



SETUP GUIDE FOR MINIORANGE AS IdP

STEP 1: Creating App in miniOrange

- Go to miniOrange Admin console <https://auth.miniorange.com/moas> and login with your miniOrange credentials.
- From the left menu, go to **Apps > Manage Apps**
- In the right upper corner, select **Configure Apps**
- In the search apps textbox, type *Confluence (SAML)*.
- Select **Confluence (SAML)** and click on **Add App**.
- Enter the following the textboxes:

Custom Application Name	App name you like to provide. Eg Confluence
SP Entity ID or Issuer	Enter SP Entity ID / Issuer from the Configure IDP tab of the plugin
ACS URL	Enter ACS (Assertion Consumer Service) URL from the Configure IDP tab of the plugin
Single Logout URL	Enter Single Logout URL from the Configure IDP tab of the plugin

- Click on Save to add the App.
- From the Configured App list, click on the Download Certificate link in the Action against the Confluence application you just added.
- Open the downloaded certificate in Notepad and keep it handy. It will be required while configuring the SAML plugin (Step 3).

Apps > Add Application

Application Name :

*Custom Application Name :

*SP Entity ID or Issuer : ⓘ

*ACS URL : ⓘ

Single Logout URL :

Relay State :

Add Attributes :

STEP 2: Creating policy for the App

- From the left menu, go to **Policies > App Authentication Policy**
- Click on **App Policy** tab.
- From the Application dropdown, select the Custom Application Name you provided before.



- Select **DEFAULT** from the Group Name dropdown.
- Enter Policy Name you would like to provide. Eg. Confluence_Policy
- Select **Password** from the First Factor Type dropdown.
- Click on **Save** to save the policy.

App Authentication Policy

[View Policy](#) [Add Policy](#)

Step 1: Select Application

Application
Confluence

Step 2: Configure Settings

Group Name
DEFAULT

Policy Name
Confluence_Policy

First Factor Type
PASSWORD

☐ Enable Second Factor

☐ Enable Fraud Prevention

[Save](#)

STEP 3: Configuring the Plugin

In the miniOrange SAML plugin, go to Configure SP tab and configure miniOrangeldP as:

- **IDPentityID:** <https://<domain>.miniorange.com/moas>
- **Single Sign On Login URL:** <https://<domain>.miniorange.com/moas/idp/samlso>
- **Single Logout URL:** <https://<domain>.miniorange.com/moas/idp/samllogout>
- **X.509 Certificate:** Copy/Paste the entire content of the certificate file opened in Notepad.

STEP 4:

In miniOrange SAML plugin, go to **Attribute Mapping** tab. Enter the following values:

- **Username:** Name of the username attribute from IDP (Keep NameID by default)
- **Email:** Name of the email attribute from IDP (Keep NameID by default)
- **FirstName:** Name of the firstname attribute from IDP
- **LastName:** Name of the lastname attribute from IDP

Attribute Mapping

Username: *

Enter the Attribute Name that contains Confluence Username. Use *NameID* if Username is in Subject element.

Email: *

Enter the Attribute Name that contains Email. Use *NameID* if Email is in Subject element.

Full Name Attribute:

Enter the Attribute Name that contains Full Name.

Separate Name
Attributes:☐

(Select this if your IDP is sending First name and Last name as separate attributes.)

First Name:

Enter the Attribute Name that contains First Name.

Last Name:

Enter the Attribute Name that contains Last Name.

STEP 5:

Go to **Role Mapping** tab. Enter the following values:

- **Role Mapping:** Name of the Role attribute from IDP

You can check the **Test Configuration Results** to get a better idea as to which values to map here.

Under the Role Mapping Section configure which GROUP value coming in the SAML response needs to be mapped to which role. The Group value coming in the SAML response will be mapped to the Role assigned here and the user will be assigned that role.

Role Mapping

Role Attribute:

Enter the Attribute Name that contains Roles of the User.

Create Users: ☐ If checked, Users will be created only if roles are mapped.

Default Group:

Select Default Group to assign to new Users.

confluence-administrators:

confluence-users:

Note: Enter semi-colon separated list of role values in the textbox.

Save

STEP 6:

Go to **Sign In Settings** tab. Enable auto-redirect to IDP using **Disable Confluence login** option.

Sign In Settings

Login Button Text:

Disable Confluence login: ☒

Enable backdoor: ☒ Use `http://localhost:8091/login.action?saml_sso=false`
For administrative tasks use `http://localhost:8091/authenticate.action?saml_sso=false`

Save