

## 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.

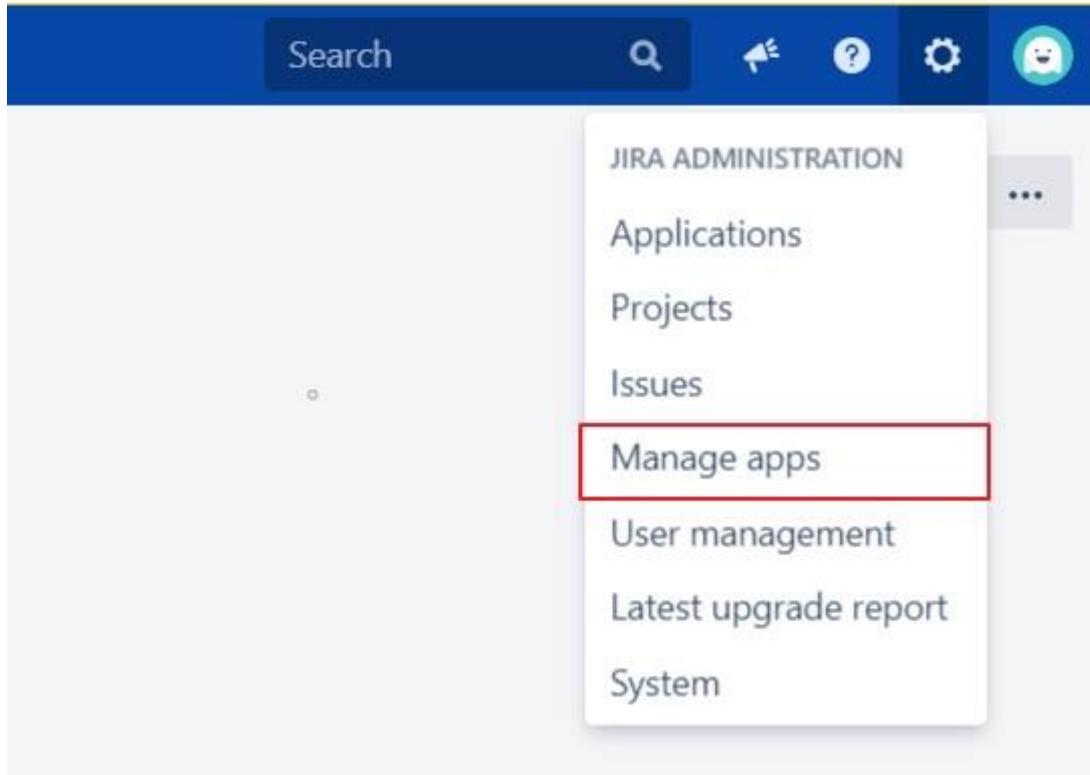
### Pre-requisites

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

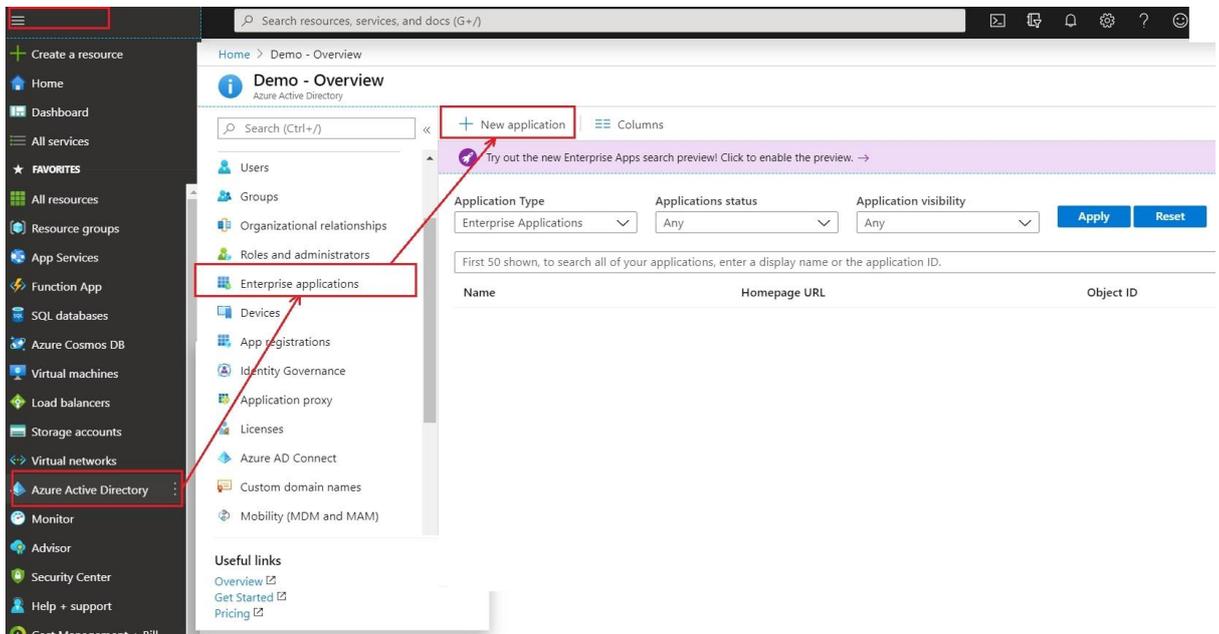
### Instructions:

**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**.

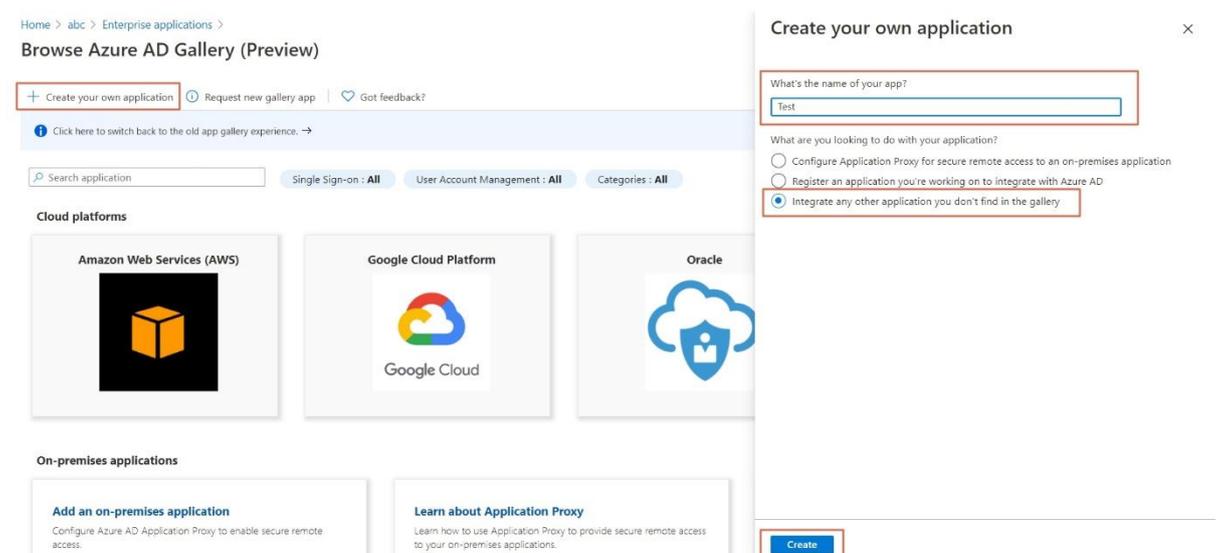
To perform **Single Logout** using Azure AD, the Atlassian instance (E.g. Jira, Confluence) must be **https enabled**.

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

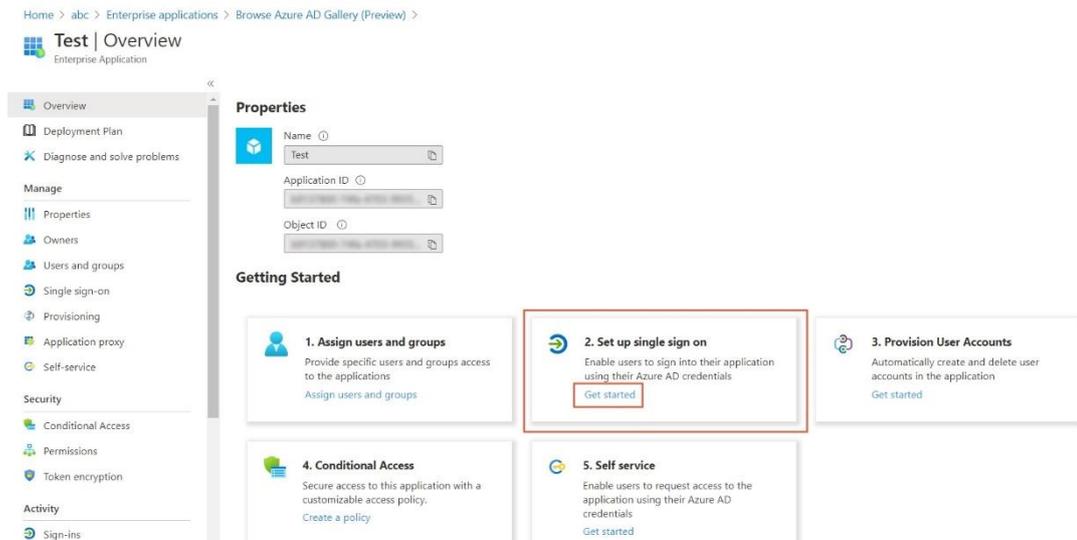
- Select ⇒ and **Azure Active Directory** ⇒ **Enterprise Applications**.



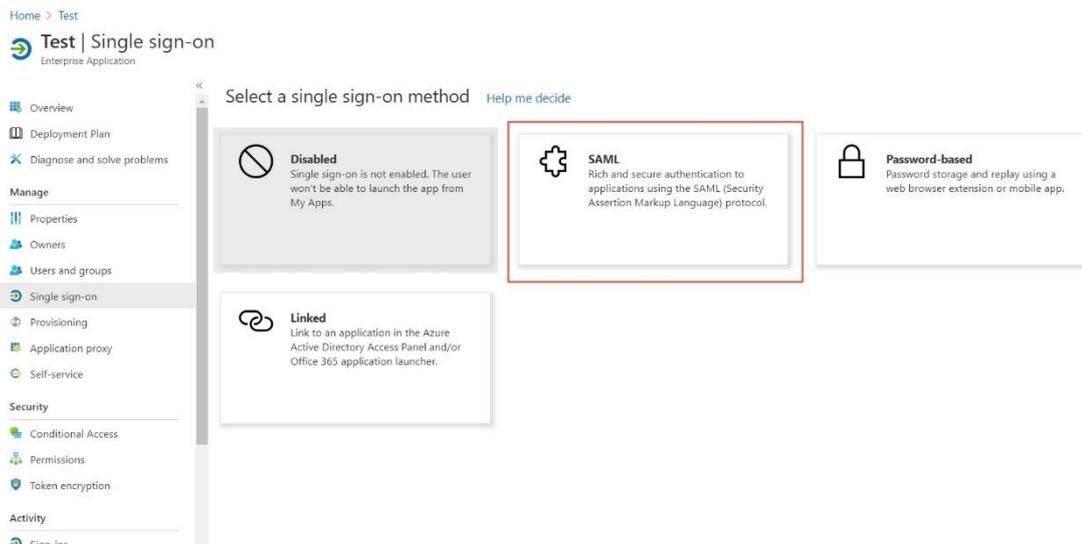
- Click on **Create your own application**. Then enter the name for your app, select the **Integrate any other application you don't find in the gallery** checkbox and click on **Create** button



- 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.

## Set up Single Sign-On with SAML

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

- ### Basic SAML Configuration

Identifier (Entity ID)	
Reply URL (Assertion Consumer Service URL)	
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional
- ### User Attributes & Claims

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

- Click on **Save** icon.

Save

Upload metadata file Change single sign-on mode

### Set up Single Sign-On with SAML

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

- #### Basic SAML Configuration

Identifier (Entity ID)	https://loc
Reply URL (Assertion Consumer Service URL)	https://loc
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional
- #### User Attributes & Claims

givenname	user.givenr
surname	user.surnar
emailaddress	user.mail
name	user.userpr
Unique User Identifier	user.userpr

Identifier (Entity ID) \* ⓘ  
The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

Reply URL (Assertion Consumer Service URL) \* ⓘ  
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

Sign on URL ⓘ  
Enter a sign on URL

- 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**

## User Attributes & Claims

+ Add new claim + Add a group claim Columns

### Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddress] ...

### Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ...

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

Home > Enterprise applications | All applications > Add an application > Test | Single sign-on > SAML-based Sign-on > User Attributes & Claims

### User Attributes & Claims

+ Add new claim + Add a group claim Columns

#### Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-f... ...

#### Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ...

#### Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

None  
 All groups  
 Security groups  
 Directory roles  
 Groups assigned to the application

Source attribute \*

sAMAccountName

Group ID

sAMAccountName

NetBIOSDomain\sAMAccountName

DNSDomain\sAMAccountName

On Premises Group Security Identifier

Namespace (optional)

Emit groups as role claims

Save

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

3 SAML Signing Certificate

Status Active

Thumbprint [redacted]

Expiration 1/16/2023, 6:15:38 PM

Notification Email [redacted]

App Federation Metadata Url [redacted]

Certificate (Base64) Download

Certificate (Raw) Download

Federation Metadata XML Download

4 Set up tests

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

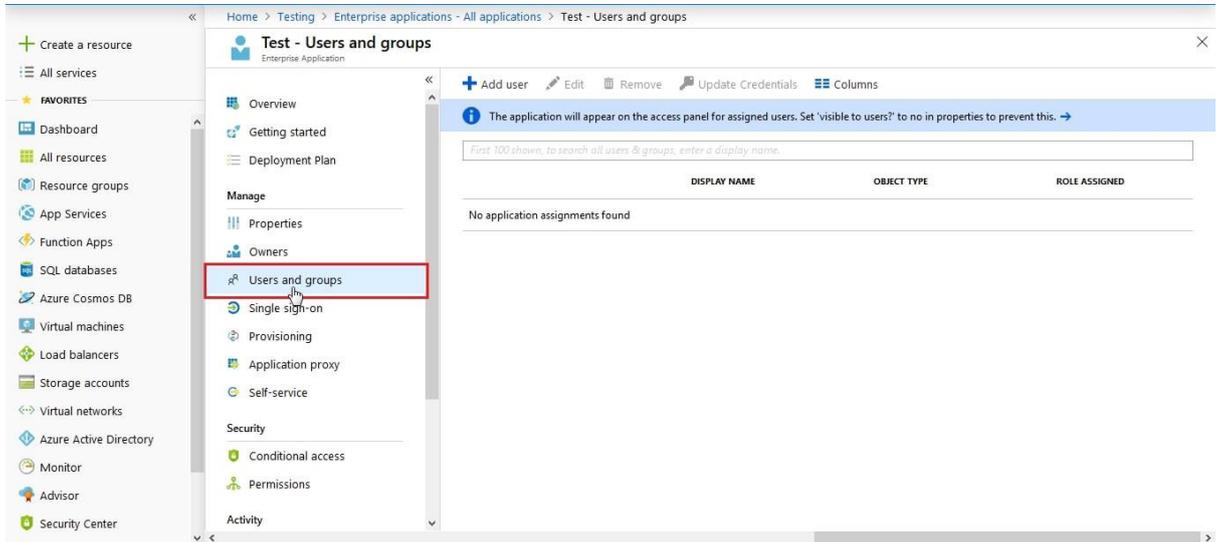
Login URL [input field]

Azure AD Identifier [input field]

Logout URL [input field]

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

- 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**

Service Provider Info Configure IDP User Profile User Groups SSO Settings Certificates Download App Settings User Directory Info

Manual Configuration Import From Metadata

Import From Metadata

IDP Name: \*   
This IDP Name will be shown in the login widget to users.

Select IDP:

Enter IDP Metadata URL:   
This URL is used to fetch your IDP settings. Please make sure that URL is accessible. Reach out to us using Support if you need any help

Metadata Rollover:  Refresh Metadata periodically?  
We will store the metadata URL and refresh IDP settings periodically.

Hourly

## 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**

### Import From Metadata

IDP Name: \*   
This IDP Name will be shown in the login widget to users.

Select IDP:  ▾

Upload IDP Metadata File:  No file chosen  
This file is used to fetch your IDP settings. Reach out to us using Support if you need any help

## 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

## Add Identity Provider

### Step 3: Configure IDP

Click on **Import From Metadata** to fetch IDP's settings from IDP metadata URL or XML file *OR* copy the URLs from Step 2 below to setup IDP details.

Need help with the configuration? Contact us using the **support/Feedback** widget or write to us at [info@xecurify.com](mailto:info@xecurify.com) and we will help you set it up very quickly.

IDP Name:\*   
This IDP Name will be shown in the login widget to users.

IDP Entity ID / Issuer:\*   
Enter the Entity ID or Issuer value of your Identity Provider. You can find its value in the entityID attribute of EntityDescriptor tag in IdP-Metadata XML file.

Send Signed Requests:   
It is recommended to keep it checked. Uncheck, only if your IdP is not accepting Signed SAML Request.

SSO Binding Type:  Use HTTP-Redirect Binding for SSO  Use HTTP-Post Binding for SSO

Single Sign On URL:\*   
Enter the Single Sign-on Service endpoint of your Identity Provider. You can find its value in SingleSignOnService tag (Binding type: HTTP-Redirect) in IdP-Metadata XML file.

SLO Binding Type:  Use HTTP-Redirect Binding for SLO  Use HTTP-Post Binding for SLO

Single Logout URL:   
Enter the Single Logout Service endpoint of your Identity Provider. You can find its value in SingleLogoutService tag in IdP-Metadata XML file. Leave blank if SLO not supported by IDP.

NameID Format:

IDP Signing Certificate:\*   
This Certificate is used to validate SAML response from Identity Provider. You can find its value in X509Certificate tag in IdP-Metadata XML file. (parent tag: KeyDescriptor use="signing").

### 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](#).

**Step 5:** Configure User Profile Attributes Mapping

Enter SAML Attributes which are configured in your IDP. Not sure what to enter? Click on **Test Configuration** button on Configure IDP. From the table, copy **Attribute Name** and paste it against the attributes below.

Disable User Profile Mapping:  Do not update attributes of existing users

If users are managed from the external user directory for e.g. AD/LDAP with the read only permission. It is recommended to enable "Disable User Profile Mapping" option. Click here for more details.

Login Jira user account by: Username: Enter the SAML-response attribute that contains JIRA Username. Use *NameID* if Username is in Subject element. Apply regular expression on username fieldEmail: Enter the SAML-response attribute that contains Email. Use *NameID* if Email is in Subject element.Full Name Attribute: 

Enter the SAML-response attribute that contains Full Name.

Separate Name Attributes:  Map First name and Last name as separate attributesFirst Name: 

Enter the SAML-response attribute that contains First Name.

Last Name: 

Enter the SAML-response attribute that contains Last Name.

## Configure User Properties(Custom Attributes)

- Configure additional user profile attributes like user's Phone, Location, Department etc.
1. Click on **Add Attributes** button.
  2. Enter **User Property Key**, e.g. *Phone*
  3. Enter **Attribute Name** from **Test Configuration** window e.g. Attribute Name contains Phone Number.

**Add Attributes****Save****Next**

Back to configuration

**Support / Feedback****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**.

## Configure User Groups Mapping

---

Disable User Creation:  If checked, New user will not be created.

---

### Default Group Configurations

Default Group:

Select Default Group(s) to assign Users.

Assign Default Group To:  New Users  All Users  None

---

### 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.

Manual Group Mapping On The Fly Group Mapping

**i** Group Mapping allows you to map your IDP's groups to your Jira groups. You can follow [these steps](#) for Group Mapping.

1. Go to Configure IDP and click on Test Configuration.
2. Copy the *Attribute Name* against the group value and enter in *Group Attribute* textbox below.
3. Against the Jira group given below, enter the name of the group(s) whose users should be added in that Jira group.

Disable Group Mapping:  If checked, groups of existing users will not be updated.

Group Attribute:   
Enter the Attribute Name that contains Groups of the User.

Restrict User Creation based on Group Mapping:  If checked, users will be created only if groups are mapped.

Add Groups + +10

All unmapped groups will be removed on saving the configuration. You can re-add them using "+" or "+10" buttons.

administrators	<input type="text" value="Groups from IDP"/>	<input type="button" value="-"/>
jira-software-users	<input type="text" value="Groups from IDP"/>	<input type="button" value="-"/>

Save Next [Back to configuration](#)

## 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.

Manual Group Mapping
On The Fly Group Mapping

**i** User will be assigned to Groups in Jira whose group name is same as groups from IDP. If the Group doesn't exists in Jira then it will be created. You can follow these steps for On-The-Fly Group Mapping.

1. Go to Configure IDP and click on Test Configuration.
2. Copy the *Attribute Name* against the group value and enter in *Group Attribute* textbox below.
3. If the user is part of some group in Jira and that group is not present in response returned by IDP, then the user will be removed from that group in Jira.
4. 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

Disable Group Mapping:  If checked, groups of existing users will not be updated.

Group Attribute:\*   
Enter the Attribute Name that contains Groups of the User.

Create New Groups:  New groups from IDP will be created if not found in Jira.

Keep Existing Users Groups  New groups will be assigned but user's existing groups will be not be affected.

Exclude Groups:

Do not remove user from these groups after SSO.

Save
Next
Back to configuration

## 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.

#### 1. Hide Sign In Settings

**Enable SSO for Jira Software**

Login Button Text:   
Set button label for SSO button shown on login page.

Relay State URL:   
Enter the absolute URL where you want to redirect the user after SSO. Keep empty to redirect user to the same URL they started with.

Auto Redirect to IdP:   
This option redirects users to IdP on access of Jira login page. **Note:** For access to administrator login page, the redirect settings will be applied according to Secure Admin Login Options.

Secure Admin Login Options:

- Login as admin only once during SSO**  
Admin will be logged in as administrator the first time. When admin session expires, administrator won't be redirected to IdP. Instead, admin login page will be shown.
- Login administrator with user permissions**  
Admin will not be directly logged in as admin but rather as user on SSO. Additionally, administrator will not be redirected to IdP on access of administrator functions or login page. **Note:** Use this only when user already exists in the system or knows the account password.
- Redirect to IdP to access Admin functions**  
Administrator will always be redirected to IdP on access of admin functions or admin login page. Admin session will be created on SSO. **Note:** Please enable backdoor URL option and copy backdoor URLs mentioned above to login in case locked out.

## 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

#### 2. Hide Service Desk SSO Settings

**Enable SSO For Servicedesk Customer Portal**

**Enable SSO Only For ServiceDesk Agents**

Agent Groups   
Select Groups to search for Agents.

## c. Custom Login Template

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

### 3. Hide Custom Login template

Custom Login Template For Jira Software:

```
<html>
<head>
<title>Login</title>
```

This is default template for Single IDP setup but you can customize it according to your need or you can design your own SSO login template.

Custom Login Template For Customer Portal (Jira Service Desk):

```
<html>
<head>
<title>Login</title>
```

This is default template for Single IDP setup but you can customize it according to your need or you can design your own SSO login template.

Use the below code to add new SSO button in login template

```
<div class="field-group"> <input type="button" class="aui-button aui-button-primary" value="Single Sign-On" onclick="authUrl('IDP ID')"> </div>
```

To get the IDP ID, edit the SAML configuration from Configure IDP tab, you will find it in the **ACS URL for IDP-Initiated SSO**. If you have configured only one IDP, this is optional.

Default Jira Software login page URL

```
http://localhost:8080/login.jsp?show_login_form=true
```

Use this option to access Jira default login page when custom login template is turned on.

Default Customer Portal login page URL

```
http://localhost:8080/serviceesk/customer/user/login?
saml_sso=false&destination=portals?show_login_form=true
```

Use this option to access Jira Customer Portal login page when custom login template is turned on.

## d. Sign Out Settings

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

### 3. Hide Sign Out Settings

Custom Logout URL:

Redirect to this URL after logging out (e.g. your IdP logout page). Leave empty to redirect on default jira login page.

OR

Use Custom Logout Template

## 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.

#### 4. Hide SSO Error Settings

---

SSO Error Message Template:  On error, redirect users to this custom error page

```
<html><head><title>SAML SSO  
Error</title>${webResourceManager.requireResource('$plugin  
nproperties.pluginkey:resources')}<meta name='decorator'  
content='atl.general'></head><body class='aui-layout
```

Define the Custom SSO error message templates. This template will be shown to the user when SSO fails.  
Use **\$baseUrl** for login page URL.

#### 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**.

#### 6. Hide Advanced SSO Settings

---

Remember Me-Cookie:  Set the Remember Me-Cookie after authentication. If enabled, user stays logged in until user explicitly logs out.

OR

Inactive user session will last for JIRA's default session timeout of **5 hours**. [Click here](#) to know how to extend JIRA's default session timeout

Validate IDP's SAML Response:  
(recommended)

Accept SAML Response with invalid timestamps *in minutes* as long as their values differ within this value.

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