

SETUP GUIDE FOR CENTRIFY AS IdP

STEP 1:

- Log into Centrify as an Administrator and go to **Apps** from the NavBar.
- Click on **Add Web Apps**

STEP 2:

- In the pop-up, click on **Custom** tab and then click on the **Add** button next to SAML.



- In the new SAML App that you created under **Application Settings** section enter **Assertion Consumer Service URL** as provided in the Step 1 of the plugin under Configure IDP tab.

Application Settings [Learn more](#)

Service Provider Info [Upload SP Metadata](#)

Assertion Consumer Service URL ⓘ

Issuer ⓘ

☐ **Encrypt Assertion** ⓘ

Encryption Certificate:

[Save](#) [Cancel](#)

- Under **User Access** section select roles that can access this app:
- Under **Advanced** section pass the following parameters to the functions in the code:



setAudience()	SP-EntityID / Issuer from Step1 of the plugin under Configure IDP Tab. E.g: <code>setAudience('https://example.com/wp-content/plugins/miniorange-saml-20-single-sign-on/')</code>
setRecipient()	Recipient URL from Step1 of the plugin under Configure IDP Tab. E.g: <code>setRecipient('https://example.com/')</code>
setHttpDestination()	Destination URL from Step1 of the plugin under Configure IDP Tab. E.g: <code>setHttpDestination('https://example.com/')</code>
setRelayState()	Default Relay State from Step1 of the plugin under Configure IDP Tab. E.g: <code>setRelayState('https://example.com/')</code>

NOTE: Please do **NOT** change any other function calls.

Application Settings

Description

User Access

Policy

Account Mapping

Advanced

App Gateway

Changelog

Workflow

Advanced [Learn more](#)

Reset Script

Test

Script to generate a SAML assertion for this application

```
1  setVersion('2');
2  setIssuer(Issuer);
3  setSubjectName(LoginUser.Username);
4  setAudience('https://example.com/wp-content/plugins/miniorange-saml-20-single-sign-on/');
5  setRecipient('https://example.com/');
6  setSignatureType('Response');
7  setServiceUrl(ServiceUrl);
8  setHttpDestination('https://example.com/');
9
10 //setRelayState('/myapps-relay-state');
11 //setAttribute('Full Name', LoginUser.Get('cn'));
12 //setAttribute('Email', LoginUser.Get('mail'));
13 //setAttributeArray('Groups', LoginUser.GroupNames);
14 //setFilteredAttributeArray('Groups', LoginUser.GroupNames, <reg-exp>);
15 //var mvArray = ["mvAttribute1"."mvAttribute2"];
```

Save

Cancel

STEP 3

- Under **Application Settings** section scroll down to **Identity Provider Info**. Keep this information handy for configuring the plugin.
- Click on **Download Signing Certificate** to download the Signing certificate.
- Go to **Configure SP** Tab in **miniOrange SAML Plugin** and enter the following details:

IDP Entity ID	Issuer from Identity Provider Info in your Centrify SAML App
Single Sign On URL	Identity Provider Sign-in URL from Identity Provider Info in your Centrify SAML APP.
Single Logout URL	Identity Provider Logout URL from Identity Provider Info in your Centrify SAML APP.
X.509 Certificate	Open the .cer certificate file in notepad and copy/paste the entire content of the file.



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:^{*}

username

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

Email:^{*}

NameID

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.

Save

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