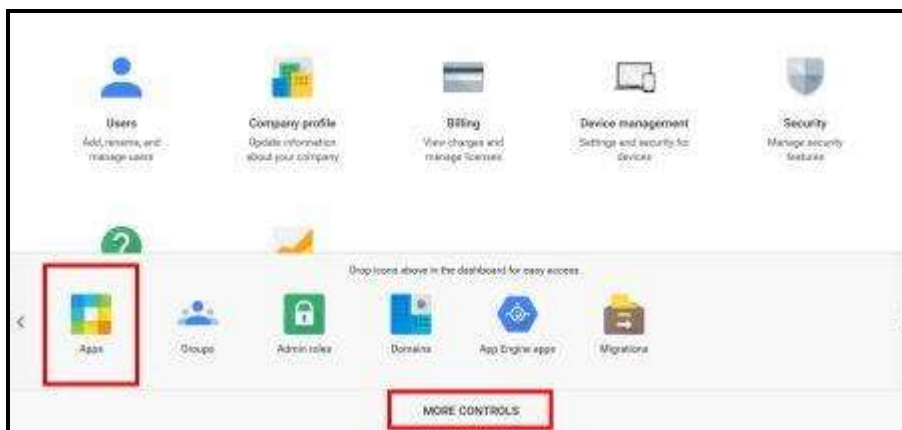




## SETUP GUIDE FOR GOOGLE APPS AS IdP

### STEP 1:

- Go to <https://admin.google.com> and login to your Google Apps Administrator account.
- On the Admin Home, select **More Controls** Apps.



- In the App Settings, select **SAML** apps.
- Click on the "+" button at the bottom right corner to create a new SAML app.
- Now select **SETUP MY OWN CUSTOM APP** from the popup.
- On the next screen, note down the SSO URL, Entity ID URLs and download the certificate. These will be required while configuring the Plugin.
- Once you have noted down the URLs and downloaded the certificate, click on **Next**.
- Enter the Application Name and Description. Click on **Next**.
- Configure the following things on the next screen:

<b>ACS URL</b>	<b>ACS (Assertion Consumer Service) URL</b> from Step1 of the plugin under Configure IDP Tab.
<b>Entity ID</b>	<b>SP-EntityID / Issuer</b> from Step1 of the plugin under Identity Configure IDP.
<b>Signed Response</b>	Checked
<b>Name ID</b>	Select Basic Information from the first dropdown. Then Primary Email from the second dropdown.

Step 4 of 5

## Service Provider Details

Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.

ACS URL \*

Entity ID \*

Start URL

Signed Response ☒

Name ID Basic Information Primary Email

PREVIOUS CANCEL NEXT

- Click on **Next**. Then click on **Finish**.

## STEP 2:

- Now go to **SAML Apps** again. Click on the menu link corresponding to your app (See the screenshot). Then select **ON for everyone**.



- From the popup, Click on **TURN ON FOR EVERYONE**.

## STEP 3:

- Go to **Configure SP** Tab in **miniOrange SAML Plugin** and enter the following details:

IDP Entity ID	The Entity ID that you noted down while configuring the Confluence site in Google Apps.
Single Sign On URL	The SSO URL that you noted down while configuring the Confluence site in Google Apps.
Single Logout URL	The Logout URL that you noted down while configuring the Confluence site in Google Apps.
X.509 Certificate	Open the downloaded certificate in the Notepad. Copy/paste the entire content of the file here.



#### **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

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

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