



intelliHR SSO Configuration

[Windows Server ADFS Configuration](#)

[Requirements](#)

[Instructions](#)

[Create a relying party trust](#)

[Edit the claims issuance policy](#)

[Configure intelliHR Settings](#)

[Configure intelliHR user for SSO](#)

[Azure AD Configuration](#)

[Requirements](#)

[Instructions](#)

[Configure an App in Azure AD](#)

[Configure intelliHR Settings](#)

Windows Server ADFS Configuration

Requirements

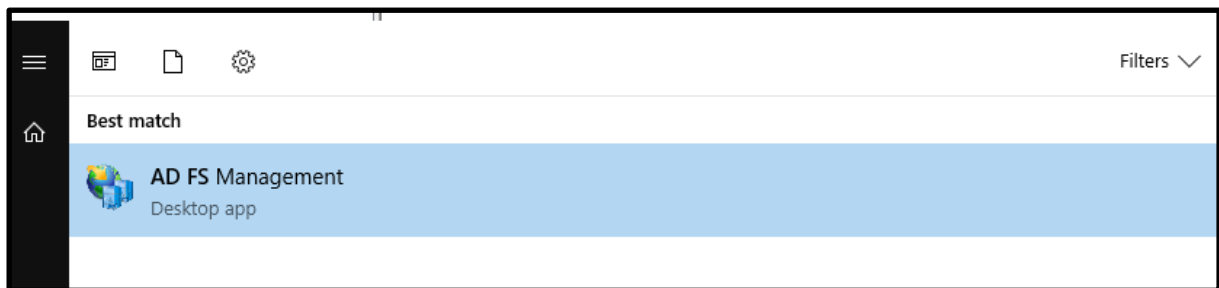
The following requirements are required before continuing this guide.

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

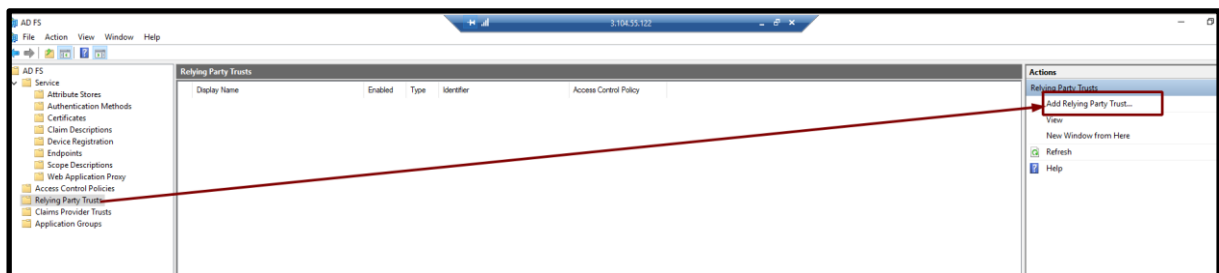
Instructions

Create a relying party trust

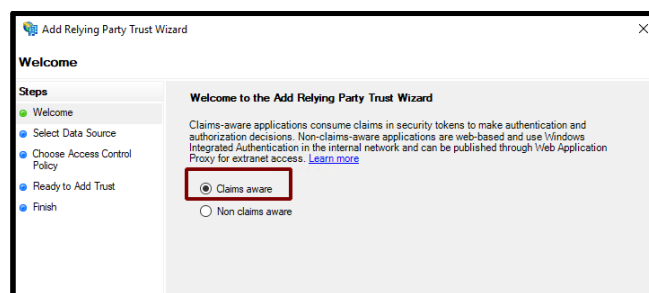
1. Open AD FS Management



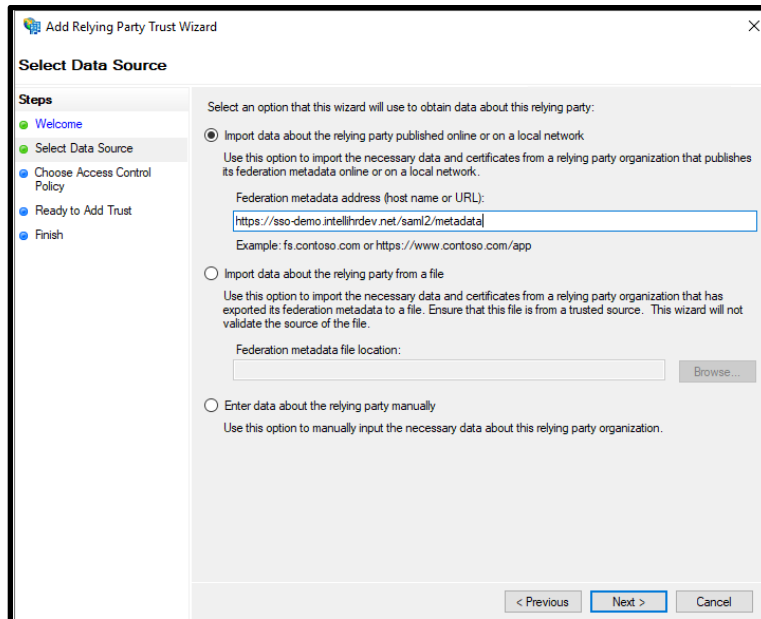
2. Go to the **Relying Trusts** folder and click **Add Relying Party Trust**



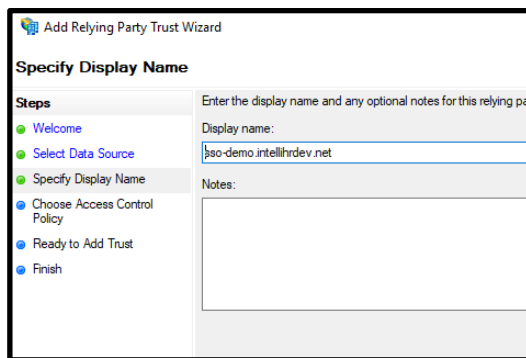
3. Select **Claims aware** and click **Next**



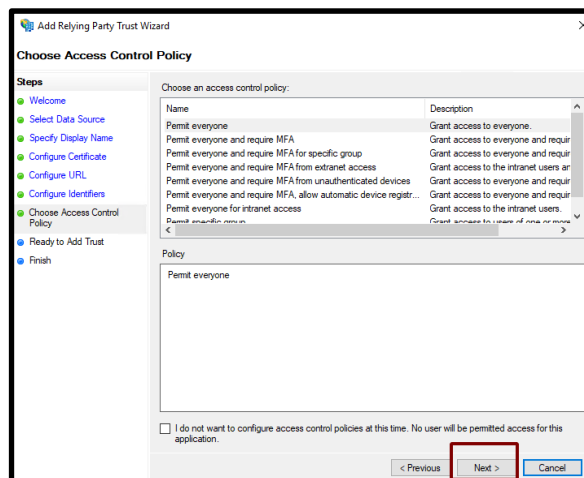
4. Select **Import data about the relying party...** and use the URL **https://<your name>.intellihr.net/saml2/metadata** then click **Next**



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



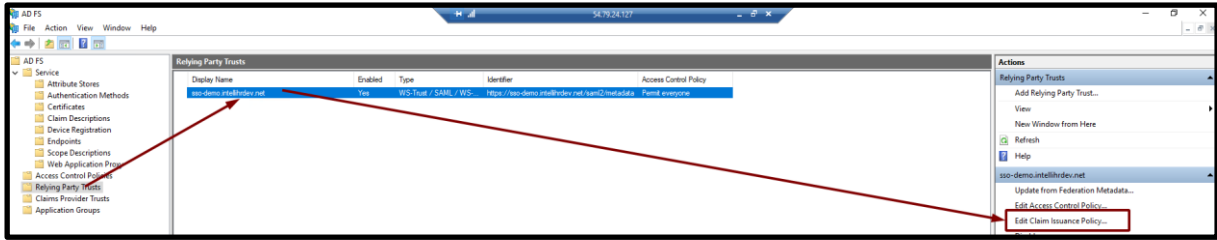
6. Optionally, configure access restrictions on who can use SSO



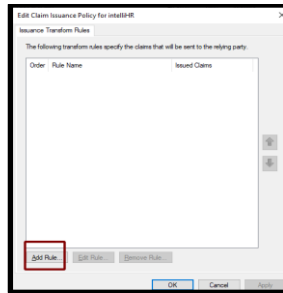
7. Select default options for the remainder of the wizard.

Edit the claims issuance policy

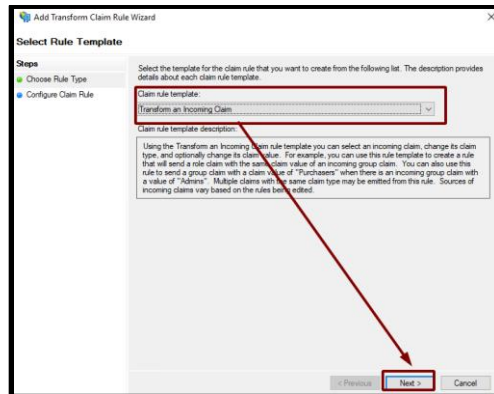
1. Edit the claims issuance policy



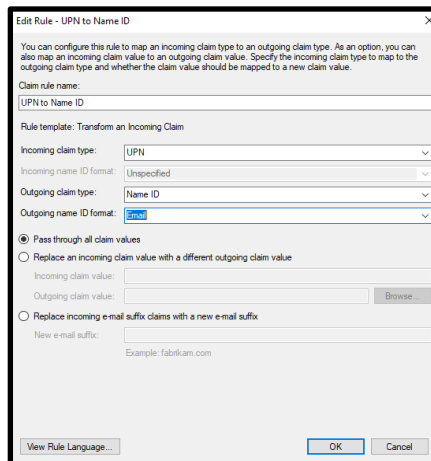
2. Click Add Rule



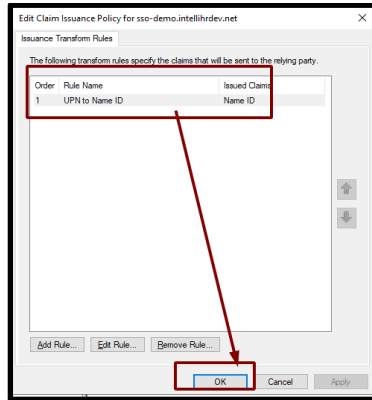
3. Select Transform an incoming claim and click Next



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.



- Verify that the rule has been added and click **OK**

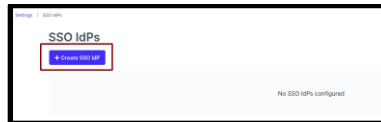


Configure intelliHR Settings

- Logon to intelliHR
- Navigate to Settings->SSO



- Click **Create SSO idP**



- 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.

Create SSO IdP

Name - required
Demo SSO

Enabled

Entity ID - required
https://ec2-54-79-24-127.ap-southeast-2.compute.amazonaws.com/adfs/services/trust

Single Sign-On URL - required
https://ec2-54-79-24-127.ap-southeast-2.compute.amazonaws.com/adfs/ls

SLO Endpoint URL - required
https://ec2-54-79-24-127.ap-southeast-2.compute.amazonaws.com/adfs/ls

Name ID Format - required
Email address

x509 Certificate - required
...

This can either be the full certificate or the fingerprint

AuthnContextClassRef
No AuthnContext

Multiple choices are allowed

Authn Comparison - required
Exact

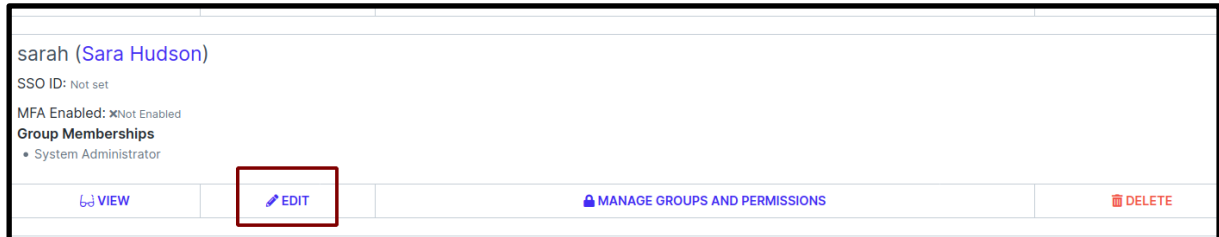
Create SSO IdP

Configure intelliHR user for SSO

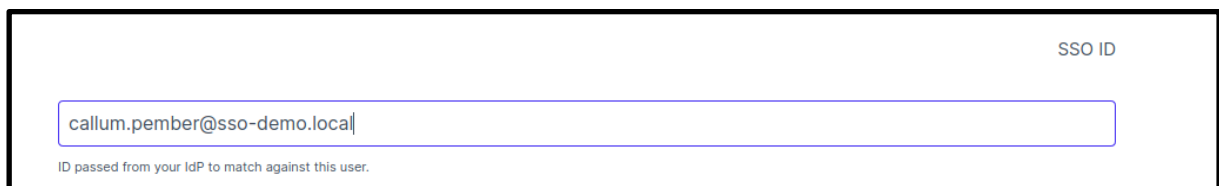
1. Go to Settings->User Accounts



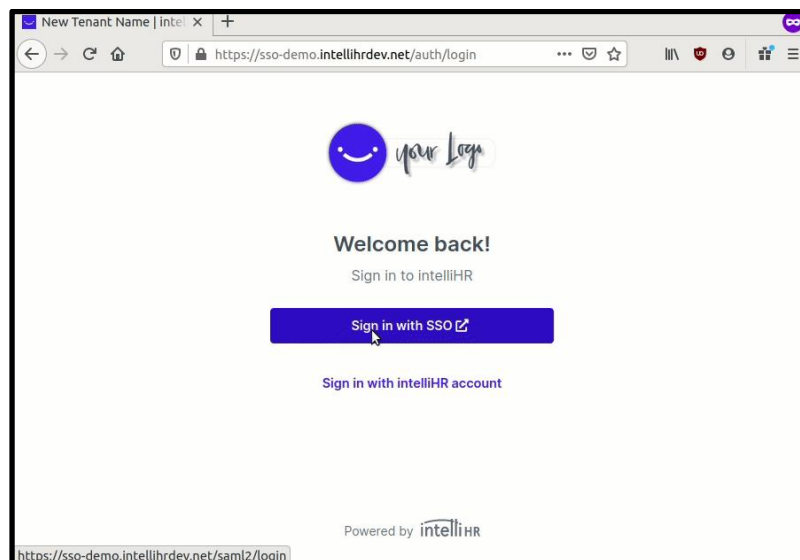
2. Click **Edit** on the user to enable for SSO



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

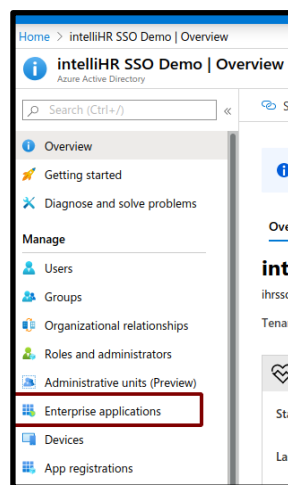
Requirements

1. An intelliHR account
2. An Azure AD tenancy

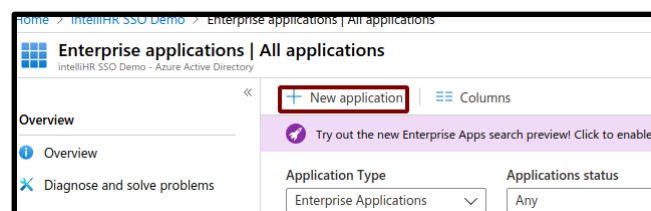
Instructions

Configure an App in Azure AD

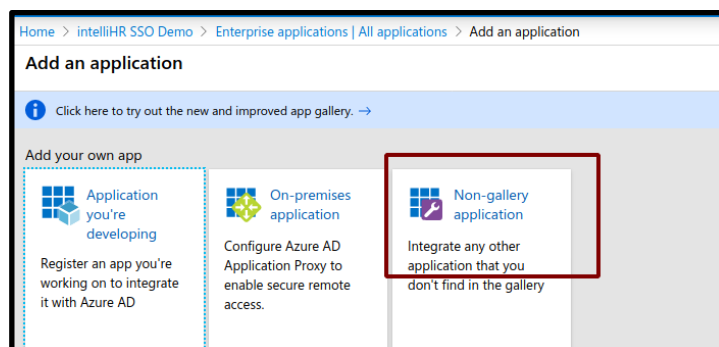
1. Logon to the Azure AD portal at <https://portal.azure.com> and click **Enterprise Applications**



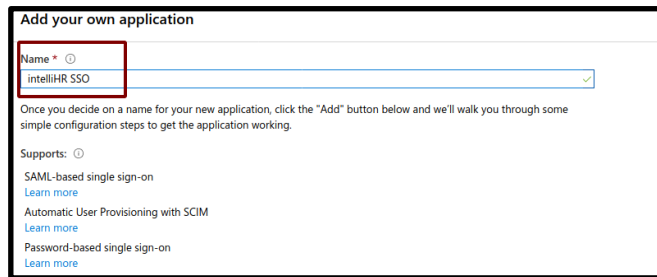
2. Click **New Application**



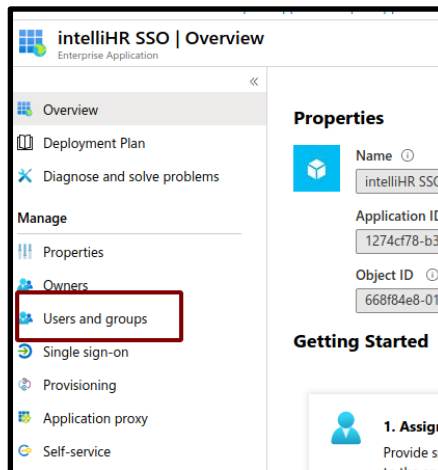
3. Click **Non-gallery Application**



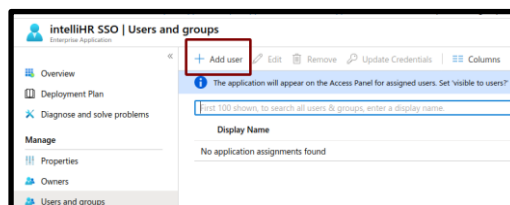
4. Give the application a name and click **Add**



5. Click on **Users and Groups**

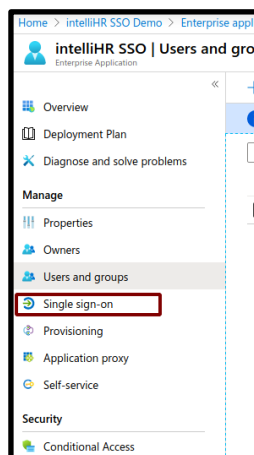


6. Click **Add User**



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

4 Set up intelliHR SSO

You'll need to configure the application to link with Azure AD.

Login URL <https://login.microsoftonline.com/8edc0761-49...>

Azure AD Identifier <https://sts.windows.net/8edc0761-49d9-43aa-9...>

Logout URL <https://login.microsoftonline.com/common/wsf...>

[View step-by-step instructions](#)

11. Click on **Edit**

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating intelliHR SSO.

1 Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Uri	Optional

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

Basic SAML Configuration

Save

Identifier (Entity ID) * Default

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Reply URL (Assertion Consumer Service URL) * Default

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Sign on URL

Relay State

Logout Uri

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

2 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

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

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.mail [nameid-formatemailAd...]

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:

```

--<RoleDescriptor xsi:type="fed:SecurityTokenServiceType" protocolSupportEnumeration="http://docs.oasis-open.org/wsfed/federation/200706">
  <KeyDescriptor use="signing">
    <X509Data>
      <X509Certificate>
        MIICBDCCAAdgAwIBAgIQMKi6ZYlg4pCmzc0rPC0ijANBgkqhkiG9w0BAQsFAADA0MTIwMAYDVQDEYlNaWNyb3NvZnQgOXP1cmUgRmVhZS9hdGVkIFNTIyBDZjJ0aWZpY2F0ZTA6
        GWJdbUFfcBpRq+OtQnh2UDCOFd78Jrcd+l0wfZjyYWHWIEAoqjl38rvLHhDyMS02+UQVyt0HFQ/19YFOEDNCCQoKUGPsAucLKfY/QOq5MbD9CAIYn4PjnZjxhZ+IdcTtvl94
        UAB5TYPUm+5w4rnh0hk4QIDAQABMA0GCsqGSIb3DOEBCwAA41BAQCIPhw8tATDmTSFngScknOK
        24lxmWwnh16C3JsPOsnYDmrUWFpefkTo9wxlaJHh09KY4N1vWYeo0pVsj+YmxCdRijraPhCNJ208nFteDTak3aVhwQPd6FnxI64OLHLDVMCA/g6Vo74aFrA2iIPri6XYth
        pchYVsfpejnTpRbm8G+kCWunqQ0px8Dkij++7ZMdfI2IraxkklCvubTHHOVAI9AaJX0LmW1Ab0Ceg4LggWln8fg1O/f6ndrSjzOqpXYRVV6x
        IQK9xv0moHyGP05kyWmzkt1rkH7zoNhs+oFBnFEuVooXOdl3xHoYNn0iFnOw6HOVICZcDs3U+S
      </X509Certificate>
    </X509Data>
  </KeyInfo>
  
```

5. The user can now login via SSO

