



Unabhängige Treuhandstelle

UNIVERSITÄTSMEDIZIN GREIFSWALD

Stand: März 2022

Web-Frontends der THS Tools mit Keycloak-basierter Authentifizierung

Hinweis: Beispiel-Screenshots nutzen exemplarisch den gPAS.

1. Realm anlegen

Legen Sie das Realm **ttp** an.

The screenshot displays the Keycloak administration interface. On the left is a dark sidebar with the 'KEYCLOAK' logo at the top. Below the logo, the realm 'Ttp' is selected. The sidebar is divided into 'Configure' and 'Manage' sections. Under 'Configure', 'Realm Settings' is highlighted. Under 'Manage', options include Groups, Users, Sessions, Events, Import, and Export. The main content area shows the configuration for the 'Ttp' realm. It has tabs for 'General', 'Login', 'Keys', 'Email', 'Themes', 'Cache', and 'Tokens'. The 'General' tab is active, showing the following fields:

- Name**: ttp
- Display name**: (empty)
- HTML Display name**: (empty)
- Enabled**: ON (toggle)
- User-Managed Access**: OFF (toggle)
- Endpoints**: OpenID Endpoint Configuration

At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

2. Client anlegen

Neuen Client für Wildfly-Zugriff (**KEYCLOAK_RESOURCE**) anlegen:

- Client ID **ths**
- **AcessType=confidential**
- **Service Accounts enabled** aktivieren

Dann unter Credentials entsprechendes **KEYCLOAK_CLIENT_SECRET** ermitteln, in der Form **1dc51f8f-0939-489a-96bb-7dccd9459037**.

Achtung: baseUrl und redirect-uri beim Client **ths** setzen

Root URL ?	<input type="text"/>
* Valid Redirect URIs ?	<input type="text" value="*"/> <input type="button" value="-"/> <input type="button" value="+"/>
Base URL ?	<input type="text" value="http://<KEYCLOAKIP>:<KEYCLOAKPORT>"/>
Admin URL ?	<input type="text"/>
Web Origins ?	<input type="text"/> <input type="button" value="+"/>
Backchannel Logout URL ?	<input type="text"/>

3. Rollen anlegen.

Komponente	Admin-Rolle	User-Rolle
gICS	role.gics.admin	role.gics.user
gPAS	role.gpas.admin	role.gpas.user
E-PIX	role.epix.admin	role.epix.user

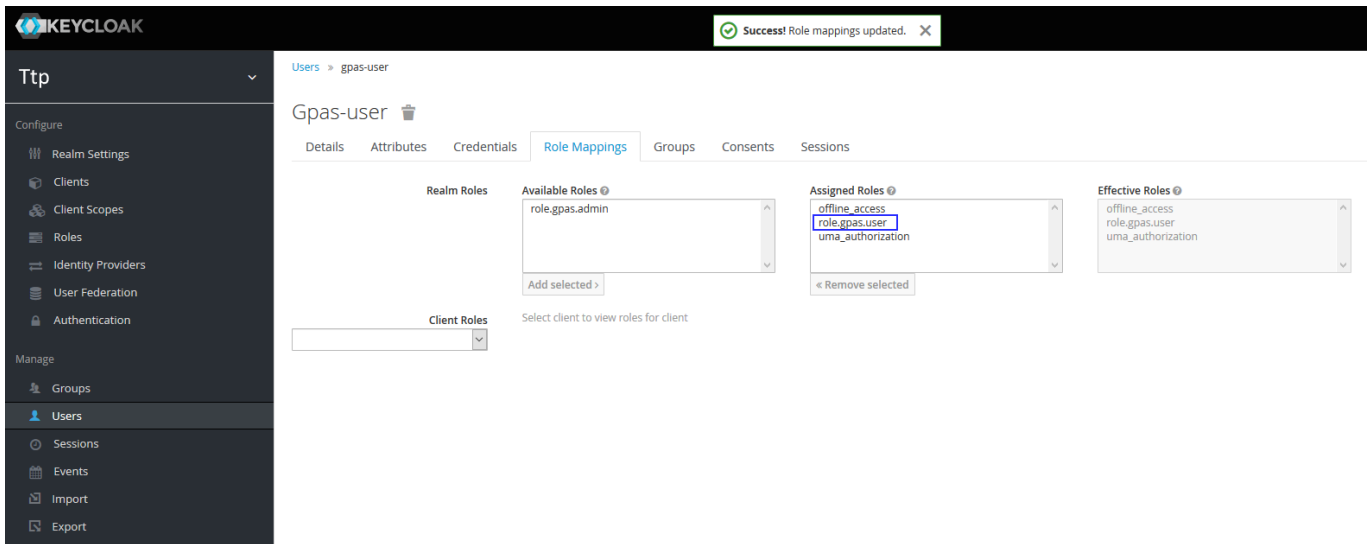
The screenshot shows the Keycloak administration interface. The left sidebar is dark and contains a navigation menu with sections 'Configure' and 'Manage'. Under 'Configure', there are options for Realm Settings, Clients, Client Scopes, Roles (highlighted), Identity Providers, User Federation, and Authentication. Under 'Manage', there are options for Groups, Users, Sessions, Events, Import, and Export. The main content area is titled 'Roles' and has two tabs: 'Realm Roles' (selected) and 'Default Roles'. Below the tabs is a search bar and an 'Add Role' button. A table lists the following roles:

Role Name	Composite	Description	Actions	
offline_access	False	\$(role_offline-access)	Edit	Delete
role.gpas.admin	False		Edit	Delete
role.gpas.user	False		Edit	Delete
uma_authorization	False	\$(role_uma_authorization)	Edit	Delete

4. User anlegen und Rollen zuweisen

User anlegen, Passwörter vergeben und den entsprechenden Rollen zuordnen.

user	Rollen
gics-admin	role.gics.admin, role.gics.user
gics-user	role.gics.user
gpas-admin	role.gpas.admin, role.gpas.user
gpas-user	role.gpas.user
epix-admin	role.epix.admin, role.epix.user
epix-user	role.epix.user



Docker-Compose Konfiguration auf Keycloak umstellen

Folgen Sie der separaten Detail-Konfiguration des jeweiligen Werkzeugs (README.md) zur Keycloak-Nutzung, um die Art der Authorisierung und die Keycloak-Details für docker-compose anzupassen.

Credits 'Keycloak for TTP-Tools'

Implementation, documentation: P. Penndorf, R. Schuldt, M. Bialke

License

License: AGPLv3, <https://www.gnu.org/licenses/agpl-3.0.en.html>

Copyright: 2022 Trusted Third Party of the University Medicine Greifswald