Projekt: adit
Rollen & Permissions

Oliver Dias odiaslal@hsr.ch, Fabian Hauser fhauser@hsr.ch, Murièle Trentini mtrentin@hsr.ch,
Nico Vinzens nvinzens@hsr.ch, Michael Wieland mwieland@hsr.ch

Änderungsgeschichte

Datum	Version	Änderung	Autor
04.05.2017	1.0	Erstellen des Dokuments	Vin
09.05.2017	1.1	Review Dokument	Hau

Inhalt

1. Einführung

1.1 Zweck

Dieses Dokument definiert die verschiedenen Permissions, welche den Benutzerrollen zugewiesen werden sowie die Standardmässig vorhandenen Rollen. Benutzer werden jeweils einer Rolle zugewiesen, welche bestimmte Rechte besitzt.

1.2 Gültigkeitsbereich

Der Gültigkeitsbereich beschränkt sich auf die Projektdauer des Modul Engineering Projekt FS17. Das Dokument wird HSR Intern verwendet.

2. Permissions

Es existieren folgende Permissions:

ID	Name	Zweck
1	basic_permission	Berechtigung für die Basis Version der Website, beinhaltet auch die Rechte für das Editieren des eigenen Profils und der eigenen Inserate.
2	supervisor_permission	Berechtigung für die Supervisor Version der Website
3	administrator_permission	Berechtigung für die Administrator Version der Website
4	edit_categories	Berechtigung um Kategorien zu löschen / ändern hinzuzufügen /
5	review_advertisements	Berechtigung um Inserate abzulehnen / freizugeben
6	edit_role	Berechtigung um Rolle von Usern zu ändern
7	edit_isActive	Berechtigung um Zustand von Usern zu ändern

3. Nicht registrierter User

Der nicht registrierte User besitzt über keinerlei Berechtigung auf der Website. Besucht er die Website, wird ihm ein Screen angezeigt, der ihn auffordert, sich einzuloggen oder zu registrieren. Es ist ihm nicht möglich, andere Screens der Website zu besuchen. Sobald er sich registriert hat, besitzt er über die Berechtigungen des Users.

4. User

Der User hat die niedrigste Berechtigungsstufe auf der Website und hat somit die Rolle «user». Sie wird erteilt, sobald sich ein User bei «adit» registriert hat.

Der User hat folgende Berechtigungen:

- Nach dem Login werden ihm alle aktiven Inserate angezeigt (auch die der anderen User)
- Er kann mittels des Suchfelds nach aktiven Inseraten suchen
- Er sieht die Buttons «Inserat erstellen», «Account», «Inserate»
- Klickt er auf «Inserat erstellen», bekommt er ein Formular für das Erstellen neuer Inserate
- Klickt er auf «Account» sieht er eine Übersicht über seinen Account, inklusive der Tabs «Profil», «Meine Inserate» und «Private Messaging»
- Unter «Account» hat er die Möglichkeit sein eigenes Profil zu bearbeiten
- Unter «Meine Inserate» sieht er alle seine Inserate unabhängig von den Zuständen der Inserate. Es ist ihm hier möglich nicht gelöschte Inserate zu löschen / editieren.
- Unter «Private Messaging» werden ihm seine Konversationen angezeigt.

5. Supervisor

Der Supervisor übernimmt gewisse administrative Aufgaben auf der Website. Er ist zwischen User und Administrator angesiedelt und hat folgende Aufgaben:

- Hinzufügen / ändern / Löschen von Inserate-Kategorien
- Inserate freischalten / ablehnen

Um diese Aufgaben zu erfüllen hat er folgende Berechtigungen:

- Er hat sämtliche Berechtigungen eines Users
- Zusätzlich sieht er auf dem Startscreen einen «Button» «Supervisorpanel»
- Klickt er auf den Button sieht er einen Screen, der nur einem Supervisor zugänglich ist (ist aber für alle Supervisor der gleiche)
- Auf diesem Screen sieht er sämtliche Inserate, die sich im «to review» Status befinden, sowie die Buttons «Inserate verwalten» und «Kategorien verwalten».
- Klickt er auf ein Inserat, sieht er das Inserat in der Detailansicht sowie zwei Buttons «declined» und «approved. Mit den Buttons versetzt er die Inserate in die respektiven Zustände.
- Klickt er auf «Kategorien verwalten» sieht er eine Übersicht der Kategorien
- In dieser Übersicht ist es ihm möglich neue Kategorien zu erstellen und alte Kategorien zu ändern / löschen.

6. Administrator

Der Administrator besitzt die höchste Berechtigungsstufe und besitzt alle Zugriffe von User und Supervisor. Zusätzlich erhält er noch die Berechtigung, die Rollen anderer User zu ändern und den Zustand von Usern zwischen «active» und «not active» zu wechseln. Es ist ihm z.B. möglich, einen User zu einem Supervisor zu machen oder einem User die Berechtigung zu entziehen die Website unter diesem User zu besuchen (= ihn auf «not active» setzen und ihn so am Login hindern).

Um diese Aufgabe zu erfüllen hat er folgende Berechtigungen:

- Er hat sämtliche Berechtigungen des Users und des Supervisors
- Zusätzlich sieht er auf dem Startscreen den Button «Adminpanel»
- Klickt er den Button sieht er sämtliche User, ihre Rollen und ihren Zustand
- Klickt er auf einen User, sieht er eine Detailansicht, in der er die Rolle des Users oder den Zustand des Users ändern kann
- Dazu gehört auch das neue Erstellen von Rollen mit den festgelegten Berechtigungen aus Kapitel 2

7. Rest-API Permissions

Die im übrigen Teil des Dokuments beschriebenen Berechtigungen führen zu folgenden Regeln für Zugriffe auf die REST-APIs, die auf dem Backend definiert

7.1 User

GET: /user/id
DELETE: /user/id

- Benötigt mindestens «basic_permission» um auf den User mit der eigenen ID zuzugreifen
- Für Zugriffe auf User mit anderen IDs muss entweder «supervisor_permission» oder «administrator_permission» vorhanden sein

PUT: /user/id

- Benötigt mindestens «basic_permission» um auf den User mit der eigenen ID zuzugreifen
- Für Zugriffe auf User mit anderen IDs muss «edit_isActive» vorhanden sein («isActive» ist das einzige Feld das geändert werden soll)

POST: /register

- Benötigt keinerlei Berechtigungen und auch keinen aktiven User (kein Token)

Für alle anderen Zugriffe wird mindestens ein Token benötigt!

7.2 Advertisement

PUT: /advertisement/id

- Benötigt mindestens «basic_permission» um auf die Advertisements in denen der User mit der eigenen ID vorhanden ist, zugreifen zu können
- Für Zugriffe auf Advertisements anderer User muss «review_advertisements» vorhanden sein

DELETE: /advertisement/id

- Benötigt mindestens «basic_permission» um auf die Advertisements in denen der User mit der eigenen ID vorhanden ist, zugreifen zu können

Für alle anderen Zugriffe wird mindestens ein Token benötigt!

7.3 Category

POST: /category
PUT: /category/id
DELETE: /category/id

- Benötigen «edit_categories»

Für alle anderen Zugriffe wird mindestens ein Token benötigt!

7.4 Role

POST: /role
PUT: /role/id
DELETE: /role/id

- Benötigen «edit_roles»

Für alle anderen Zugriffe wird mindestens ein Token benötigt!

7.5 Authentication

POST: /authenticate

- Benötigt keine Permissions und auch kein Token