Configure Keycloak for external authentication

censhare WP requires external authentication using Keycloak as identity broker. Keycloak runs on a dedicated authentication server. Learn how to configure Keycloak to use it with censhare WP.

Prerequisites

- Write permissions to the installation directory
- Installation of censhare WP
- Installation of Keycloak

Introduction

Keycloak is used as authentication server for censhare WP (as of 2021.2).

- You can use Keycloak as an external identity provider. Keycloak then serves as an identity broker between the identity provider and censhare WP.
- You can also use Keycloak with the censhare standard authentication. Keycloak then serves as a gatekeeper to the censhare Server.

The configuration of the authentication method is not part of this documentation.

Keycloak realms

In Keycloak, you work in a realm, which is a space where you manage objects such as applications or a group of users.

You must set up a realm for censhare.

Keycloak clients

In Keycloak, clients are entities that can request Keycloak to authenticate users. Most often, clients are applications and services that want to use Keycloak to secure themselves and provide a single sign-on solution.

The censhare realm contains two clients to handle the login:

- login from a web browser (censhare Web)
- login from a censhare Client or censhare Admin Client

Create Keycloak system admin account

If you already use a Keycloak server and want to configure this server to authenticate censhare users, you can skip this step.

After successfully installing censhare WP and all required components, censhare WP must be configured.

As the first step of the initial censhare WP configuration, you must configure the Keycloak server. For a full list of censhare WP configuration steps, see censhare WP - Initial configuration.

Before you can use Keycloak, you need to create a system admin account which you use to log in to the Keycloak admin console. Then you need to start the Keycloak server.

The Keycloak configuration is done in the Keycloak administration console. To start and access Keycloak, do the following:

1. Add a system admin user to access Keycloak. In the location where censhare WP is installed, run the following shell script:

   ```
   /opt/jboss/keycloak/bin/add-user-keycloak.sh -u admin
   ```

2. Enter a password and click **Return**.
3. To load the system admin user, restart the Keycloak server with the following command:

   ```
   systemctl restart keycloak
   ```

With the **admin** user that you created, you can access the Keycloak admin console from the URL of the Keycloak server at port 8080:

`http://[KEYCLOAK_BASE_URL]:8080`

Test open ports with `sudo lsof -i -Pn`.

Port 8080 is Keycloak.

REST API reference for the Keycloak Admin:
https://www.keycloak.org/docs-api/9.0/rest-api/index.html

Configure the censhare realm

When you start KeyCloak, there is only the master realm. This master realm is only used for managing other realms. Therefore, you have to create a separate realm for censhare. Everything that has to do with censhare as an application is stored in the censhare realm.

Before you start

Make sure that the Keycloak server is running, that you can access it and log in with the **admin** user that you created in the previous step.

1. Log in to Keycloak and go to the Keycloak Admin Console.
2. On the left sidebar, click the **Master** realm and select **Add realm** in the menu.
3. Under **Name** enter a realm name and click **Create**. The default name of the realm is **censhare**.

Configure realm keys

The authentication protocols that are used by Keycloak require cryptographic signatures and sometimes encryption. Keycloak supports encryption algorithms (**Key Providers**) that are not known to censhare (Spring security library). For successful login to the censhare Server, you need to disable these key providers in Keycloak.

a. Log into the **Keycloak** Admin Console.
b. At the top of the side navigation, select the **censhare** realm.
c. In the side navigation, select **Realm Settings**.
d. Select the **Keys** tab.
e. Click the **Providers** tab.
f. Click the **Active** tab.
g. Select the provider **rsa-enc-generated** and toggle **Enabled** to **OFF.**
h. Select the provider **fallback-ES256** and toggle **Enabled** to **OFF.**
i. Click **Save**.

Create internal admin user

For administration purposes, the **Keycloak admin client service** of the censhare Server must access Keycloak. Therefore, you must create a specific **adm in user** that the **censhare Server** uses to retrieve data from **Keycloak**.

Make sure you are in the **censhare** realm that you just created.

1. In the left navigation, click **Users**.
2. In the table header, at the right, click **Add user**.
3. Enter a **Username** and click **Save**.
4. Go to the **Credentials** tab, enter a password, confirm the password, and switch the **Temporary** toggle to **OFF**.
5. Click **Save**.

Assign realm management roles to the **admin user** that you just created:

1. Go to the **Role Mappings** tab.
2. In the **Client Roles** area, open the **Client Roles** drop-down list and select **realm-management**. The fields **Available Roles**, **Assigned Roles**, and **Effective Roles** display.
3. Select all **Available Roles**, and click **Add selected**.

Configure the censhare web application client

The web application client authenticates users from the web-based **censhare WP** client. To configure the client, do the following:

1. Log in to the **Keycloak** administration console.
2. At the top of the side navigation, select the **censhare** realm.
3. In the side navigation, select **Clients**.
4. At the top right of the **Clients** table, click **Create**.
5. In the **Client ID** field, enter **censhare5** and click **Save**.
6. Configure the client as follows:

Field	Value	Remarks
Client ID	Default is **censhare5**	Any other ID is allowed. The ID is required to configure the keycloak_service
Name	Default is **censhare 5 OpenID client**	Any other name is allowed.
Description		Optional. Enter a short description of the client.

Enabled	ON	
Consent Required	OFF	
Login Theme		Select a custom branding and layout for the login page. If you do not select any theme, the default theme is used.
Client Protocol	openid-connect	
Access Type	confidential	
Standard Flow Enabled	ON	
Implicit Flow Enabled	OFF	
Direct Access Grants Enabled	ON	
Service Accounts Enabled	ON	
Authorization Enabled	ON	
Root URL	[CENSHARE_WEB_BASE_URL]	Enter the URL from which users access the web-based censhare WP client.
Valid Redirect URIs	[CENSHARE_WEB_BASE_URL]*	Enter the URL from which users access the web-based censhare WP client, followed by the asterisk (*).
Base URL		not required
Admin URL		not required
Web Origins	*	Do not remove the asterisk (*).

Use our censhare5.json configuration file to create this configuration. To do so, click Select file in the Add Client dialog and upload the configuration.

7. Click **Save**.
8. Go to the **Credentials** tab.
9. Copy the Secret. You need this secret to set up the Keycloak service in the censhare Admin Client, and for the configuration of the Cloud Gateway.

If you imported the **JSON configuration file** to set up the client, the **Secret** field shows a **[CREATE_SECRET]** placeholder. Click **Regenerate Secret** to generate a valid secret and copy it

Configure the censhare desktop application client

In Keycloak, clients are entities that can request Keycloak to authenticate users. Most often, clients are applications and services that want to use Keycloak to secure themselves and provide a single sign-on solution.

The desktop application client authenticates users at the **censhare Clients** and the **censhare Admin Clients**. To configure the client, do the following:

1. Log into the **Keycloak** Admin Console.
2. At the top of the side navigation, select the **censhare** realm.
3. In the side navigation, select **Clients**.
4. At the top right of the **Clients** table, click **Create**.
5. In the **Client ID** field, enter **desktop-app** and click **Save**.
6. Configure the client as follows:

Field	Value	Remarks
Client ID	Default is **desktop-app**	Any other ID is allowed. The ID is required to configure the Keycloak service.
Name	Default is **censhare Desktop Application OpenID client**	Any other name is allowed.
Description		Optional. Enter a short description of the client.
Enabled	ON	
Consent Required	OFF	

Login Theme		Select a custom branding and layout for the login page. If you do not select any theme, the default theme is used.
Client Protocol	openid-connect	
Access Type	confidential	
Standard Flow Enabled	ON	
Implicit Flow Enabled	OFF	
Direct Access Grants Enabled	ON	
Service Accounts Enabled	OFF	
Authorization Enabled	OFF	
Root URL	[KEYCLOAK_BASE_URL]	Enter the Keycloak server URL (absolute URL). The base URL must be accessible from the client computers inside your corporate network.
Valid Redirect URIs	[KEYCLOAK_BASE_URL]* http://localhost:*	Enter the Keycloak server URL (absolute URL), followed by the asterisk (*). Do not remove the **localhost** entry!
Base URL		not required
Admin URL	[KEYCLOAK_BASE_URL]	Enter the Keycloak server URL (absolute URL).
Web Origins	[KEYCLOAK_BASE_URL]	Enter the Keycloak server URL (absolute URL).

   Use our censhare5.json configuration file to create this configuration. Click **Select file** in the **Add Client** dialog and upload the configuration.
7. Click **Save**.
8. Go to the **Credentials** tab.
9. Copy the Secret. You need this secret to set up the Keycloak service, and for the configuration of the Cloud Gateway.

If you imported the **JSON configuration file** to set up the client, the **Secret** field shows a **[CREATE_SECRET]** placeholder. Click **Regenerate Secret** to generate a valid secret and copy it.

Configure the censhare CI HUB application client

Follow the steps described in CI HUB - Setup in censhare

You can omit this task, if you do not use the CI HUB integration.

Configure the hosts.xml

In the **censhare Client** and **censhare Admin Client**, the authentication method must be set to **external** in the respective **hosts.xml** files.

1. Open the **hosts.xml** file. The default path on macOS is **/Users/USER/Library/Preferences/censhare/hosts.xml**.
2. In the entry of the desired server, set the attribute **authentication-method="external"**.
3. Save the configuration.

Configure censhare Server to access Keycloak

The Keycloak service connects the censhare Server to the Keycloak server and queries the user data from the Keycloak server.

You need the admin user credentials from the censhare realm and both secrets from the clients that you created in Keycloak.

The configuration is done in the censhare Admin Client.

1. In the **censhare Admin Client**, open the **Configuration/Services/Keycloak admin client service** directory, and open the **Configuration** file.

2. Select the **Service enabled** field.
3. In the **Invocations** field, select the maximum number of parallel processes. The default is 2.
4. Leave the **Version** field unaltered.
5. In the **Authentication serve**r setup area, configure the service for the web-based **censhare WP** client:

Base URL	Enter the hostname of the Keycloak server (absolute URL). Keycloak must be accessible internally (from the censhare Server) through this URL. **Important:** Add the certificate for this host to the censhare Server truststore! If the censhare Server is installed inside of Kubernetes, you can use the service name instead.
Realm name	Enter the realm name that you configured in the Keycloak administration console. Default is **censhare**.
Admin user access name	Enter the user credentials of the system user that retrieves the data from **Keycloak**.
Admin user access password	
Keycloak OAuth2 client ID	Enter the client ID of the censhare web application client in Keycloak. Default is **censhare5**.
OAuth client secret	Enter the secret of the censhare web application client in Keycloak. The secret is generated automatically and can be found in the client settings in the **Credentials** tab.

6. In the **Authentication credentials for native client setup**, configure the service for the desktop applications **censhare Client** and the **censhare Admin Client**. The native client service uses the same realm and admin user as the web client setup. Only the client ID and secret are required:

Base URL (exposed to client)	Enter the Keycloak URL that is accessible from any native Client in your corporate network.
Keycloak OAuth2 client ID	Enter the client ID of the censhare desktop application client in Keycloak. Default is **desktop-app**.
Keycloak OAuth native application secret	Enter the secret of the desktop application client in Keycloak. The secret is generated automatically and can be found in the client settings in the **Credentials** tab.

7. Click OK to save the configuration.
8. Restart the censhare Server. If necessary, synchronize the remote servers.

Test desktop client login via Keycloak

Start either the **censhare Client** or the **censhare Admin Client** and try to log in with the user that you created above. When you select the corresponding censhare-Server in the dialog, the **login** and **password** fields are disabled. Instead, you are forwarded to the Keycloak login page in your default browser. Enter the credentials (login name and password) of the user that you created in Keycloak.

If the login was successful, switch back to the **censhare Client** or the **censhare Admin Client** applications. The login process starts automatically and you can access and work with the application.

Result

The Keycloak server is installed and configured in the **censharewp** instance in your organizational network. To verify the authentication, log in either from a **censhare Client** or from **censhare Web**. From both instances, you are forwarded to the Keycloak login page. After successful login, you are redirected to the censhare Client or the censhare web application.

Next steps

Carry on with the censhare WP configuration.

Configure the censhare Standard login, or add and configure the authentication via LDAP or SAML to log in censhare users.