# **ZingHR - Azure AD SSO Integration with Azure AD SAML Toolkit**

## **Add Azure AD SAML Toolkit from the gallery**

To configure the integration of Azure AD SAML Toolkit into Azure AD, you need to add Azure AD SAML Toolkit from the gallery to your list of managed SaaS apps.

1. Sign in to the Azure portal using either a work or school account, or a personal Microsoft account.
2. On the left navigation pane, select the ****Azure Active Directory**** service.
3. Navigate to ****Enterprise Applications**** and then select ****All Applications****.
4. To add new application, select ****New application****.
5. In the ****Add from the gallery**** section, type ****Azure AD SAML Toolkit**** in the search box. Select ****Azure AD SAML Toolkit**** from results panel and then add the app.

## **Configure Azure AD SSO**

Follow these steps to enable Azure AD SSO in the Azure portal.

1. In the Azure portal, on the **Azure AD SAML Toolkit** application integration page, find the **Manage** section and select **single sign-on**.
2. On the **Select a single sign-on** method page, select **SAML**.
3. On the **Set up single sign-on** **with SAML** page, click the pencil icon for **Basic SAML Configuration** to edit the settings.



1. On the ****Basic SAML Configuration**** section, perform the following steps :

Note : Below mentioned URLs are **case sensitive**, Replace the **{{CompanyCode}}** placeholder with your actual company code and should be in lowercase

1. In the ****Reply URL**** text box, type the below URL :

**UAT** : <https://clientuat.zinghr.com/SAML/Pages/Callback.aspx?sub={{CompanyCode}}>

**Production** : <https://portal.zinghr.com/SAML/Pages/Callback.aspx?sub={{CompanyCode}}>

1. In the ****Sign on URL**** text box, type the URL :

**UAT** : [https://clientuat.zinghr.com/SAML/Auth/Signin/{{CompanyCode}}](https://clientuat.zinghr.com/SAML/Auth/Signin/%7B%7BCompanyCode%7D%7D)

**Production** : [https://portal.zinghr.com/SAML/Auth/Signin/{{CompanyCode}}](https://portal.zinghr.com/SAML/Auth/Signin/%7B%7BCompanyCode%7D%7D)

1. Set name if format to email address :





1. On the ****Set up single sign-on with SAML**** page, in the ****SAML Signing Certificate**** section, find ****Certificate (Base64)**** and select ****Download**** to download the certificate and save it on your computer.



1. On the ****Set up Azure AD SAML Toolkit**** section, copy the below URL(s)



1. Share downloaded **Certificate**, **Copied URL(s)** and List of **EmployeeCodes with NameIds** with **ZingHR Administrator** to configure your app and user assignment in ZingHR system.

### **Assign the Azure AD User**

In this section, you'll enable B.Simon to use Azure single sign-on by granting access to Azure AD SAML Toolkit.

1. In the Azure portal, select ****Enterprise Applications****, and then select ****All applications****.
2. In the applications list, select ****Azure AD SAML Toolkit****.
3. In the app's overview page, find the ****Manage**** section and select ****Users and groups****.
4. Select ****Add user****, then select ****Users and groups**** in the ****Add Assignment**** dialog.
5. In the ****Users and groups**** dialog, select ****the desired user**** from the Users list, then click the ****Select**** button at the bottom of the screen.
6. If you are expecting a role to be assigned to the users, you can select it from the ****Select a role**** dropdown. If no role has been set up for this app, you see "Default Access" role selected.
7. In the ****Add Assignment**** dialog, click the ****Assign**** button.

**After completing all the configuration and user mapping in Azure Active Directory and ZingHR system please use below link to login to ZingHR Portal using Azure AD credentials.**

**UAT** : [https://clientuat.zinghr.com/SAML/Auth/Signin/{{CompanyCode}}](https://clientuat.zinghr.com/SAML/Auth/Signin/%7B%7BCompanyCode%7D%7D)

**Production** : [https://portal.zinghr.com/SAML/Auth/Signin/{{CompanyCode}}](https://portal.zinghr.com/SAML/Auth/Signin/%7B%7BCompanyCode%7D%7D)

**Users can also access ZingHR portal from O365, Please refer below screenshot**

****