Configure Keycloak for external authentication

censhare WP (BETA) requires external authentication. The external authentication uses Keycloak as identity broker. Keycloak runs on a dedicated authentication server. You can install Keycloak from an RPM package together with censhare WP (BETA), or use an existing Keycloak server in your network.

Context

The installation is done with the RPM packages for censhare WP (BETA). The setup is done in the Keycloak administration console.

Prerequisites

- Write permissions to the installation directory
- Installation of censhare WP
- An administration account for the Keycloak server

Introduction

censhare WP uses external authentication for the censhare Server in combination with Spring cloud gateway and the new webpacked censhare client. censhare supports Keycloak as authentication server. Keycloak can be installed from the RPM packages together with the static resource server (webpacked client) and Cloud Gateway. If you already use Keycloak in your organizational network, you can connect the censhare Server to this instance within a censhare realm.

The censhare realm contains two clients to handle the login from a web browser (censhare Web), and the login from a censhare Client or censhare Admin Client. censhare Web and censhare WP can be used in parallel operation.

If you use an external identity provider, Keycloak serves as an identity broker between the identity provider and censhare. If you use Keycloak with the censhare standard authentication, Keycloak serves as a gatekeeper to the censhare Server. The configuration of the authentication method is not part of this documentation. For the configuration of the login method, see the

Keycloak server startup & admin access

Note: If you use already a Keycloak server and want to configure this server to authenticate censhare user, you can skip this step and continue with the

After successfully installing censhare WP and all required components, the Keycloak server must be configured. The configuration is done in the Keycloak administration console. To start and access Keycloak, do the following:

1. Add an admin user to access Keycloak. In the Kubernetes cluster 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 press Return.
3. To load the 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
```

Configure the censhare realm in Keycloak

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. Proceed as follows:

1. Log in and go to the Keycloak administration console.
2. At start, Keycloak shows the **Master** realm. To add a new realm, click **Master** at the top of the left navigation, and click **Add realm**.
3. Enter a name and click **Create**. The default name of the realm is **censhare**.

Next, create a **system user** that the **censhare Server** uses to retrieve data from **Keycloak**. You need this user to configure the

For more information, see the Keycloak service in the censhare Admin Client:

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

   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**.
6. Go to the **Role Mappings** tab.

7. 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.
8. Select all **Available Roles**, and click **Add selected**.

Configure the censhare web application client in Keycloak

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 setup the Keycloak service in the censhare Admin Client, and for the configuration of the Cloud Gateway.

f 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

The desktop application client authenticates users at the **censhare Clients** and the **censhare Admin Clients**. 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 **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 hostname (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 hostname (absolute URL), followed by the asterisk (*). Do not remove the **localhost** entry!
Base URL		not required
Admin URL	[KEYCLOAK_BASE_URL]	Enter the Keycloak hostname (absolute URL).
Web Origins	[KEYCLOAK_BASE_URL]	Enter the Keycloak hostname (absolute URL).

   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 setup 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 a custom theme for Keycloak

The login page of censhare Web and the censhare clients are managed in Keycloak. To customize the look and feel of these pages, you must configure a custom theme in Keycloak. Themes can also be applied to the internal administration pages of Keycloak.

A theme consists of HTML templates, stylesheets, messages, scripts, images, and theme properties. Themes must be created and edited in an external editor.

To add a custom theme, do the following:

1. Create a new theme. For more information, see this Keycloak documentation.
2. On the Keycloak server, perform the following checks to ensure that custom themes are enabled. If custom themes are already enabled on your Keycloak instance, you can skip this step:
    - The **COMPOSE_FILE** property must include a reference to sso.themes.yml with a colon as delimiter:

      `COMPOSE_FILE=sso.base.yml:sso.themes.yml`
    - The **ARG_CENSHARE_SSO_THEME_CACHE_DISABLED** property must be set to **true:**

      `ARG_CENSHARE_SSO_THEME_CACHE_DISABLED=true`
    - The path to the directory that stores the custom theme must be specified:

      `ARG_CENSHARE_SSO_THEMES_PATH=/opt/censhare/authentication/dockerfiles/sso-server-themes`
3. Build and run the Keycloak server. To do so, change to the **standalone webserver directory**, and run the **./build.sh** command.
4. Add your custom theme to the directory configured in step 2.
5. Open the Keycloak URL and log in with your administration credentials.
6. At the top of the side navigation, select the **censhare** realm.
7. Open the **Realm settings** and go to the **Themes** tab.
8. In the **Login Theme** field, select your custom theme.

Instead of the realm, you can assign a custom theme to a specific client only. To do so, select the desired client, and in the **Settings** tab, in the **Login theme** field, select the desired theme.

Configure the Keycloak service in the censhare Admin Client

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

This configuration is done in the **censhare Admin Client**. You need the admin user credentials from the censhare realm and both secrets from the clients that you created in Keycloak. Proceed as follows:

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 is 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**.
Keycloak 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.

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

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