



SETUP GUIDE FOR SALESFORCE AS IdP

STEP 1: Log into salesforce and go to Setup.

STEP 2: From the left pane, select **App Setup » Create » Apps**

STEP 3: Under **Connected Apps**, select **New**

STEP 4: Enter Connected App Name, API Name and Contact Email

Basic Information

Connected App Name:

API Name:

Contact Email:

Contact Phone:

Logo Image URL:
[Upload logo image](#) or [Choose one of our sample logos](#)

Icon URL:
[Choose one of our sample logos](#)

Info URL:

Description:

▼ API (Enable OAuth Settings)

Enable OAuth Settings: ☐

▼ Web App Settings

Start URL:

Enable SAML: ☐

STEP 5: Under **Web App Settings**, check the **Enable SAML** checkbox and enter the following values:

Entity ID	SP-EntityID / Issuer from Step1 of the plugin under Configure IDP Tab.
ACS URL	ACS (AssertionConsumerService) URL from Step1 of the plugin under Configure IDP Tab.
Subject Type	Username
Name ID Format	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

▼ Web App Settings

Start URL:

Enable SAML: ☒

Entity ID:

ACS URL:

Subject Type:

Name ID Format:

Issuer:

Verify Request Signatures: ☐

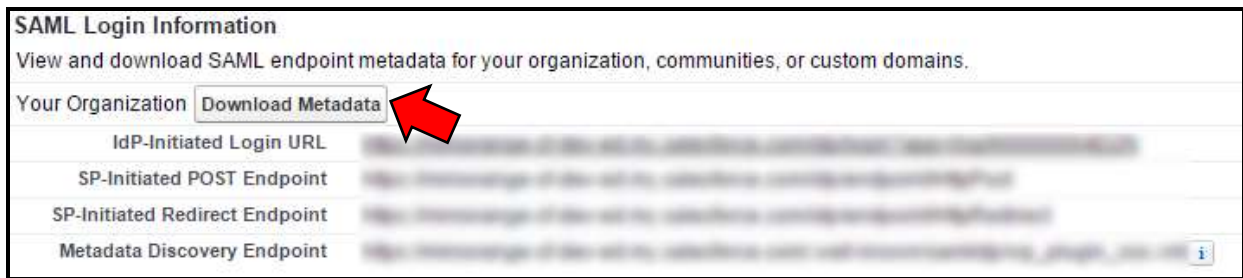
Encrypt SAML Response: ☐

STEP 6:

- Now from left pane, under **Administration Setup**, select **Manage Apps » Connected Apps**
- Click on the App you just created.
- Under **Manage Profiles**, Select the profiles you want to give access to login through this app.

STEP 7:

- Under **SAML Login Information**, click on **Download Metadata**.
- Open the downloaded file in some browser like chrome, firefox, IE
- Search for "**ds:X509Certificate**" tab and copy the entire string under this tag. String would be like this:
"MII...."
- Keep this certificate value handy for next steps



STEP 8:

In miniOrange SAML plugin, go to **Configure SP** tab. Enter the following values:

- **IDP Entity ID:** https://<your domain>.my.salesforce.com
- **Single Sign On URL:** https://<your domain>.my.salesforce.com /idp/endpoint/HttpRedirect
- **Single Logout URL:** https://<your domain>.my.salesforce.com /
- **X.509 Certificate:** Paste the certificate value you copied from the Metadata file.

STEP 9:

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 10:

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 11:

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