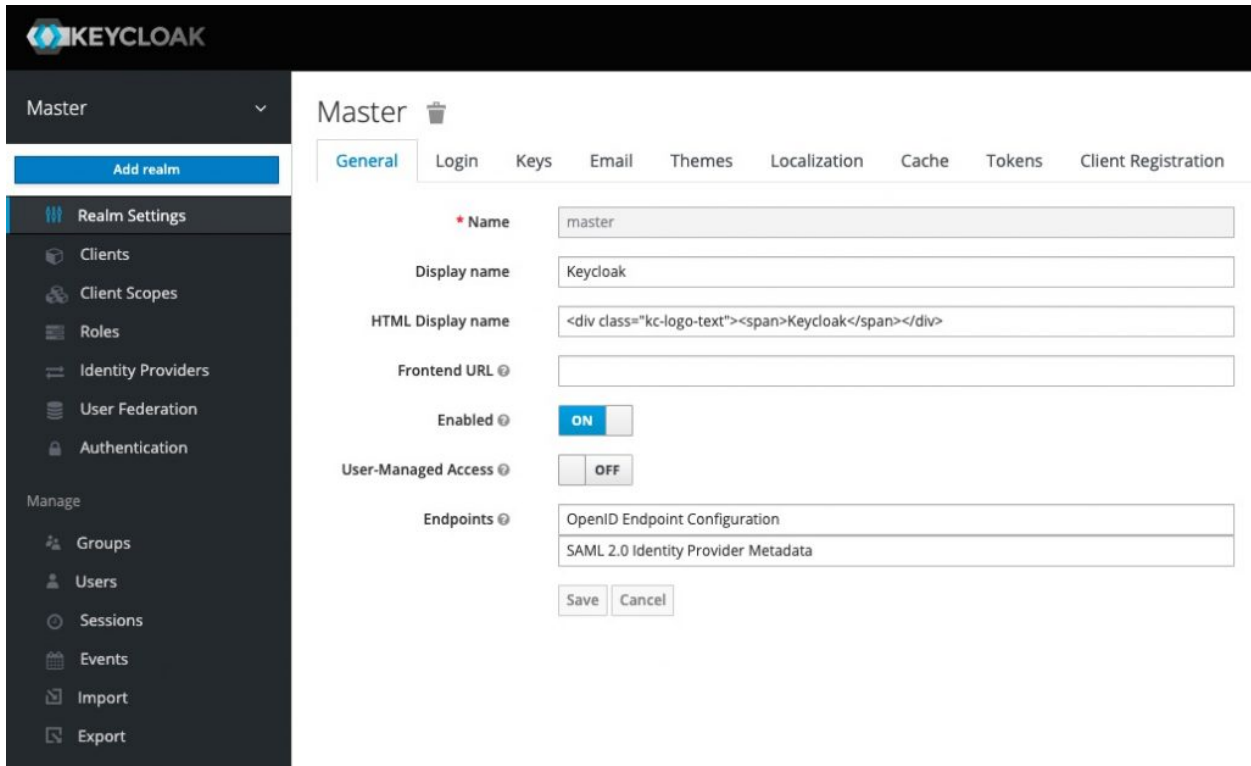


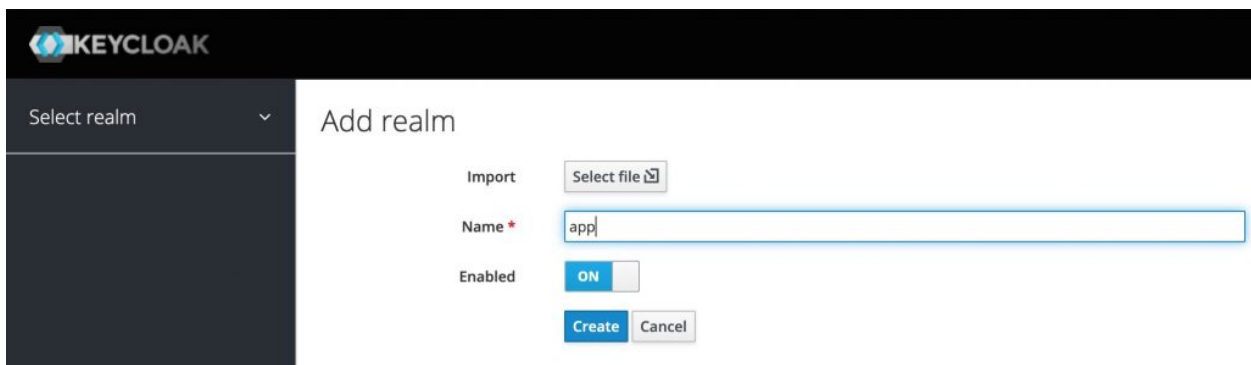
Create a new realm, client and users (Keycloak version 18)

1) Enter inside the Keycloak admin console (<http://localhost:8080/auth/admin>). The default username and password is **admin**. Move the mouse over **Master** and click in the Add realm button.



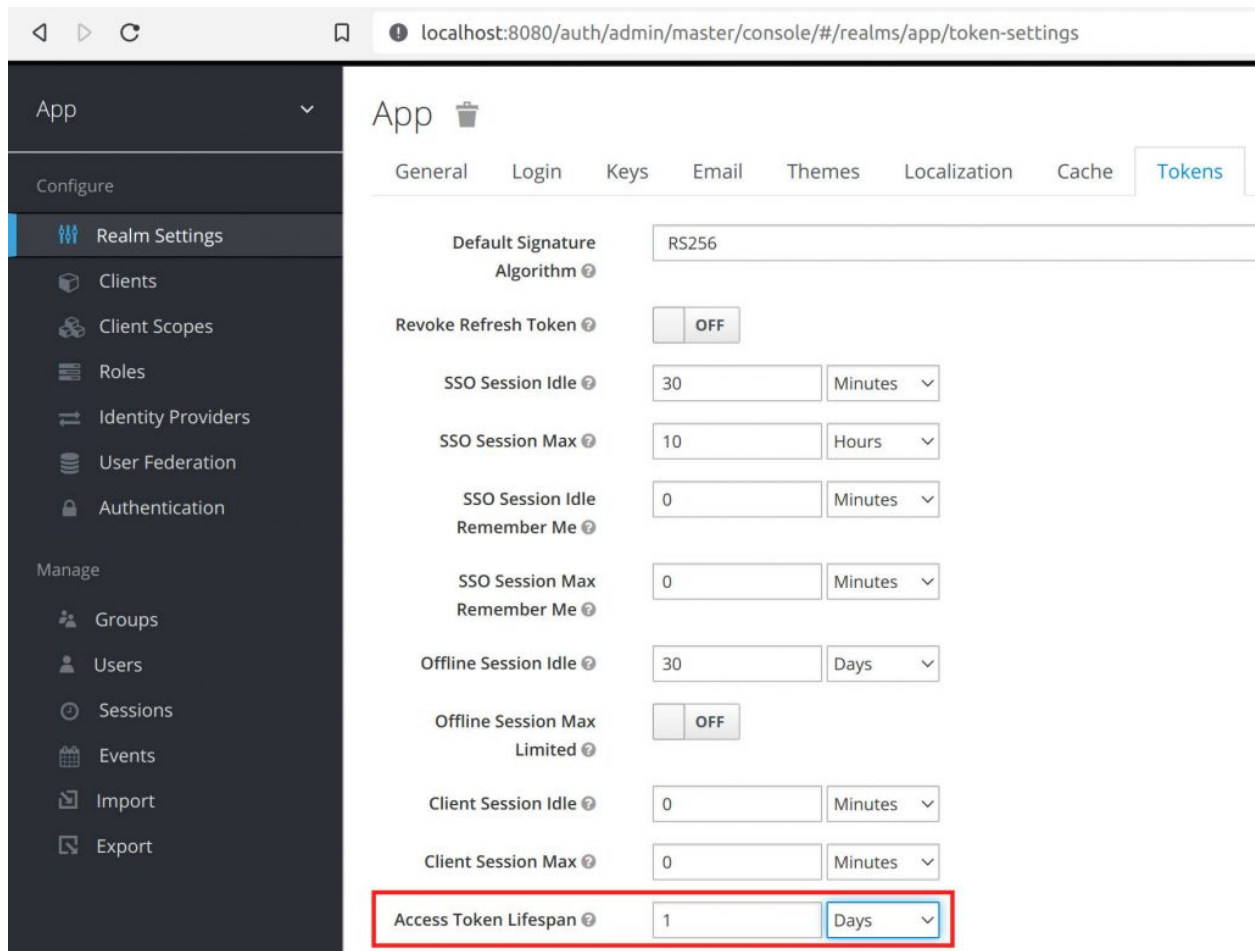
The screenshot shows the Keycloak Admin Console interface. On the left, there is a sidebar with a 'Master' dropdown menu and an 'Add realm' button. Below this, a list of management options is visible: Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication, Groups, Users, Sessions, Events, Import, and Export. The main content area is titled 'Master' and contains tabs for General, Login, Keys, Email, Themes, Localization, Cache, Tokens, and Client Registration. The 'General' tab is active, displaying fields for Name (set to 'master'), Display name (set to 'Keycloak'), HTML Display name (set to '<div class="kc-logo-text">Keycloak</div>'), Frontend URL, Enabled (toggle set to ON), User-Managed Access (toggle set to OFF), and Endpoints (listing OpenID Endpoint Configuration and SAML 2.0 Identity Provider Metadata). At the bottom of the form are 'Save' and 'Cancel' buttons.

2) Fill the name of the realm with **app** and click the Create button.

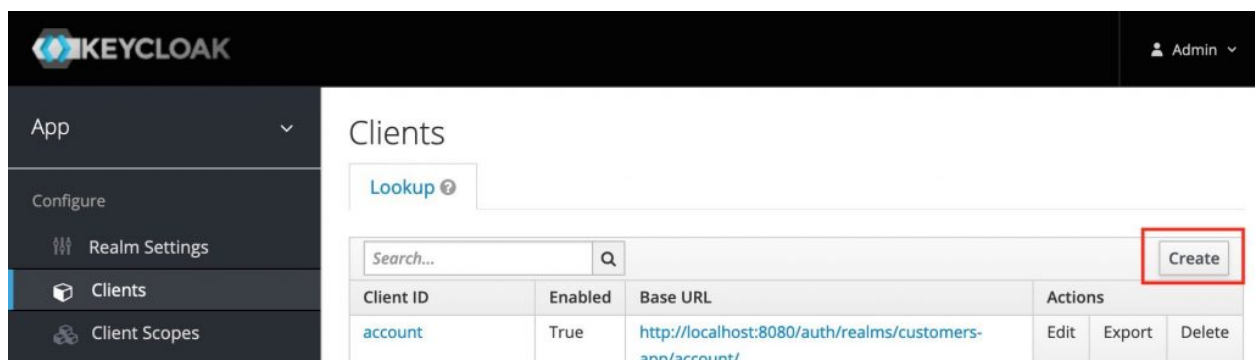


The screenshot shows the 'Add realm' form in the Keycloak Admin Console. The sidebar on the left has a 'Select realm' dropdown menu. The main content area is titled 'Add realm' and contains an 'Import' section with a 'Select file' button. Below this, there is a 'Name' field (marked with a red asterisk) containing the text 'app', an 'Enabled' toggle set to ON, and 'Create' and 'Cancel' buttons at the bottom.

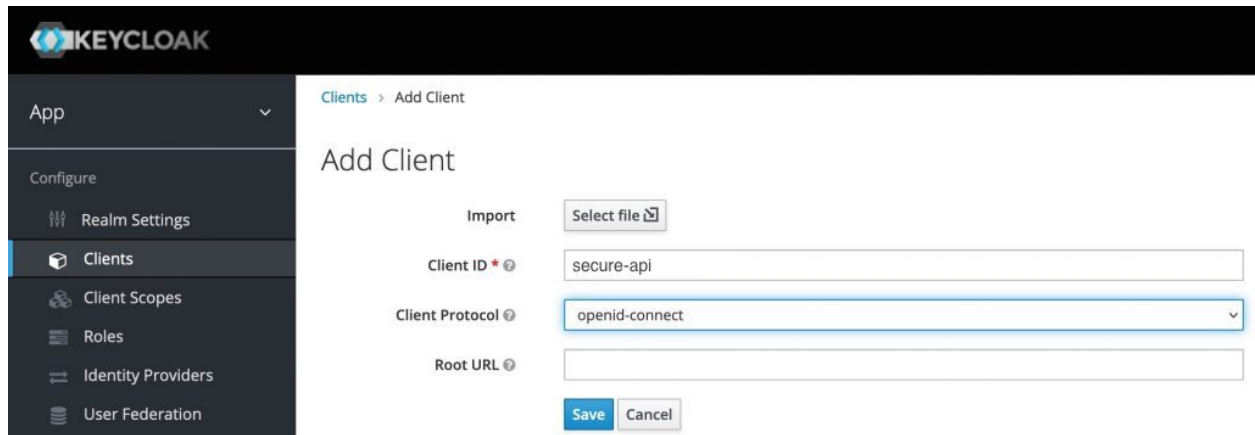
3) After the realm be created with success, click on the Tokens tab and change the Access Token Lifespan to 1 day.



4) Click on the Clients menu and after that, click the Create button.



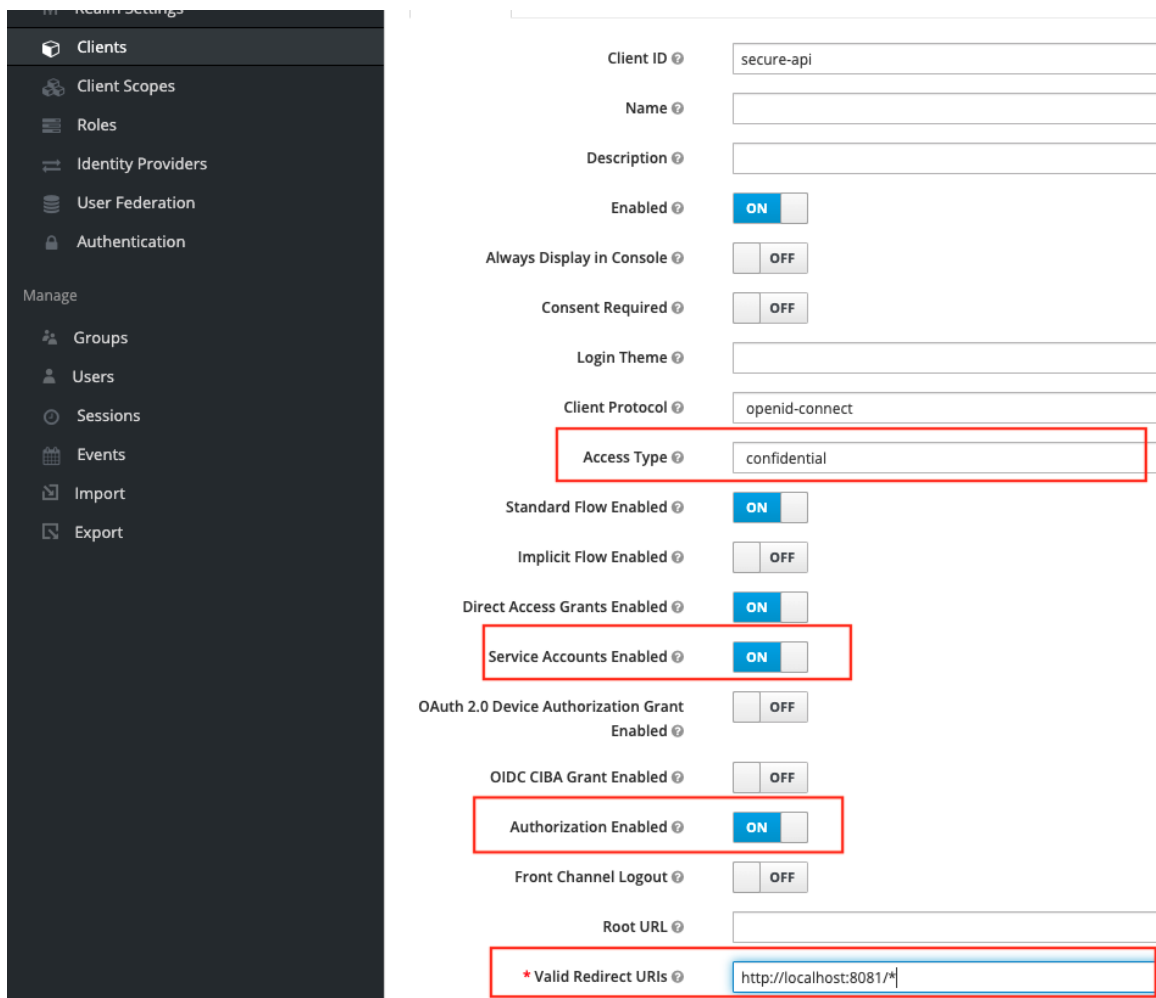
5) Fill the name with the client as **secure-api** and click the Save button.



The image shows the 'Add Client' form in the Keycloak administration console. The left sidebar contains the navigation menu with 'Clients' selected. The main form area is titled 'Add Client' and includes the following fields:

- Import:** A button labeled 'Select file'.
- Client ID:** A text input field containing 'secure-api'.
- Client Protocol:** A dropdown menu set to 'openid-connect'.
- Root URL:** An empty text input field.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

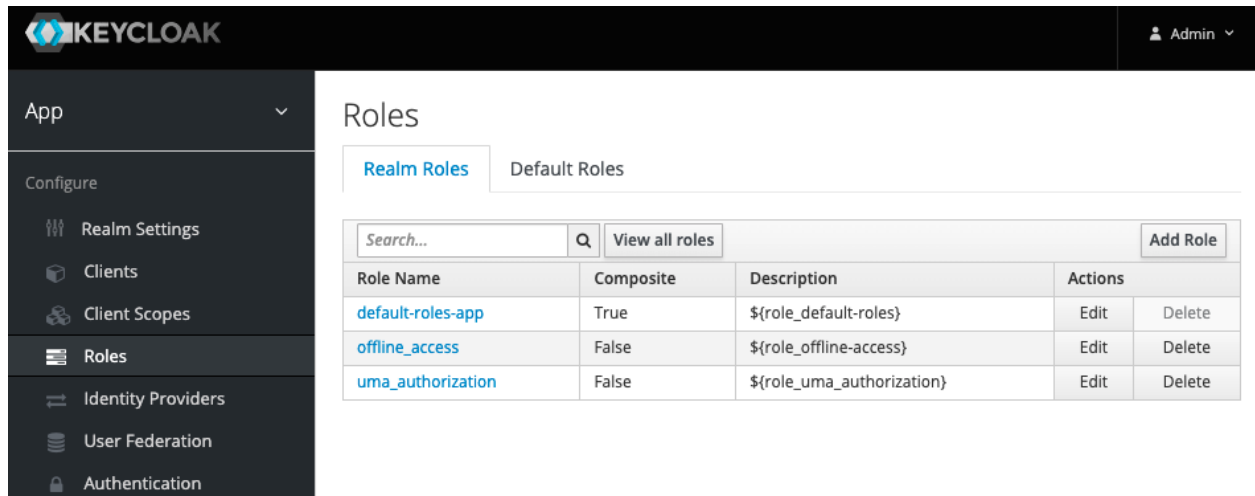
6) Go to the Clients menu again and click on the client you just created. Change the options to match the configuration below and click the Save button.



The image shows the configuration page for the 'secure-api' client in Keycloak. The left sidebar shows the navigation menu with 'Clients' selected. The main configuration area includes the following settings:

- Client ID:** secure-api
- Name:** (empty)
- Description:** (empty)
- Enabled:** ☒ ON
- Always Display in Console:** ☐ OFF
- Consent Required:** ☐ OFF
- Login Theme:** (empty)
- Client Protocol:** openid-connect
- Access Type:** confidential (highlighted with a red box)
- Standard Flow Enabled:** ☒ ON
- Implicit Flow Enabled:** ☐ OFF
- Direct Access Grants Enabled:** ☒ ON
- Service Accounts Enabled:** ☒ ON (highlighted with a red box)
- OAuth 2.0 Device Authorization Grant Enabled:** ☐ OFF
- OIDC CIBA Grant Enabled:** ☐ OFF
- Authorization Enabled:** ☒ ON (highlighted with a red box)
- Front Channel Logout:** ☐ OFF
- Root URL:** (empty)
- * Valid Redirect URIs:** http://localhost:8081/* (highlighted with a red box)

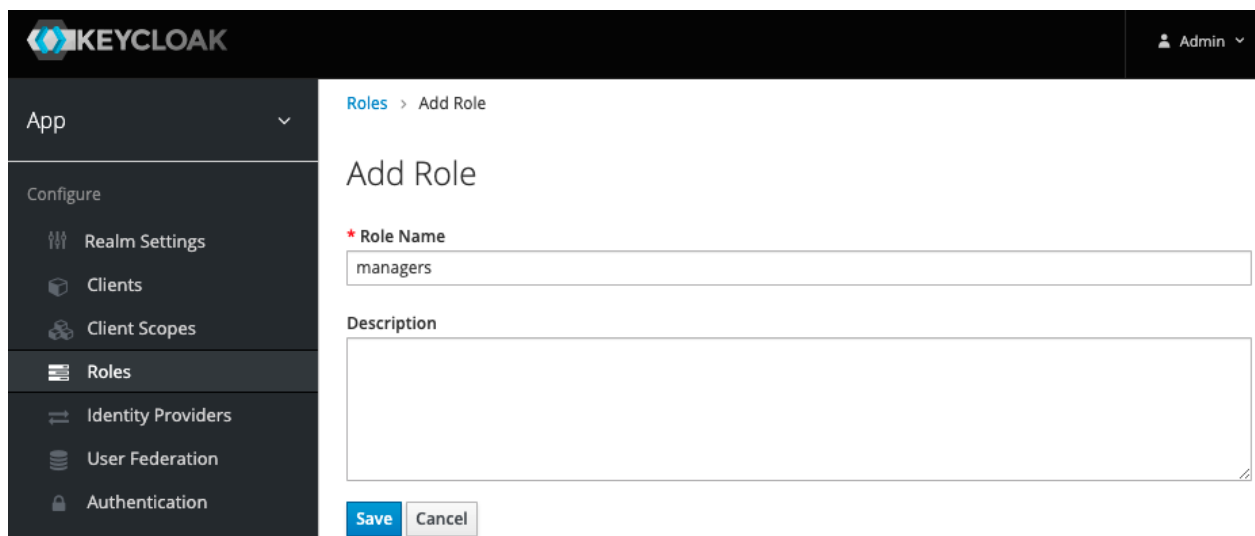
7) Click on the Roles menu, click Add role button.



The screenshot shows the Keycloak administration console. The left sidebar contains a navigation menu with 'App' at the top and 'Configure' below it. Under 'Configure', there are links for 'Realm Settings', 'Clients', 'Client Scopes', 'Roles' (which is highlighted), 'Identity Providers', 'User Federation', and 'Authentication'. The main content area is titled 'Roles' and has two tabs: 'Realm Roles' (selected) and 'Default Roles'. Below the tabs is a search bar with the text 'Search...' and a magnifying glass icon, followed by a 'View all roles' button and an 'Add Role' button. A table lists the roles:

Role Name	Composite	Description	Actions	
default-roles-app	True	\${role_default-roles}	Edit	Delete
offline_access	False	\${role_offline-access}	Edit	Delete
uma_authorization	False	\${role_uma_authorization}	Edit	Delete

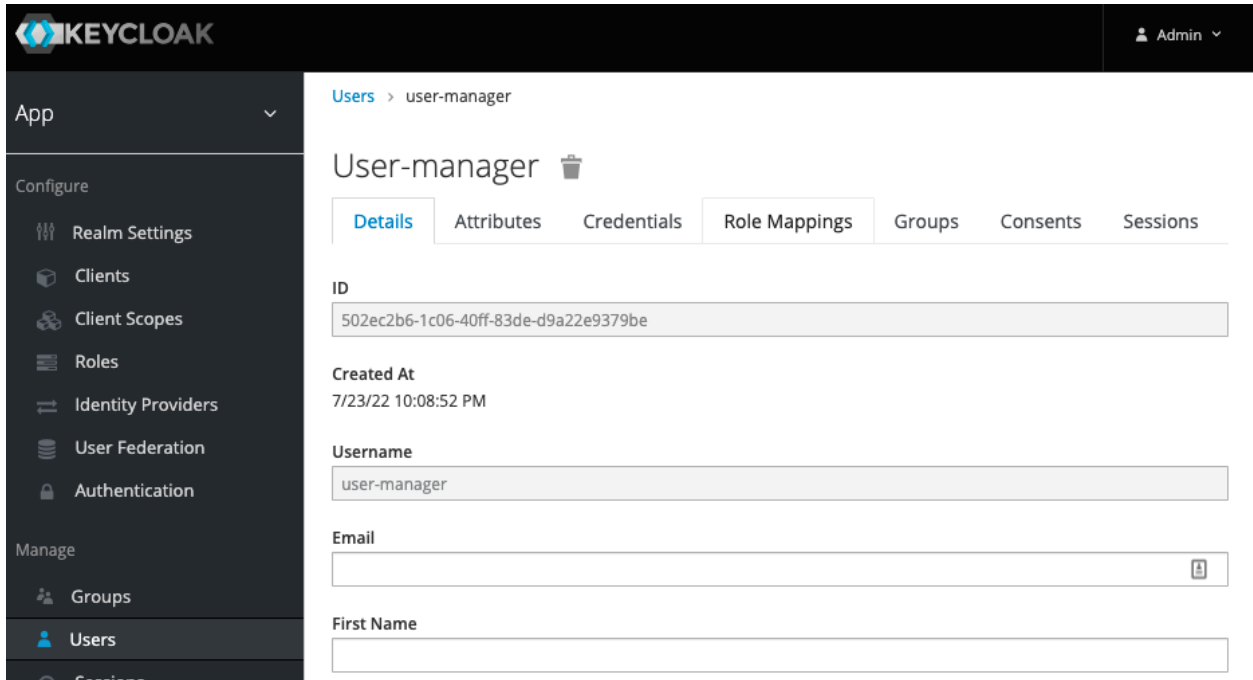
8) Fill the Role name input with **managers** and click the Save button.



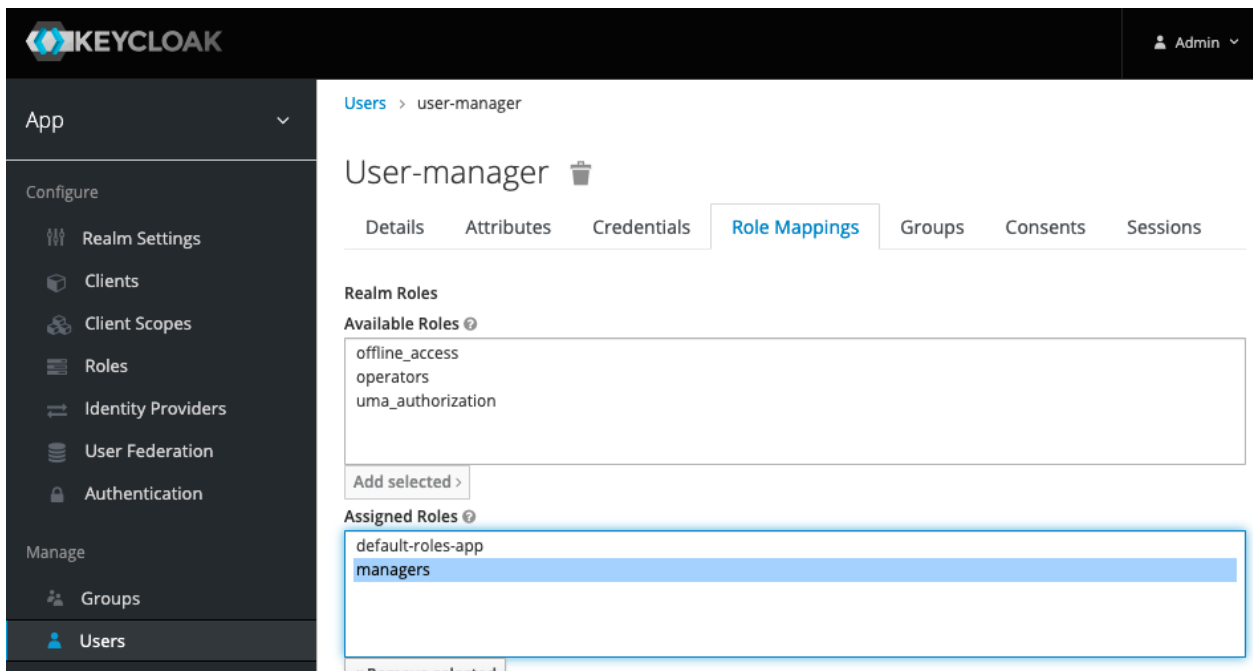
The screenshot shows the 'Add Role' form in the Keycloak administration console. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Add Role' and has a breadcrumb 'Roles > Add Role'. There is a red asterisk next to the 'Role Name' label. The 'Role Name' input field contains the text 'managers'. Below it is a 'Description' text area. At the bottom of the form are 'Save' and 'Cancel' buttons.

9) Repeat the last two steps to create another role called **operators**.

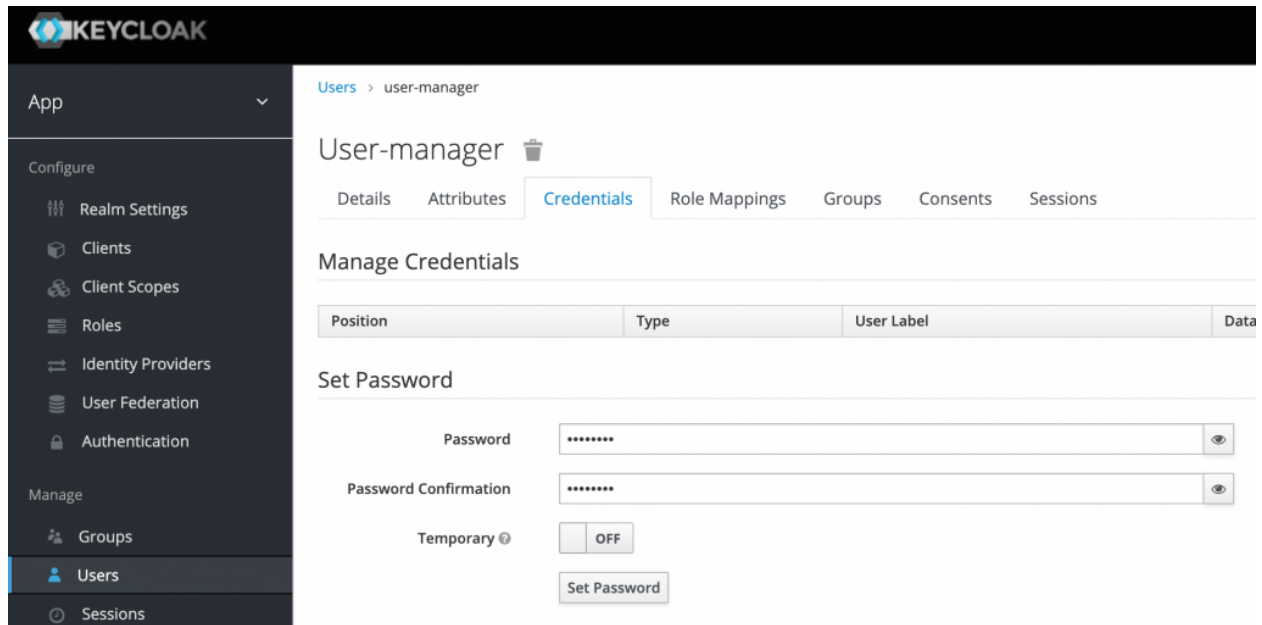
10) Go to the Users menu, click on Add user button, fill in the Username field user-manager and click the Save button.



11) Go to the Role Mappings tab, select the manager's role.



12) Go on the Credentials tab, create a password for the user (uncheck the temporary checkbox) and click the Set password button.



13. Repeat from step #10 to create another new user with username **user-operator**, and make sure to use the role **operators** inside the Role Mappings.