

Configuring Auth0 Identity provider

If your organization uses [Auth0](#) Identity Provider (IdP) for user authentication, you can configure [SAML Service provider](#) to allow your users to log in to your [ConcreteCMS](#) website using their [Auth0](#) IdP credentials.

Configuration for SAML must be done in two places: at the IdP ([Auth0](#)) and at the SP (Our [SAML Service provider](#) package) .In the next sub-chapters, we'll provide guidelines for a basic configuration of [Auth0](#) IdP and how to set up it as your identity provider .

These steps reflect a third-party application and are subject to change without our knowledge. If the steps described here do not match the screens you see in your IdP account, you can use the general SAML configuration steps, along with the Auth0 IdP's documentation .

This document assumes that you've already created an account with your selected Identity Provider.

1) Add our Service provider information to [Auth0](#)

The next step enables you to retrieve the information [Auth0](#) needs to work with our [SAML Service provider](#) .

Go to " *Dashboard > SAML Service Provider > Configuration and Settings* " page in our package .

SAML Info

Name

Concrete SAML service provider

Issuer / EntityID

http://127.0.0.1/c584/index.php/610be2dedb093



Unique identifier of the service provider.

Assertion Consumer Service Endpoint (Redirect / POST Binding)

http://127.0.0.1/c584/index.php/xw/sso/callback



Specifies the endpoint that receives the SAML authentication response. We support POST/Redirect Binding

In the next step, you will need the following information before heading to the Configuration of [Auth0](#)

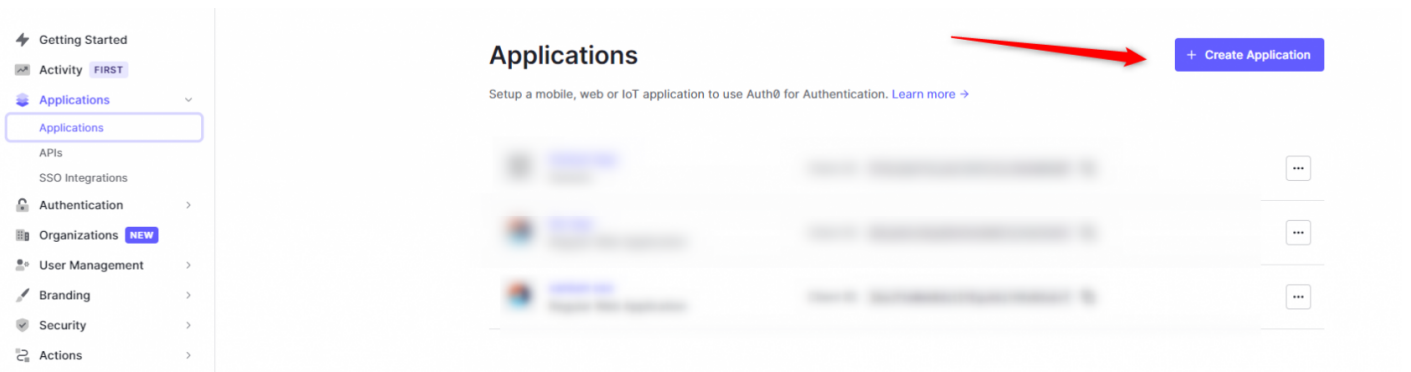
- **Issuer / EntityId**
- **Assertion Consumer Service Endpoint**

2) Setup [Auth0](#) IdP

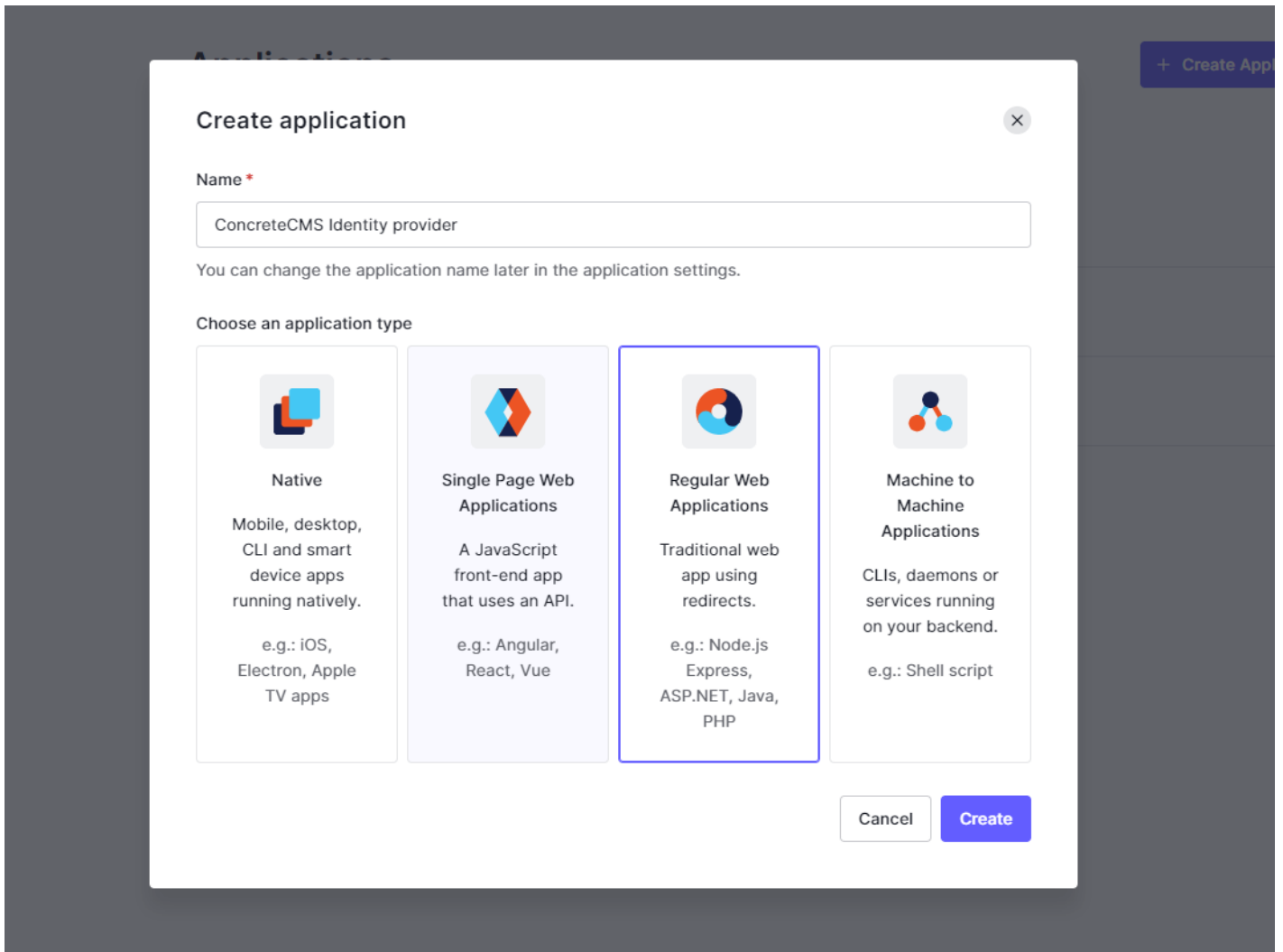
Follow the steps below to configure [Auth0](#) as an Identity Provider :

Log in to your [Auth0](#) admin portal.

Select Dashboard > Applications in the top menu and *select **Create Application*** .



Enter your display name and choose **Regular Web Applications** and click **Save** .



Navigate to the **Addons** tab and activate **SAML2 WEB APP** .

← Back to Applications



ConcreteCMS Identity provider

Regular Web Application

Client ID

Quick Start

Settings

Addons

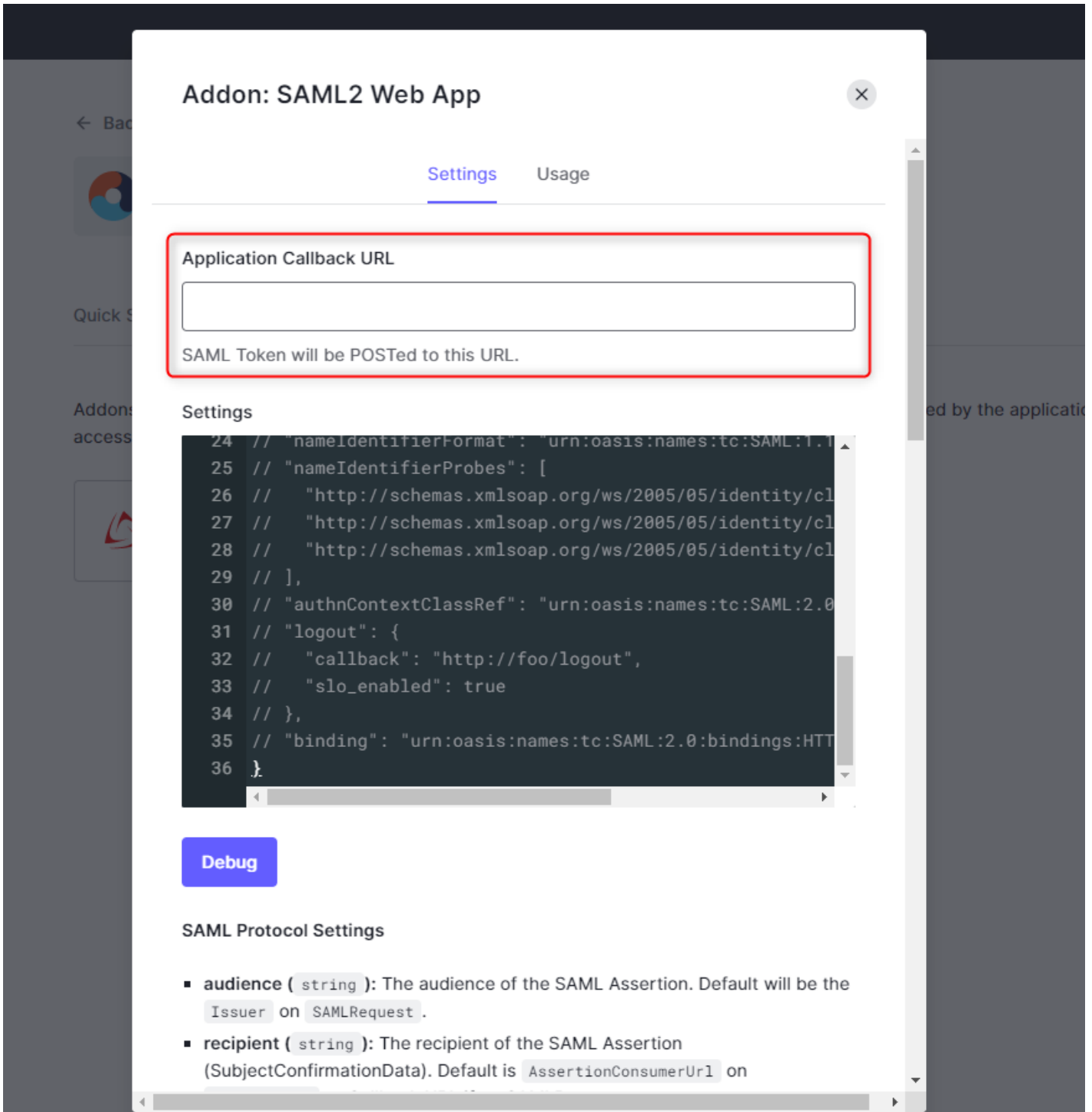
Connections

Organizations

Addons are plugins associated with an Application in Auth0. These are SAML or WS-FED web apps used by the application, which Auth0 generates access tokens for.



A new popup has been opened , navigate to the **Settings**



Add this values respectfully .

Auth0 **Application Callback URL**

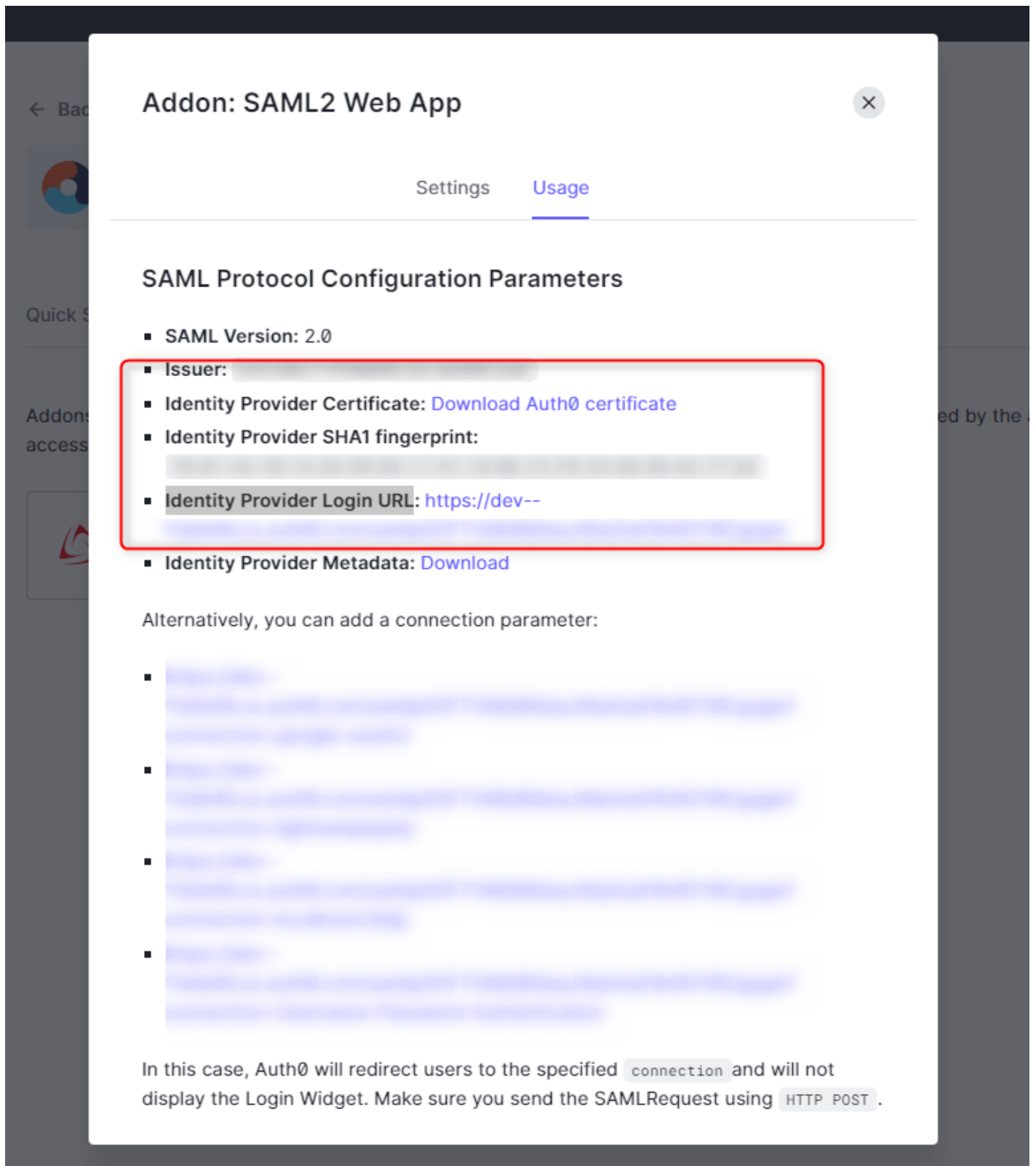
Our **Assertion Consumer Service Endpoint** from Step1

Click **Enable**.

In the next step, you will need the following **Auth0** IdP informations before heading to the Configuration of our **SAML Service provider**

- **Issuer**
- **Identity Provider Login URL:**
- **Identity Provider Certificate:**

Navigate to the **Usage** tab .



Add-on: SAML2 Web App ✕

Settings Usage

SAML Protocol Configuration Parameters

- SAML Version: 2.0
- Issuer: [blurred]
- Identity Provider Certificate: [Download Auth0 certificate](#)
- Identity Provider SHA1 fingerprint: [blurred]
- Identity Provider Login URL: <https://dev-->
- Identity Provider Metadata: [Download](#)

Alternatively, you can add a connection parameter:

- [blurred]
- [blurred]
- [blurred]
- [blurred]

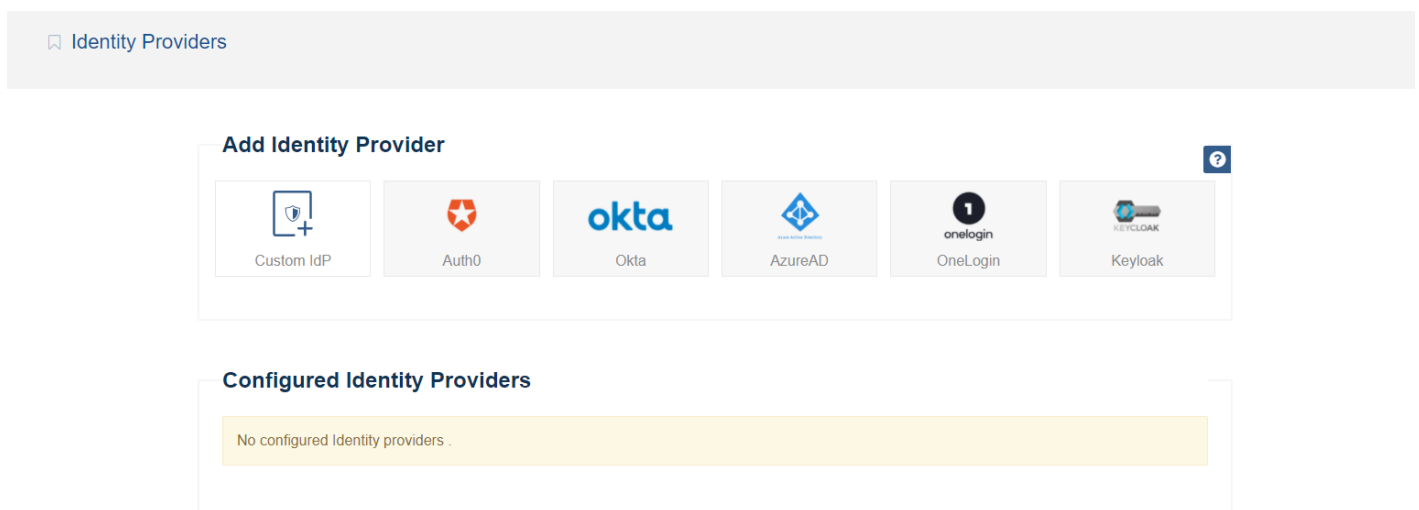
In this case, Auth0 will redirect users to the specified `connection` and will not display the Login Widget. Make sure you send the SAMLRequest using `HTTP POST` .

Or you can download an XML Metadata file of [Auth0](#) IdP SAML configuration , on the same last page click to **Identity Provider Metadata** download link .

3) Add [Auth0](#) IdP information Into our [SAML Service provider](#)

Go back to our [SAML Service provider](#) package and go to " Dashboard > SAML Service Provider > Identity providers " page

and select [Auth0](#) IdP from list shown .



[Import MetaData](#)

[See Setup Guides](#)

Details

Name

Auth0

Description

Auth0 SAML Identity provider

Issuer / EntityID

Unique identifier of the identity provider.

Single Sign On Service Endpoint (Redirect binding)

Specifies the Redirect binding endpoint that receives our SAML authentication request.

Attribute Mapping

Username

NameID

Email Address

NameID

First Name

Last Name

Add this values respectfully .

Issuer / EntityID

Auth0 **Issuer**

Single Sign On Service Endpoint (POST binding)

Auth0 **Identity Provider Login URL:**

Certificate

Auth0 **Certificate** ([Download Auth0 certificate](#) and view it in TextEditor and copy it's value)

Details

Name
Auth0

Description
Auth0 SAML Identity provider

Issuer / EntityID
urn:dev--f1sbk46.us.auth0.com
Unique identifier of the identity provider.

Single Sign On Service Endpoint (Redirect binding)
https://dev--f1sbk46.us.auth0.com/samlp/OFT1IXKjWQeqJtKpGrpF0zRZYBCgxcgw
Specifies the Redirect binding endpoint that receives our SAML authentication request.

Single Sign On Service Endpoint (POST binding)
https://dev--f1sbk46.us.auth0.com/samlp/OFT1IXKjWQeqJtKpGrpF0zRZYBCgxcgw
Specifies the POST binding endpoint that receives our SAML authentication request.

Certificate
X509 Signing Certificate Edit Download

```
-----BEGIN CERTIFICATE-----
MIIDOTCCAFWgAwIBAgJJA0+aqz4ouwCHMA0GCSqGSIb3DQEBCwUAMC0xijAgBgNV
BAMTGWVrdl0ZfzYms0Nl51cy5hdXR0eS5jb20wHhcNMjAwMTIwMTUxMjU0WWh0
MzQwNzZmMTUxMjU0WjA0MSIwIAYDVQQDEikzYXZlYXZlYXZlYXZlYXZlYXZlYXZl
YXZlYXZlYXZlYXZlYXZlYXZlYXZlYXZlYXZlYXZlYXZlYXZlYXZlYXZlYXZlYXZl
-----
```

Attribute Mapping

Username

Email Address

First Name

Last Name

Or you can do the last step by importing Metadata file . The last XML Metadata file contains all the information requested in following sections. If you have this file, you can click in **Import Metadata** button . And you can now upload it . Select that file and click in **Upload** button, and the system will parse it to populate the required fields in following sections.

[Configure Auth0 Identity Provider](#)

Import MetaData
See Setup Guides

Details

Name
Auth0

Description
Auth0 SAML Identity provider

Issuer / EntityID

Unique identifier of the identity provider.

Single Sign On Service Endpoint (Redirect binding)

Specifies the Redirect binding endpoint that receives our SAML authentication request.

Attribute Mapping

Username

Email Address

First Name

Last Name

Upload Metadata



File

Choose File

...m-metadata (4).xml

Upload

Click on **Save**

Details

Name

Auth0

Description

Auth0 SAML Identity provider

Issuer / EntityID

urn:dev--f1sbk46.us.auth0.com

Unique identifier of the identity provider.

Single Sign On Service Endpoint (Redirect binding)

https://dev--f1sbk46.us.auth0.com/samlp/OFT1XKjWQeqJIKpGrpF0zRZYBCgxcgw

Specifies the Redirect binding endpoint that receives our SAML authentication request.

Single Sign On Service Endpoint (POST binding)

https://dev--f1sbk46.us.auth0.com/samlp/OFT1XKjWQeqJIKpGrpF0zRZYBCgxcgw

Specifies the POST binding endpoint that receives our SAML authentication request.



Certificate

X509 Signing Certificate

Edit

Download

Identity provider public key used by us to validate the signature on the SAML Response or Assertions

Attribute Mapping

Username

NameID

Email Address

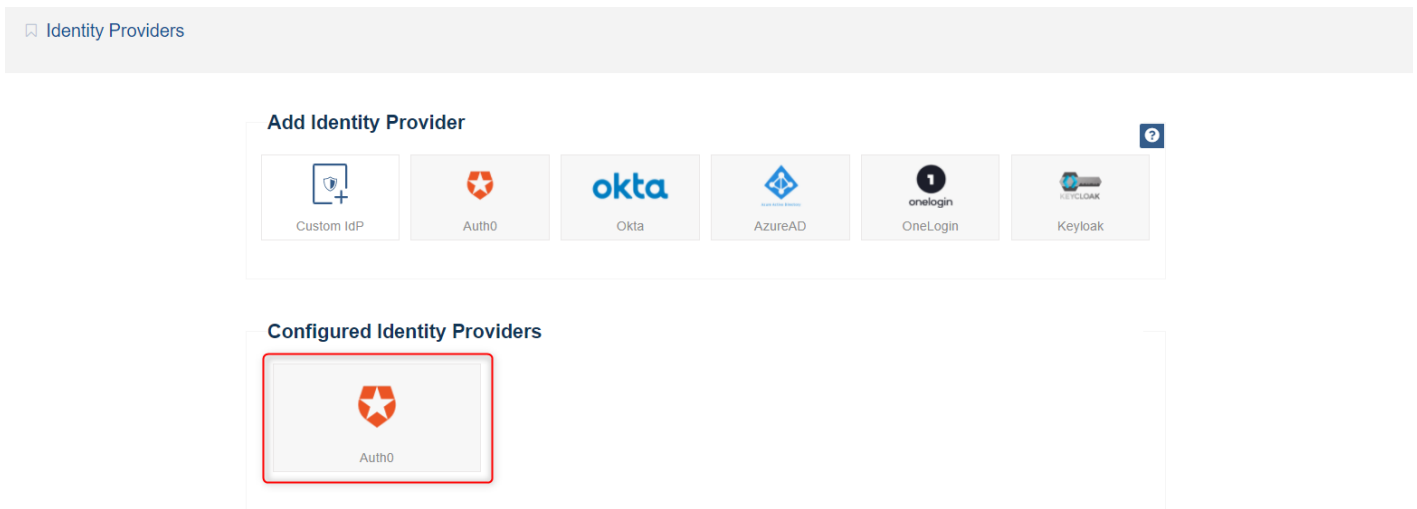
NameID

First Name

Last Name

Your configured IdP will be shown in " Dashboard > SAML Service Provider > Identity providers "

page .



Identity Providers

Add Identity Provider

Custom IdP Auth0 Okta AzureAD OneLogin Keycloak

Configured Identity Providers

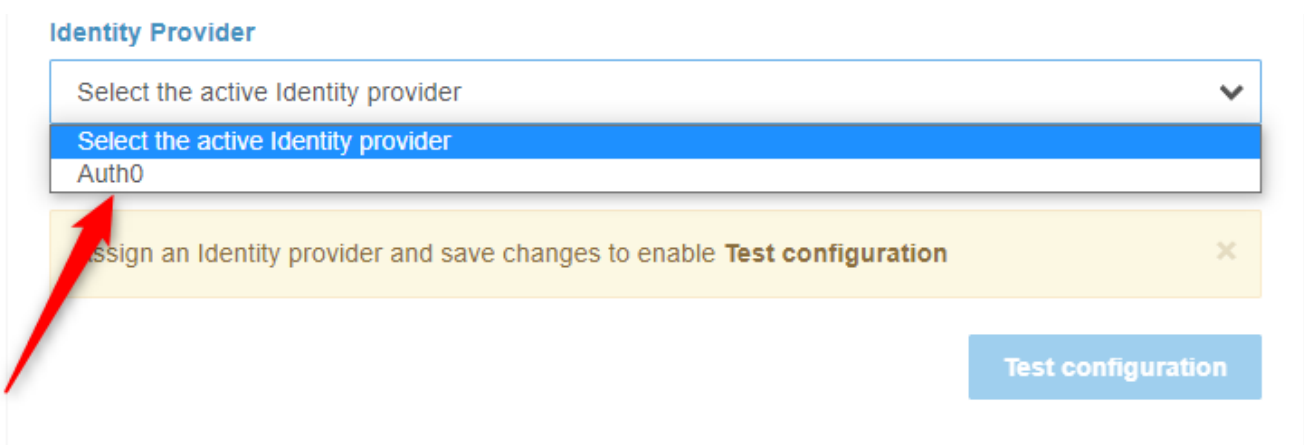
Auth0

And at this point, you have successfully configured [Auth0](#) as an Identity provider in the system .

If you have some wrong inputs in previous step , you can edit your configured identity providers by clicking it .

Go to " Dashboard > SAML Service Provider > Configuration and Settings " page .

In **Settings** section, select your configured Identity provider ([Auth0](#)) (from step above) appeared in the configured IdPs list .



Identity Provider

Select the active Identity provider

Select the active Identity provider

Auth0

Assign an Identity provider and save changes to enable **Test configuration**

Test configuration

Click on **Save** .

After successfully test your connection, you must check your settings in **Settings** and **Appearance** sections in the same page .

Activate the system to show your End Users the Login form .

Settings

Activate

Activate/Disable the system and show End-User Login form .

JIT provisioning (Allow automatic registration)

Create User if not exist and select default Group to enter on registration. Otherwise use only pre-existing Users...

Force Authentication

This will force user to provide credentials on IdP on each login attempt even if the user is already logged in to IdP.

Default After Login Redirect Url

Redirect target url after success authentication

Identity Provider

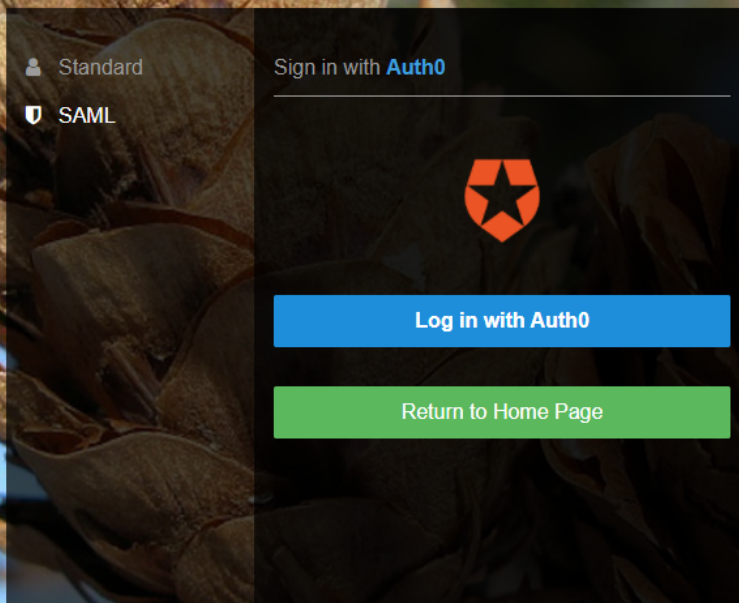
▼ 👁

Current assigned Identity provider.

Click on **Save** .

You should now be able to see a **'SAML'** option in the [ConcreteCMS](#) login screen . This will redirect users to login to the [Auth0](#) instance for their username/password and will create a new [ConcreteCMS](#) user account with chosen group (If **JIT provisioning** is enabled) .

Sign in.



For a better understanding and more advanced configuration please check out the official [Auth0](#) documentation. Also please refer to previous pages in this documentation.

If you are experiencing issues while testing the connection to the [Auth0](#), first double-check the configuration options in [SAML Service provider](#) package and [Idp \(Auth0 \)](#) side . You may also inspect the [ConcreteCMS](#) logs to help pinpointing the problem cause. Debug logs may contain more detailed information about the issues

Once you've completed the setup steps, it's important to test to make sure everything is working properly.

If you encounter any issues, check to make sure that the values in your IdP and your Service provider match .

You can also refer to the Troubleshooting section: see [Troubleshooting](#).

Revision #24

Created Tue, Aug 10, 2021 1:12 PM by bilel

Updated Tue, Aug 23, 2022 10:41 AM by bilel