

Configuring Keycloak Identity provider

If your organization uses [Keycloak](#) 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 IdP [Keycloak](#) credentials.

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

Prerequisite : You must have an Install [Keycloak](#) server in your Host and run it .

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 [Keycloak](#) IdP's documentation (<https://www.keycloak.org/documentation>) .

1) Add our Service provider informations to [Keycloak](#)

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

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

Click **Export Metadata** button in the bottom of **SAML Info** section to download an XML file of your SAML configuration settings to send to [Keycloak](#) Identity provider.

Sign Request (Optional)



When enabled, all SAML authentication requests must be signed. Download the certificate and give it to your Identity Provider that will receive the signed request so it can validate the signature .

Want Signed Assertions (Optional)



When enabled, the Identity Provider keep in mind that his response must contain signed Assertions, otherwise we ignore it, Note that the identity provider is not obligated by this, but is being made aware of the likelihood that an unsigned assertion will be insufficient .



Export MetaData

2) Setup Keycloak IdP

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

Go to your [Keycloak Admin](#) console, select the **realm** that you want to use.

Select *Clients* in the right menu and select **Create**

Client ID	Enabled	Base URL	Actions		
account	True	https://keycloak.xanium.io/auth/realms/master/account/	Edit	Export	Delete
account-console	True	https://keycloak.xanium.io/auth/realms/master/account/	Edit	Export	Delete
admin-cli	True	Not defined	Edit	Export	Delete
broker	True	Not defined	Edit	Export	Delete
http://127.0.0.1/c584/index.php/610e2dedb093	True	http://127.0.0.1/c584/index.php/	Edit	Export	Delete
master-realm	True	Not defined	Edit	Export	Delete
security-admin-console	True	https://keycloak.xanium.io/auth/admin/master/console/	Edit	Export	Delete

Use **Select file** to open the xml file you've saved earlier. (Step 1)

Add Client

Import

Client ID *

Client Protocol

Client SAML Endpoint

Once imported, **Save** your settings.

Add Client

Import

Client ID *

Client Protocol

Client SAML Endpoint

You'll see the following screen, leave its settings untouched unless you know what to configure beyond standard configuration.

Settings | Keys | Roles | Client Scopes | Mappers | Scope | Sessions | Offline Access | Clustering | Installation

Client ID

Name

Description

Enabled

Always Display in Console

Consent Required

Login Theme

Client Protocol

Include AuthnStatement

Include OneTimeUse Condition

Force Artifact Binding

Sign Documents

Optimize REDIRECT signing key lookup

Sign Assertions

Signature Algorithm

SAML Signature Key Name

Canonicalization Method

Encrypt Assertions

Client Signature Required

Force POST Binding

Front Channel Logout

Force Name ID Format

Name ID Format

Root URL

Valid Redirect URIs

Base URL

Master SAML Processing URL

IDP Initiated SSO URL Name

IDP Initiated SSO Relay State

3) Add Keycloak IdP informations Into our [SAML Service provider](#)

Navigate to *Realm Settings*, click on **SAML 2.0 Identity Provider Metadata** mentioned as Endpoints in the **General Tab**.

and **Save XML File** from that link .

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

and select [Keycloak](#) Idp from list shown .

Add Identity Provider

Custom IdP Oauth Okta AzureAD OneLogin

Configured Identity Providers

No configured Identity providers .

The last 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.

[Import MetaData](#) [See Setup Guides](#)

Details

Name

Keycloak

Description

Keycloak SAML Identity provider

Entity ID / Issuer

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

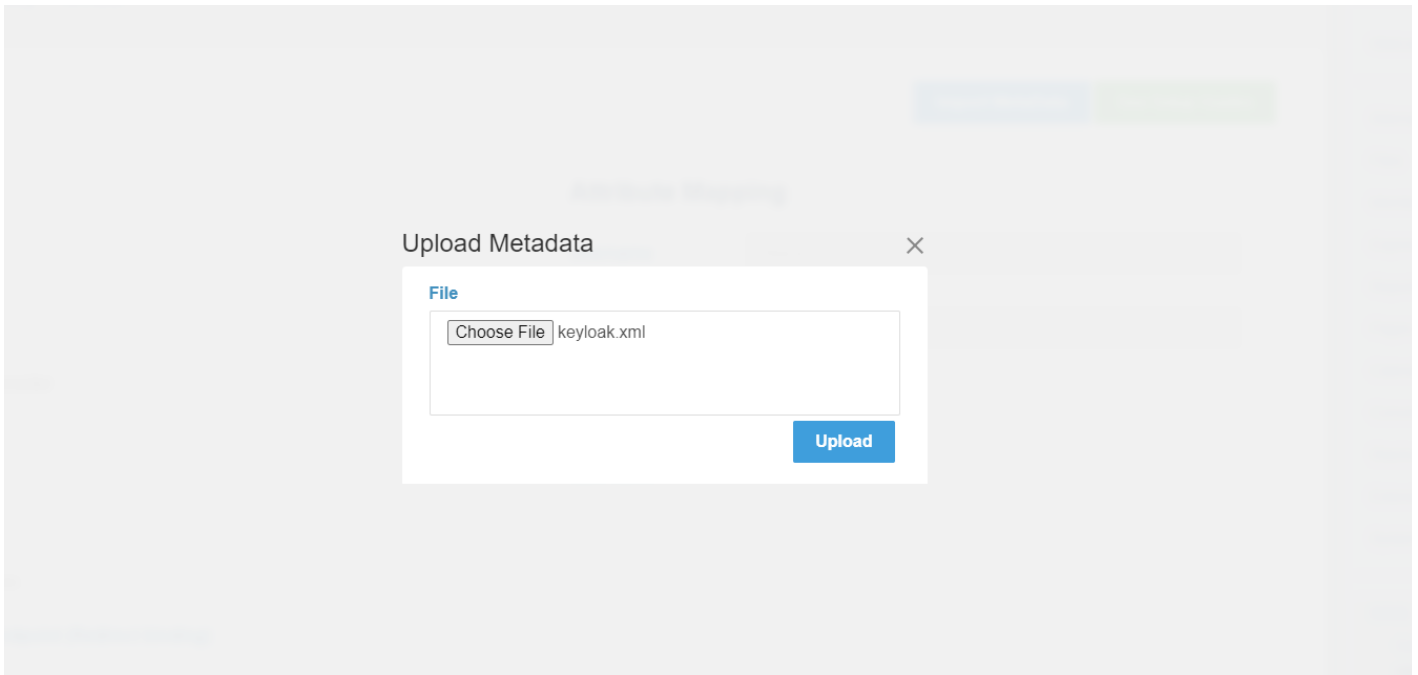
NameID

Email Address

NameID

First Name

Last Name



Click on **Save**

Details

Name
Keyloak

Description
Keyloak SAML Identity provider

Entity ID / Issuer
Unique identifier of the identity provider.

Single Sign On Service Endpoint (Redirect binding)
Specifies the Redirect binding endpoint that receives our SAML authentication request.

Single Sign On Service Endpoint (POST binding)
Specifies the POST binding endpoint that receives our SAML authentication request.

Certificate
X509 Signing Certificate
Identity provider public key encoded in PEM or CER format, used by us to validate the signature on the SAML Response or Assertions

Attribute Mapping

Username NameID

Email Address NameID

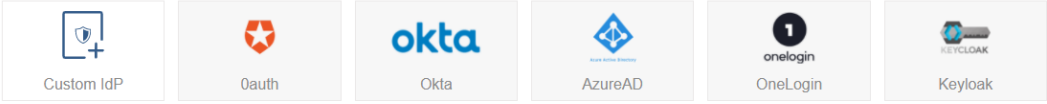
First Name

Last Name

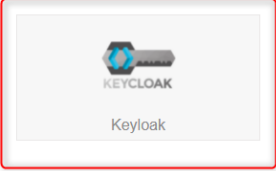
Cancel Want AuthnRequest Signed Save

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

Add Identity Provider



Configured Identity Providers



And at this point, you have successfully configured [Keycloak](#) 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 (from step above) appeared in the configured IdPs list .

Identity Provider

Select the active Identity provider



Select the active Identity provider

Keycloak

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



Test configuration

Appearance

Save

Authentication Types Display Name / Icon

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 the 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



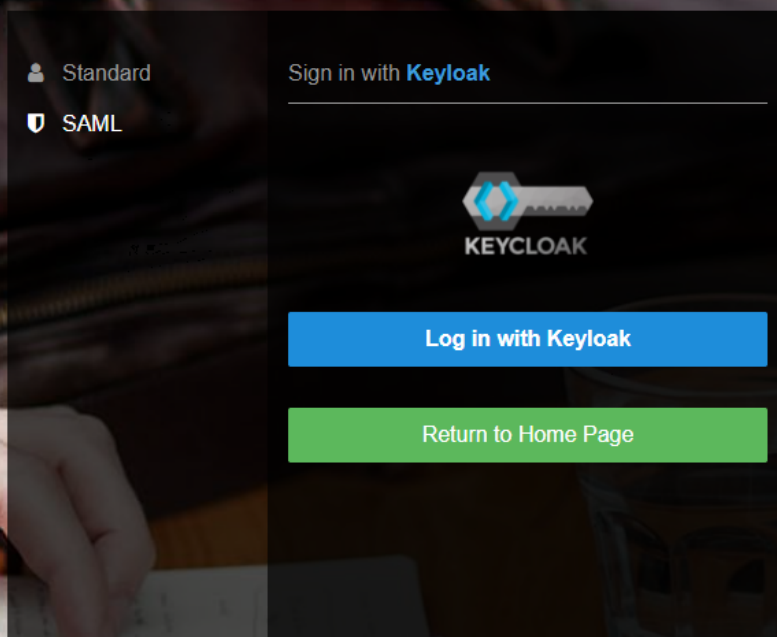
Current assigned Identity provider.

Test configuration

Click on **Save** .

You should now be see a **'SAML'** option in the [ConcreteCMS](#) login screen . This will redirect users to login to the [keycloak](#) 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 Keycloak documentation. Also please refer to previous pages in this documentation.

If you are experiencing issues while testing the connection to the [Keycloak](#) server, first double-check the configuration options in [SAML Service provider](#) package and in Idp ([keycloak](#)) side . Also check Troubleshooting && FAQ page

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 #67

Created Mon, Aug 2, 2021 3:57 PM by bilel

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