



SETUP GUIDE FOR ONELOGIN AS IdP

STEP 1:

- Log into OneLogin as an Administrator and go to **Apps > Add Apps** from the NavBar.
- In the search box, type **SAML Test Connector (SP)** and click on the App to add it.
- Enter the display name and click **Save**.
- After saving, go to **Configuration** tab and enter the following:

Audience	Audience URI from Step1 of the plugin under Configure IDP Tab.
Recipient	Recipient URL from Step1 of the plugin under Configure IDP Tab.
ACS (Consumer) URL Validator	ACS (AssertionConsumerService) URL from Step1 of the plugin under Configure IDP Tab.
ACS (Consumer) URL	ACS (AssertionConsumerService) URL from Step1 of the plugin under Configure IDP Tab.
Single Logout URL	Single Logout URL from Step1 of the plugin under Configure IDP Tab.

- Click on **Save**.

STEP 2

- Go to **SSO** tab. Note down the URL/Endpoints. These will be required while configuring the plugin.

- Click on View Details in X.509 Certificate heading. Copy the X.509 Certificate textarea value and keep it handy.

The screenshot shows the miniOrange SAML configuration interface. At the top, the 'Key length' is set to '2048-bit'. Below this, the 'SHA fingerprint' section shows a dropdown menu set to 'SHA1' and a fingerprint value: '3C:9A:9F:77:70:F8:56:4A:9C:61:B8:E9:7D:E5:BA:23:3E1'. The 'X.509 Certificate' section is highlighted with a red box. It contains a text area with the following text:


```
-----BEGIN CERTIFICATE-----
MIIEHTCCAwIqAwIBAgIUHnn30sCIIOore7z3XY1dHxG1yWwQYJkoZihvcNAQEF
BQAwIjELMAkGA1UEBhMCVVMxEzARBghNVBAQhCm1pbn1PcmFuZ2UxFTATBgNVBAQh
DE9uZUxvZ21uIE1kUDEwB0GA1UEAwkT251TG9naW4gQXNja3VudCA3Mzc8MDAe
Fw0xITEyMDgwMTE4MzNaFw0yMDExMDkxMTE4MzNaFw0xITEyMDgwMTE4MzNaFw0x
EQYDVQQKDAptaw5pT3JhbG91eWYyVGVVQVQxPheVb2dpb181ZFAxHzAdBgNV
BAUwIjE9uZUxvZ21uIEFjY291bnQghzH3NDAwggE1MA0GCSqGSIb3DQEBBQUAA4IB

```

 Below the text area, there is a dropdown menu set to 'X.509 PEM' and a blue 'DOWNLOAD' button.

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

IDP Entity ID	Issuer URL from the SSO tab in Onelogin
Single Sign On URL	SAML 2.0 Endpoint (HTTP) from the SSO tab in Onelogin
Single Logout URL	SLO Endpoint (HTTP) from the SSO tab in Onelogin
X.509 Certificate	Paste the X.509 Certificate textarea value

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.

Save

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.

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.

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