Joget SharePoint SSO Integration

Introduction

Recently, there have been questions from customers, partners and the community asking for comparisons between Joget Workflow and Microsoft SharePoint. Actually, the two products are not competing, but in fact complement each other.

SharePoint is a web application portal platform for team collaboration, intranets and enterprise document and content management. While it is possible to extend the capabilities of SharePoint through apps, developing apps for SharePoint is not easy as it requires traditional programming, as described in the SharePoint 2013 development overview article at https://msdn.microsoft.com/en-us/library/office/jj164084.aspx.

On the other hand, Joget is a platform to easily build web apps and automate processes. With single sign-on (SSO) integration from SharePoint to Joget, organizations can easily extend the capability of SharePoint by allowing users to seamlessly access custom apps, visually design their own custom applications, or download ready made apps from the Joget Marketplace.

This article describes how SSO can be achieved using Active Directory Federation Services (https://msdn.microsoft.com/en-us/library/bb897402.aspx), which supports the Security Assertion Markup Language (SAML) standard.

Configuring Joget SharePoint SSO

i. Pre-requisites

Before configuring the SharePoint-Joget SSO integration, you will need to have installed and configured:

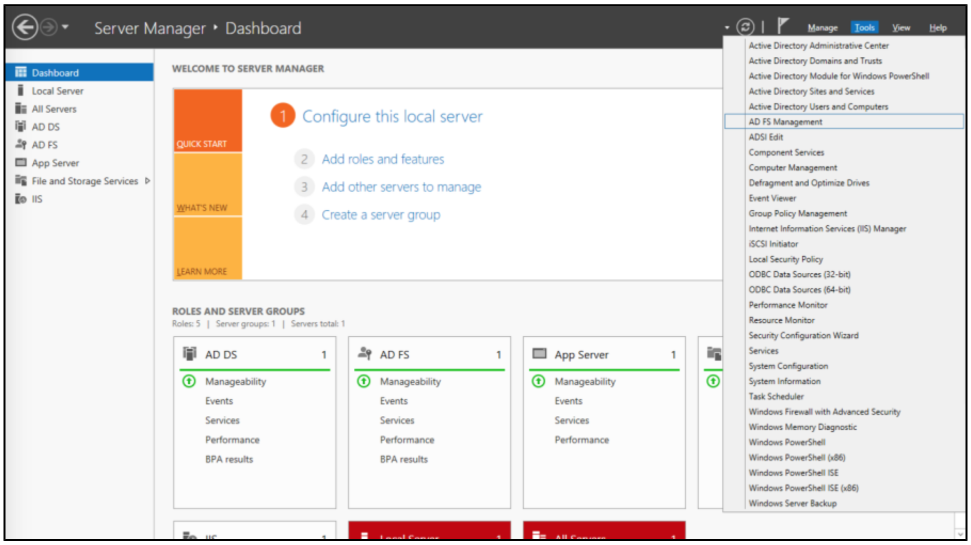
- SharePoint integrated with Active Directory Federation Services
- Joget

The appendices provide some resources on installing and configuring these pre-requisites.

ii. Configure SAML for Joget

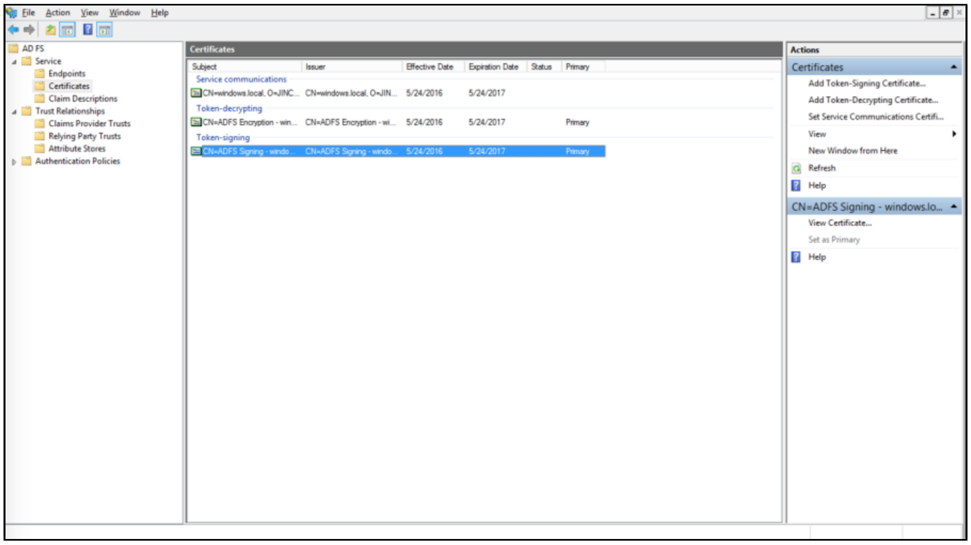
Export AD FS Token Signing Certificate

1. In the Windows Server Manager, launch **Tools** > **AD FD Management**



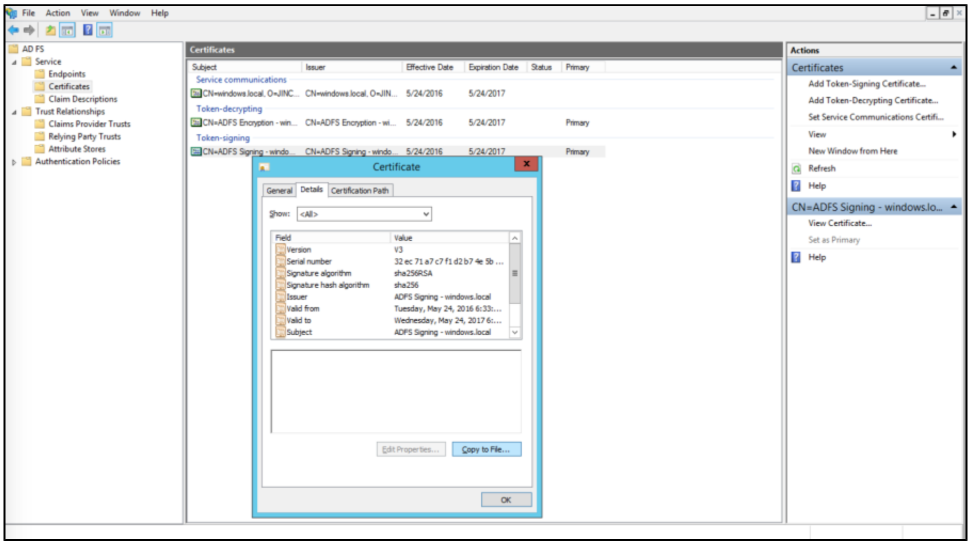
2. In the AD FS Management console, select **Service** > **Certificates** in the left navigation pane.

3. Select the Token-signing certificate and click on the **View Certificate** link on the right pane.



Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
CN=windows.local, O=JINC...	CN=windows.local, O=JIN...	5/24/2016	5/24/2017		
Token-decrypting					
CN=ADFS Encryption - win...	CN=ADFS Encryption - wi...	5/24/2016	5/24/2017		Primary
Token-signing					
CN=ADFS Signing - windo...	CN=ADFS Signing - windo...	5/24/2016	5/24/2017		Primary

4. Click on the **Details** tab, and click on the **Copy to File...** button



Certificates

Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
CN=windows.local, O=JINC...	CN=windows.local, O=JIN...	5/24/2016	5/24/2017		
Token-decrypting					
CN=ADFS Encryption - win...	CN=ADFS Encryption - wi...	5/24/2016	5/24/2017		Primary
Token-signing					
CN=ADFS Signing - windo...	CN=ADFS Signing - windo...	5/24/2016	5/24/2017		Primary

Show: <All>

Field	Value
Version	V3
Serial number	32 ec 71 a7 c7 f1 d2 b7 4e 5b ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ADFS Signing - windows.local
Valid from	Tuesday, May 24, 2016 6:33:...
Valid to	Wednesday, May 24, 2017 6:...
Subject	ADFS Signing - windows.local

5. This starts the Certificate Export Wizard. On the Welcome to the Certificate Export Wizard page, click **Next**.

6. On the Export Private Key page, click **No**, do not export the private key, and then click **Next**.

7. On the Export File Format page, select **Base-64 encoded X.509 (.CER)**, and then click **Next**.

8. On the File to Export page, type the name and location of the file that you want to export, and then click **Next**. For example, enter C:\ADFS.cer.

9. On the Completing the Certificate Export Wizard page, click **Finish**.

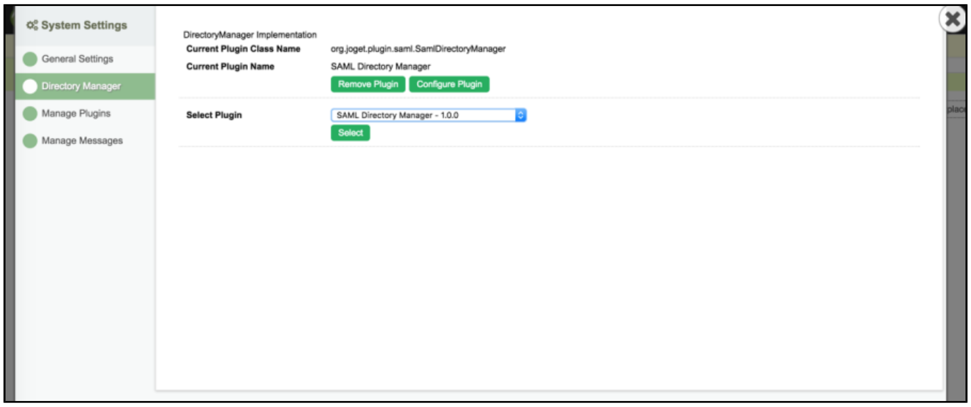
Configure SAML Directory Manager for Joget

1. Download the SAML Directory Manager from the Joget Marketplace

2. In Joget, login as an administrator

3. In **Settings** > **Manage Plugins**, click on **Upload Plugin**. Select the downloaded JAR file and click on the **Upload** button to upload the downloaded JAR file

4. In **Settings** > **Directory Manager**, choose the SAML Directory Manager and click on **Select**.

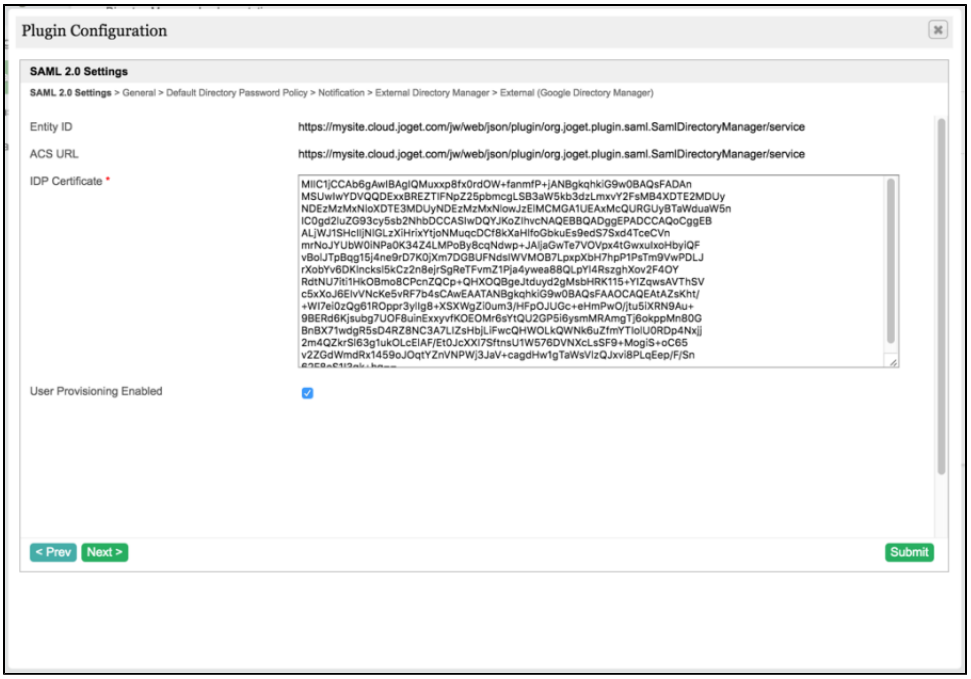


DirectoryManager Implementation

Current Plugin Class Name	org.joget.plugin.saml.SamlDirectoryManager
Current Plugin Name	SAML Directory Manager
Select Plugin	SAML Directory Manager - 1.0.0

5. Open the contents of the exported AD FS certificate in a text editor and copy the contents.

6. In the Plugin Configuration page, paste the contents into the IDP Certificate field (copy-paste without the BEGIN and END lines)



Plugin Configuration

SAML 2.0 Settings

SAML 2.0 Settings > General > Default Directory Password Policy > Notification > External Directory Manager > External (Google Directory Manager)

Entity ID: https://mysite.cloud.joget.com/jw/web/json/plugin/org.joget.plugin.saml.SamlDirectoryManager/service

ACS URL: https://mysite.cloud.joget.com/jw/web/json/plugin/org.joget.plugin.saml.SamlDirectoryManager/service

IDP Certificate *

```
MIIC1jCCAb6gAwIBAgIQMuxxp8fx0rdOW+fanmfP+jANBgkqhkiG9w0BAQsFADAn
MSUwIwYDVQQDExxBREZTIFNpZ25pbmcgLSB3aW5kb3dzLmxvY2FsMB4XDTE2MDUy
NDEzMzMxNloXDTE3MDUyNDEzMzMxNlowJzElMCMGA1UEAxMcQURGUyBTaWduaW5n
IC0gd2luZG93cy5sb2NhbDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ALjWJ1SHcIljNIGLzXiHrixYtjoNMuqcDCf8kXaHlfoGbkuEs9edS7Sxd4TceCVn
mrNoJYUbW0iNPa0K34Z4LMPoBy8cqNdwp+JAljaGwTe7VOVpx4tGwxulxoHbyIQF
vBolJTpBqg15j4ne9rD7K0jXm7DGBUFNdslWVMOB7LpxpXbH7hpP1PsTm9VwPDLJ
rXobYv6DKlncksI5kCz2n8ejrSgReTFvmZ1Pja4ywea88QLpYI4RszghXov2F4OY
RdtNU7iti1HkOBmo8CPcnZQCp+QHXOQBgeJtduyd2gMsbHRK115+YIZqwsAVThSV
c5xXoJ6ElvVNcKe5vRF7b4sCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAtAZsKht/
+WI7ei0zQg61ROppr3yllg8+XSXWgZi0um3/HFpOJUGc+eHmPwO/jtu5iXRN9Au+
9BERd6Kjsubg7UOF8uinExxyvfKOEOMr6sYtQU2GP5i6ysmMRAmgTj6okppMn80G
BnBX71wdgR5sD4RZ8NC3A7LIZsHbjLiFwcQHWOLkQWNk6uZfmYTIolU0RDp4Nxjj
2m4QZkrSl63g1ukOLcElAF/Et0JcXXI7SftnsU1W576DVNXcLsSF9+MogiS+oC65
v2ZGdWmdRx1459oJOqtYZnVNPWj3JaV+cagdHw1gTaWsVlzQJxvi8PLqEep/F/Sn
```

User Provisioning Enabled ☑

7. Copy the value of the **ACS URL** (to be used in AD FS configuration later).

8. With User Provisioning Enabled checked, a user will be created on first login if the username does not already exist. To integrate with Active Directory directly to retrieve users and groups, configure the External Directory Manager to LDAP Directory Manager https://dev.joget.org/community/display/KBv5/LDAP+Directory+Manager

9. Click on **Submit** to save the settings.

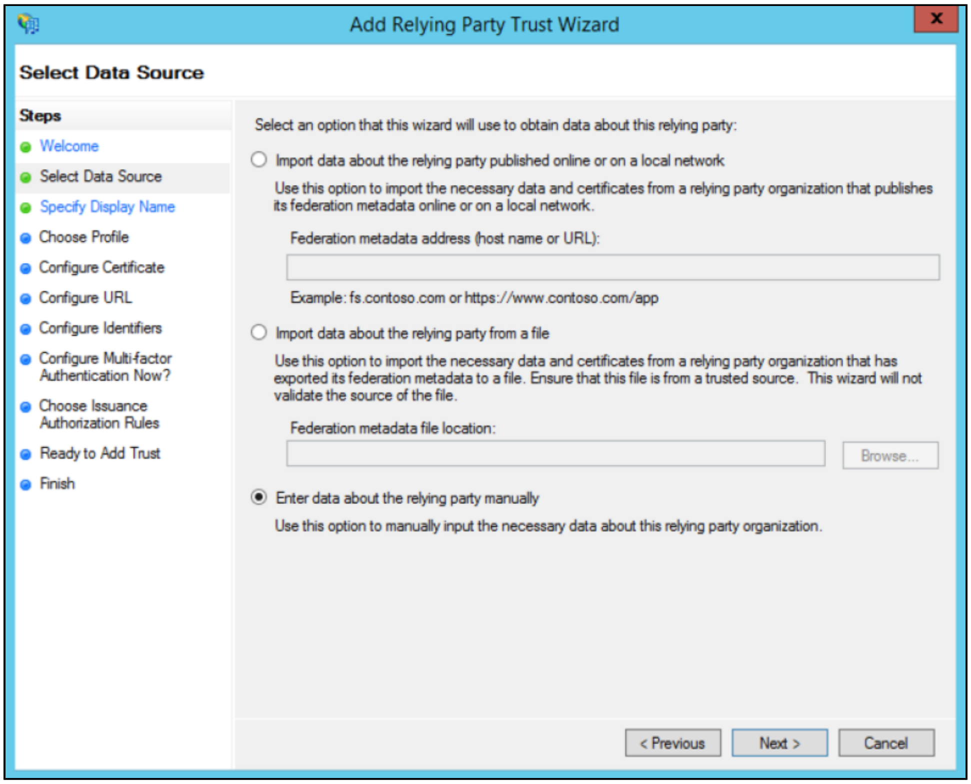
iii. Configure Relying Party Trust between AD FS and Joget

Add Relying Party Trust

1. In the Windows Server Manager, launch **Tools** > **AD FD Management**

2. In the AD FS Management console, click on **Trust Relationships** > **Relying Party Trusts** in the left navigation pane.

3. In the right page, click on **Add Relying Party Trust**.



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:

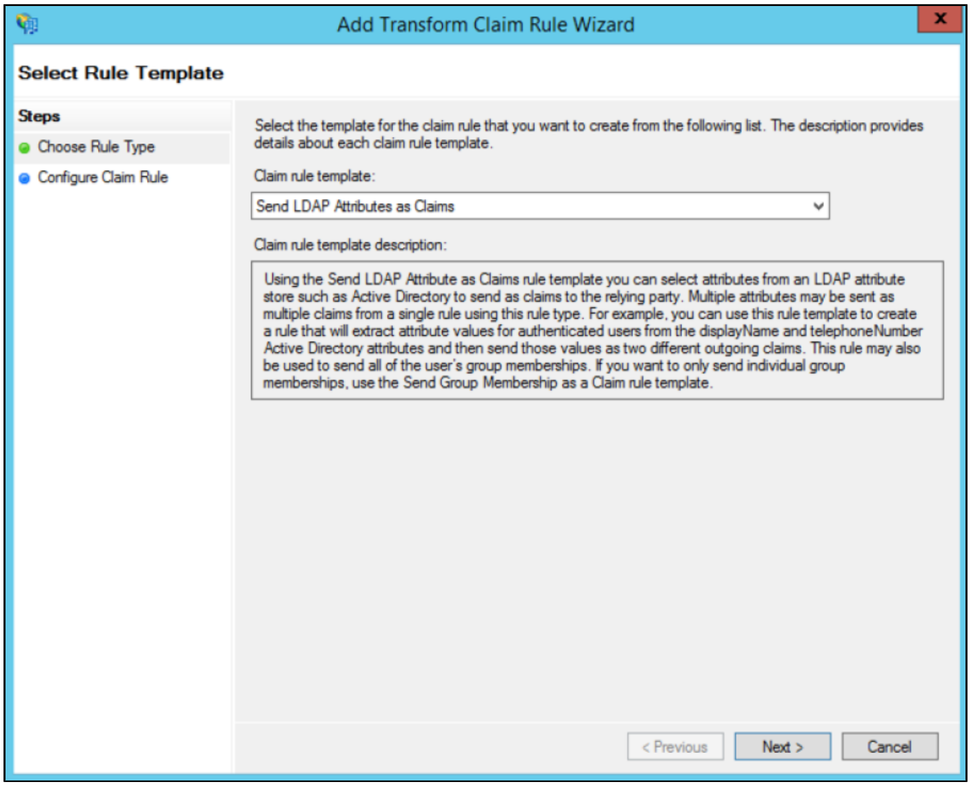
● Enter data about the relying party manually

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

4. On the Welcome to the Add Relying Party Trust Wizard page, click **Start**.
5. Select Enter data about the relying party manually, and then click **Next**.
6. Type a relying party name (e.g. Joget) and then click **Next**.
7. Make sure Active Directory Federation Services (AD FS) 2.0 Profile is selected, and then click **Next**.
8. Do not use an encryption certificate. Click **Next**.
9. Click to select the **Enable support for the SAML 2.0 WebSSO** protocol check box.
10. In the Relying party SAML 2.0 SSO service URL field, type the URL copied from the Joget SAML Directory Manager earlier, e.g. https://mysite.cloud.joget.com/jw/web/json/plugin/org.joget.plugin.saml.SamlDirectoryManager/service
11. Paste the URL into the relying party trust identifier, and then click **Add**. Click **Next**.
12. Select Permit all users to access this relying party. Click **Next**.
13. On the Ready to Add Trust page, there is no action required, click **Next**.
14. On the Finish page, click **Close**. This opens the Rules Editor Management console.

Edit Claim Rules

1. On the Issuance Transform Rules tab, click **Add Rule**.


Add Transform Claim Rule Wizard

Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

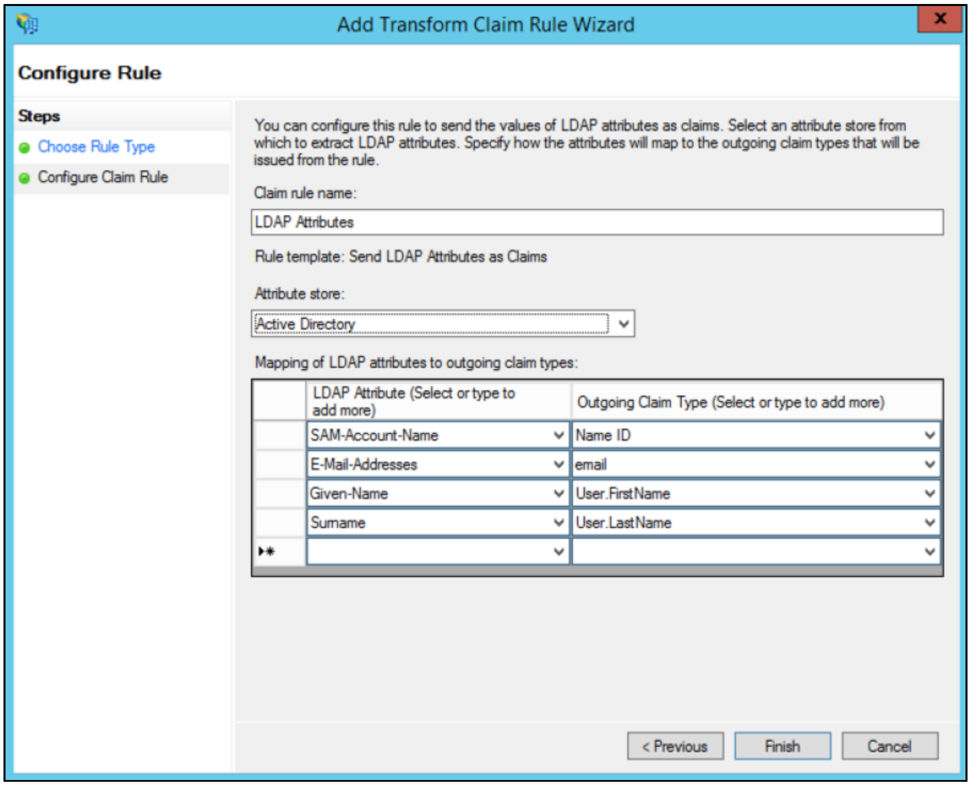
2. On the Select Rule Template page, select **Send LDAP Attributes as Claims**. Click **Next**.

3. On the Configure Rule page, type the name of the claim rule in the Claim rule name field e.g. User Attributes.

4. From the Attribute Store drop-down list, select Active Directory.

5. In the Mapping of LDAP attributes to outgoing claim types section, key in the following mappings:

LDAP Attribute	**Outgoing Claim Type**
SAM-Account-Name	Name ID
E-Mail-Addresses	email
Given-Name	User.FirstName
Surname	User.LastName



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim 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:

LDAP Attributes

Rule template: Send LDAP Attributes as Claims

Attribute store:

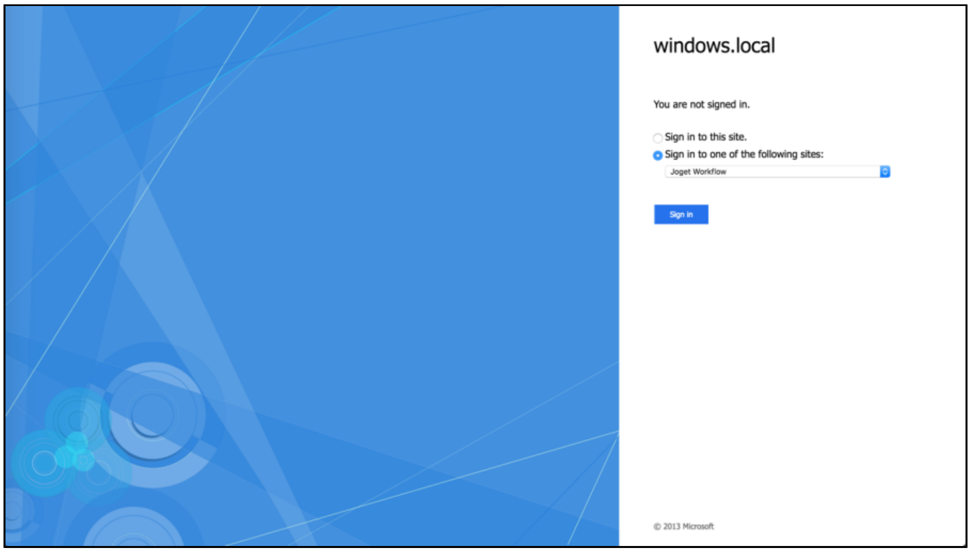
Active Directory

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)
	SAM-Account-Name	Name ID
	E-Mail-Addresses	email
	Given-Name	User.FirstName
	Surname	User.LastName
▸*		

6. Click **Finish**, and then click **OK**.

7. At this point, the SSO should be operational. Test the login by accessing the the AD FS login page e.g. https://windows.local/adfs/ls/idpinitiatedsignon.aspx



windows.local

You are not signed in.

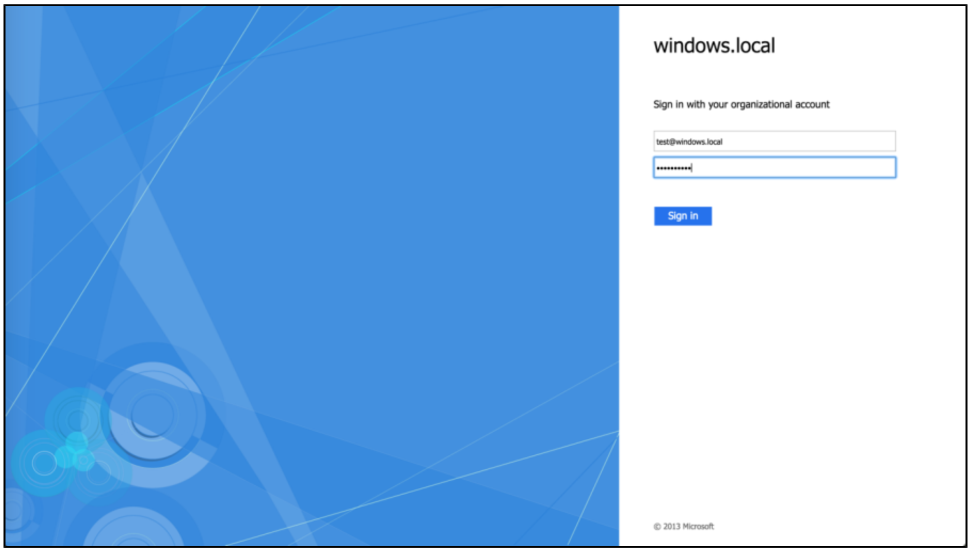
○ Sign in to this site.

● Sign in to one of the following sites:

Joget Workflow

8. Select the appropriate site e.g. Joget and click on **Sign in**.

9. Login to SharePoint using your AD account



windows.local

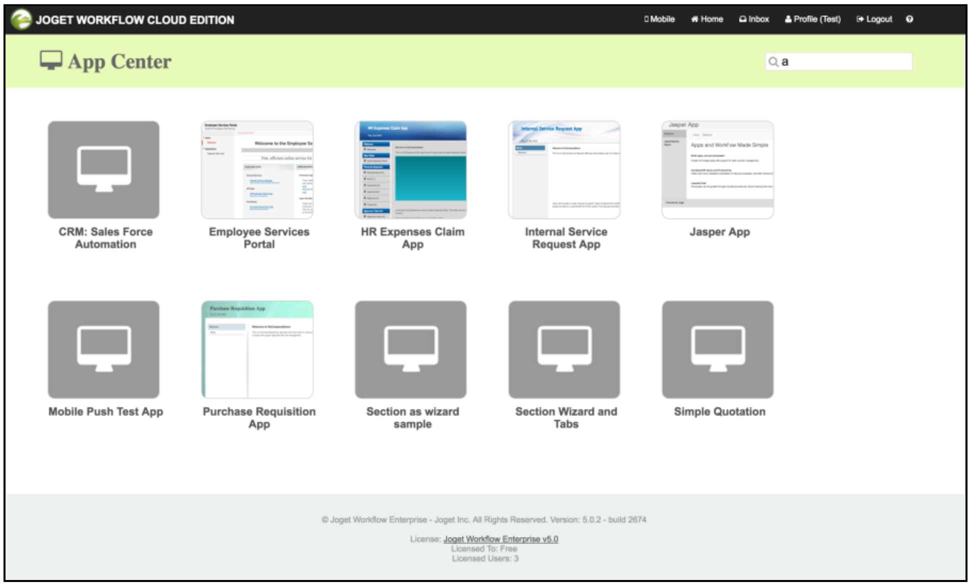
Sign in with your organizational account

test@windows.local

••••••••••

© 2013 Microsoft

10. On successful login, you should be automatically logged into Joget

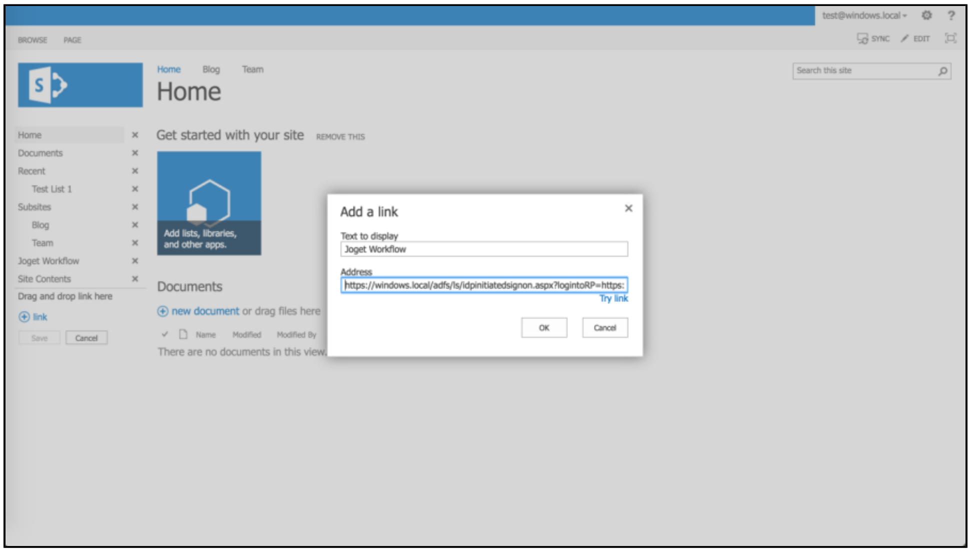


© Joget Workflow Enterprise - Joget Inc. All Rights Reserved. Version: 5.0.2 - build 2674

License: Joget Workflow Enterprise v5.0
Licensed To: Free
Licensed Users: 3

iv. Add Link in SharePoint site

1. In SharePoint, click on **Edit Links** in the left menu

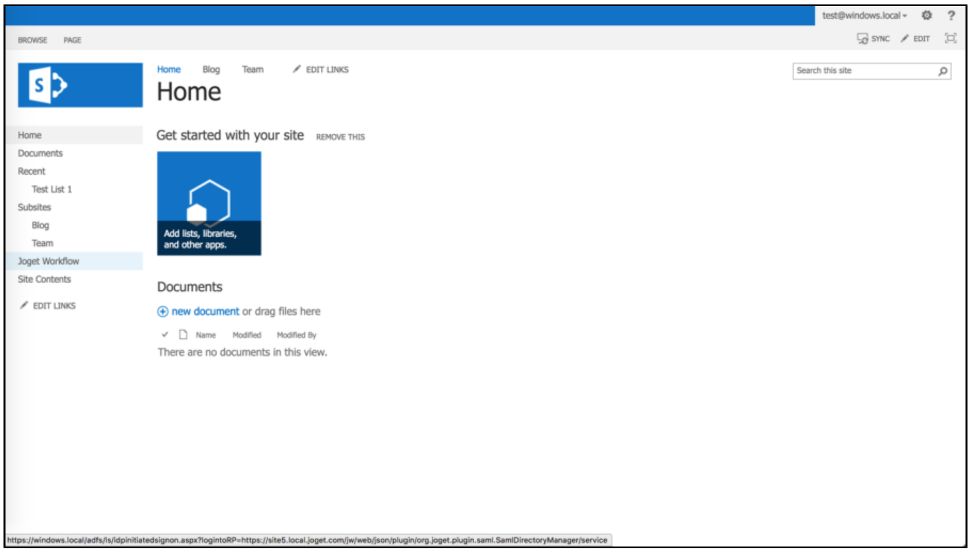


Add a link

Text to display: Joget Workflow

Address: https://windows.local/adfs/ls/idpinitiatedsignon.aspx?logintoRP=https:

2. Click on ⊕ **link**, and key in the text to display (e.g. Joget) and the direct SSO link e.g. assuming the AD FS server is https://windows.local and the Joget server is https://mysite.cloud.joget.com, the link will be https://windows.local/adfs/ls/idpinitiatedsignon.aspx?logintoRP=https://mysite.cloud.joget.com/jw/web/json/plugin/org.joget.plugin.saml.SamlDirectoryManager/service



https://windows.local/adfs/ls/idpinitiatedsignon.aspx?logintoRP=https://site5.local.joget.com/jw/web/json/plugin/org.joget.plugin.saml.SamlDirectoryManager/service

3. Once the link is created, clicking on the link will SSO the user into the Joget installation.

Appendix: Resources for Installing Pre-requisites

Install SharePoint Foundation 2013

1. Download SharePoint Foundation 2013: https://www.microsoft.com/en-us/download/details.aspx?id=35488

2. Install SharePoint 2013 on a single server with a built-in database: https://technet.microsoft.com/en-us/library/cc263202.aspx

3. Fix SharePoint installation issues on Windows 2012 R2:

   a. http://www.someshinyobject.com/posts/server-2012-r2-and-sharepoint-2013-the-tool-was-unable-to-install-application-server-role-web
   b. https://www.axian.com/2014/06/11/sharepoint-2013-configuration-wizard-issues-when-installing-local-development-instance/

    c. http://sandbox2010.kwizcom.com/sites/demo-data-view-plus/admin-corner-blog/Lists/Posts/Post.aspx?ID=4

Install Active Directory Federation Services (AD FS)

1. Install the AD FS software on Windows Server 2012 R2: https://msdn.microsoft.com/en-us/library/azure/dn528857.aspx

Configure SharePoint to use AD FS

1. Configure SAML-based claims authentication with AD FS in SharePoint 2013: https://technet.microsoft.com/en-us/library/hh305235.aspx

Install Joget

1. Options for installing Joget:

    a. Install On-Premise: Installation Guide
    b. Install on Docker: Joget on Docker
    c. Install on OpenShift: Joget on OpenShift
    d. Sign up for Joget Workflow On-Demand: https://cloud.joget.com