Authentifizierung und Autorisierung bei gICS, E-PIX und gPAS

Version 1.0 vom 10.02.2019

Herausgeber:

Universitätsmedizin Greifswald K.d.ö.R.

Ersteller:

Martin Bialke

Ellernholzstr. 1-2
17475 Greifswald

Tel. 03834 / 86-7851, Fax: 03834 / 86-7580
E-Mail: martin.bialke@uni-greifswald.de

Inhalt

1 Die Web-Auth-Versionen der Werkzeuge

1.1 Web-Auth-Version

Seit gICS 2.11.0 und gPAS 1.9.1 werden jeweils zwei Docker-Compose Varianten der Werkzeuge über Github bereitgestellt (E-PIX ist derzeit noch in Vorbereitung):

gICS Standard-Version: https://github.com/mosaic-hgw/gICS/tree/master/docker/standard

gICS Web-Auth-Version: https://github.com/mosaic-hgw/gICS/tree/master/docker/web-auth

gPAS Standard-Version: https://github.com/mosaic-hgw/gPAS/tree/master/docker/standard

gPAS Web-Auth-Version: https://github.com/mosaic-hgw/gPAS/tree/master/docker/web-auth

E-PIX Standard-Version: https://github.com/mosaic-hgw/E-PIX/tree/master/docker/standard

Die Web-Auth-Version stellt Authentifizierungs- und Autorisierungsmechanismen für die Web-Oberfläche der Werkzeuge bereit. Nutzer müssen sich für die Nutzung des Werkzeugs mittels Benutzernamen und Passwort einloggen. Je nach zugeordneter Rolle enthalten sie unterschiedliche Berechtigungen. Eine Übersicht der Rollen und Rechte ist in der nachstehenden **Tabelle 1-1** zu finden.

Standardmäßig wird zwischen Admin-Nutzer und Standard-Nutzer unterschieden. Bei der Installation des Werkzeugs mittels Docker werden standardmäßig ein Admin-Nutzer „admin“, sowie ein Standard-Nutzer „employee“ angelegt. Die Anmeldung erfolgt unter Angabe der Domäne „THS“.

```
[Default-Admin] username="admin@ths", password="ttp-tools"
[Default-User] username="employee@ths", password="ttp-tools"
```

Die Autorisierung kann werkzeugübergreifend erfolgen. So kann ein und dieselbe Person z.B. beim E-PIX Standard-Nutzer und beim gICS Admin-Nutzer sein.

1.2 Übersicht der Rollen und Rechte in der Web-Oberfläche

Tabelle 1-1: Nutzer der Gruppe Admin und Standard haben unterschiedliche Zugriffsreche in der Web-Oberfläche am Beispiel des gICS.

Bereich/Seite	Zugang ohne Login	Zugang mit Standard-Rechten	Zugang mit Admin-Rechten
Dokumente: Einwilligungen		×	×
Dokumente: Widerrufe		×	×
Dokumente: Verweigerungen		×	×
Dokumente: Suche		×	×
Formulare: Templates			×
Formulare: Module			×
Formulare: Policies			×
Analysen: Einwilligungsstatus		×	×
Analysen: Statistiken		×	×
Einstellungen: Domänen			×
Einstellungen: Import / Export			×
Einstellungen: Info	×	×	×

1.3 Verwaltung der Nutzer, Rollen und Rechte mittels MySQL und Docker EXEC

Die Verwaltung der Nutzer (anlegen, aktivieren, deaktivieren, Passwort ändern) und das Zuweisen von Rechten kann direkt in der entsprechenden Datenbank (gRAS) oder per *Docker EXEC* auf dem entsprechenden Datenbank-Container (hier: gics-2.11.0-mysql) erfolgen.

Die Verwaltung erfolgt auf Basis entsprechender MySQL-Prozeduren. Diese werden im Zuge der Docker-Installation der Web-Auth-Version automatisch angelegt.

Nutzer anlegen

⚠ ***Hinweis:*** *Das Nutzer-Passwort wird zwar im Klartext angegeben, die Prozedur jedoch erzeugt automatisch einen SHA-256-Hash, der in der gRAS-Datenbank gespeichert wird.*

in Docker

```
docker exec -it gics-2.11.0-mysql mysql -ugras_user -pgras_password
-e "use gras;call createUser('BENUTZERNAME','PASSWORT','KOMMENTAR');"
```

in SQL

```
use gras;

call createUser("BENUTZERNAME","PASSWORT","KOMMENTAR");
```

Rechtevergabe

Nutzer haben standardmäßig keine Berechtigungen. Die Vergabe dieser erfolgt je Werkzeug („Projekt“) unter der Angabe von *epix*, *gpas* oder *gics* (Schreibweise wie hier dargestellt).

Admin-Rechte vergeben

⚠ ***Hinweis:*** *Admin-Rechte beinhalten die Standard-Rechte.*

in Docker

```
docker exec -it gics-2.11.0-mysql mysql -ugras_user -pgras_password
-e "use gras;call grantAdminRights('PROJEKTNAME','BENUTZERNAME');"
```

in SQL

```
use gras;

call grantAdminRights("gics","BENUTZERNAME");
```

Standard-Rechte vergeben

in Docker

```
docker exec -it gics-2.11.0-mysql mysql -ugras_user -pgras_password
-e "use gras;call grantStandardRights('PROJEKTNAME','BENUTZERNAME');"
```

in SQL

```
use gras;

call grantStandardRights("epix","BENUTZERNAME");
```

Passwort ändern

in Docker

```
docker exec -it gics-2.11.0-mysql mysql -ugras_user -pgras_password -e "use
gras;call changePassword('BENUTZERNAME','NEUES_PASSWORT');"
```

in SQL

```
use gras;

call changePassword("BENUTZERNAME","NEUES_PASSWORT");
```

Nutzer aktivieren/deaktivieren

⚠ ***Hinweis:*** *Diese Änderungen werden erst nach einem Neustart des Wildfly übernommen.*

in Docker

```
docker exec -it gics-2.11.0-mysql mysql -ugras_user -pgras_password -e "use
gras;call disableUser('BENUTZERNAME');"
```

in SQL

```
call disableUser("BENUTZERNAME"); -- Benutzer deaktivieren

call enableUser("BENUTZERNAME"); -- Benutzer aktivieren
```

2 Empfehlungen zur Absicherung des Anwendungsservers

Der Zugriff auf relevante Anwendungs- und Datenbankserver der Treuhandstellen-Werkzeuge sollte nur für autorisiertes Personal und über autorisierte Endgeräte möglich sein. Wir empfehlen die Umsetzung nachfolgender IT-Sicherheitsmaßnahmen:

- Betrieb der relevanten Server in separaten Netzwerkzonen (getrennt von Forschungs- und Versorgungsnetz)
- Verwendung von Firewalls und IP-Filtern
- Zugangsbeschränkung auf URL-Ebene mit Basic Authentication (z.B. mit NGINX oder Apache)