SAML Single Sign On (SSO) into Confluence using Azure AD as IDP

Upgrade

Atlassian / Confluence SAML Single Sign On / AD IDPs

Version 5.X.X - 2.2.9x

You can refer the steps to configure Azure AD for Confluence SAML SSO from the video or documentation given below

Contents

- Pre-requisites
- Download And Installation
- Step 1. Setup Azure AD as IdP
- Step 2. Setup Confluence as SP
- Step 3. Test Profile
- Step 4. User Groups
- Step 5. SSO Settings
- Additional Resources

Confluence SAML app gives the ability to enable SAML Single Sign On for Confluence Software. Confluence Software is compatible with all SAML Identity Providers. Here we will go through a guide to configure Microsoft Azure Active Directory and your Identity Provider. By the end of this guide, users from your Identity Provider should be able to login and register to Confluence Software.

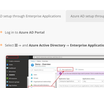
Pre-requisites:

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

- Confluence should be installed and configured.
- Admin credentials are set up in Confluence.
- Valid Confluence license is required (optional).
- Valid Confluence Server and Data center License.

Download And Installation

- Log into your Confluence instance as an admin.
- Navigate to the settings menu and Click **Manage Apps**.
- Click on **Find new apps** or **Find new add-ons** from the left hand side of the page.
- Locate Confluence SSO Single Sign On, SAML SSO via search.
- Click **Try Free** to begin a new trial or **Buy now** to purchase a license for **Confluence SSO Single Sign On, 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 use **App Registration Configuration**.

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

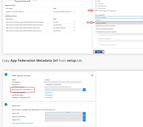
Azure AD setup through Enterprise Applications | Azure AD setup through App Registrations

- Log in to **Azure AD Portal**
- Select ☰ and **Azure Active Directory** → **Enterprise Applications**

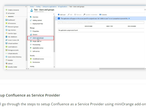
- Click on **Create your own application**. Then enter the name for your app, select the **Integrate any other application you don't find in the gallery** checkbox and click on **Create** button

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

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



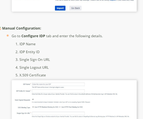
- Edit the option 1. **Basic SAML Configuration** to configure single endpoints.
- Enter the **SP Entity ID** in **Identifier** and the **ACS URL** for **Reply URL** from **Service Provider Info** tab of the plugin.



- Click on **Save** icon.

- By default, the following **Attributes** will be sent in the SAML token. You can save 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 Confluence as Service Provider

Now we will go through the steps to setup Confluence as a Service Provider using miniOrange add-on.

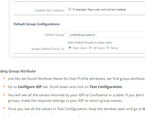
Configure Single Identity Provider (IdPs) | Configure Multiple Identity Providers (IdPs)

Configure Identity Provider

Step 1. Adding IDP settings in add-on

- With the information you have been given by your IDP, you can configure IdP settings in 3 ways.
  - By Metadata URL
  - By uploading Metadata XML file
  - Manual Configuration
- **By Metadata URL:**
  - Click on **Import from Metadata** in **Configure IDP** tab.
  - **Select IDP**: Import From Metadata URL.
  - Enter your metadata URL.

  If your IDP changes certificates at intervals(E.g. Azure AD), you can select **Refresh metadata** periodically. Select **5 minutes** for the best results.
  - Click **Import**.



- **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**.

- **Manual Configuration:**
  - Go to **Configure IDP** tab and enter the following details.
    1. IDP Name
    2. IDP Entity ID
    3. Single Sign On URL
    4. Single Logout URL
    5. X.509 Certificate

Step 3: Setting up Confluence user profile attributes

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

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 Confluence 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 mapped if you want to let users register. If you want existing users to only login, configure the attribute using which you will match user in Confluence.

c. Matching a User

When user logs into Confluence, one of the user's data/attribute coming in from the IDP is used to search the user in Confluence. This is used to detect the user in Confluence and login the user to the same account.

- Go to **User Profile** tab.
- Select Username or Email for Login/Search Confluence 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 Confluence. 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 below. **None** if you don't want to assign any default group to SSO users. Using the option **Enable Default Groups for**.

b. Finding Group Attributes

- Just like we found Attribute Name for User Profile attributes, we find group attributes.
- Go to **Configure IDP** tab. Scroll down and click on **Test Configuration**.
- You will see all the values returned by your IDP to Confluence 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.

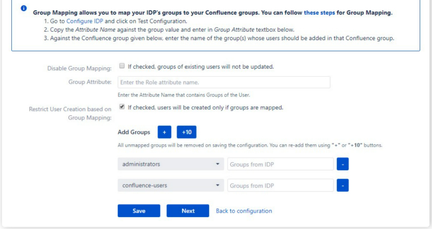
c. Group Mapping

Group Mapping can be done in two ways:

- **Manual group mapping**: if the names of groups in Confluence 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 Confluence and IDP are same, you should use On-The-Fly group mapping.

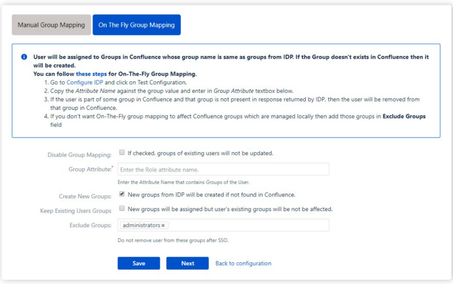
i. Manual Group Mapping

- 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 Confluence group from the dropdown which lists all groups present in Confluence 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 confluence users, you will need to select confluence-users from the dropdown and enter 'dev' against confluence-users.
- Use '+' and '-' 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 Confluence.
- If the user is part of some group in Confluence and that group is not present in the SAML response returned by IDP, then the user will be removed from that group in Confluence.
- If you don't want On-The-Fly group mapping to affect Confluence groups which are managed locally then add those groups in *Exclude Groups* field.

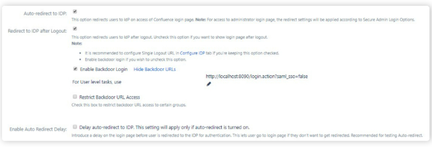


Step 5: SSO Settings

The settings in **Sign In Settings** tab define the user experience for Single Sign On

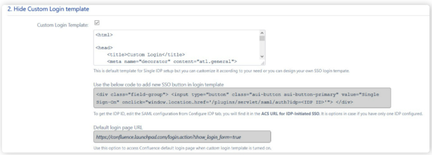
a. Sign In Settings

- 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



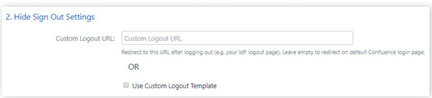
b. Custom Login Template

- Set custom login template to redirect users to a custom login page instead of Confluence default login page. This won't work if you have Auto-redirect to IDP enabled.
- Don't forget to copy default login page URL in case of emergency.



c. Sign Out Settings

- Enter a custom logout URL to redirect your users to a pre-defined logout page
- Set a custom logout template to show custom logout page to users on logout

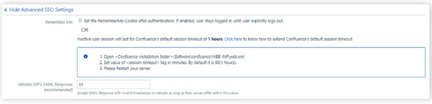


d. SSO Error Settings

- 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.

e. Advanced Settings

- **Remember Me**: If enabled, user stays logged in until user explicitly logs out.
- You can extend Confluence default session timeout using these steps. By default it is set to 60 minutes.
- **Validate IDP's SAML Response**: Configure time difference(in minute) here In case Confluence server time is not in sync with your IDP's time.



Additional Resources

- What is SAML?
- Setup Azure AD as a SAML 2.0 Identity Provider
- Attribute Mappings
- Group Mappings
- Bulk User Management
- Jenkins Single Sign On (SSO)
- SonarQube Single Sign On (SSO)
- Frequently Asked Questions (FAQs)

Our Other Apps: SAML SSO Apps | OAuth Apps | 2FA Apps | Crowd Apps | REST API Apps | Kerberos/NTLM Apps | User Sync Apps | Bitbucket Git Authentication App | Jenkins SSO | SonarQube SSO

If you are looking for anything which you cannot find, please drop us an email on info@xecurify.com

miniOrange

+1 978 658 9387 (US)
+91 97178 45846 (India)
info@xecurify.com

STAY CONNECTED

SIGN UP FREE

Product
Single Sign On
Identity Brokering
OAuth / OpenID Connect Server
Multi Factor Authentication
Adaptive Authentication
User Provisioning
Directory Services

Solutions
SAML Solutions
OAuth Solutions
2FA Solutions
Mobile Solutions
Directory Integrations
Federation Integrations
Windows Solutions
SSO Connectors
Secure Browser SSO
View All

Why miniorange
Our Success Stories
Content Library
Videos
FAQs
Forum
Company
Overview
News
Partners
Customers
Contact Us

Hello there!
Need Help? We are right here!

@ Copyright 2021 miniOrange. All Rights Reserved.