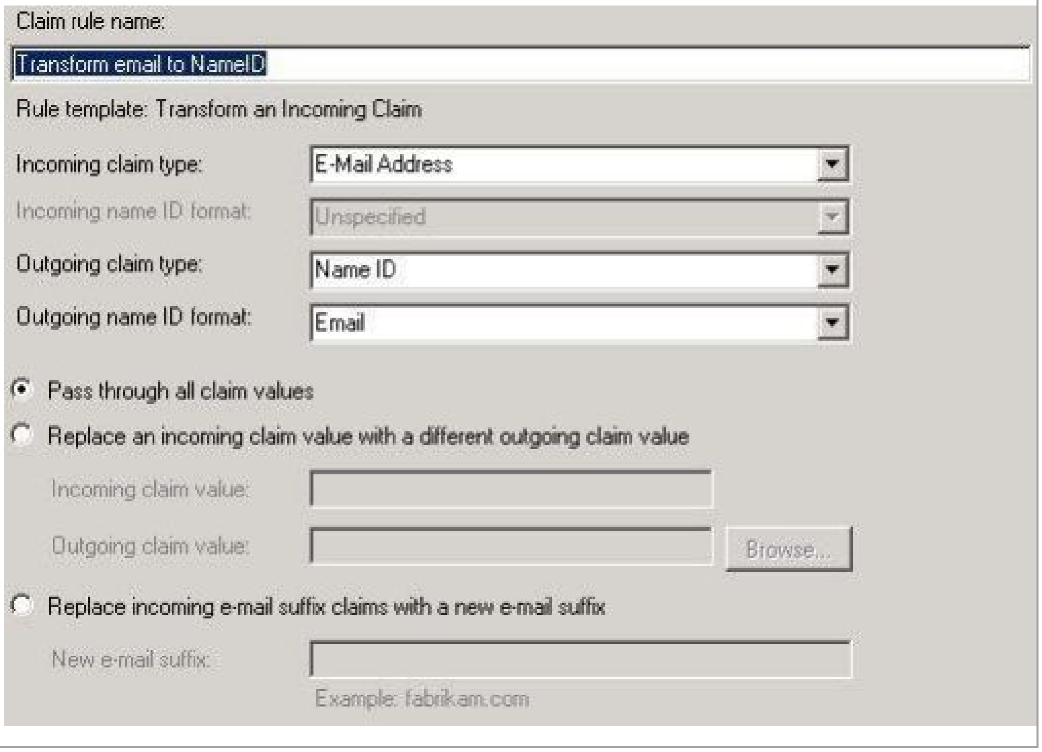
<b>1.</b>



Claim rule name:
Send LDAP attributes from AD
Rule template: Send LDAP Attributes as Claims
Attribute store:
Active Directory
Mapping of LDAP attributes to outgoing claim types:

<table>
<tr><th></th><th>LDAP Attribute</th><th>Outgoing Claim Type</th></tr>
<tr><td>▶</td><td>E-Mail-Addresses</td><td>email_address</td></tr>
<tr><td></td><td>Given-Name</td><td>first_name</td></tr>
<tr><td></td><td>Surname</td><td>last_name</td></tr>
<tr><td></td><td>E-Mail-Addresses</td><td>E-Mail Address</td></tr>
<tr><td>*</td><td></td><td></td></tr>
</table>

<b>2.</b>



Claim rule name:
Transform 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:

○ Replace incoming e-mail suffix claims with a new e-mail suffix
New e-mail suffix:
Example: fabrikam.com

</td>
</tr>
</table>

Configure SAML settings on https://{{subdomain}}.assetsonar.com

Prerequisites

You must be Company Owner can configure SAML Add On

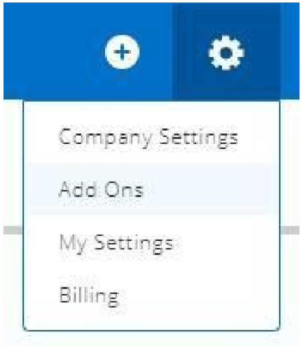
To set Company Owner:

1. **Login to https://{{subdomain}}.assetsonar.com**
2. **Go to Settings**
3. **Go to Company Settings -> Company Profile**

Find Company Owner field and change the owner to required person:
Note: you will not be able to change yourself back to the owner, so use it with care. In order to change back the owner, the new owner should change back this option to your profile.

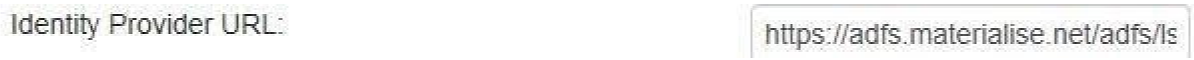
SAML Add On configuration

1. **Login to https://{{subdomain}}.assetsonar.com**
2. **Go to Settings**



3. **Go to Company Settings -> Add Ons**
   Find SAML Integration Add On and enable it.
4. **Configure required fields:**

Identity Provider URL:



Identity Provider URL: https://adfs.materialise.net/adfs/ls

Set to your ADFS URL

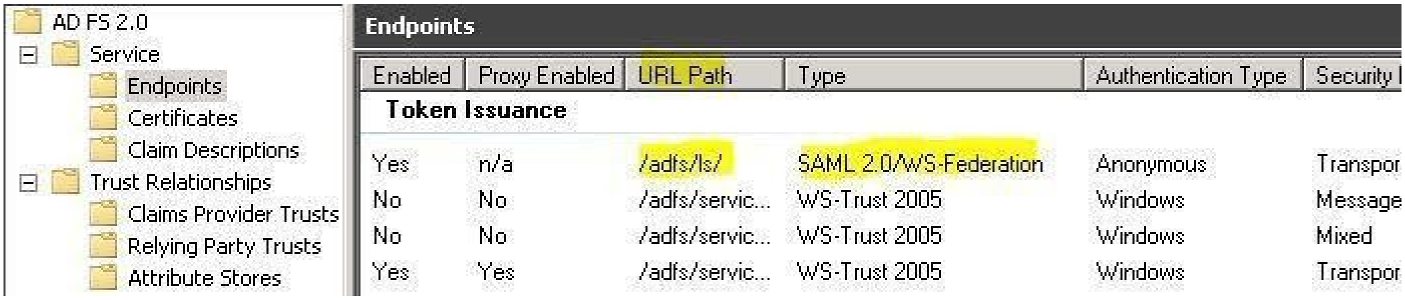
To find this option on your ADFS server:

Option 1:

1. **Open AD FS management console**

2. **Go to Service -> Endpoints**

   Search for endpoint type called "SAML 2.0/WS-Federation"

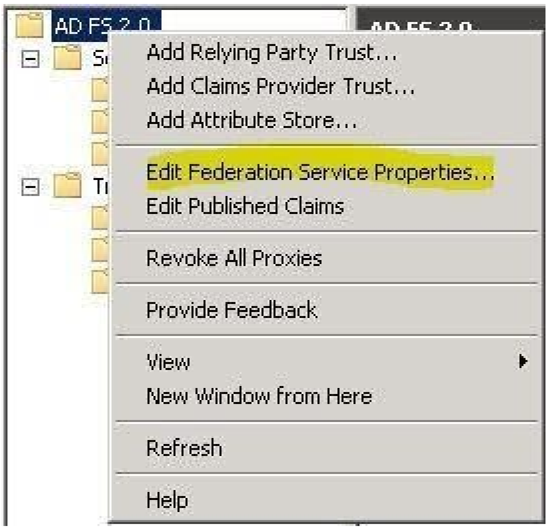


Endpoints

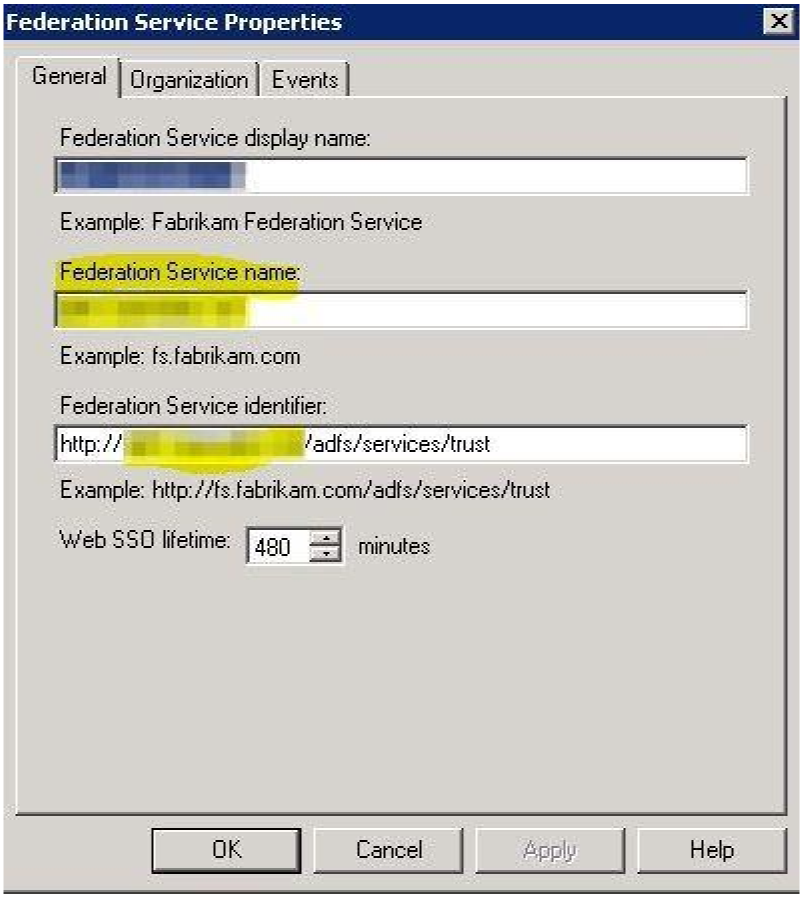
Enabled	Proxy Enabled	URL Path	Type	Authentication Type	Security I
Token Issuance					
Yes	n/a	/adfs/ls/	SAML 2.0/WS-Federation	Anonymous	Transpor
No	No	/adfs/servic...	WS-Trust 2005	Windows	Message
No	No	/adfs/servic...	WS-Trust 2005	Windows	Mixed
Yes	Yes	/adfs/servic...	WS-Trust 2005	Windows	Transpor

In the URL you can find the path relative to your ADFS root path In order to get first part of URL

1. Right click on AD FS 2.0 and select “Edit Federation Service Properties…”



2. Find “Federation Service identifier” in General tab:



Federation Service display name:
[redacted]

Example: Fabrikam Federation Service

Federation Service name:
[redacted]

Example: fs.fabrikam.com

Federation Service identifier:
http://[redacted]/adfs/services/trust

Example: http://fs.fabrikam.com/adfs/services/trust

Web SSO lifetime: 480 minutes

This will be linked to the first part of the path. Also make necessary changes If you are using HTTPS

Identity Provider Certificate

Description: The certificate format is PEM. i.e. Base64 encoded DER wrapped around "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"

Identity Provider Certificate:

```
-----BEGIN CERTIFICATE-----
MIIC5DCCAcygAwIBAgIQEzd
wEQq3trRFJHfjmgj+pDANBg
```

You need to get the public key portion of a token-signing certificate and paste it in this field.

In order to get public key you need to:

Option1:

Follow instruction: https://technet.microsoft.com/en-us/library/cc737522(v=ws.10).aspx

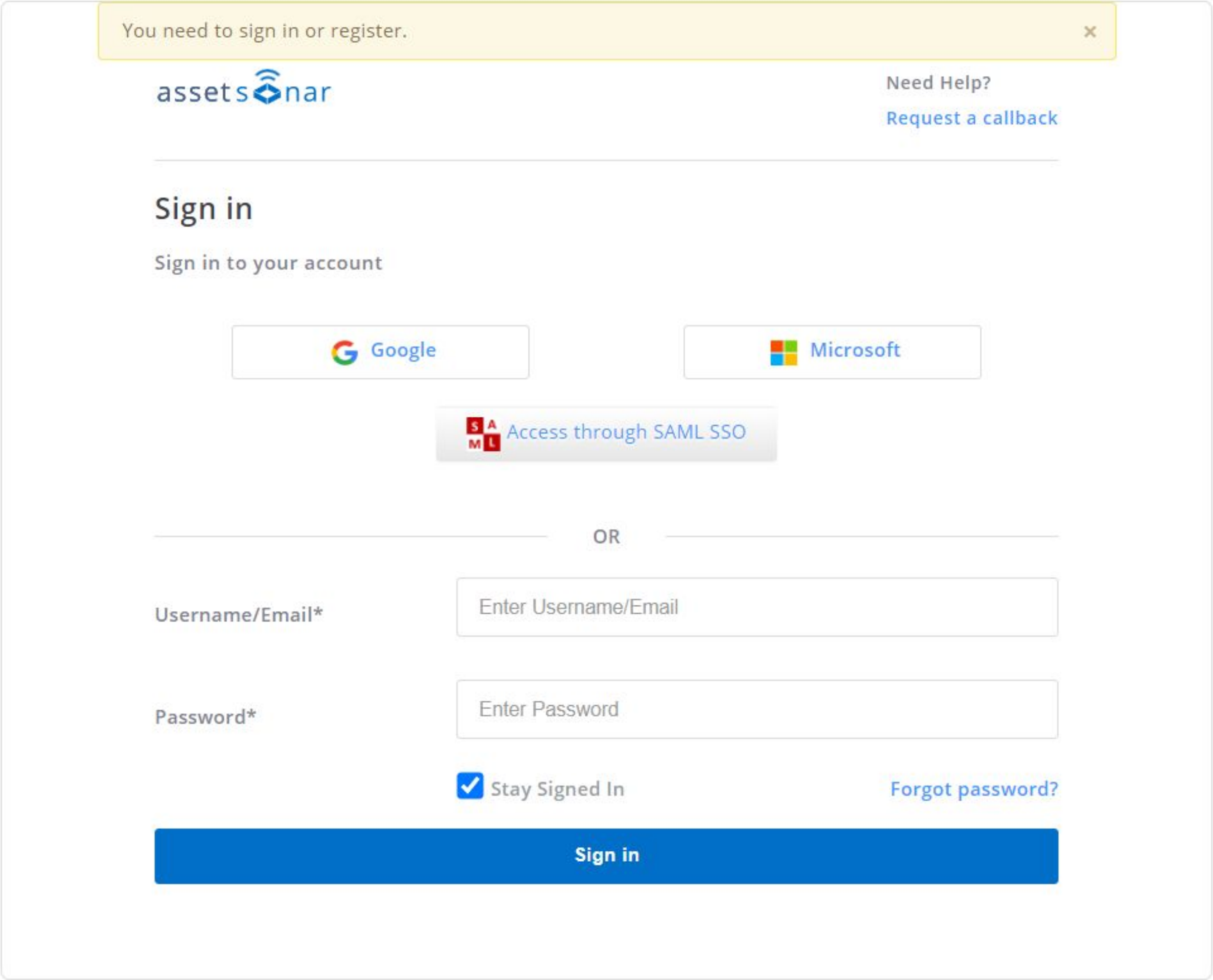
Select Base-64 encoded X.509 (.CER)

Login Button Text

Login Button Text: (?)

Login thru SAML

Just type your text, it will be shown to users on the login page:



You need to sign in or register.

Sign in

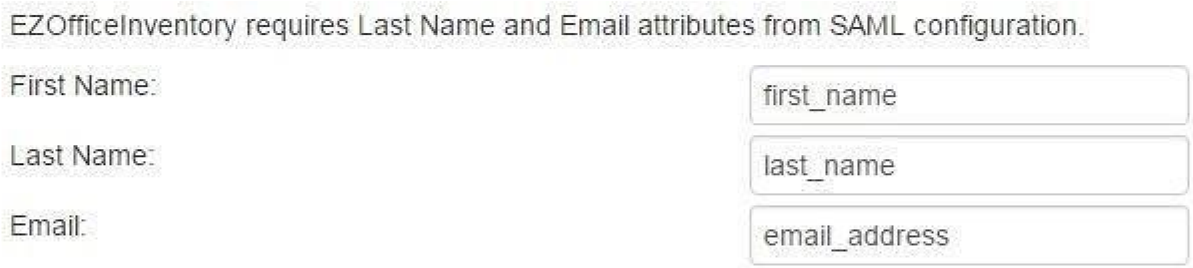
Sign in to your account

First Name, Last Name and Email

Description: In the AssetSonar system, since we need to map resources e.g. (assets, stock assets etc) against users, we need to create them in our end. For us to create the Users, we require the fields.

Q: Do you filter from your side email address domain attribute, for example you accept logins only from users with an email domain?

A: No. All Users that successfully authenticate through SAML are assumed to be valid users.



EZOfficeInventory requires Last Name and Email attributes from SAML configuration.

First Name:	first_name
Last Name:	last_name
Email:	email_address

You will need next claims which we later define in ADFS:

first_name
last_name
email_address
nameidentifier

Note: nameidentifier claim usually required by everySAML

Note: you can create your claims with custom names. Make sure that the name defined in AssetSonar and in ADFS is the same

Note: I did not manage to make it work with ADFS default claims: given name, surname, email address, but custom claims above work ok.

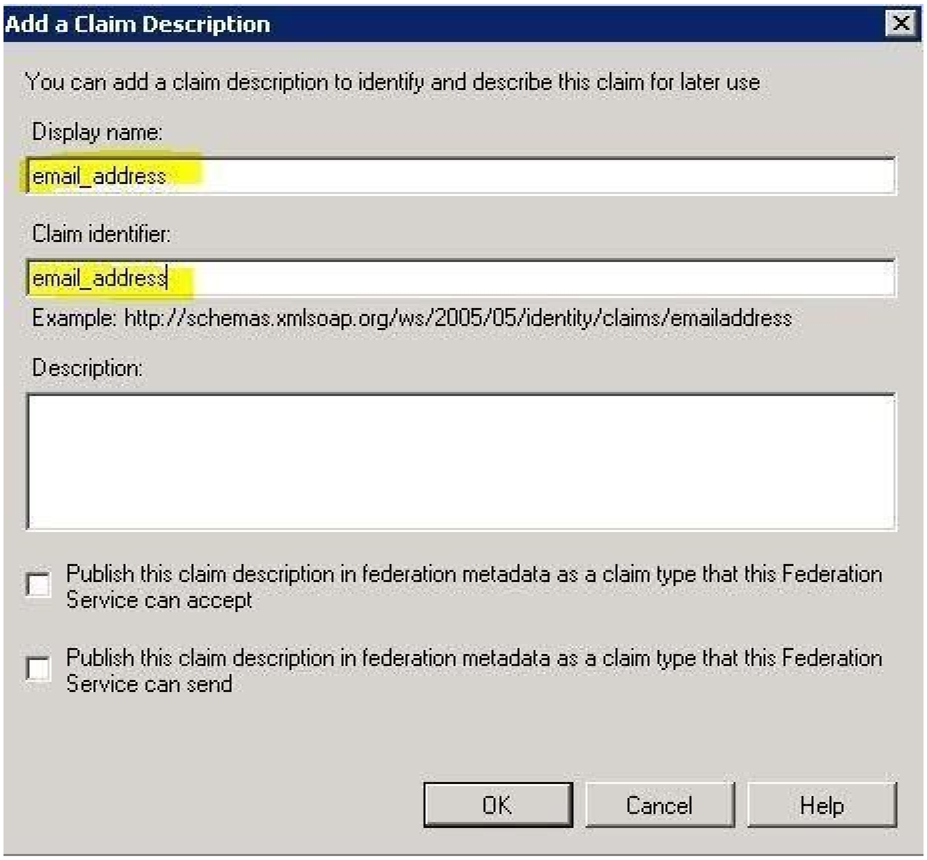
Configure Microsoft AD FS 2.0

Create custom claims descriptions

1. **Open AD FS management console**

2. **Go to Service -> Claim Descriptions and click Add Claim Description…**

3. **Define claim as below:**



Add a Claim Description

You can add a claim description to identify and describe this claim for later use

Display name:

email_address

Claim identifier:

email_address

Example: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

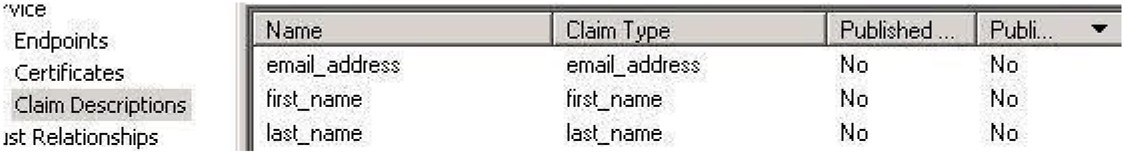
Description:

□ Publish this claim description in federation metadata as a claim type that this Federation Service can accept

□ Publish this claim description in federation metadata as a claim type that this Federation Service can send

4. Do the same for first_name and last_name claims

Note: do not "Publish" these claims, if you need to publish them, specify full URL in Claim identifier, for example: http://schemas.xmlsoap.org/claims/email_address. Otherwise your metadata web-page will stop working.
Result should look like this:

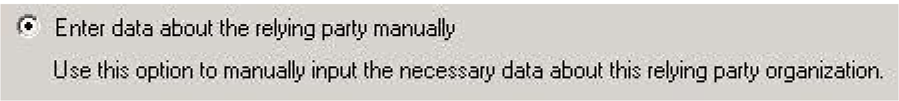
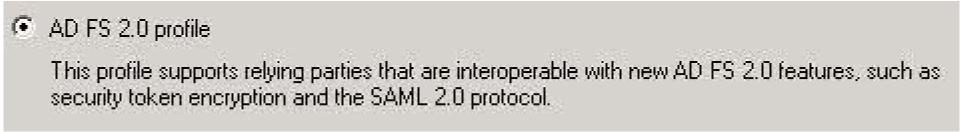


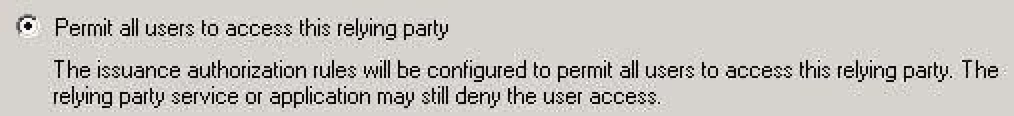
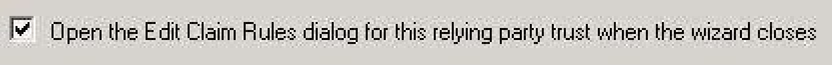
vice
Endpoints
Certificates
Claim Descriptions
ust Relationships

Name	Claim Type	Published ...	Publi...
email_address	email_address	No	No
first_name	first_name	No	No
last_name	last_name	No	No

Create Relying Party

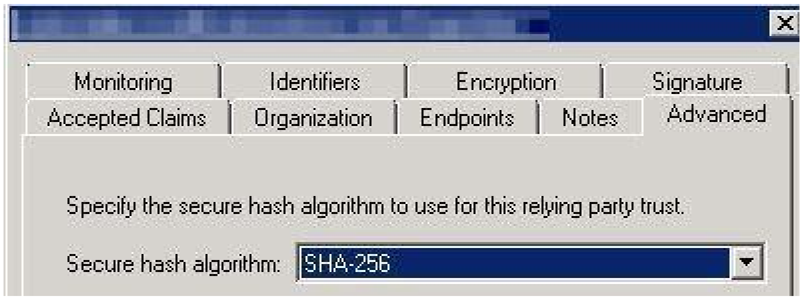
5. Open AD FS management console
6. Go to Trust Relationships -> Relying Party Trusts and click Add Relying Party Trust…

Step	Configuration
Welcome	Click Start
SelectData Source	Choose Enter data about the relying party manually  ● Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.
Specify DisplayName	Type your display name, for example:subdomain.assetsonar.com
Choose Profile	Choose AD FS 2.0 profile  ● AD FS 2.0 profile This profile supports relying parties that are interoperable with new AD FS 2.0 features, such as security token encryption and the SAML 2.0 protocol.
Configure Certificate	Skip this step. Click Next
ConfigureURL	Select "Enable support for the SAML 2.0 WebSSO protocol." "In the Relying party SAML 2.0 SSO service URL:" type "The AssetSonar consume service url" (you can get it from Add On page SAML Integration addon on AssetSonar Settings web-page) This URL will be used to POST responses with ADFS tokens (claims) to the AssetSonar It can be found in Federation request as <samlp:AuthnRequest AssertionConsumerServiceURL

Configure Identifiers	**In Relying party trust identifier specify https://ezo.io/assetsonar/** **If you are not sure about this identifier, then ask AssetSonar support. It can be found in Federation Request as <saml:Issuer>**
Choose Issuance Authorization Rules	**Select Permit all users to access this relying party**  ● 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. **Later you can configure what users should have access, if you need.**
Read to Add Trust	**Click Next**
Finish	**Left this option:**  ☑ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes **Click Close.**

Note: Default Secure hash algorithm after rule creation is SHA-256. It is supported by AssetSonar.

If you need to change this go to relying party Properties -> Advanced and change it:



[redacted]

Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-256

Configure Claim Rules for Relying Party

After the previous wizard has finished you will see new windows where you can edit claim rules.

To access this menu later:

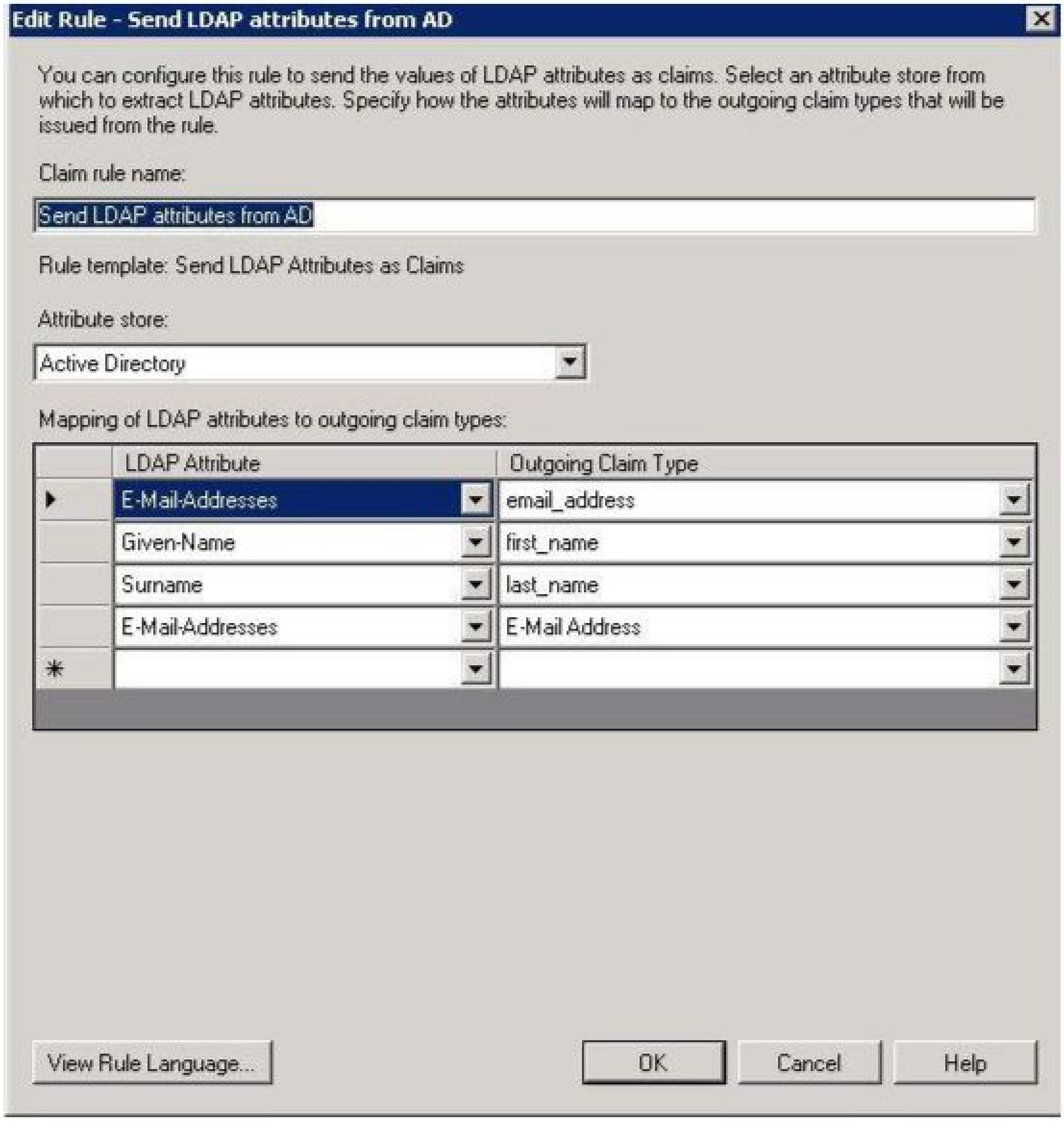
1. **Select required relying party trust.**
2. **Click Edit Claim Rules**

On the Issuance Transform Rules tab click Add Rule…

We will need 2 rules:

1st rule to get user attributes from AD

Step	**Configuration**
Choose RuleType	**Select "Send LDAP Attributes as Claims"**
Configure Claim Rule	**Define name you wish, for example: "Send LDAP attributes from AD"** **Select Active Directory as Attribute store** **Configure attributes mapping as below:**

Edit Rule - Send LDAP attributes from AD

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:

Send LDAP attributes from AD

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

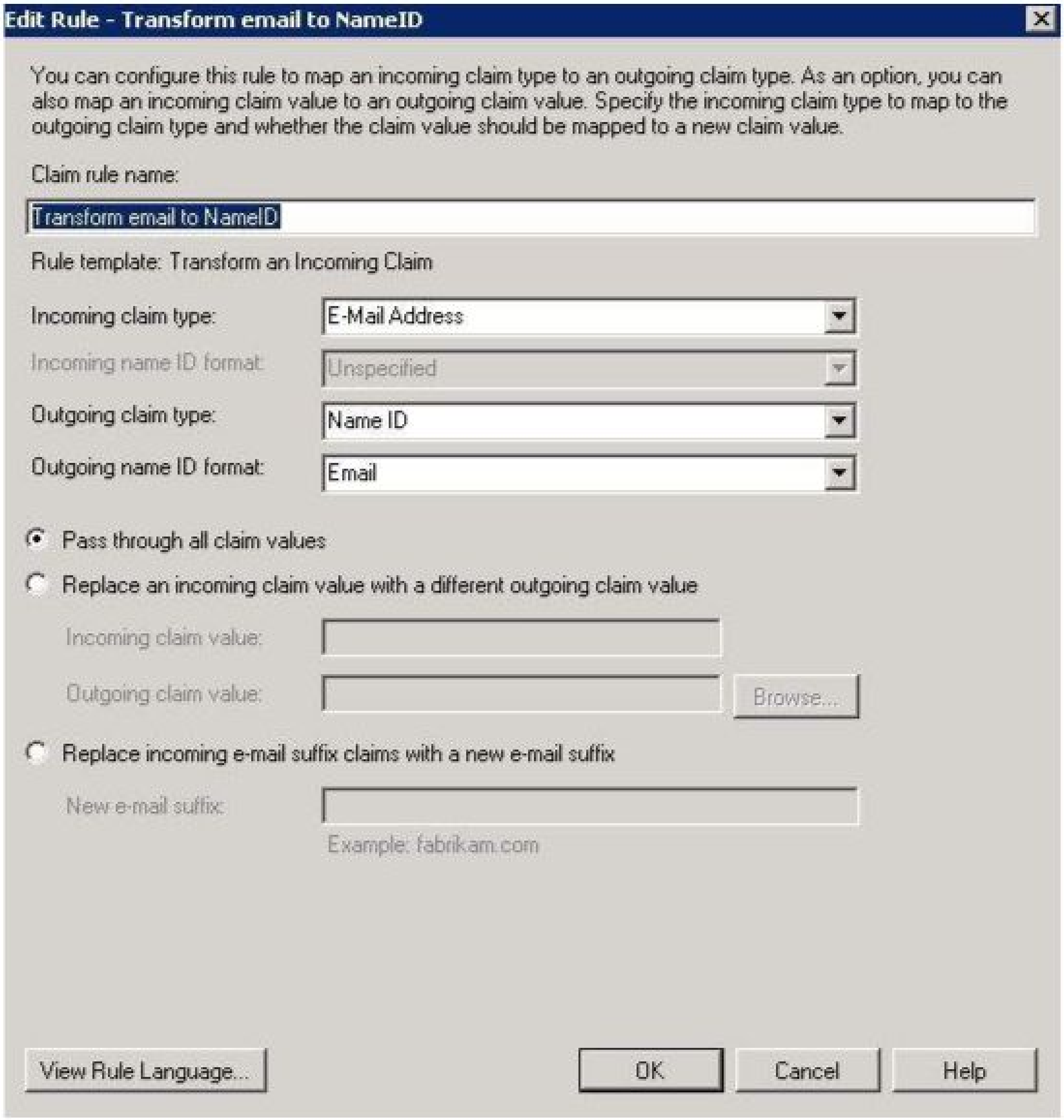
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
▶	E-Mail-Addresses	email_address
	Given-Name	first_name
	Surname	last_name
	E-Mail-Addresses	E-Mail Address
*		

2nd rule is to transform previously taken E-Mail-Address AD 4th attribute on screenshot above and transform it to Name ID "Email" format, required by AssetSonar:

<NameIDFormat="urn:oasis:names:tc:SAML:1.1:nameidformat:emailAddress">sohaib@assetsonar.com</NameID>

Step	Configuration
Choose RuleType	**Select "Transform an Incoming Claim"**
Configure Claim Rule	**Define name you wish, for example: "Transform email to NameID"** **Select Active Directory as Attribute store** **Configure attributes mapping as below:**



Edit Rule - Transform 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:

Transform 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:

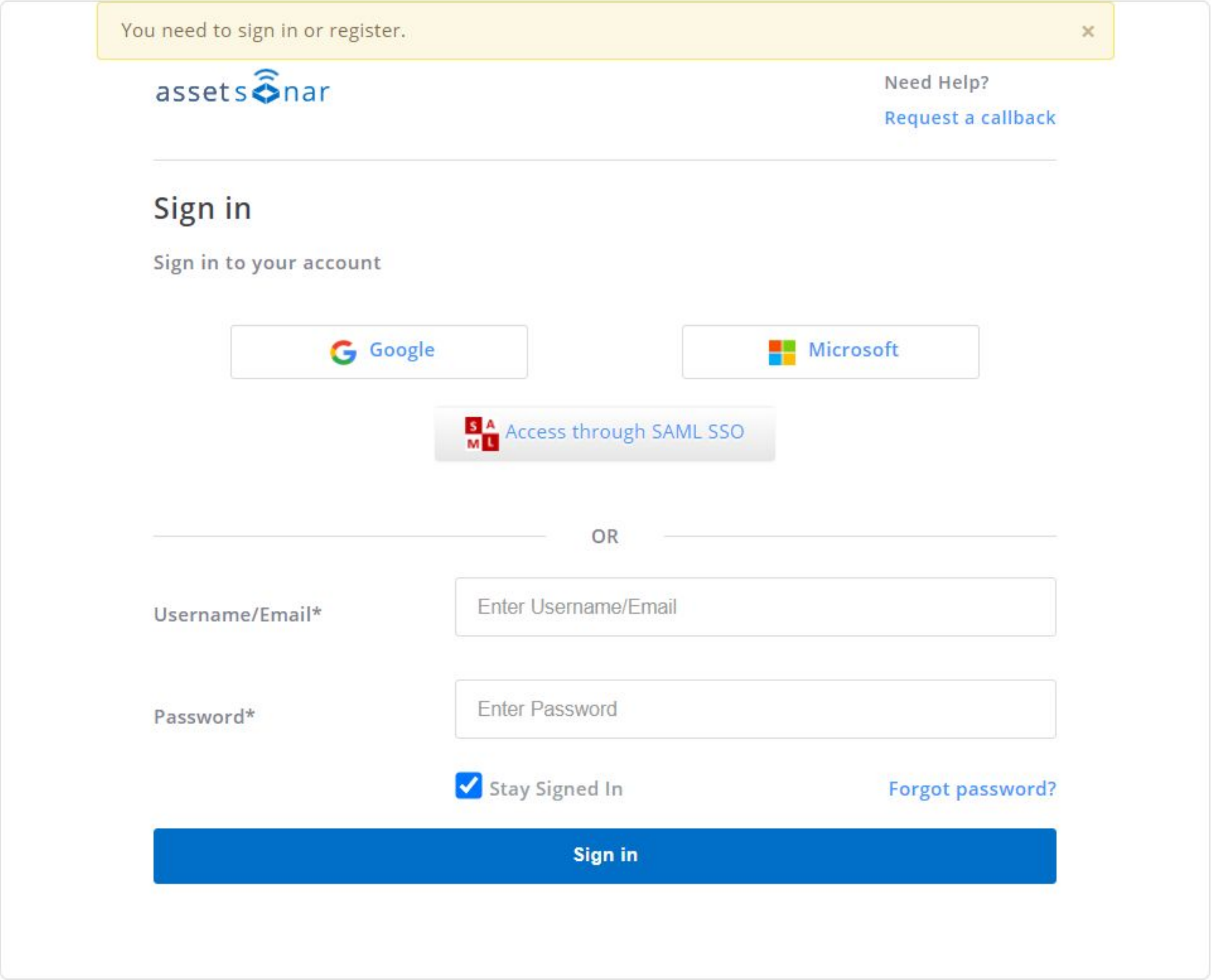
○ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

Verify how it works

1. **Go to AssetSonar Sign In pagehttps://{{subdomain}}.assetsonar.com/users/sign_in**
2. **Click Login with SAML button.**
   Alternatively you can use this direct link to skip this step
   https://{{subdomain}}.assetsonar.com/users/auth/saml



You need to sign in or register. ×

assetsonar

Need Help?

Request a callback

Sign in

Sign in to your account

Google

Microsoft

Access through SAML SSO

OR

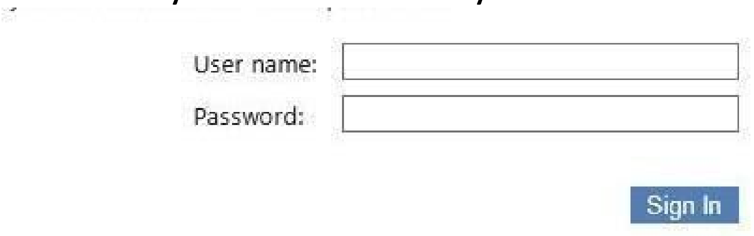
Username/Email* Enter Username/Email

Password* Enter Password

☑ Stay Signed In Forgot password?

Sign in

After this you will be redirected to your ADFS server which will perform authentication.



User name:

Password:

Sign In

3. Enter your ADFS account username and password
   4. If authentication was successful, then you will be redirected back to AssetSonar web-site and work with it.

Troubleshooting

For troubleshooting please contact support@ezo.io.