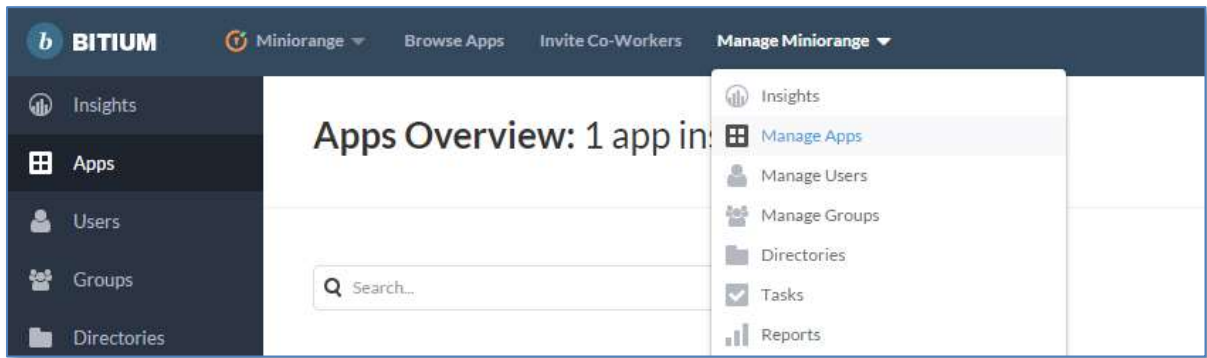




SETUP GUIDE FOR Bitium AS IDP

STEP 1:

- Log into Bitium Admin Portal.
- Once you have logged into your Bitium Admin portal, click on the Manage button in the top nav bar for your organization, and then click on Manage Apps.



- In the top right corner, click on Add More Apps. You'll see a search box, so search for Confluence, and add the app to your Bitium account.
- Here we'll start configuring SSO. First, select a name for your page, then select SAML Authentication from the dropdown menu. Once you're done, click on Install App.

- On the next screen, click on Configure Single Sign-On.

Secure Note


Bookmarks

Single Sign-On

Select a Single Sign-On Provider

To set up Bitium to use an alternate sign on method for this application, select it below.

SAML Authentication




☐ Use a 3rd party identity provider (IdP)

SAML URL

This is the URL where Bitium will send SAML requests for Jira On-Prem

Copy the values below into the appropriate places in the SAML configuration section of Confluence

Entity ID 

- Here, we'll exchange a few values between Bitium and Confluence.

SAML URL	Copy/Paste ACS (Assertion Consumer Service) URL from Step1 of the plugin under Configure IDP Tab
----------	---

- Click on **Save**.

STEP 2

- Copy the following URL/Endpoints. These will be required while configuring the plugin.

Copy the X.509 Certificate textarea value and keep it handy.

[illegible]

- Now, assign the Confluence app to your users in the Apps Overview section.
- Go to **Configure SP Tab** in **miniOrange SAML Plugin** and enter the following details:

IDP Entity ID	Entity ID from the Single Sign On tab in Bitium
Single Sign On URL	Login URL from the Single Sign On tab in Bitium
Single Logout URL	Logout URL from the Single Sign Ontab in Bitium
X.509 Certificate	Paste the X.509 Certificate value from Single Sign On tab in Bitium

STEP 3:

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 4:

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.



Account Configure IDP Configure SP Attribute Mapping Role Mapping Sign In Settings Certificates Support

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 5:

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

Account Configure IDP Configure SP Attribute Mapping Role Mapping Sign In Settings Certificates Support

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