

# Joget Workflow SharePoint SSO Integration

- Introduction
- Configuring Joget Workflow SharePoint SSO
  - i. Pre-requisites
  - ii. Configure SAML for Joget Workflow
    - Export AD FS Token Signing Certificate
    - Configure SAML Directory Manager for Joget Workflow
  - iii. Configure Relying Party Trust between AD FS and Joget Workflow
    - Add Relying Party Trust
    - Edit Claim Rules
  - iv. Add Link in SharePoint site
- Appendix: Resources for Installing Pre-requisites
  - Install SharePoint Foundation 2013
  - Install Active Directory Federation Services (AD FS)
  - Configure SharePoint to use AD FS
  - Install Joget Workflow

## 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 Workflow is a platform to easily build web apps and automate processes. With single sign-on (SSO) integration from SharePoint to Joget Workflow, 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 Workflow SharePoint SSO

### i. Pre-requisites

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

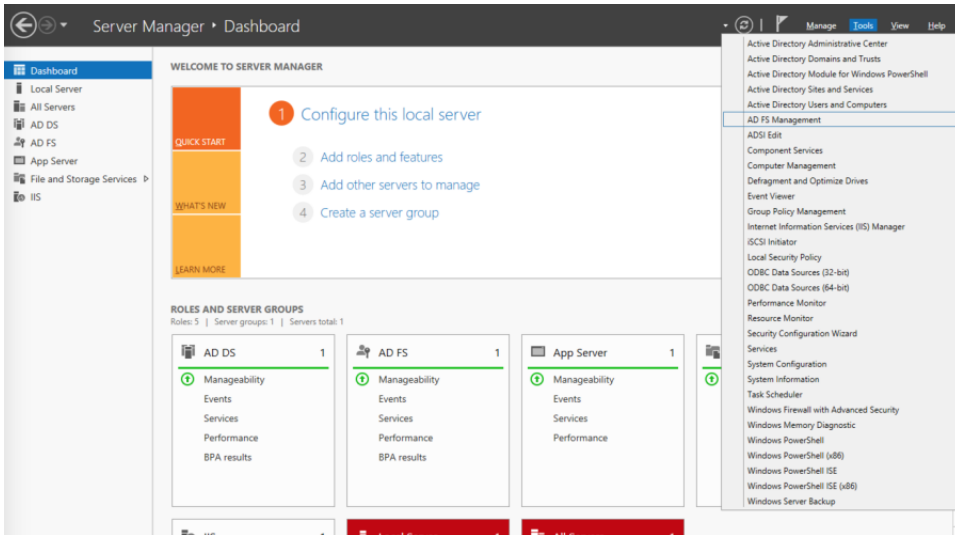
- SharePoint integrated with Active Directory Federation Services
- Joget Workflow

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

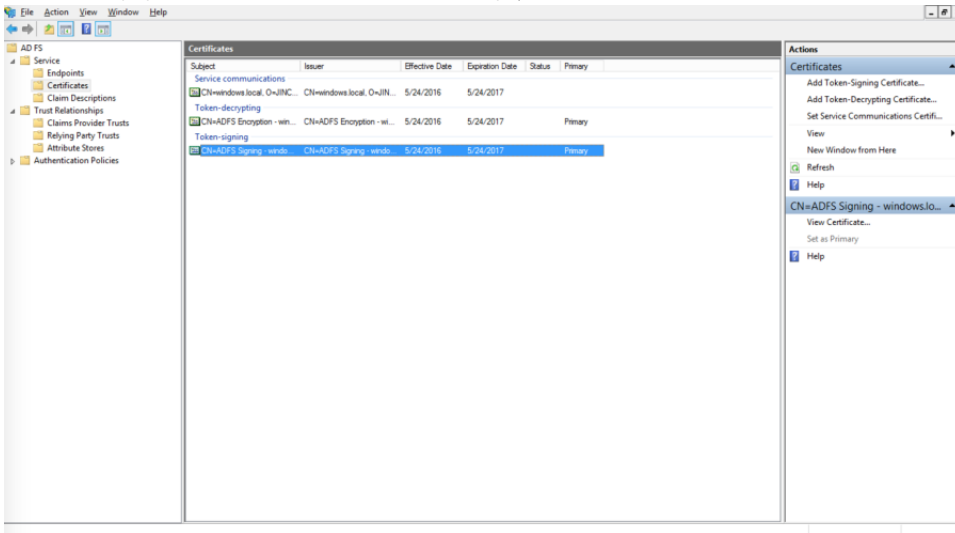
### ii. Configure SAML for Joget Workflow

#### Export AD FS Token Signing Certificate

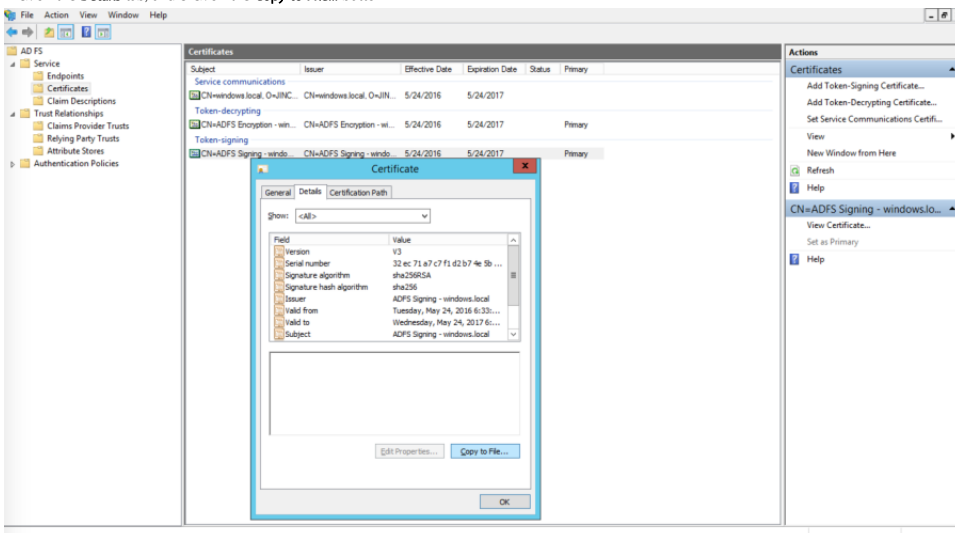
1. In the Windows Server Manager, launch **Tools > AD FS Management**



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.



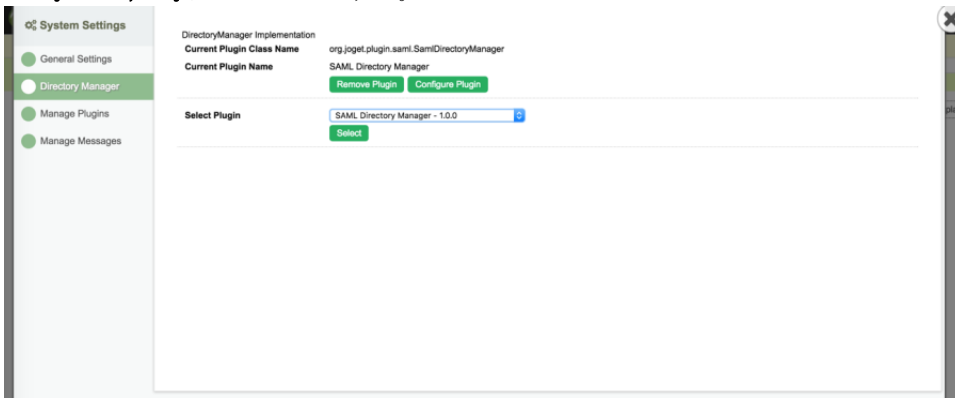
4. Click on the **Details** tab, and click on the **Copy to File...** button



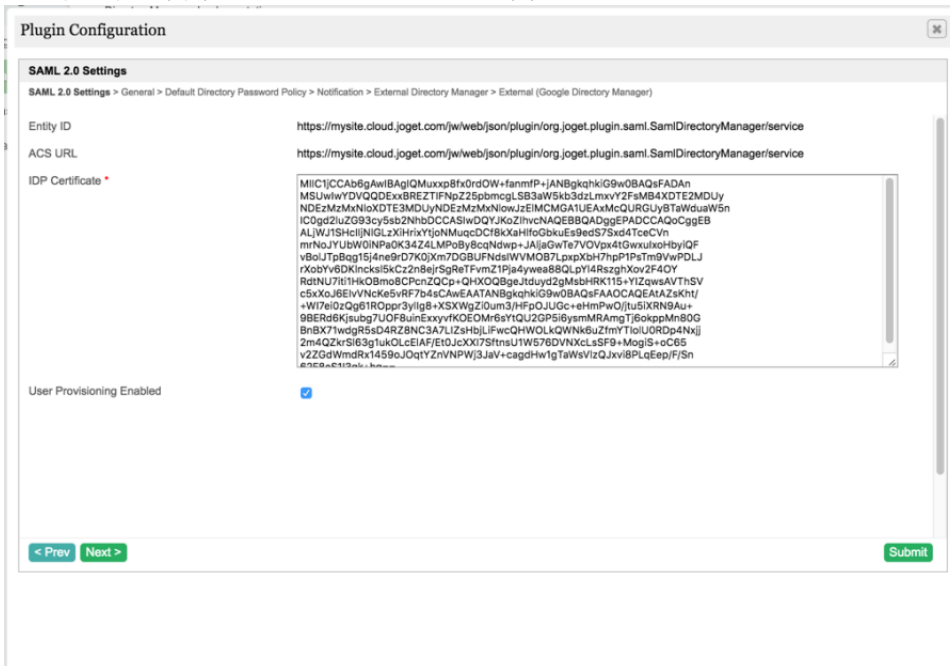
5. This starts the Certificate Export Wizard. On the Welcome to the Certificate Export Wizard page, click **Next**.
6. On the Export Private Key page, click **No**, do not export the private key, and then click **Next**.
7. On the Export File Format page, select **Base-64 encoded X.509 (.CER)**, and 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 Workflow

1. Download the [SAML Directory Manager from the Joget Marketplace](#)
2. In Joget Workflow, 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**.



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)



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 Workflow

### Add Relying Party Trust

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

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar is blue with the text 'Add Relying Party Trust Wizard' and a close button. The main area is titled 'Select Data Source'. On the left, there is a 'Steps' list with the following items: Welcome, Select Data Source (highlighted), Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-Factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main content area has the instruction 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network' with a description and a text field for 'Federation metadata address (host name or URL)'. 2. 'Import data about the relying party from a file' with a description and a text field for 'Federation metadata file location' with a 'Browse...' button. 3. 'Enter data about the relying party manually' (selected) with a description. At the bottom right are buttons for '< Previous', 'Next >', and 'Cancel'.

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 Workflow) 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**.

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box. The title bar is blue with the text 'Add Transform Claim Rule Wizard' and a close button (X). The main area is titled 'Select Rule Template'. On the left, there is a 'Steps' panel with two items: 'Choose Rule Type' (selected with a green dot) and 'Configure Claim Rule' (with a blue dot). The main content area has a heading '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.' Below this, there is a 'Claim rule template:' dropdown menu showing 'Send LDAP Attributes as Claims'. Underneath is a 'Claim rule template description:' section with a text box containing the following text: '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.' At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

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
▶*	

< Previous Finish Cancel

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

7. At this point, the SSO should be operational. Test the login by accessing 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:

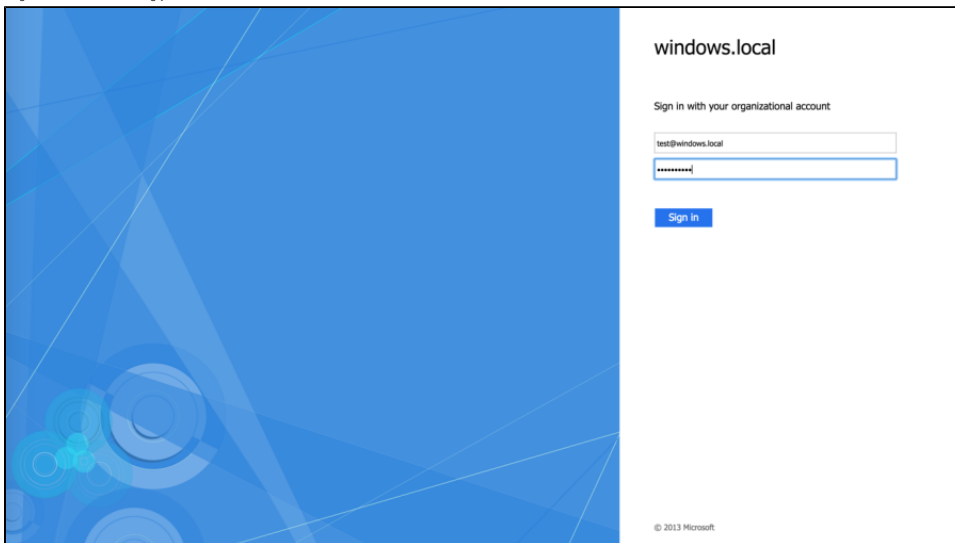
Joget Workflow

Sign in

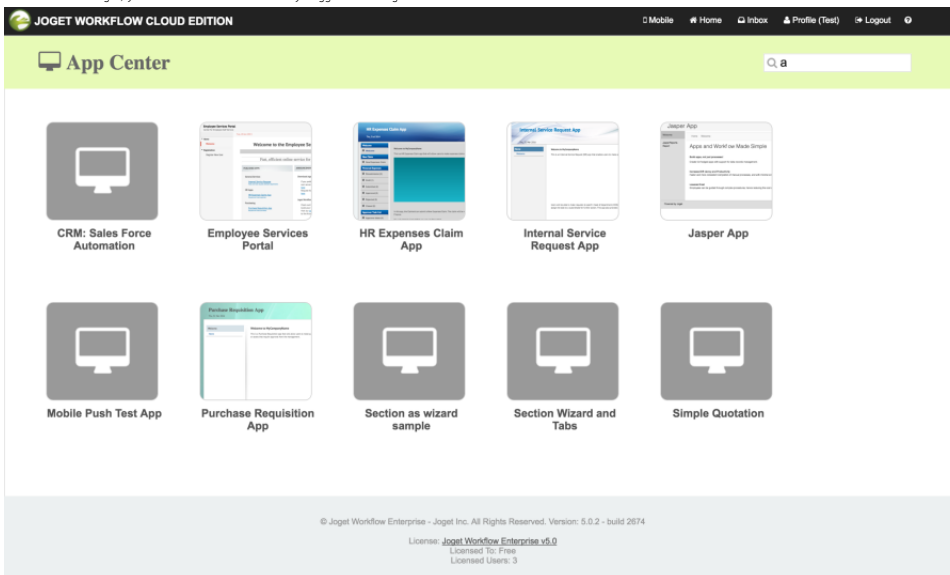
© 2013 Microsoft

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

9. Login to SharePoint using your AD account

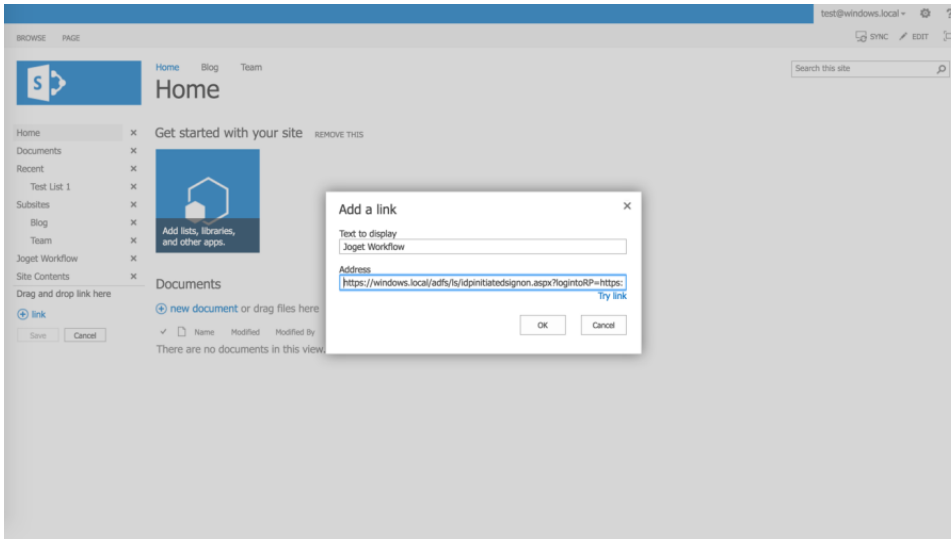


10. On successful login, you should be automatically logged into Joget Workflow

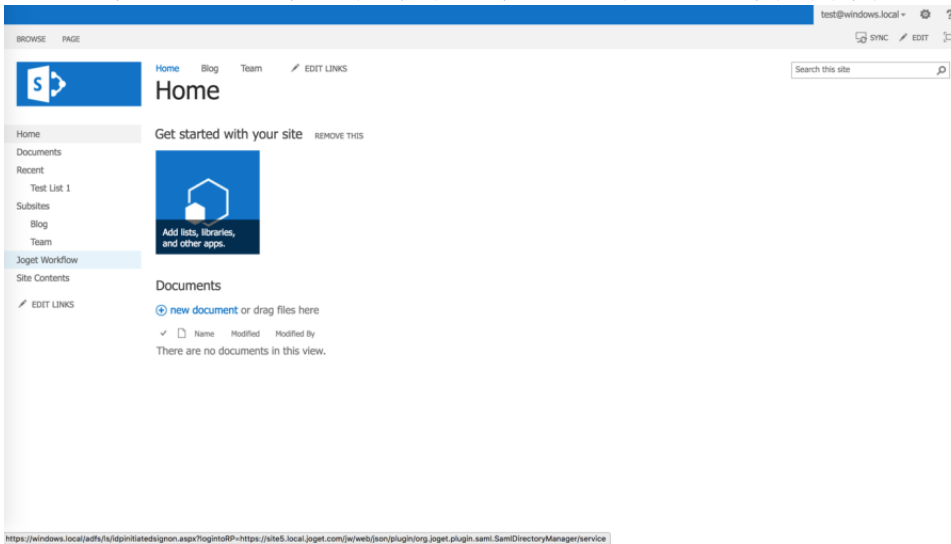


- iv. Add Link in SharePoint site

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



2. Click on **+ link**, and key in the text to display (e.g. Joget Workflow) and the direct SSO link e.g. assuming the AD FS server is <https://windows.local> and the Joget Workflow 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>



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

1. Options for installing Joget Workflow:
  - a. Install On-Premise: <https://dev.joget.org/community/display/KBv5/Installation>
  - b. Install on Docker: <https://dev.joget.org/community/display/KBv5/Joget+Workflow+on+Docker>
  - c. Install on OpenShift: <https://dev.joget.org/community/display/KBv5/Joget+Workflow+on+OpenShift>
  - d. Sign up for Joget Workflow On-Demand: <https://cloud.joget.com>