JIRA SAML SSO with Azure IDP Setup

Jira SAML app gives the ability to enable SAML Single Sign-On for Jira Software and Jira Service Desk. Jira Software and Jira Service Desk are compatible with all SAML Identity Providers. Here we will go through a guide to configure SAML SSO between Jira and your Identity Provider. By the end of this guide, users from your Identity Provider should be able to login and register to Jira Software and Service Desk.

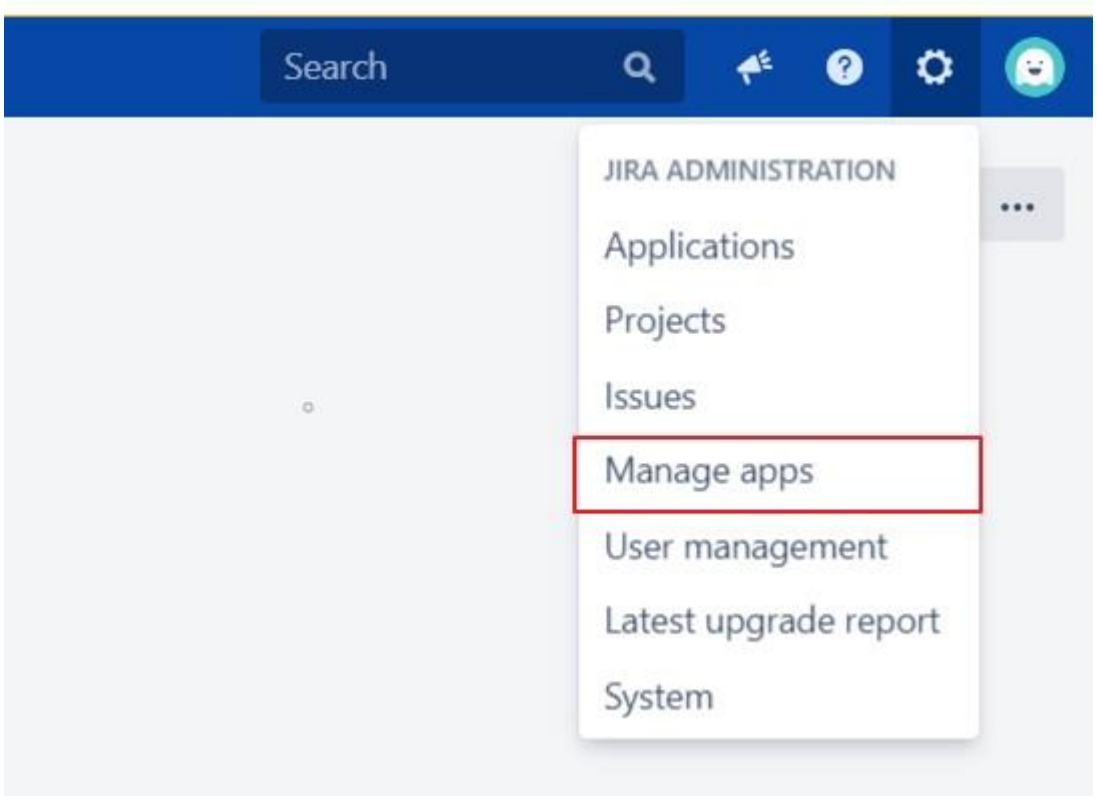
Pre-requisites

To integrate your Identity Provider(IDP) with Jira, you need the following items:

- Jira should be installed and configured.
- Jira Server is https enabled (optional).
- Admin credentials are set up in Jira.
- Valid Jira Server and Data center Licence.

Download And Installation

- Log into your Jira instance as an admin.
- Navigate to the settings menu and Click **Manage Apps**.
- Click **Find new apps** or **Find new add-ons** from the left-hand side of the page.
- Locate Jira SSO / Single Sign On, Jira SAML SSO via search.
- Click **Try free** to begin a new trial or **Buy now** to purchase a license for **Jira SSO / Single Sign On, Jira SAML SSO**.
- Enter your information and click Generate license when redirected to **MyAtlassian**.
- Click Apply license.



Step 1: Setup Azure AD as Identity Provider

Prerequisites:

Copy these values from the **Service Provider Info** tab of the SAML plugin.

- SP Entity ID
- ACS URL

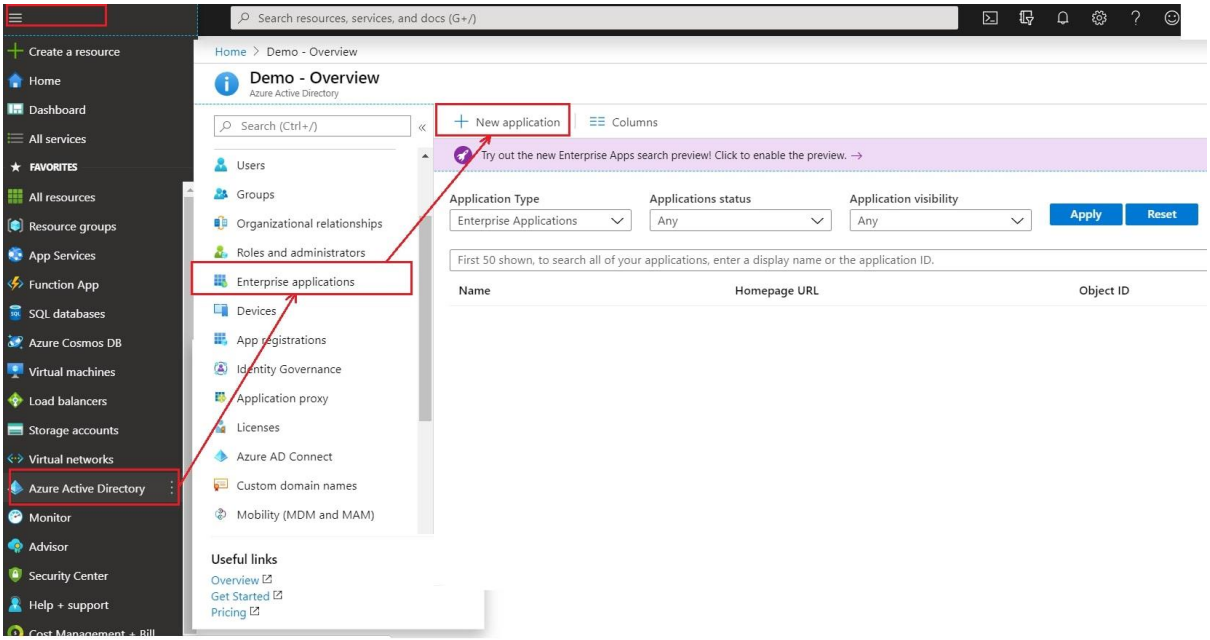
Instructions:

Note: Enterprise app configuration is the recommended option for SAML . If you do not have Azure subscription or using free account please setup **App Registration Configuration.**

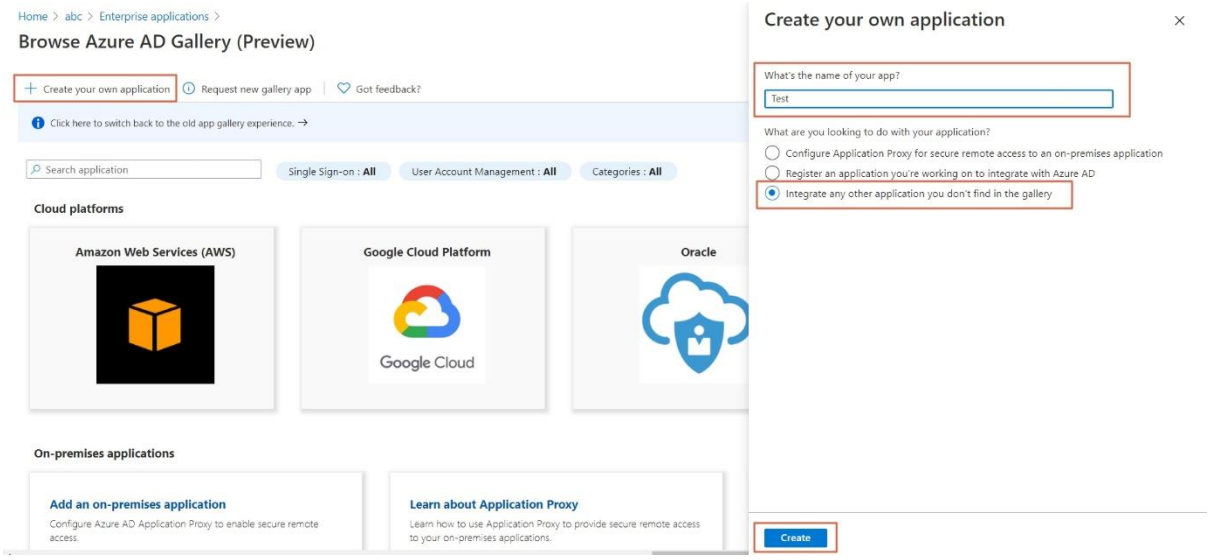
To perform **Single Logout** using Azure AD, the Atlassian instance (E.g. Jira,Confluence) must be **https enabled**.

- Azure AD setup through Enterprise Applications
- Azure AD setup through App Registrations
- Log in to **Azure AD Portal**

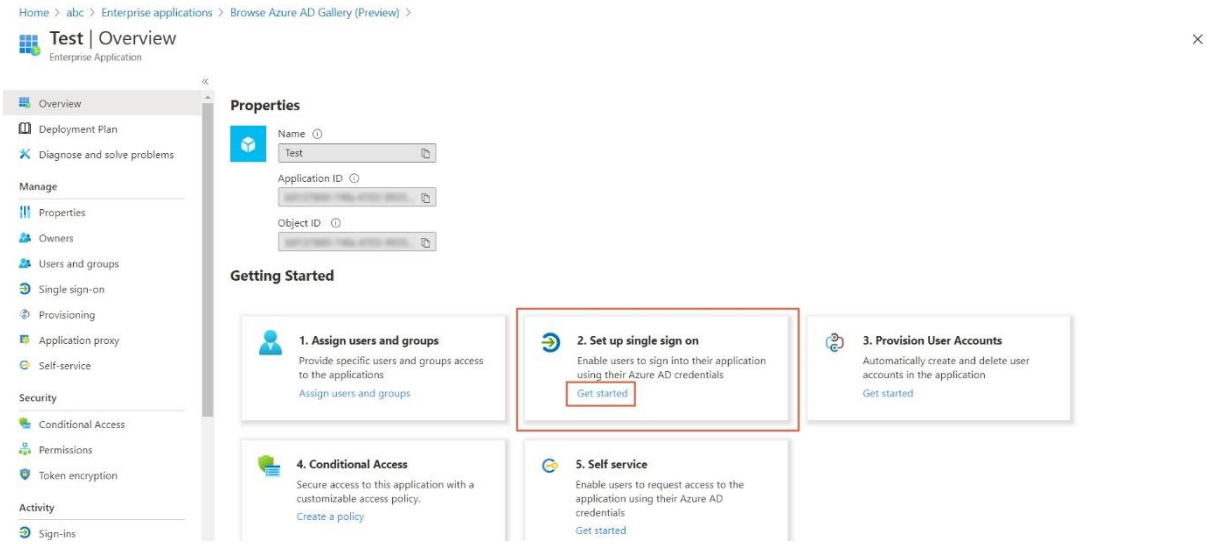
- Select ⇒ and **Azure Active Directory ⇒ Enterprise Applications**.



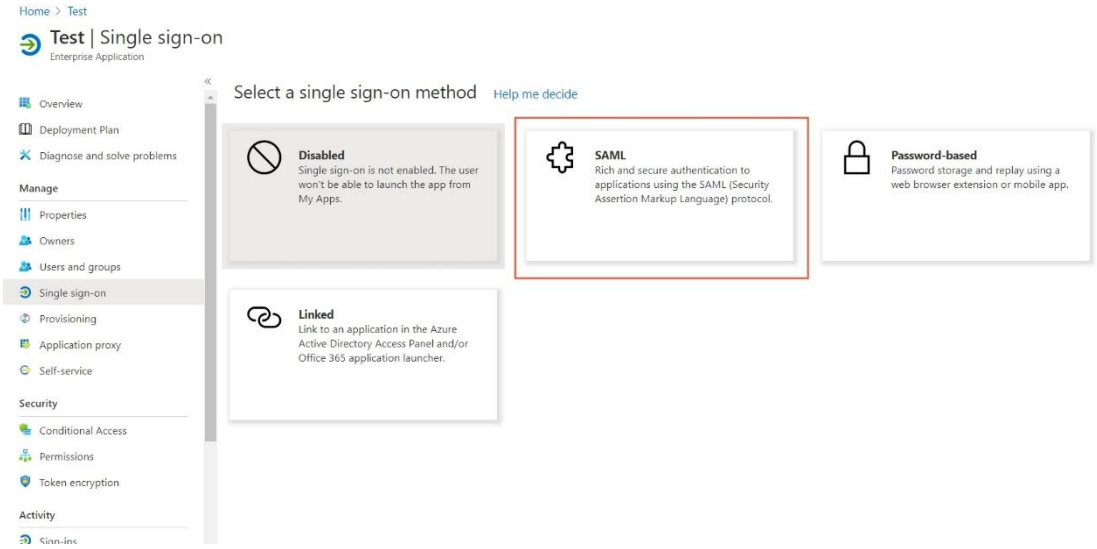
- Click on **Create your own application**. Then enter the name for your app, select the **Integrate any other application you don't find in the gallery** checkbox and click on **Create** button



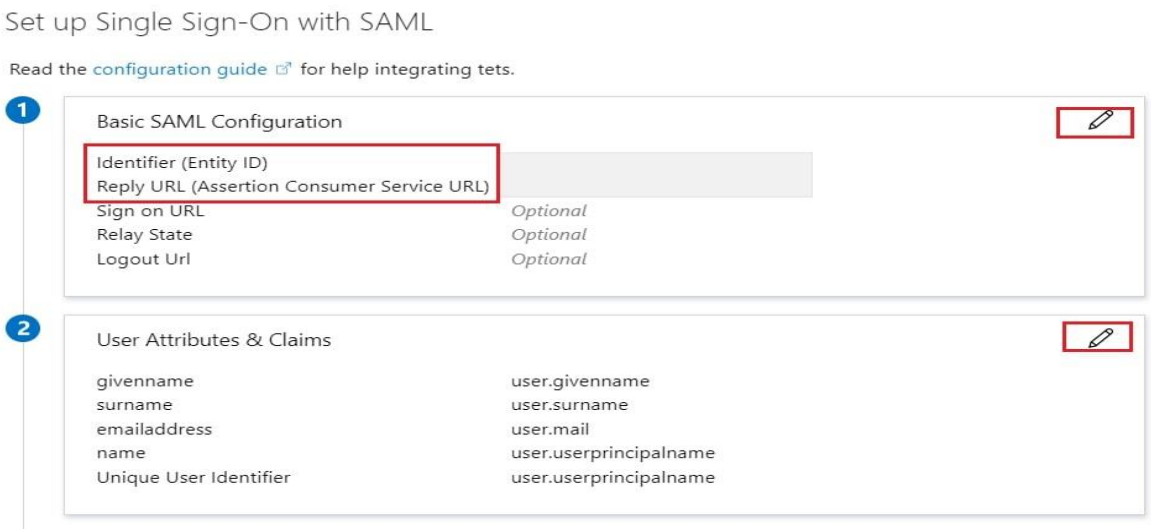
- Click on **Set up Single sign-on**.



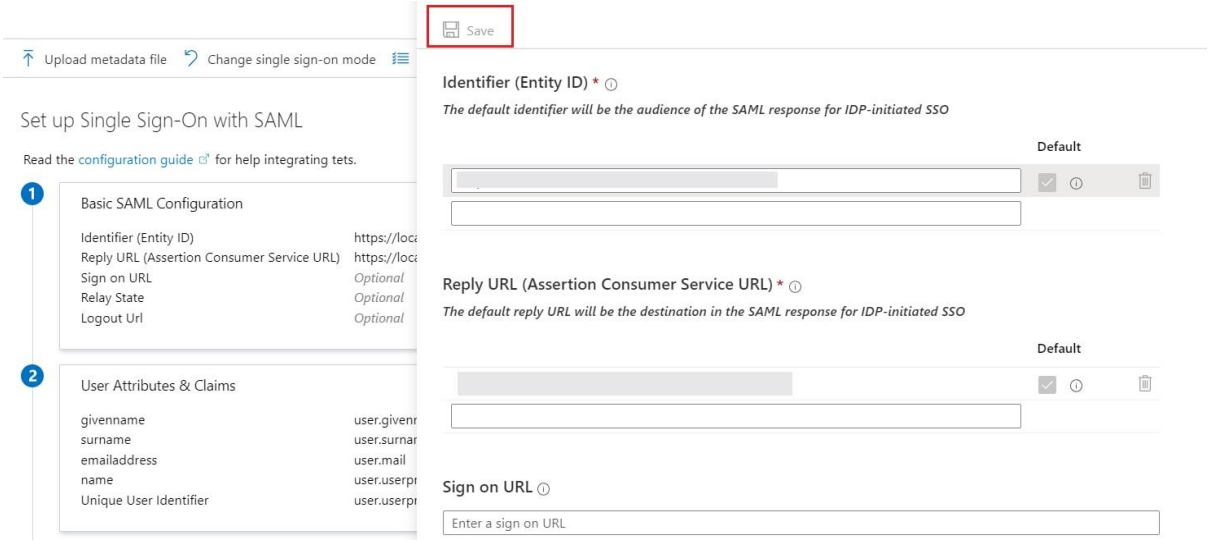
- The next screen presents the options for configuring single sign-on. Click on **SAML**.



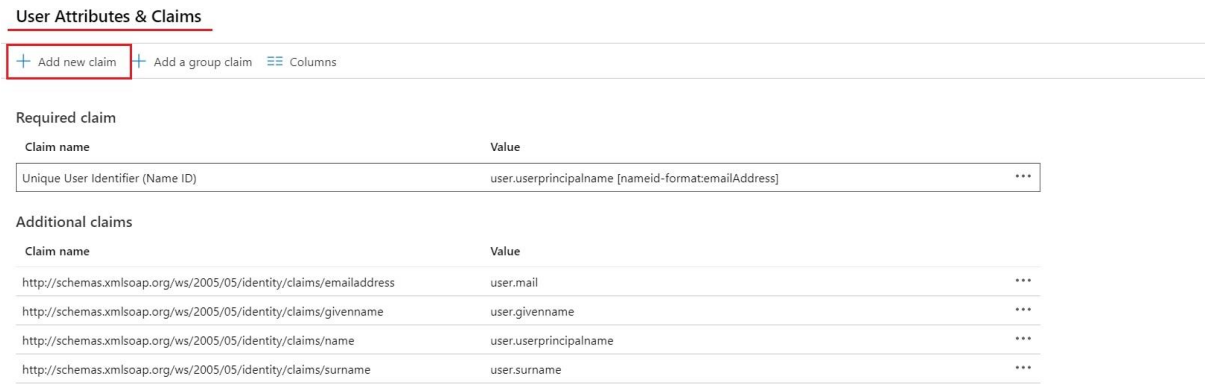
- Edit the option **1 :Basic SAML Configuration** to configure plugin endpoints.
- Enter the **SP Entity ID** for **Identifier** and the **ACS URL** for **Reply URL** from **Service Provider Info** tab of the plugin.



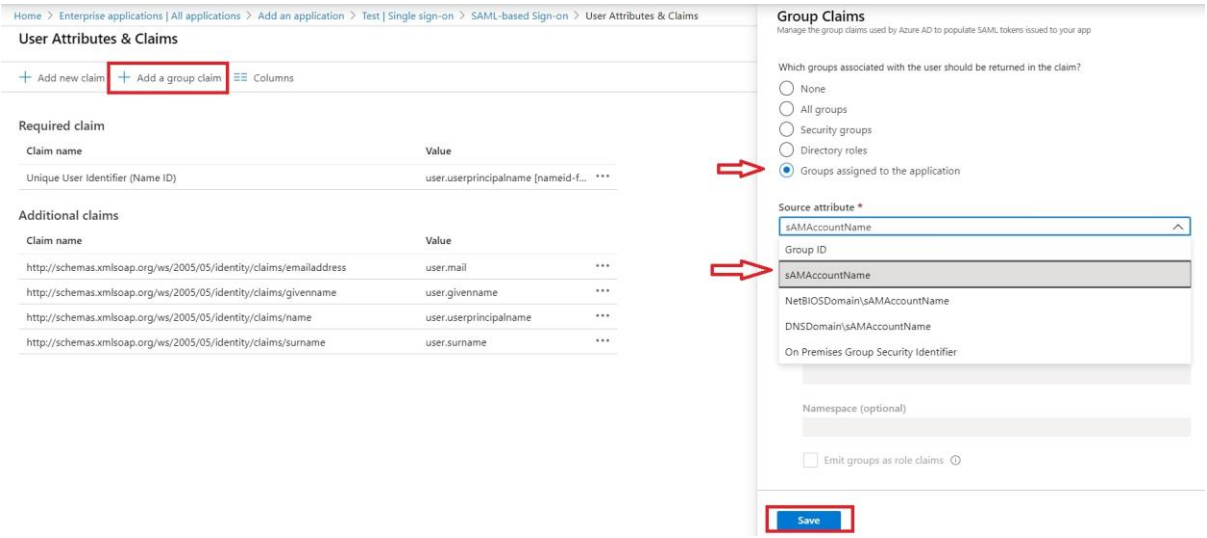
- Click on **Save** icon.



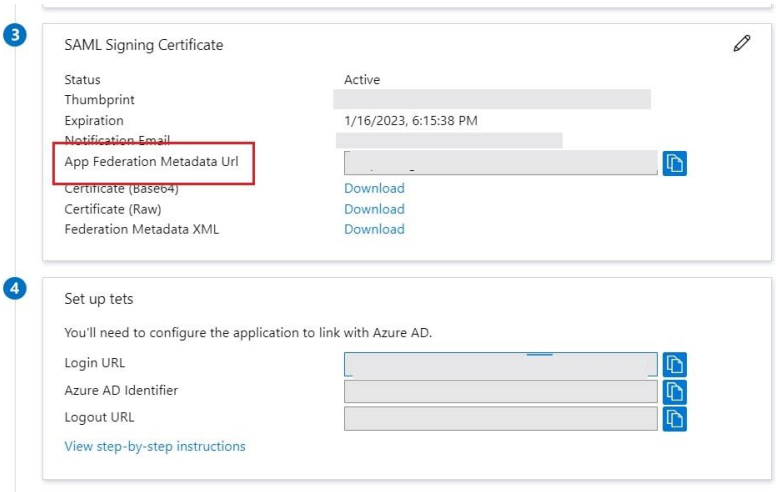
- By default, the following **Attributes** will be sent in the SAML token. You can view or edit the claims sent in the SAML token to the application under the **User Attributes & Claims** tab.
- You can add attribute using **Add new claim**



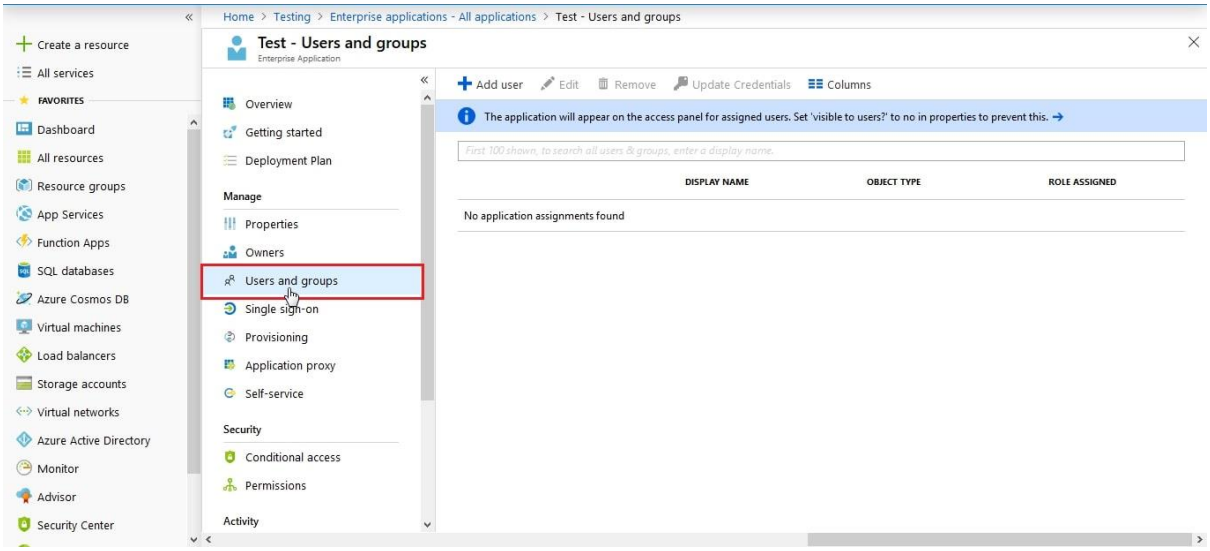
- You can add group attribute claim using **Add a group claim**



- Copy **App Federation Metadata Url** from **setup** tab.



- Click on **User and groups** from the applications left-hand navigation menu. The next screen presents the options for assigning the users/groups to the application.



Step 2: Setup Jira as Service Provider

- Configure Single Identity Provider Setup
- Configure Multiple Identity Provider(IdP) Setup

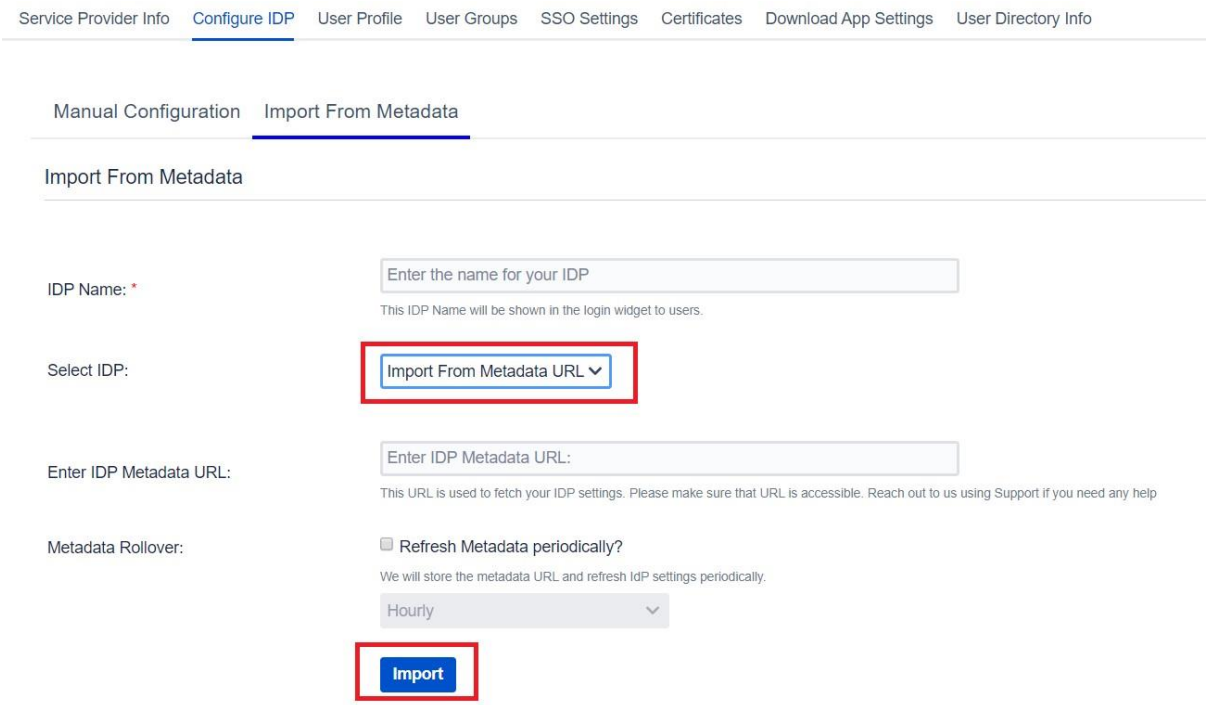
Configuring Single IDP

With the information you have been given by Your IDP team, you can configure IDP settings in 3 ways:

- By Metadata URL
- By uploading Metadata XML file
- Manual Configuration

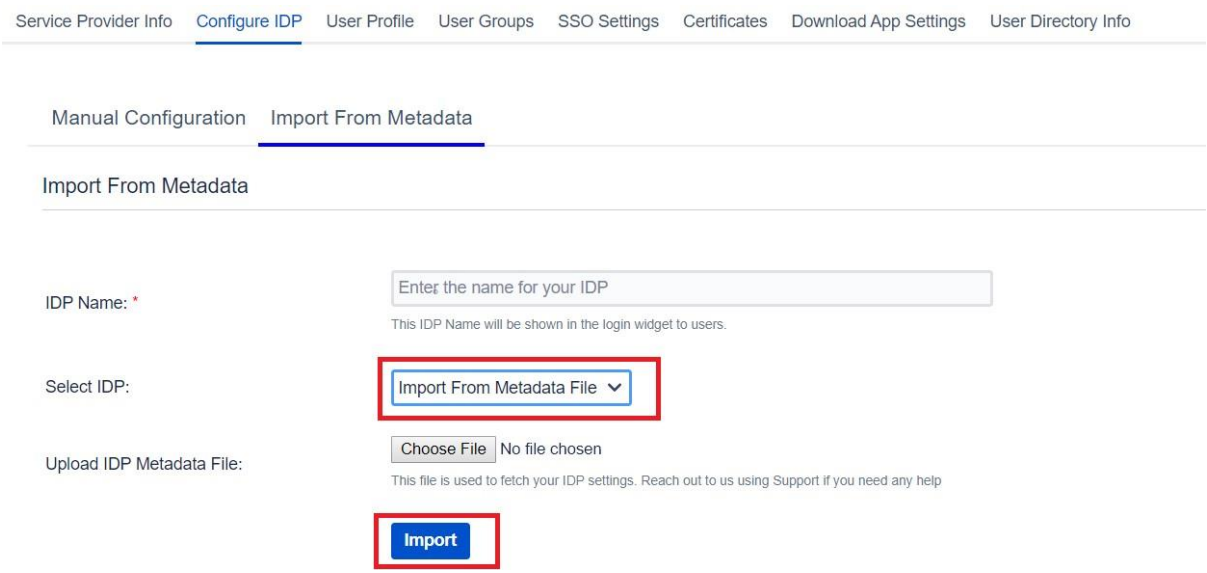
A. **By Metadata URL**

- Click on **Import from Metadata** in **Configure IDP** tab
- **Select IDP**: Import From Metadata URL
- **Enter IDP metadata URL:** Enter your metadata URL
- If your IDP changes certificates at intervals (Eg. Azure AD), you can select **Refresh metadata** periodically. Select **5 minutes** for the best results.
- Click **Import**



B. **By Uploading Metadata XML File**

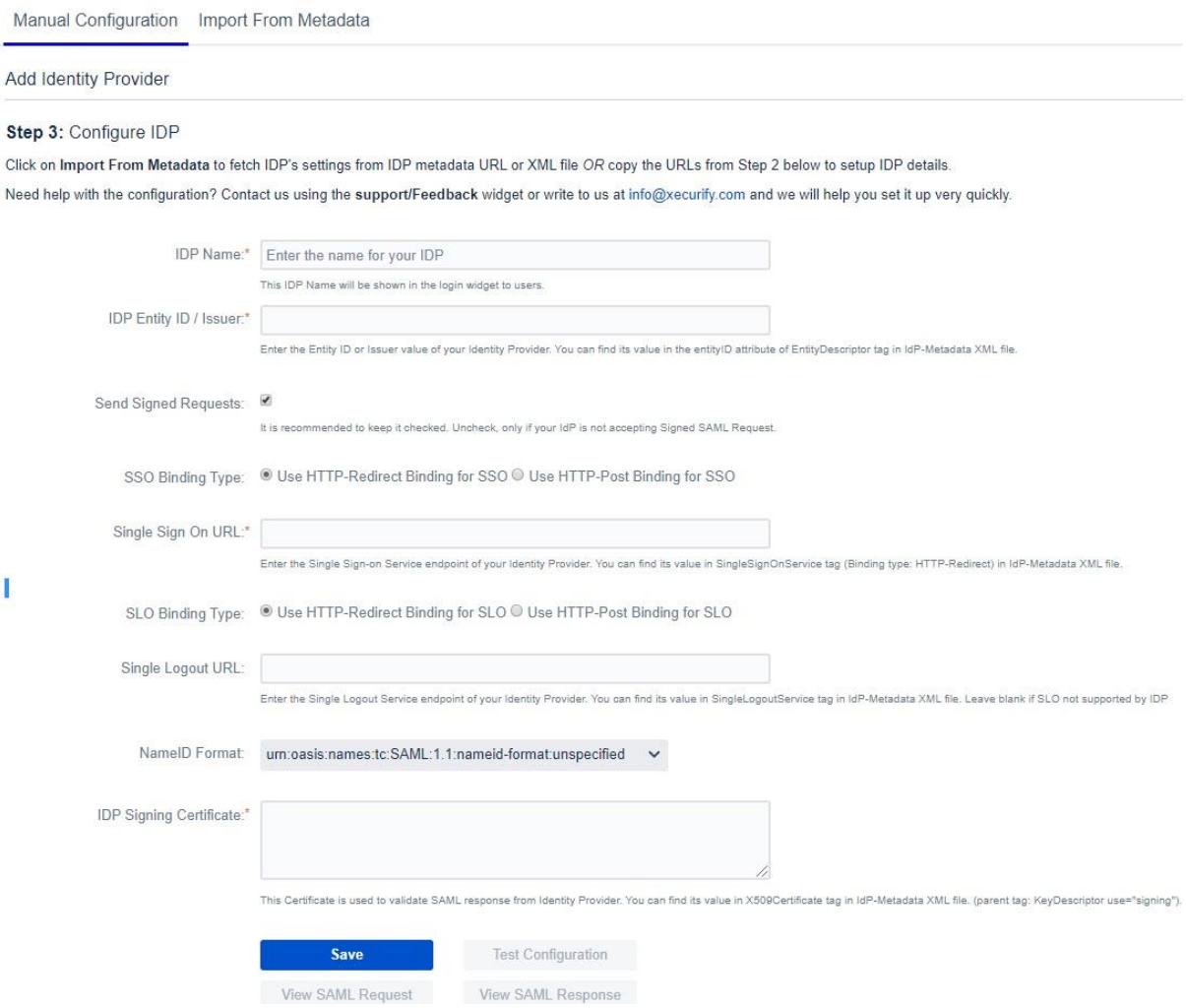
- Click on **Import from Metadata** in **Configure IDP** tab
- **Select IDP: Import from Metadata File**
- Upload metadata file
- Click **Import**



C. **Manual Configuration**

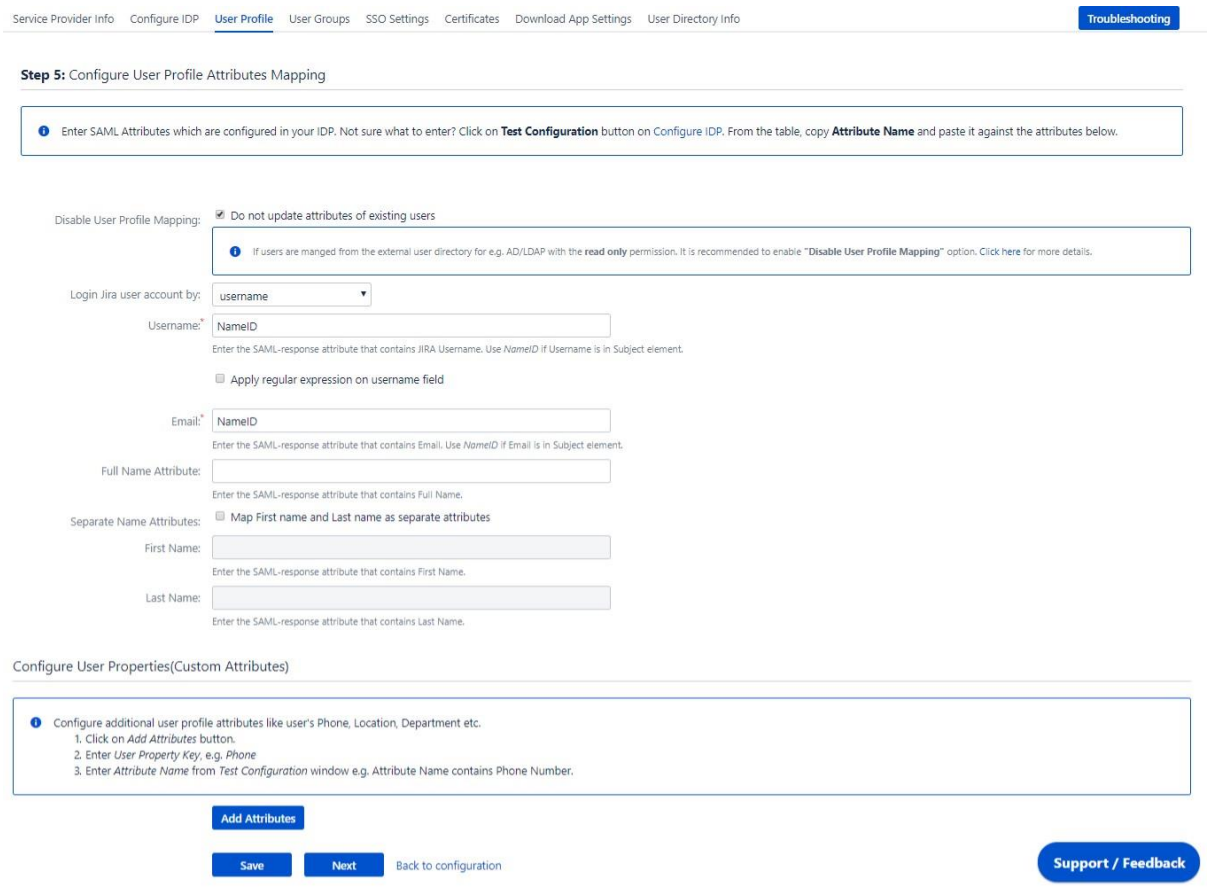
Go to **Configure IDP** tab and enter the following details

- IDP Entity ID
- Single Sign On URL
- Single Logout URL
- X.509 Certificate



Step 3: Setting up Jira user profile attributes

We will be setting up user profile attributes for Jira. If your users are stored in a directory that is **Read Only**, please check **Disable Attribute Mapping** in **User Profile** tab and follow steps given in Matching a User.



a. Finding correct attributes

- Go to **Configure IDP** tab. Scroll down and click on **Test Configuration**.
- You will see all the values returned by your IDP to Jira in a table. If you don't see value for First Name, Last Name, Email or Username, make the required settings in your IDP to return this information.
- Once you see all the values in Test Configuration, keep the window open and go to **User Profile** tab.

b. Setting profile attributes

- In this tab, fill the values by matching the name of the attribute. For instance, if the Attribute Name in the **Test Configuration** window is **NameID**,
  enter **NameID** against **Username**

- Setting up both **Username and Email** is required if you want to let users register. If you want existing users to only login, configure the attribute using which you will match the user in Jira.

c. Matching a User

When the user logs into Jira, one of the user's data/attribute coming in from the IDP is used to search the user in Jira. This is used to detect the user in Jira and log in the user to the same account.
You can configure it using steps given below:

- Go to **User Profile** tab
- Select Username or Email for **Login/Search Jira user account by**
- Enter the attribute name from IDP which corresponds to Username or Email using Finding Correct Attributes

Step 4: Assigning groups to users

We will be setting up user group attributes for Jira. If your users are stored in a directory that is **Read Only**, please check **Disable Group Mapping** in **User Groups** tab and skip to Setting default group.

a. Setting default group

- Select the users' **Default Group** in the tab **User Groups**. If no group is mapped, users are added by default to this group.
- You can enable default groups for **All Users** or **New Users** using the option.Select **None** if you don't want to assign any default group to SSO users. Using the option **Enable Default Groups for**.

b. Finding Group Attribute

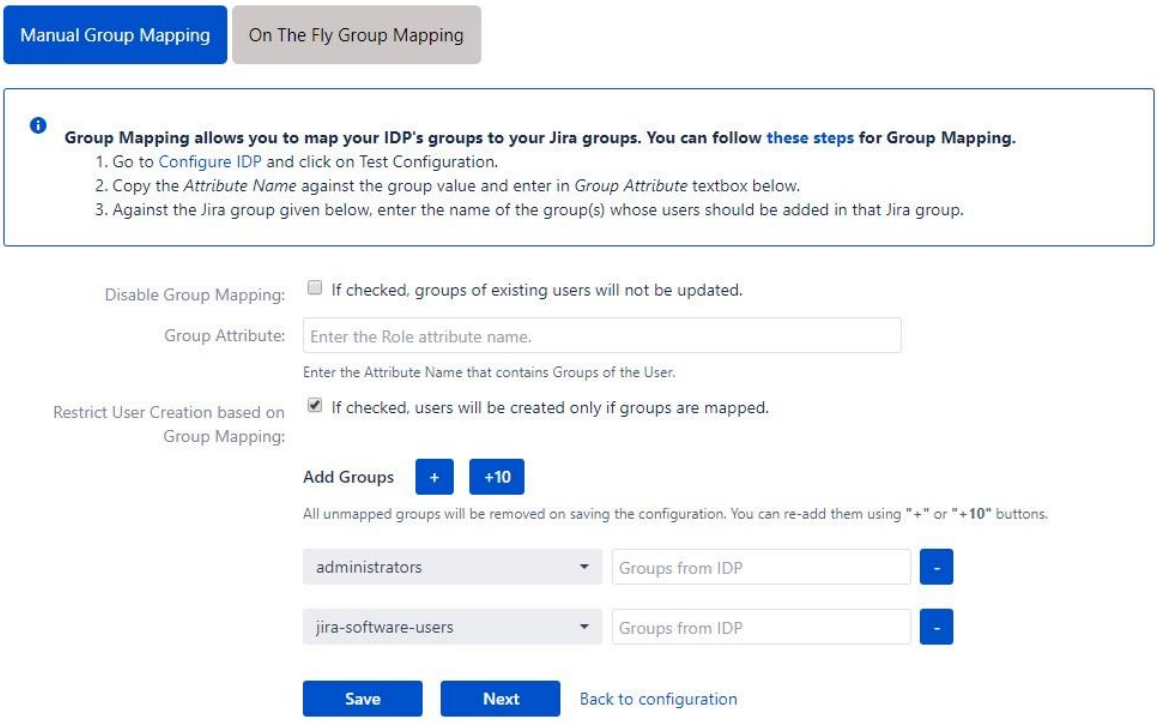
- Just like we found Attribute Name for User Profile attributes, we find group attribute.
- Go to **Configure IDP** tab. Scroll down and click on **Test Configuration**.
- You will see all the values returned by your IDP to Jira in a table. If you don't see value with groups, make the required settings in your IDP to return group names.
- Once you see all the values in Test Configuration, keep the window open and go to **User Groups** tab.
- Enter the Attribute Name of group against ***Group Attribute***.
- Check ***Disable Group Mapping*** option if you don't want to update groups of existing users.

c. Group Mapping

Group Mapping can be done in two ways:

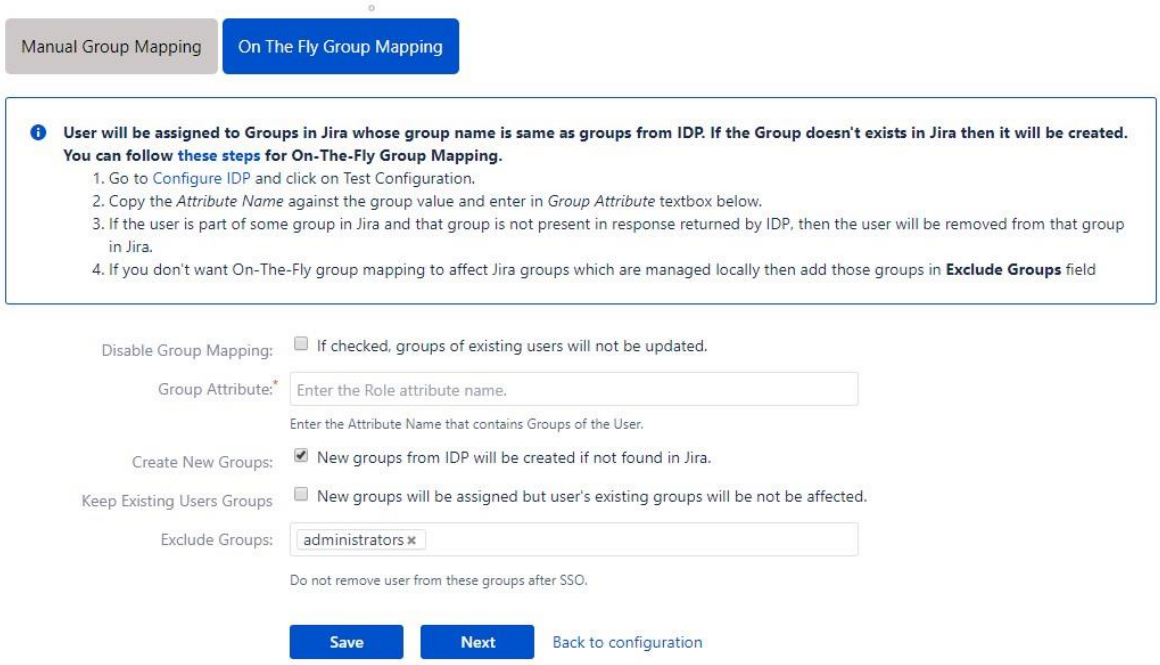
- **Manual group mapping:** If the names of groups in Jira are different than the corresponding groups in IDP, then you should use **Manual group mapping**.
- **On-The-Fly group mapping:** If the names of groups in Jira and IDP are same, you should use **On-The-Fly group mapping**.

- **I. Manual Group Mapping**
  - Check ***Restrict User Creation Based on Group Mapping*** option if you want new users to be created only if at least one of the user's IDP groups is mapped to a group in the application.
  - For mapping, first select a Jira group from the dropdown which lists all groups present in Jira and then enter the name of the IDP group to be mapped in the textbox beside
  - For example, if you want all users in 'dev' group in IDP to be added to jira-software-users, you will need to select jira-software-users from the dropdown and enter 'dev' against jira-software-users.
  - Use ***'+1'*** and ***'+10'*** buttons to add extra mapping fields.
  - Use *'-'* button next to each mapping to delete that mapping.



- **II. On-The Fly Group Mapping**
  - Check ***Create New Groups*** option if you want new groups from IDP to be created if not found in Jira.

- If the user is part of some group in Jira and that group is not present in the SAML response returned by IDP, then the user will be removed from that group in Jira.
- If you don't want **On-The-Fly group mapping** to affect Jira groups which are managed locally then add those groups in ***Exclude Groups*** field.



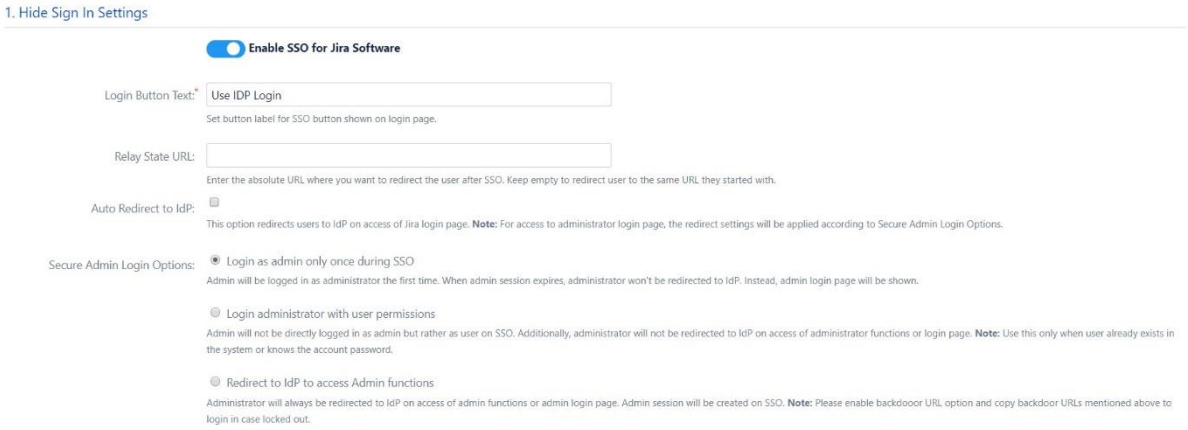
Step 5: SSO Settings

The settings in SSO Settings tab define the user experience for Single Sign On.

a. Sign In Settings

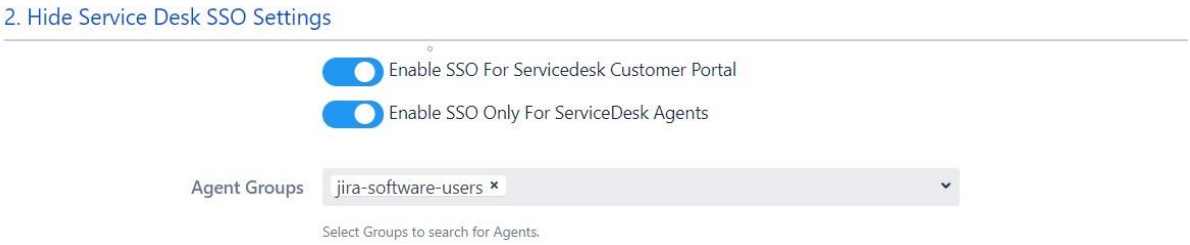
- Set **Enable SSO for Jira Software** to allow SSO for Jira Software users.
- Set button text for button on login page using **Login Button Text**
- Set redirect URL after login using **Relay State**. Keep this empty for coming back to the same page user started from
- Enable **Auto-redirect to IDP** if you want to allow users to login only using IDP. Enable **backdoor** for emergency

- Select **Secure Admin Login Options** to control admin access.



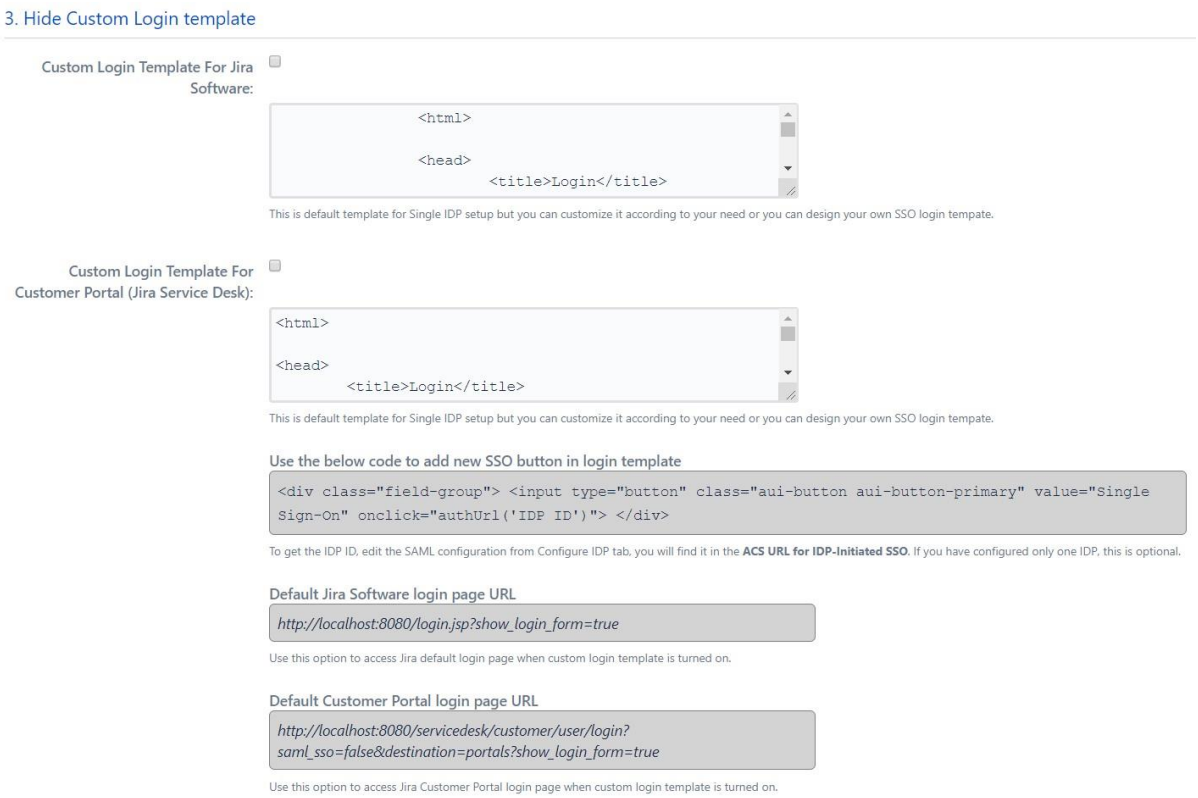
b. Service Desk SSO Settings

- Set **Enable SSO For ServiceDesk Customer Portal** to allow SSO for Service Desk user.
- Set Enable SSO Only For Agents to allow SSO only for specific set of users



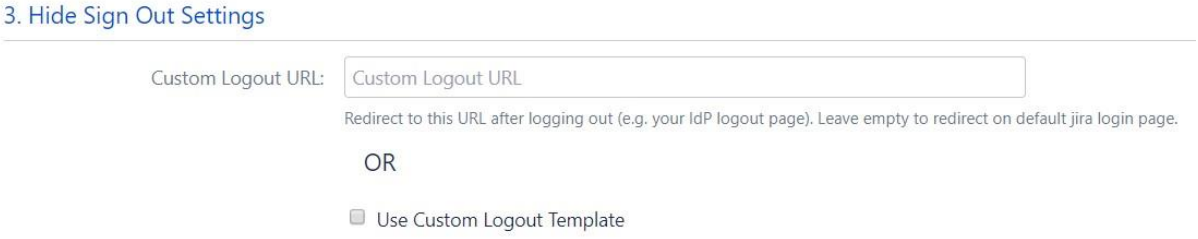
c. Custom Login Template

- Design your **own login template** that will be used to intitate SSO.



d. Sign Out Settings

- Set **Logout URL** or **Logout Template** to redirect users after logout action.

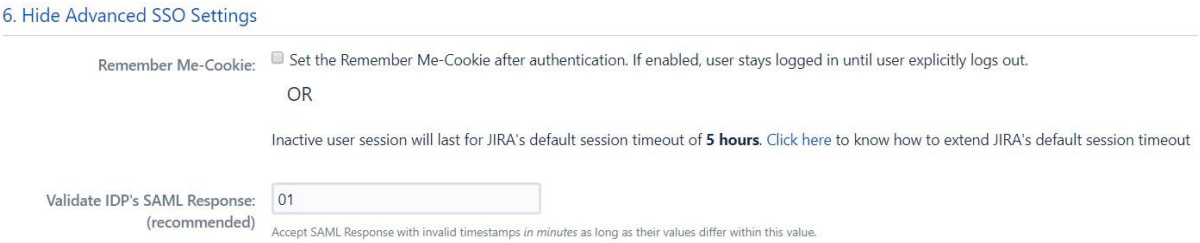


e. SSO Error Settings

- Set **error template** to redirect users to a **custom error** page instead of login page. Use this if you have **Auto-redirect to IDP** enabled.

f. Advanced settings

- **Remember Me-cookie**: If enabled, user stays logged in until user **explicitly logs out**.
- You can extend Jira default session timeout. By default it is set to 300 mins.
- **Validate IDP's SAML Response**: Configure time difference(in minute) here In case Jira server time is not in **sync with your IDP's time**.



----------THE END----------