

Joget SSO with Microsoft Entra ID (Azure Active Directory) using SAML

- [SAML SSO Configuration Steps](#)
 - [1. Install Joget SAML Plugin and Obtain ACS URL](#)
 - [2. Configure Microsoft Entra ID for SAML](#)
 - [3. Configure SAML IDP Certificate in the Joget SAML Plugin](#)
 - [4. Configure Custom User Attributes](#)
 - [5. Test the SAML SSO](#)
- [Source Code](#)
- [References](#)

SAML SSO Configuration Steps

1. Install Joget SAML Plugin and Obtain ACS URL

1. Install the [Joget SAML Plugin](#) from the Joget Marketplace.
2. In the Joget **System Settings** > **General Settings**, set **API Domain Whitelist** to *

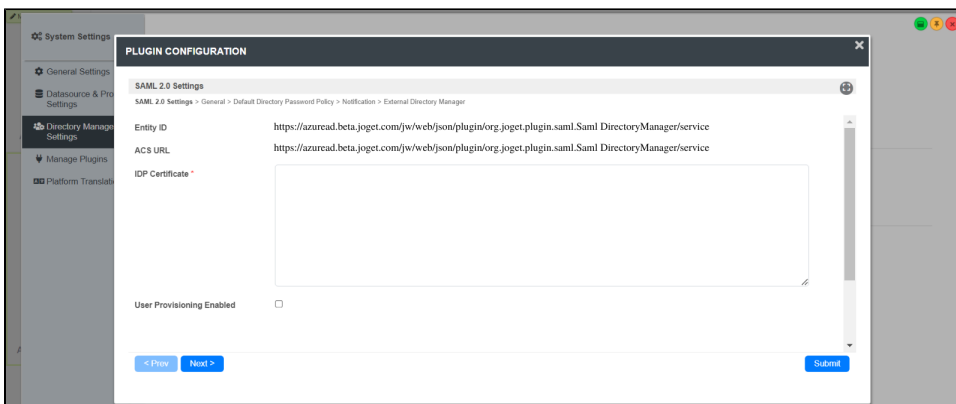
Important Note

If this is not set, you will get a 400 Forbidden error when performing the SSO.

3. In the Joget **System Settings** > **Directory Manager**, select the Joget SAML Plugin.
4. In the Joget SAML Plugin configuration, copy the **Entity ID** and **ACS URL**.

Important Note

Azure AD requires the ACS URL to be HTTPS so your Joget installation must be running under HTTPS.



2. Configure Microsoft Entra ID for SAML

1. Sign in to the [Azure](#) portal and navigate to **Azure > Browse Microsoft Entra Gallery > Create your own application**. Name your application and select the **Integrate any other application you don't find in the gallery** option and click **Create** to add an application.

The screenshot shows the 'Create your own application' page in the Azure portal. The page is titled 'Create your own application' and has a 'Get feedback?' link. Below the title, there is a text block explaining the Microsoft Entra App Gallery and a search bar. The page is divided into several sections: 'Cloud platforms' (AWS, Google Cloud, Oracle, SAP), 'On-premises applications' (Add an on-premises application, Learn about Application Proxy, On-premises application provisioning), and 'Featured applications' (Adobe Identity Management (SAML), Atlassian Cloud, AWS Single-Account Access, Box). On the right side, there is a form to create a new application. The form has a 'What's the name of your app?' field with the value 'Joget SAML SSO'. Below the name field, there are three radio button options: 'Configure Application Proxy for secure remote access to an on-premises application', 'Register an application to integrate with Microsoft Entra ID (App you're developing)', and 'Integrate any other application you don't find in the gallery (Non-gallery)'. The third option is selected. At the bottom right, there is a 'Create' button.

2. Select the application, select **Set up single sign-on**, then select **SAML**.

The screenshot shows the 'Joget SAML SSO | Overview' page in the Azure portal. The page is titled 'Joget SAML SSO | Overview' and has a 'Properties' section on the left. The 'Properties' section shows the application name 'Joget SAML SSO' and the application ID '0b5443a71b-453f-81c9-...'. Below the 'Properties' section, there is a 'Getting Started' section with five steps: 1. Assign users and groups, 2. Set up single sign-on, 3. Provision User Accounts, 4. Conditional Access, and 5. Self-service. Each step has a 'Get started' link. Below the 'Getting Started' section, there is a 'What's New' section with three items: 'Sign in charts have moved!', 'Delete Application has moved to Properties', and 'Getting started has moved to Overview'.

The screenshot shows the 'Joget SAML SSO | Single sign-on' page in the Azure portal. The page is titled 'Joget SAML SSO | Single sign-on' and has a 'Single sign-on' section on the left. The 'Single sign-on' section shows the application name 'Joget SAML SSO' and the application ID '0b5443a71b-453f-81c9-...'. Below the 'Single sign-on' section, there is a 'Select a single sign-on method' section with four options: 'Disabled', 'SAML', 'Password-based', and 'Linked'. The 'SAML' option is selected. Below the 'Select a single sign-on method' section, there is a 'What's New' section with three items: 'Sign in charts have moved!', 'Delete Application has moved to Properties', and 'Getting started has moved to Overview'.

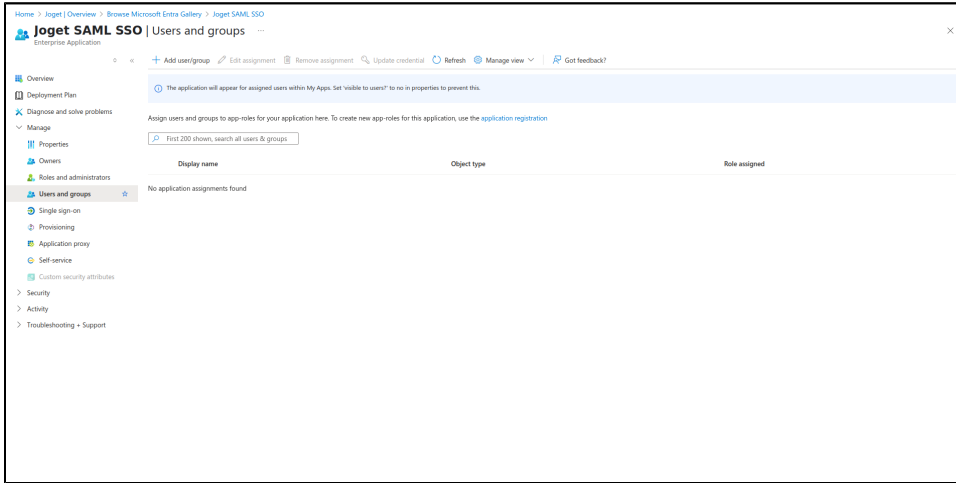
3. Under **Basic SAML Configuration**, select the **Edit pencil icon** and key in the Joget SAML Identifier (Entity ID) and Reply URL (Assertion Consumer Service (ACS) URL) copied earlier, then **Save**.

4. Edit **User Attributes & Claims**, and configure the claims

Claim Name	Value
Unique User Identifier (Name ID)	user.userprincipalname
email	user.mail
User.FirstName	user.givenname
User.LastName	user.surname

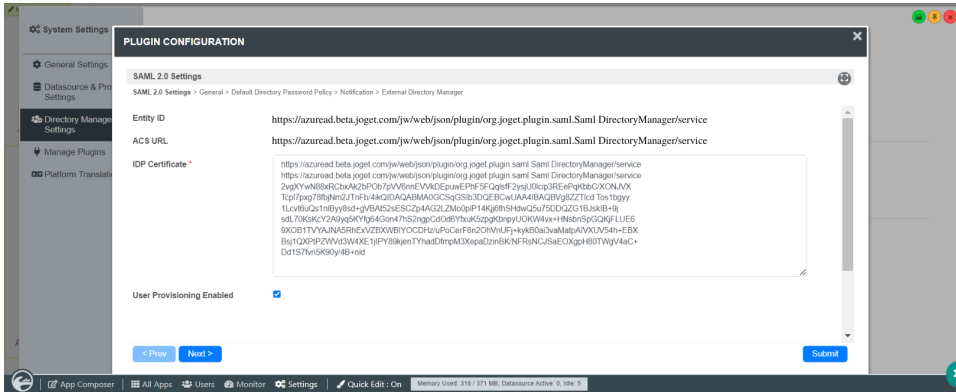
5. Under **SAML Certificates**, download the **Certificate (Base64)**. This certificate file will be used to configure the Joget SAML Plugin later.

6. Select the **Users and groups** menu item on the left, and add the users allowed to access Joget. You may add yourself to the listing so that you can test the login later.



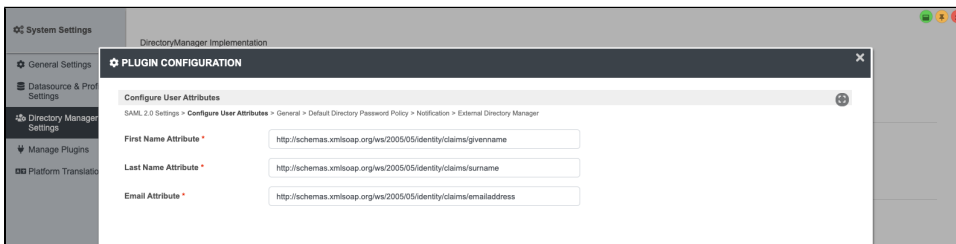
3. Configure SAML IDP Certificate in the Joget SAML Plugin

1. Open the downloaded certificate file and copy the contents into the **IDP Certificate** field in the **Joget SAML Plugin** configuration (NOTE: copy without the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines)



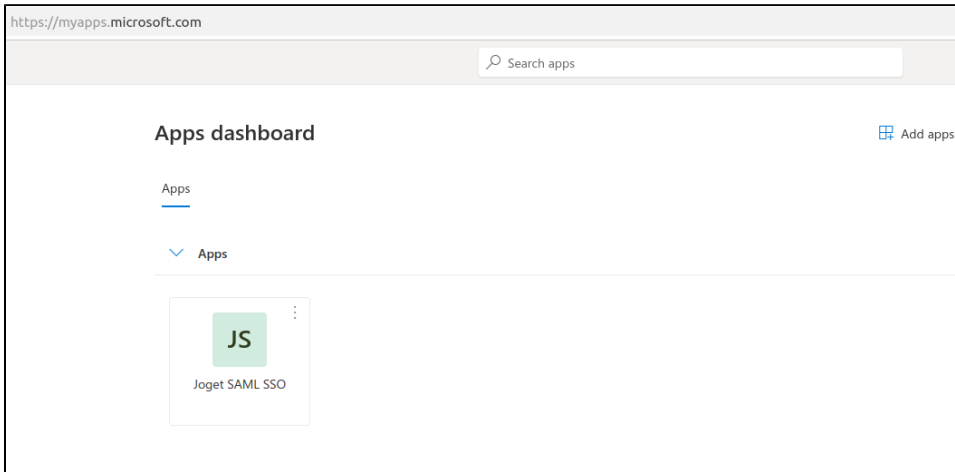
4. Configure Custom User Attributes

1. Key in the values of the user attributes



5. Test the SAML SSO

1. Access the Azure [My Apps Portal](#), click on the application, and select the user to perform the SSO.



2. If the SSO configuration is correct, the current user will be logged into Joget.

Source Code

This plugin source code is available in a new open source repository at <https://github.com/JogetOSS/>. JogetOSS is a community-led team for open source software related to the Joget no-code/low-code application platform. Projects under JogetOSS are community-driven and community-supported, and you are welcome to contribute to the projects.

References

1. <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-single-sign-on-non-gallery-applications>
2. <https://dev.joget.org/community/display/DX7/Joget+SharePoint+SSO+Integration>