Configuring Zoom SSO With ADFS

(N.Witheridge, 12th March 2015)

Overview

The high-level steps involved in configuring Zoom for SSO with ADFS are:

1. Obtain your institutional ADFS SAML metadata (.xml)

2. Using your Zoom admin account, access the Zoom SSO configuration page and enable SSO
3. Open the “SAML” tab and enter your institutional SAML metadata (obtained from your ADFS SAML metadata file .xml)

4. Access your institutional ADFS configuration interface
5. Configure the source of SAML relying-party metadata
6. Configure the relying-party display name as “Zoom”
7. Configure relying-party Assertion Consumer and Logout end-points
8. Add claim rules:
    a. Map and send attributes for E-Mail-Addresses, User-Principal-Name, Given-Name and Surname.
    b. Configure E-Mail Address as the Name ID outgoing claim type

9. Test SSO to Zoom

Detailed Steps

1) Find and download/view your ADFS XML metadata at

https://[SERVER]/FederationMetadata/2007-06/FederationMetadata.xml

*[SERVER] is the domain name of your ADFS server (adfs.example.com)

```
https://adfs.uws.edu.au/FederationMetadata/2007-06/FederationMetadata.xml
```

Comment: *UWS ADFS folk, what’s your server name? Could you interpret this URL and map it to what you have, and send me the metadata please*

2) From the Zoom Admin page, click on Single Sign-on to View the SAML tab.

Information entered below under the SAML tab is your IdP SAML metadata for the Zoom SP.

3) Enter the following information into the SAML tab options:

Sign-in page URL:
`https://[SERVER]/adfs/ls/idpinitiatedsignon.aspx?logintoRP=[Vanity].zoom.us`

Sign-out page URL: `https://[SERVER]/adfs/ls/?wa=wsignout1.0`

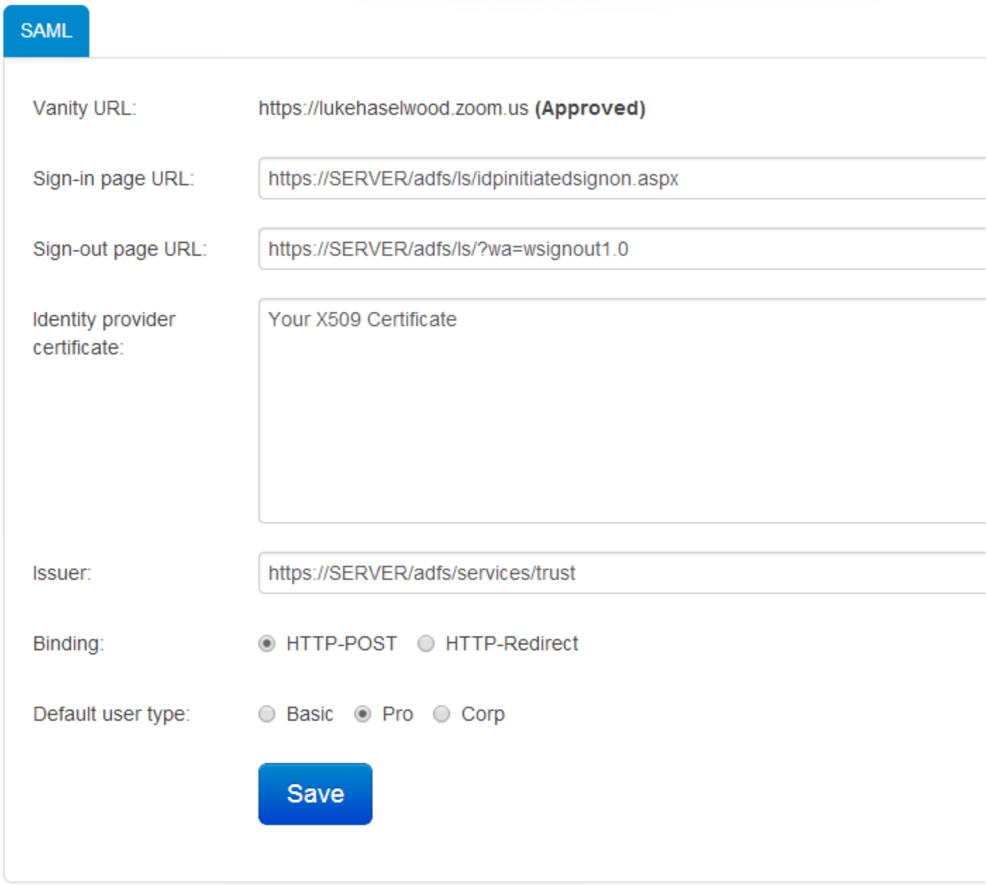
Identity provider certificate: Note, use the “Signing” certificate.
X509 Certificate from XML Metadata in step 1
*Use the first X509 Certificate in the XML file:

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <KeyInfo zmlns="http://www.w3.org/2000/09/xmldsig#">
       <X509Data>
           <X509Certificate>
```

Issuer: `http` or `https://[SERVER]/adfs/services/trust` (entityID in metadata)

Binding: `HTTP-POST`

Default user type: As per your plan



Vanity URL:	https://lukehaselwood.zoom.us **(Approved)**
Sign-in page URL:	https://SERVER/adfs/ls/idpinitiatedsignon.aspx
Sign-out page URL:	https://SERVER/adfs/ls/?wa=wsignout1.0
Identity provider certificate:	Your X509 Certificate
Issuer:	https://SERVER/adfs/services/trust
Binding:	● HTTP-POST ○ HTTP-Redirect
Default user type:	○ Basic ● Pro ○ Corp

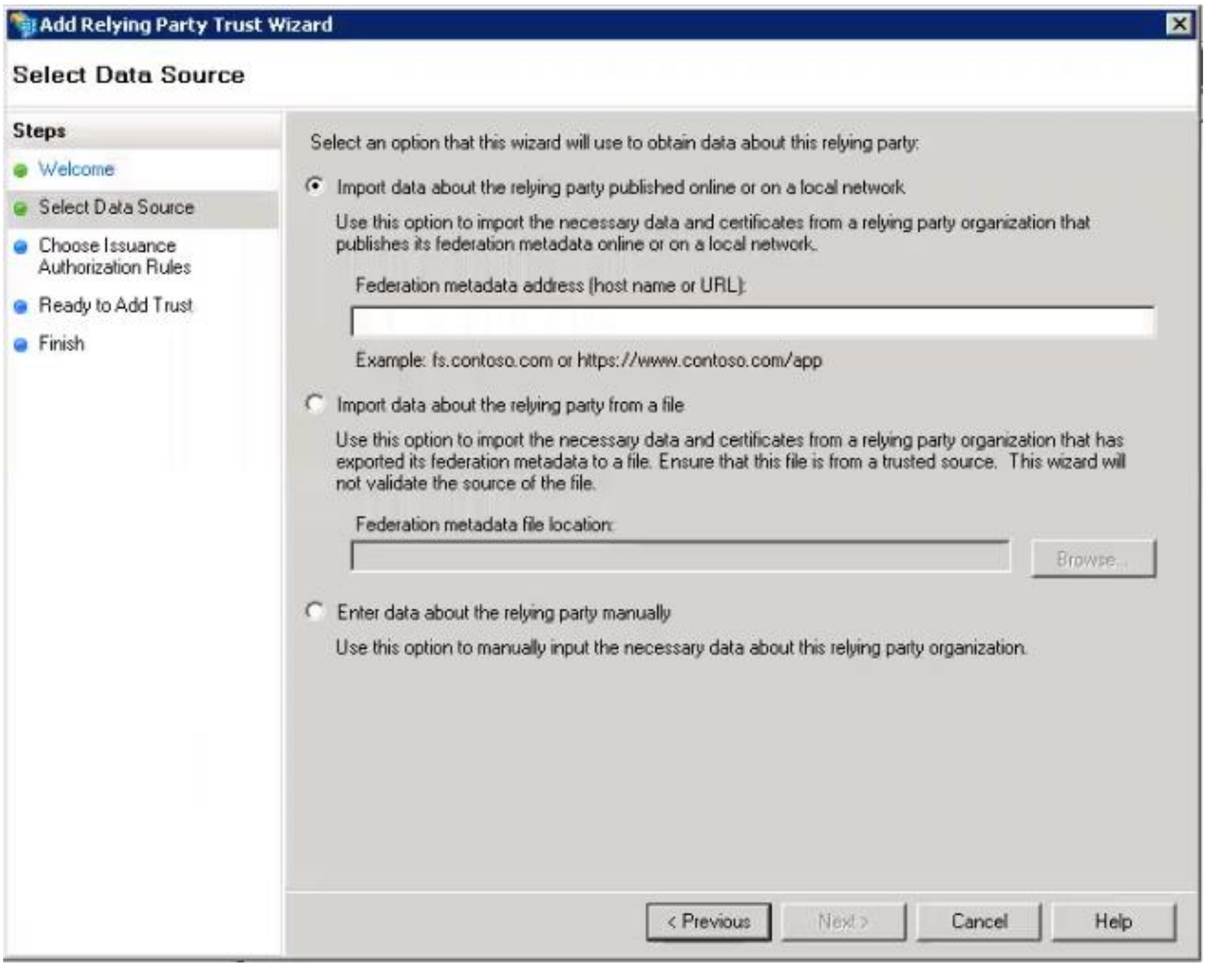
4) Login to your ADFS server, open ADFS 2.0 MMC

Open the administrative interface of ADFS

5) Add a Relying Party Trust

Select Import data about the relying party published online or on a local network

Federation metadata address: https://YOURVANITY.zoom.us/saml/metadata/sp



Add Relying Party Trust Wizard

Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

● Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

○ Enter data about the relying party manually

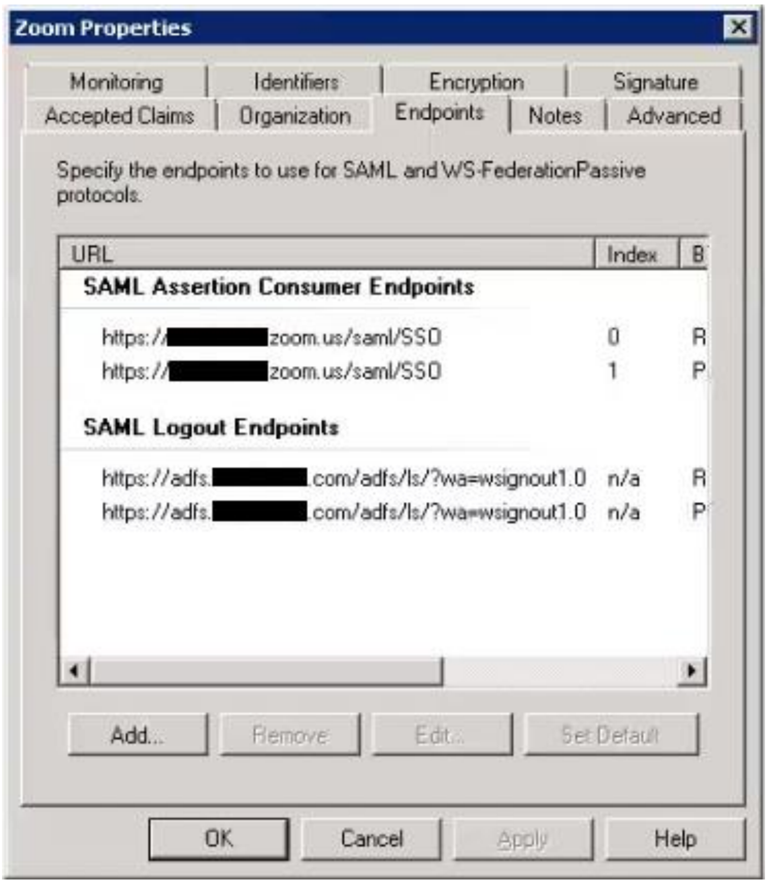
Use this option to manually input the necessary data about this relying party organization.

6) Add a display name ("Zoom") and finish the Wizard with default settings

Question: What step is adding a display name under?

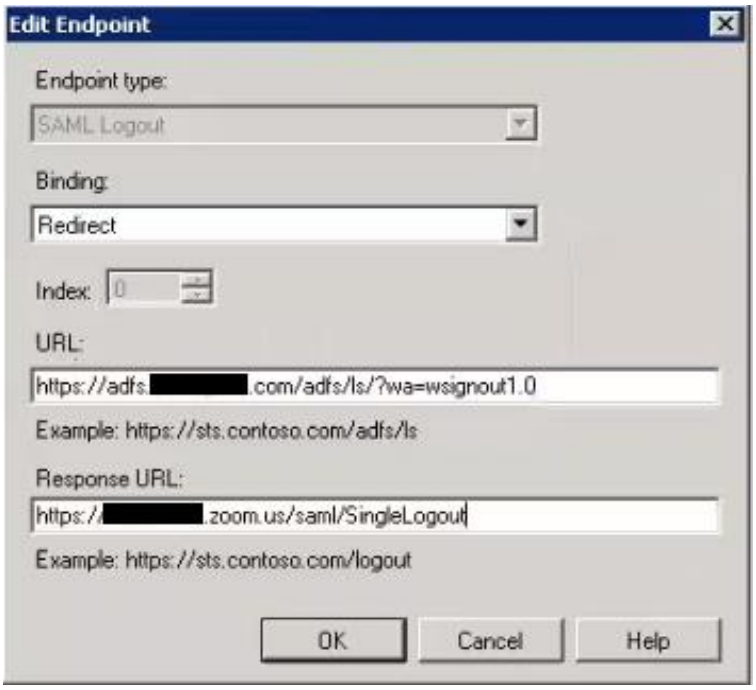
7) Change both Redirect and Post SAML Logout Endpoint URLs to:
(Right click the new Relying Party Trust > Properties > Endpoints Tab)

https://SERVER/adfs/ls/?wa=wsignout1.0



Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	B
SAML Assertion Consumer Endpoints		
https://[redacted]zoom.us/saml/SSO	0	R
https://[redacted]zoom.us/saml/SSO	1	P
SAML Logout Endpoints		
https://adfs.[redacted].com/adfs/ls/?wa=wsignout1.0	n/a	R
https://adfs.[redacted].com/adfs/ls/?wa=wsignout1.0	n/a	P



Endpoint type: SAML Logout

Binding: Redirect

Index: 0

URL: https://adfs.[redacted].com/adfs/ls/?wa=wsignout1.0

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

Response URL: https://[redacted].zoom.us/saml/SingleLogout

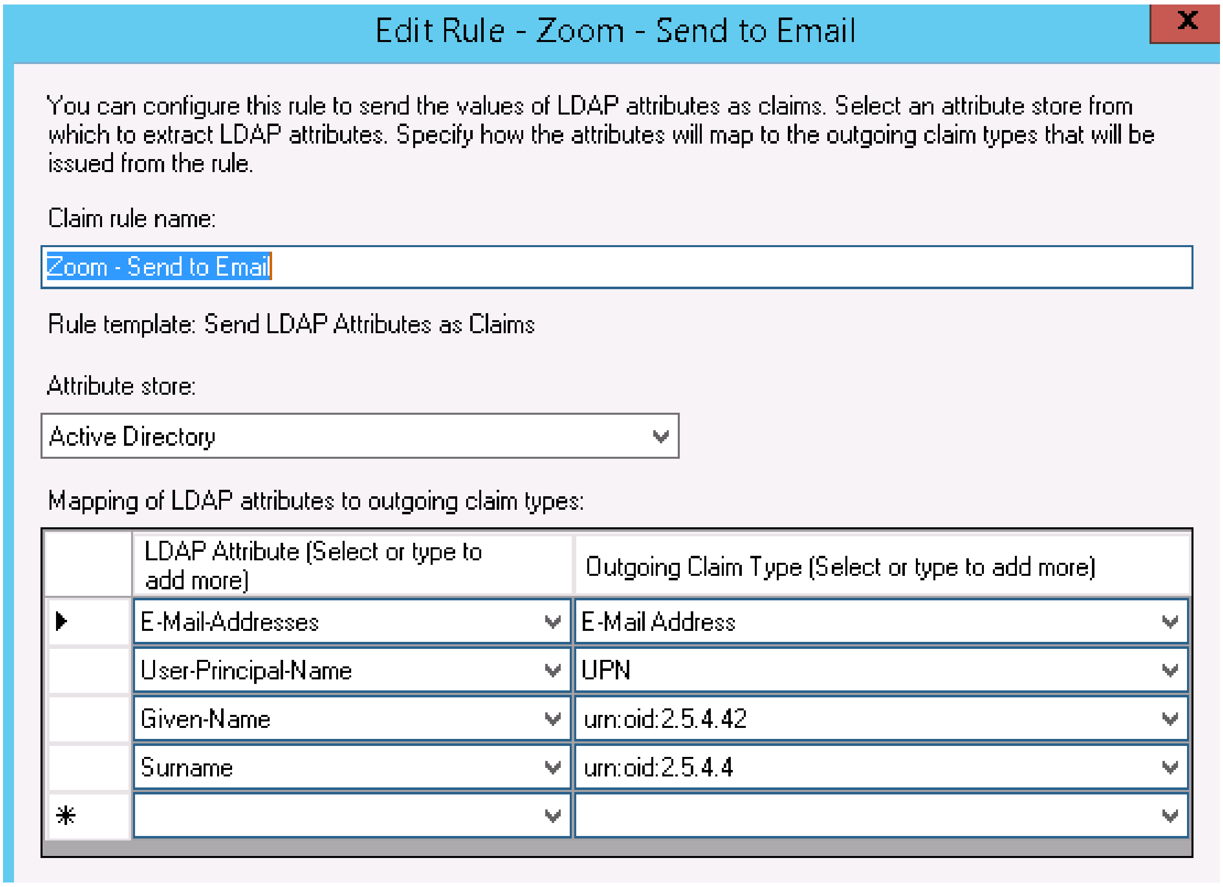
Example: https://sts.contoso.com/logout

*Note:
If you are unable to change the logout endpoints, open the Monitor tab and *uncheck* "Automatically update relying party" and Apply changes.

8) Add two claim rules

a) First claim rule

Type:	Send LDAP Attributes as Claims
Name:	Zoom - Send to Email
Mappings:	E-Mail-Addresses > E-Mail Adresss
	User-Principal-Name > UPN
	Given-Name > urn:oid:2.5.4.42
	Surname > urn:oid:2.5.4.4



Edit Rule - Zoom - Send to Email

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:

Zoom - Send to Email

Rule template: Send LDAP Attributes as Claims

Attribute store:

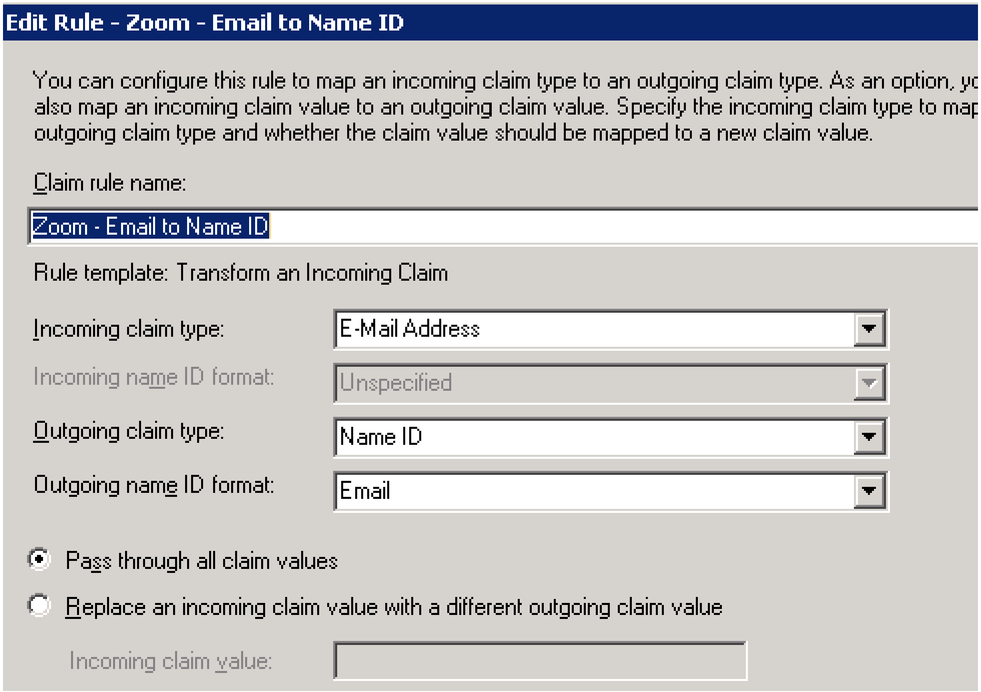
Active Directory

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
	User-Principal-Name	UPN
	Given-Name	urn:oid:2.5.4.42
	Surname	urn:oid:2.5.4.4
*		

b) Second Claim Rule

Type:	Transform Incoming Claim
Name:	Zoom - Email to Name ID
Incoming claim type:	E-Mail Address
Outgoing claim type:	Name ID
Outgoing name ID format:	Email



Edit Rule - Zoom - Email to Name ID

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, yc
also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map
outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Zoom - Email to Name ID

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:

9) Test SSO by visiting http://YOURVANITY.zoom.us and selecting Login.

You should see your institutional login screen.

Troubleshooting Tips

Issue 1. Unable to log in using Google Chrome or Firefox

If you are unable to log in using Chrome or Firefox, and are seeing an 'Audit Failure' event with "Status: 0xc000035b" in the Event Viewer on the ADFS server, you will need to turn off Extended Protection. Chrome and Firefox do not support the Extended Protection of ADFS (IE does).

1. Launch IIS Manager
2. In the left panel, navigate to Sites > Default Web Site > ADFS > LS
3. Double-click Authentication icon
4. Right-click Windows Authentication
5. Select Advanced Settings
6. Turn OFF Extended Protection.