intelliHR SSO Configuration

Windows Server ADFS Configuration

Requirements

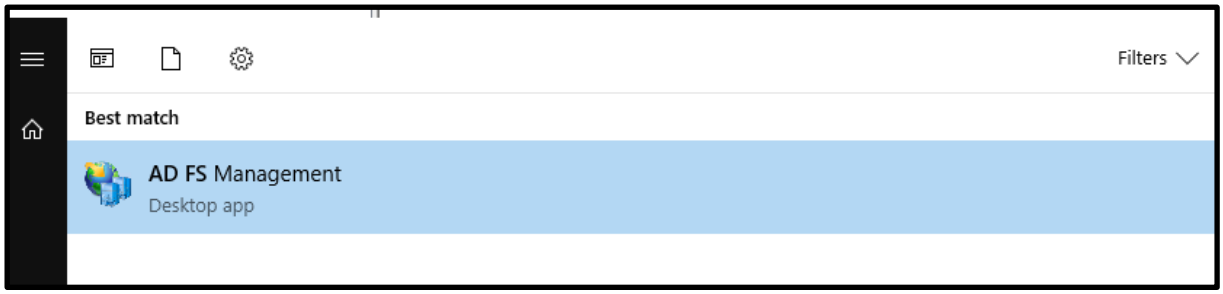
The following requirements are required before continuing this guide.

1. An intelliHR account
2. A Microsoft Windows Server running Active Directory Federation Services (ADFS). This guide uses Windows Server 2019.

Instructions

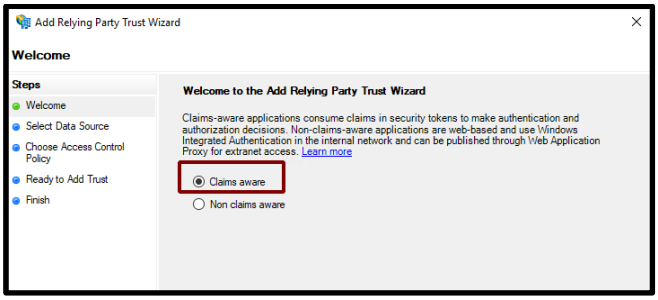
Create a relying party trust

1. Open AD FS Management

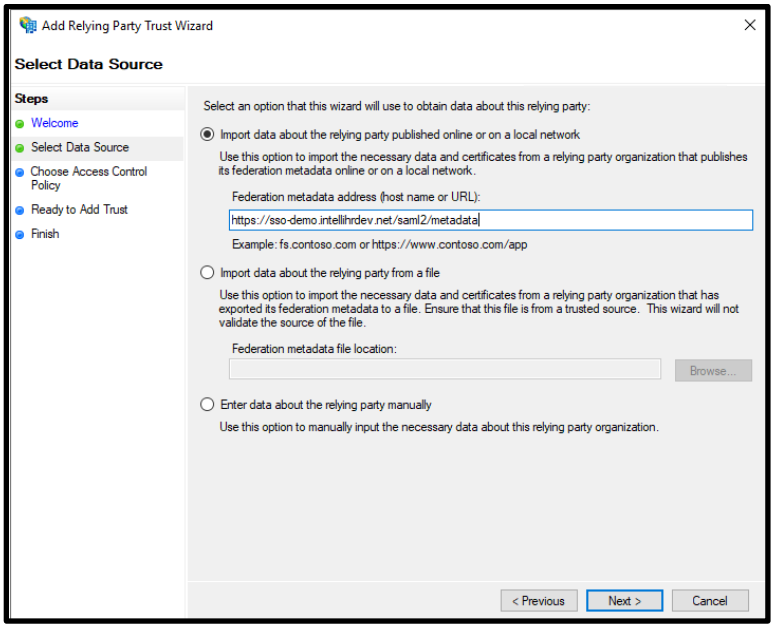


2. Go to the **Relying Trusts** folder and click **Add Relying Party Trust**

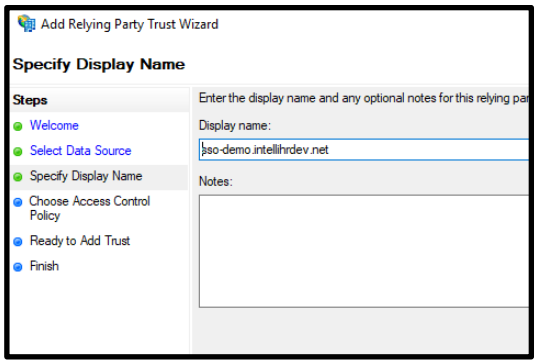
3. Select **Claims aware** and click **Next**



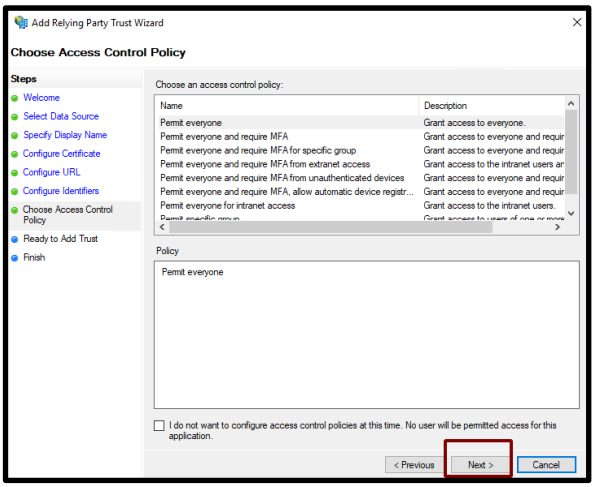
4. Select **Import data about the relying party…** and use the URL **https://<your name>.intellihr.net/saml2/metadata** then click **Next**



5. Select a display name to use for the trust and click **Next**



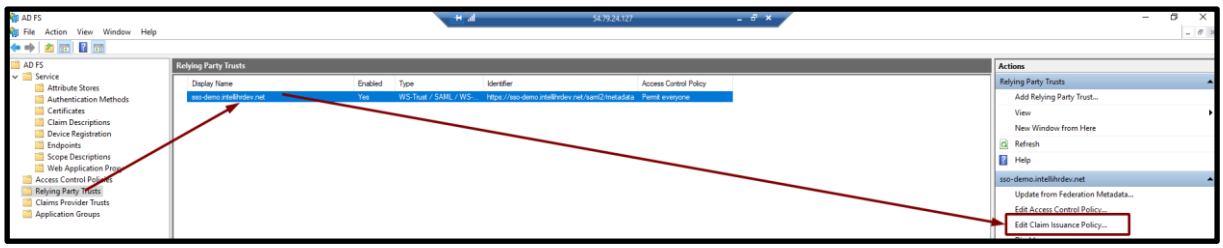
6. Optionally, configure access restrictions on who can use SSO



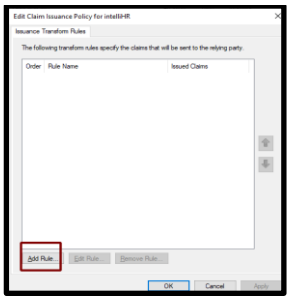
7. Select default options for the remainder of the wizard.

Edit the claims issuance policy

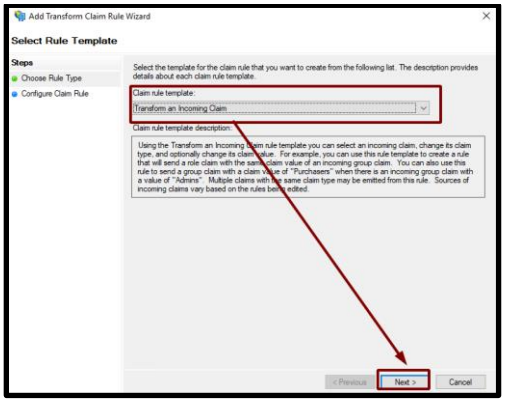
1. Edit the claims issuance policy



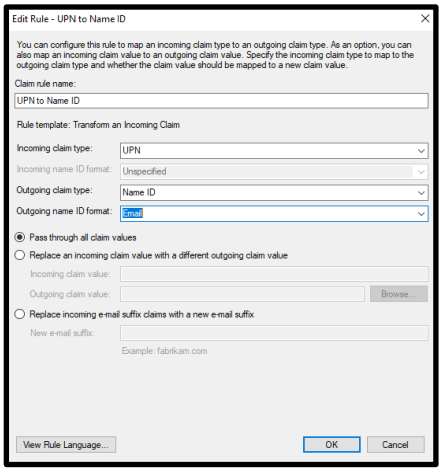
2. Click **Add Rule**



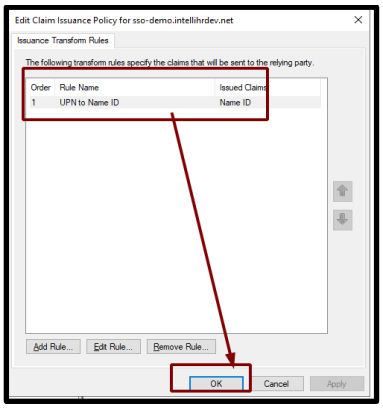
3. Select **Transform an incoming claim** and click **Next**



4. Create a transformation for the property type of your choice to **Name ID in Email format**. In this case we are using UPN. Then click **Finish**.



5. Verify that the rule has been added and click **OK**

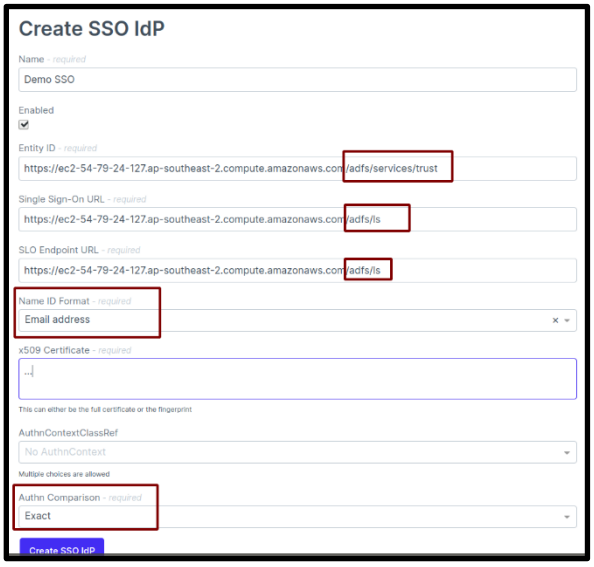


Configure intelliHR Settings

1. Logon to intelliHR
2. Navigate to Settings->SSO

3. Click **Create SSO idP**

4. Configure the required options, taking note of the URLs used and click **Create SSO idP**. Note: you can obtain the x509 Certificate at the following URL **https://<your ADFS server>/FederationMetadata/2007-06/FederationMetadata.xml**. Use the **signing** certificate from the xml.

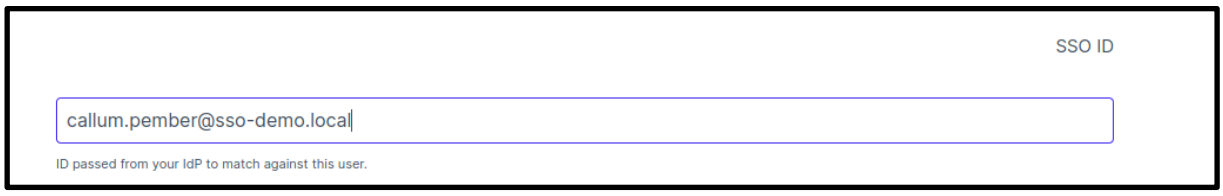


Configure intelliHR user for SSO

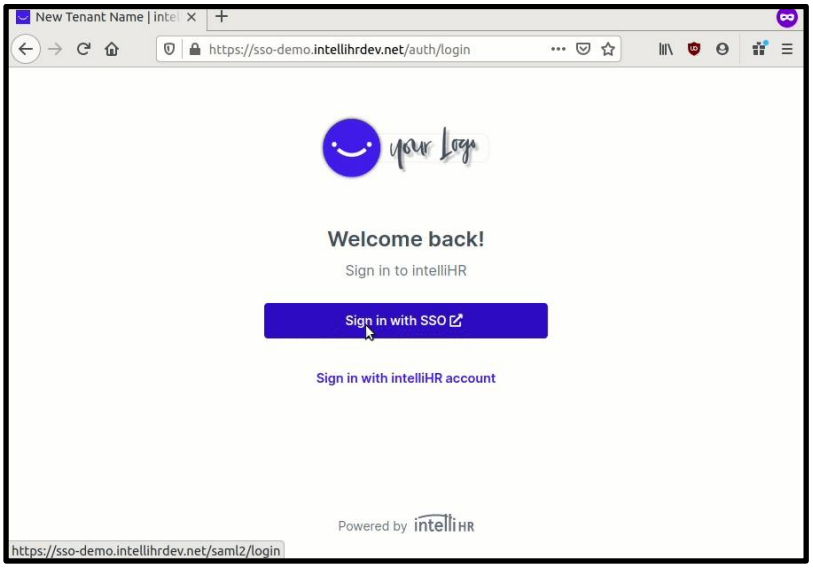
1. Go to Settings->User Accounts

2. Click **Edit** on the user to enable for SSO

3. Set the SSO ID of the user and save. The SSO ID should be the user's UPN or other unique identifier setup in the idP.



4. The user can now login via SSO



Azure AD Configuration

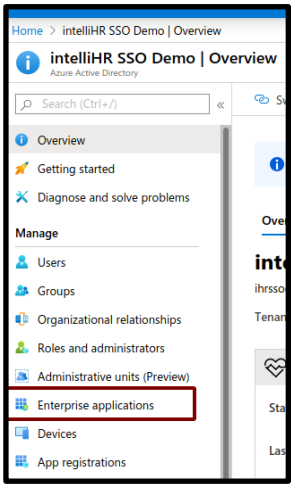
Requirements

1. An intelliHR account
2. An Azure AD tenancy

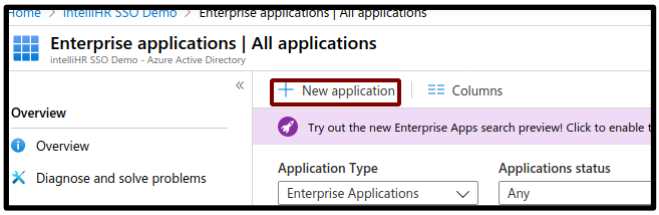
Instructions

Configure an App in Azure AD

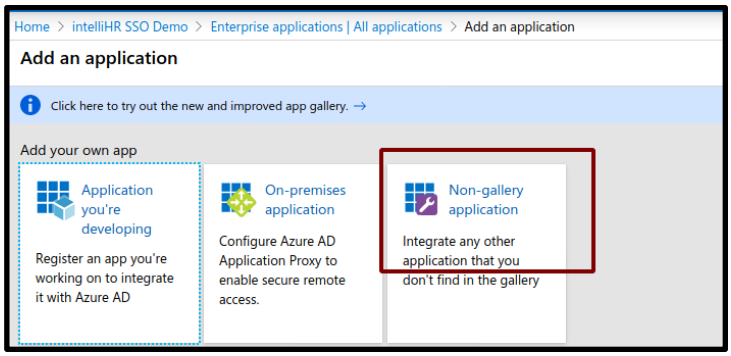
1. Logon to the Azure AD portal at https://portal.azure.com and click **Enterprise Applications**



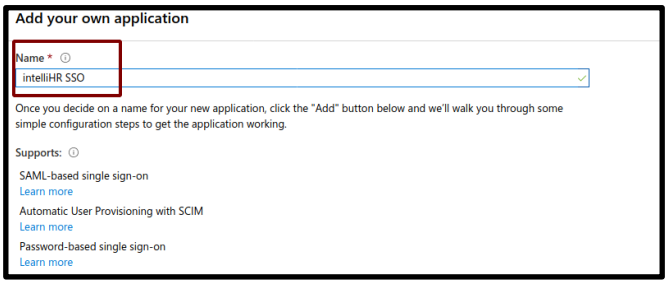
2. Click **New Application**



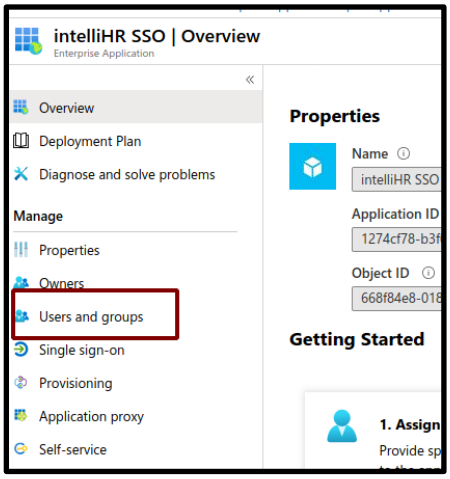
3. Click **Non-gallery Application**



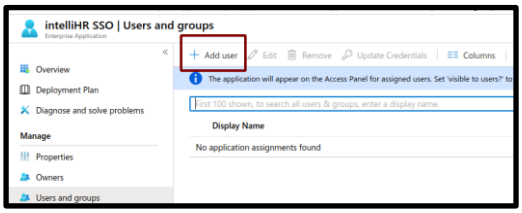
4. Give the application a name and click **Add**



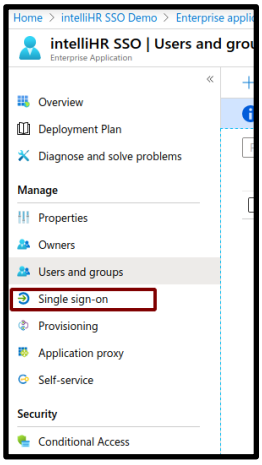
5. Click on **Users and Groups**



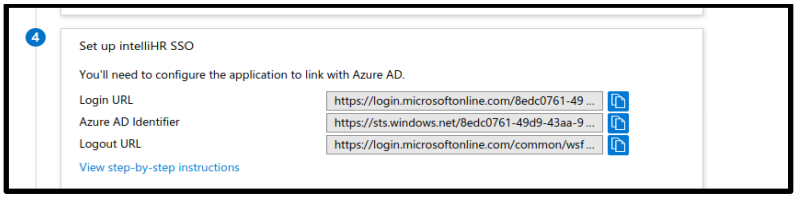
6. Click **Add User**



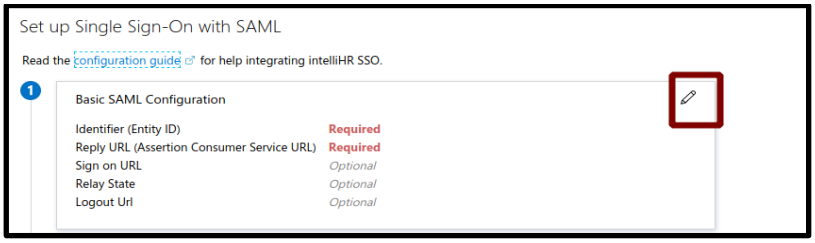
7. Add users as required
8. Select **Single sign-on** from the menu



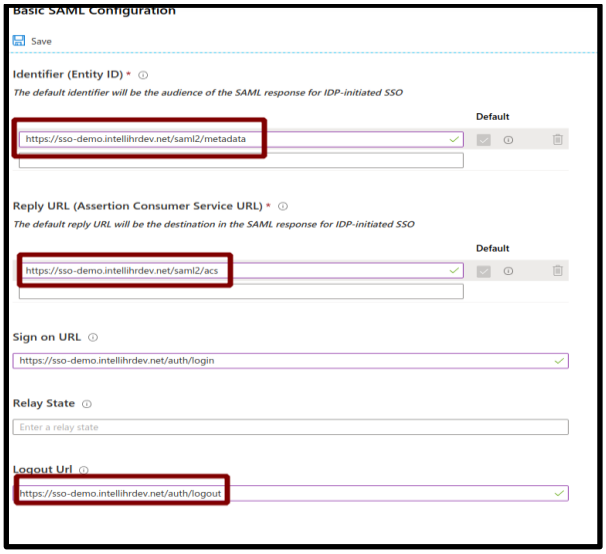
9. Select **SAML**
10. Save the following details for quick reference to configure the intelliHR side



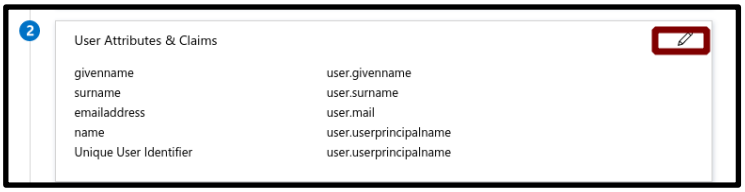
11. Click on **Edit**



12. Use the URLs supplied in the image below, replacing **sso-demo.intellihrdev.net with <your name>.intellihr.net** and save the configuration.



13. Click on the edit button in section 2 to edit **User Attributes and Claims**



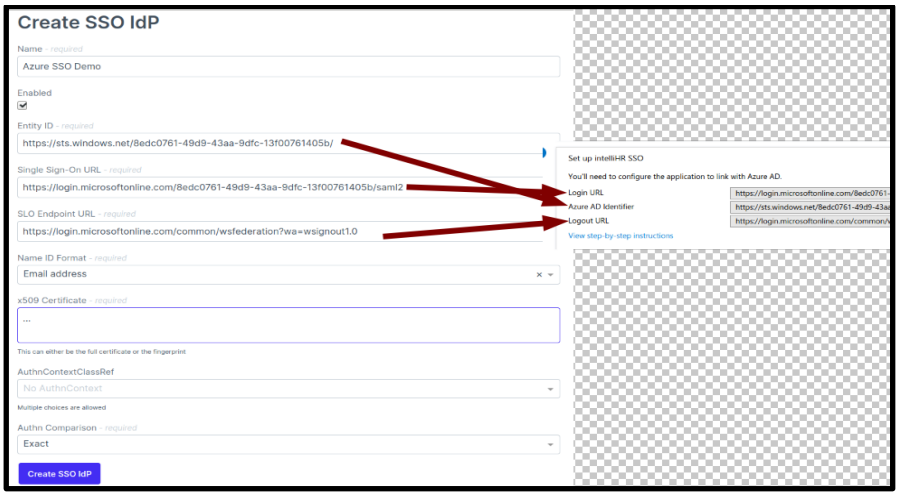
14. Edit Name ID to be the value you wish to use for SSO (in this case email address) and save.

Configure intelliHR Settings

1. Logon to intelliHR
2. Navigate to Settings->SSO

3. Click **Create SSO idP**

4. Configure options as shown in the image below. For x509 certificate, this can be found when visiting the Identity Provider metadata URL, which will provide an XML document that looks like the below:



5. The user can now login via SSO