

EZOfficeInventory Microsoft ADFS SAML 2.0 configuration instruction

Contents

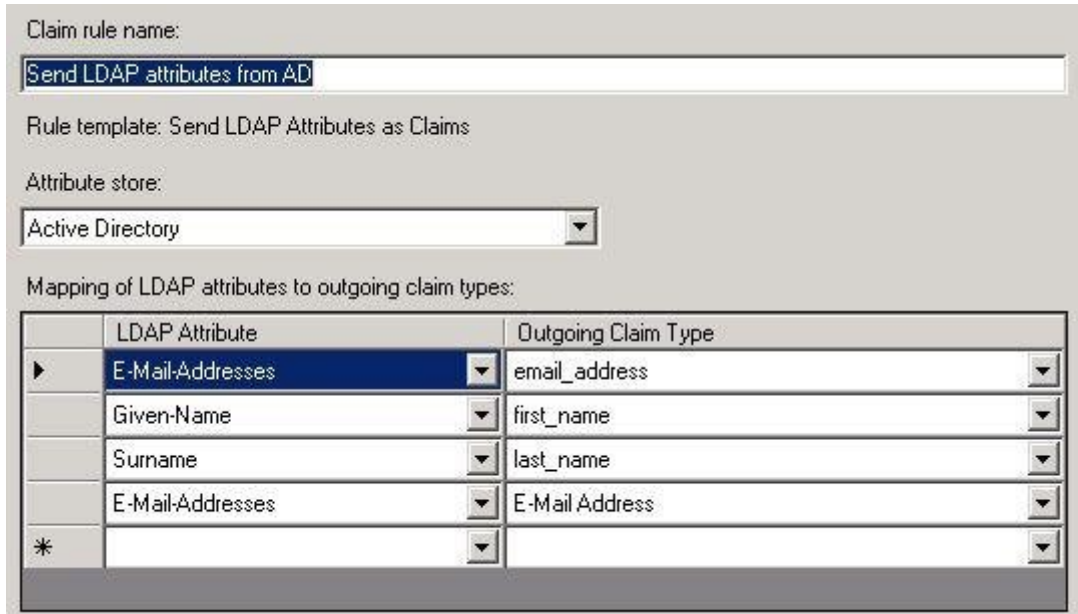
Configuration short summary:	2
Configure SAML settings on https://{{subdomain}}.ezofficeinventory.com	3
Prerequisites	3
SAML Add On configuration	4
Identity Provider URL:	4
Identity Provider Certificate	6
Login Button Text	6
First Name, Last Name and Email	7
Configure Microsoft AD FS 2.0	8
Create custom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

Configuration short summary:

EZOfficeinventory configuration:

identity provider url	Microsoft Active Federation Service URL
Identity Provider 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)

Microsoft AD FS 2.0 configuration

display name	{{subdomain}}.ezofficeinventory.com																		
relying party identifier	https://ezo.io/ezofficeinventory/																		
secure hash algorithm	SHA-256																		
POST endpoint	https://{{subdomain}}.ezofficeinventory.com/users/auth/saml/callback																		
Claim rules	<p>1.</p>  <table border="1"> <thead> <tr> <th></th> <th>LDAP Attribute</th> <th>Outgoing Claim Type</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>2.</p>		LDAP Attribute	Outgoing Claim Type	▶	E-Mail-Addresses	email_address		Given-Name	first_name		Surname	last_name		E-Mail-Addresses	E-Mail Address	*		
	LDAP Attribute	Outgoing Claim Type																	
▶	E-Mail-Addresses	email_address																	
	Given-Name	first_name																	
	Surname	last_name																	
	E-Mail-Addresses	E-Mail Address																	
*																			

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

Configure SAML settings on <https://{{subdomain}}.ezofficeinventory.com>

Prerequisites

You must be Company Owner can configure SAML Add On

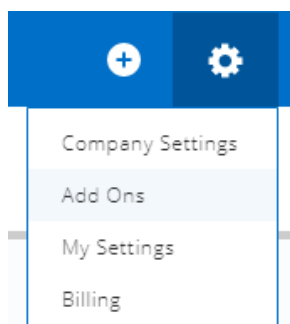
To set Company Owner:

1. Login to <https://{{subdomain}}.ezofficeinventory.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 new owner should change back this option to your profile.

SAML Add On configuration

1. Login to <https://{{subdomain}}.ezofficeinventory.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>

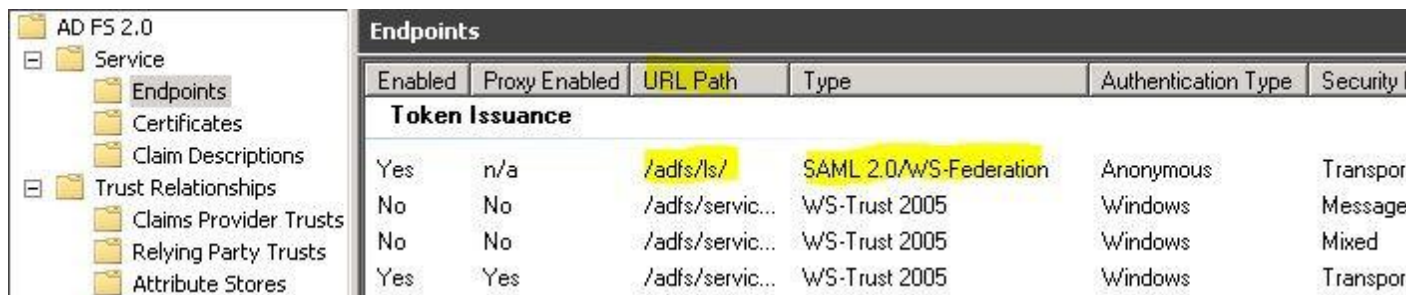
Set to your ADFS URL

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"



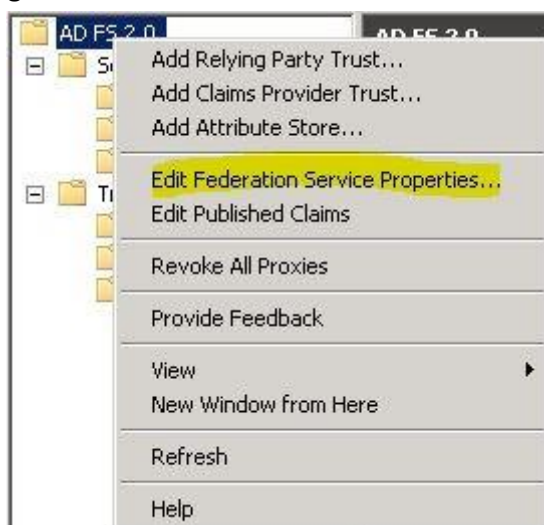
The screenshot shows the AD FS 2.0 management console. On the left, the tree view is expanded to 'Service' > 'Endpoints'. On the right, the 'Endpoints' table is displayed. The table has columns: Enabled, Proxy Enabled, URL Path, Type, Authentication Type, and Security. The first row, under the 'Token Issuance' section, is highlighted in yellow and shows a 'SAML 2.0/WS-Federation' endpoint with the URL path '/adfs/ls/'.

Enabled	Proxy Enabled	URL Path	Type	Authentication Type	Security
Yes	n/a	/adfs/ls/	SAML 2.0/WS-Federation	Anonymous	Transport
No	No	/adfs/service/...	WS-Trust 2005	Windows	Message
No	No	/adfs/service/...	WS-Trust 2005	Windows	Mixed
Yes	Yes	/adfs/service/...	WS-Trust 2005	Windows	Transport

In the URL you can find the path relative to your ADFS root path

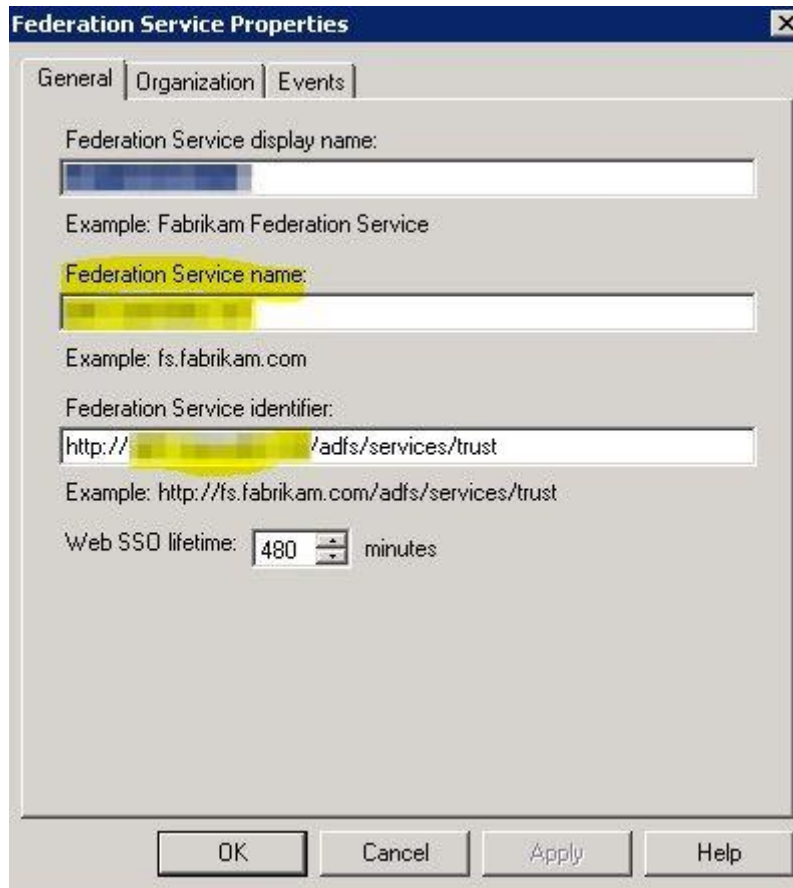
In order to get first part of URL

1. Right click on AD FS 2.0 and select "Edit Federation Service Properties..."



The screenshot shows the AD FS 2.0 management console with a context menu open over the 'AD FS 2.0' folder. The menu items are: Add Relying Party Trust..., Add Claims Provider Trust..., Add Attribute Store..., Edit Federation Service Properties... (highlighted in yellow), Edit Published Claims, Revoke All Proxies, Provide Feedback, View, New Window from Here, Refresh, and Help.

2. Find "Federation Service identifier" in General tab:



This will be link 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:



You need to get 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](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:

EZOffice SAML DEMO

Sign in







OR

Login ID *

Password *

Sign in

Stay Signed In

| [Forgot your password?](#) | [Privacy Policy](#)

Powered By : EZOfficeInventory

First Name, Last Name and Email

Description: In EZOfficeInventory 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:	<input type="text" value="first_name"/>
Last Name:	<input type="text" value="last_name"/>
Email:	<input type="text" value="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 every SAML

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

Note: I did not manage to make it work with AD FS default claims: givenname, surname, emailaddress, 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

OK Cancel Help

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 to work.

Result should look like this:

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

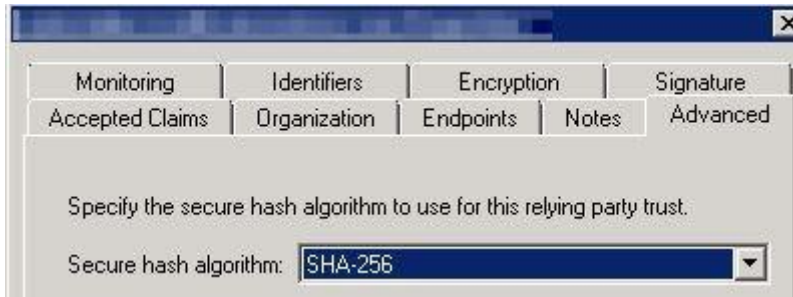
5. Open AD FS management console

6. Go to Trust Relationships -> Relying Party Trusts and click Add Relying Party Trust...

Step	Configuration
Welcome	Click Start
Select Data Source	<p>Choose Enter data about the relying party manually</p> <p><input checked="" type="radio"/> Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.</p>
Specify Display Name	Type your display name, for example: subdomain.ezofficeinventory.com
Chose Profile	<p>Choose AD FS 2.0 profile</p> <p><input checked="" type="radio"/> 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.</p>
Configure Certificate	Skip this step. Click Next
Configure URL	<p>Select "Enable support for the SAML 2.0 WebSSO protocol." "In the Relying party SAML 2.0 SSO service URL:" type "The EZOfficeInventory consume service url" (you can get it from Add On page SAML Integration addon on EZOfficeInventory Settings web-page)</p> <p>This URL will be used to POST responses with ADFS tokens (claims) to the EZOfficeInventory It can be found in Federation request as <samlp:AuthnRequest AssertionConsumerServiceURL</p>
Configure Identifiers	In Relying party trust identifier specify https://ezo.io/ezofficeinventory/ If you are not sure about this identifier, then ask EZOfficeInventory support. It can be found in Federation Request as <saml:Issuer>
Choose Issuance Authorization Rules	<p>Select Permit all users to access this relying party</p> <p><input checked="" type="radio"/> 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.</p> <p>Later you can configure what users should have access, if you need.</p>
Read to Add Trust	Click Next
Finish	<p>Left this option:</p> <p><input checked="" type="checkbox"/> Open the Edit Claim Rules dialog for this relying party trust when the wizard closes</p> <p>Click Close</p>

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

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



Configure Claim Rules for Relying Party

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

To access this menu later:

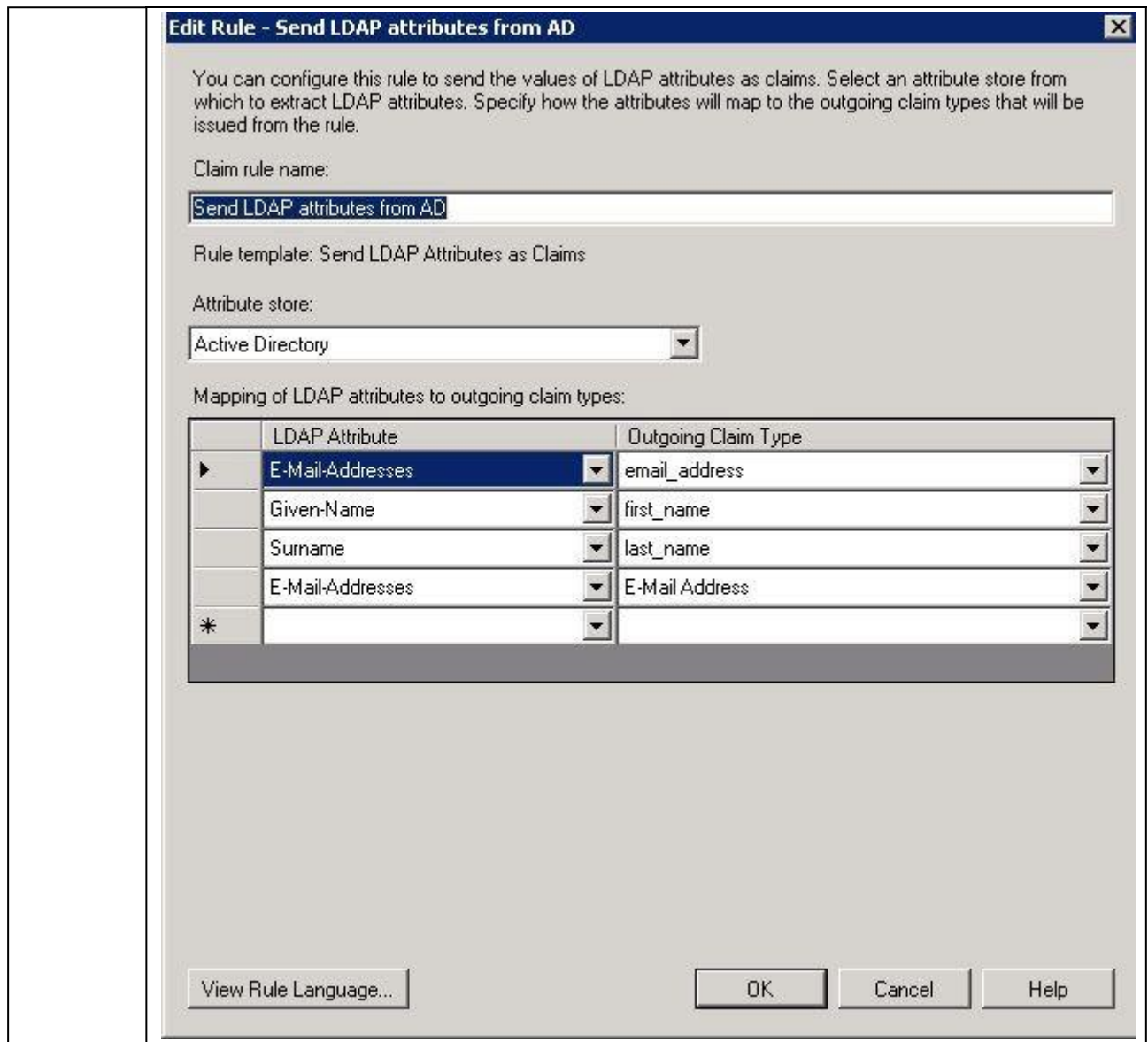
1. Select required relying party trust.
2. Click Edit Claim Rules

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 Rule Type	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:



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 EZOfficeInventory:

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

Step	Configuration
Choose Rule Type	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:

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

Verify how it works

1. Go to EZOfficeInventory Sign In page https://{{subdomain}}.ezofficeinventory.com/users/sign_in
2. Click Login with SAML button
Alternatively you can use this direct link to skip this step
<https://{{subdomain}}.ezofficeinventory.com/users/auth/saml>

EZOffice SAML DEMO

Sign in

OR

Login ID *

Password *

Sign in

Stay Signed In

[| Forgot your password?](#) | [Privacy Policy](#)

Powered By : EZOfficeInventory

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

User name:

Password:

Sign In

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

Troubleshooting

For troubleshooting please contact support@ezo.io.