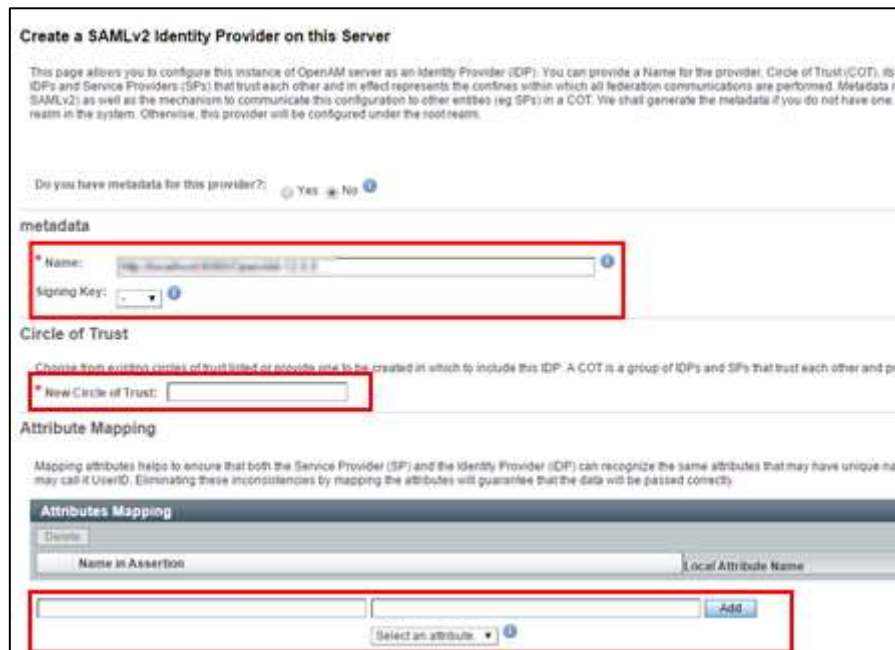


SETUP GUIDE FOR OPENAM AS IdP

STEP 1: Create Hosted Identity Provider:

- Login to your OpenAm admin console.
- Click on **Create Hosted Identity Provider** to set up OpenAM as an Identity Provider.
- Under the **metadata** section give a URL to identify your IDP. This URL is used to identify the IDP to other Identity Providers and Service Providers. This is the **IDP Entity Identity**.
- **Select a Signing Key** from the list provided. If you do not have your own Signing Key then you can use the **default Test Certificate** which has the alias name **"test"**.
- Enter a new **Circle of Trust**. The name provided here is used to identify your Service Provider or Identity Provider. You can name it **Confluence**. Remember this name as you will need it for setting up your Service Provider Settings in STEP 2.
- **Map the Attributes** you want to send over the SAML Response. Give each attribute a name which will be sent in the SAML Assertion and map it to the **Local Attribute Name**. You can select the attributes you want to map from the select box.



Create a SAMLv2 Identity Provider on this Server

This page allows you to configure this instance of OpenAM server as an Identity Provider (IDP). You can provide a Name for the provider, Circle of Trust (COT), its IDPs and Service Providers (SPs) that trust each other and in effect represents the confines within which all federation communications are performed. Metadata (e.g. SAMLv2) as well as the mechanism to communicate this configuration to other entities (e.g. SPs) in a COT. We shall generate the metadata if you do not have one. If you have one, this provider will be configured under the root realm.

Do you have metadata for this provider? ☐ Yes ☒ No

metadata

* Name:

Signing Key:

Circle of Trust

Choose from existing circles of trust listed or provide one to be created in which to include this IDP. A COT is a group of IDPs and SPs that trust each other and provide a common set of attributes.

* New Circle of Trust:

Attribute Mapping

Mapping attributes helps to ensure that both the Service Provider (SP) and the Identity Provider (IDP) can recognize the same attributes that may have unique names. Eliminating these inconsistencies by mapping the attributes will guarantee that the data will be passed correctly.

Name in Assertion	Local Attribute Name
<input type="text" value=""/>	<input type="text" value=""/>

Select an attribute:

- Click on the **Configure** button to save your settings.

STEP 2: Register Remote Service Provider:

- Click on **Register Service Provider** link to configure your Service Provider settings.
- **Copy the Metadata URL** from the SAML plugin's **Configure IDP Tab**.
- Paste the above URL in the **Service Provider Configuration** where it asks to provide the Service Provider metadata URL.
- Next choose your **Circle of Trust**. Choose the name from the select box. This is the new Circle of Trust you created earlier in STEP 1.
- **Map the Attributes** you want to send over the SAML Response for the Service Provider. Give each attribute a name which will be sent in the SAML Assertion and map it to the **Local Attribute Name**. You can select the attributes you want to map from the select box.

Create a SAMLv2 Remote Service Provider

This page allows you to register a remote Service Provider (SP). You need two things: Circle of Trust (COT) and metadata of the provider. A COT is a group of confines within which all federation communications are performed. Metadata represents the configuration necessary to execute federation protocols (eg SAML) (eg IDPs) in a COT.

Where does the metadata file reside?:

☒ URL ☐ File ?

* URL where metadata is located:

?

Circle of Trust

Choose from existing circles of trust listed or provide one to be created in which to include this SP. A COT is a group of IDPs and SPs that trust each other and

Circles of Trust: ☒ Add to existing ☐ Add to new

* Existing Circle of Trust:

Attribute Mapping

Attributes Mapping

Name in Assertion

Local Attribute Name

Select an attribute. ?

- Click on the **Configure** button to save your settings.

STEP 3: Setup Confluence SAML Plugin:

- Go to **Federation Tab** in your OpenAM admin dashboard.
- In the **Entity Providers Table** click the **IDP** we created in STEP 1.
- Click on the **Configure SP** within your IDP settings.
- Keep this page handy for the next step.



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

Identity Provider Name	OpenAM
SAML Login URL	<a href="http://<YOUR_OPENAM_DOMAIN>/IDPSloRedirect/metaAlias/idp">http://<YOUR_OPENAM_DOMAIN>/IDPSloRedirect/metaAlias/idp
IdP Entity ID or Issuer	The IDP Name value that you updated in STEP 1.
X.509 Certificate*	Paste the IDP Signing Certificate value.
Response Signed	UnChecked
Assertion Signed	Checked

* By default OPENAM is shipped with the following certificate:

```
-----BEGIN CERTIFICATE-----
MIICQDCCAakCBEeNB0swDQYJKoZIhvcNAQEEBQAwZzELMAkGA1UEBhMCVVMxEzARBgNVBAGTCkNh
bGlmb3JuaWExFDASBgNVBACTC1NhbnRhIENsYXJhMQwwCgYDVQQKEwNTdW4xEDAOBgNVBAStB09w
ZW5TU08xDALBgNVBAMTBHRlc3QwHhcNMMDgwMTE1MTkxOTM5WhcNMTEyMTkxOTM5WjBnMQsw
CQYDVQQGEwJVUzETMBEGA1UECBMQ2FsaWZvcml5YUJUMTA1UEBxMLU2FudGEgQ2xhcml5DDAK
BgNVBAoTA1N1bGJlQMA4GA1UECzMHT3BlblNTTzENMAsGA1UEAxMEdGVzdDCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEArsQc/U75GB2AtKhbGS5piiLkmJzqEsp64rDxbMJ+xDrye0EN/q1U5Of+
RkDsaN/igkAvV1cuXEGtL6RlafFPcUX7QxZhBhsYF9pbwtMzi4A4su9hnXIHURebGEmxKW9qJNY
Js0Vo5+IgjxuEwnjnnVgHTs1+mq5QYTA7E6ZyL8CAwEAATANBgkqhkiG9w0BAQQFAAOBgQB3Pw/U
QzPKTPTYi9upbFXlrAKMwtFf2OW4yvGWwv1cwcNSZJmTJ8ARvVYOMEVNbsT4Ofcfu2/PeYoAdiDA
cGy/F2Zuj8XJJpuQRSE6PtQqBuDEHjJmOQJ0rV/r8m01ZCtHRhpZ5zYRjhRC9eCbjx9VrFax0JDC
/FfwWigmrW0Y0Q==
-----END CERTIFICATE-----
```

If you have changed the Certificate for your server then you can use this link to get the X.509 Signing certificate from the IDP metadata:

http://<your_OPENAM_domain>/saml2/jsp/exportmetadata.jsp

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 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 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