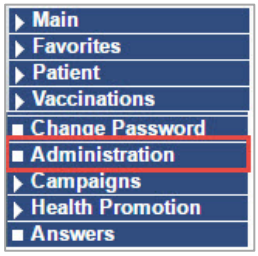
Modify Keycloak Roles in IWeb for Single Sign-On (SSO) Application Access

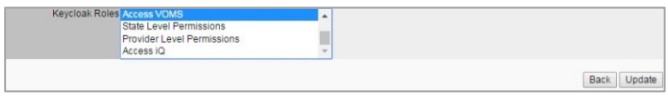
The following instructions allow administrative users to add, edit, or remove Keycloak roles to an existing user in order to grant (or revoke) user permissions for single sign-on (SSO) access to one or more STC applications.

1. Log in to SSO-enabled IWeb as a Registry Client user and click **Administration** on the left navigation menu.



2. On the Administration Main Menu page, scroll down to the User Management section and click **Search / Add User**.

3. On the Web User Search page, enter search parameters for the user to which you want to add single sign-on privileges, and then click **Search**.
4. Locate the user in the search result list and click the row to open the Web User Maintenance [Detail] page for that user.
5. At the bottom of the page, click **Update** to open the Web User Maintenance [Update] page.
6. Scroll down to the Keycloak Roles section of the page. **Note:** Since a valid email address is required to reset forgotten passwords, it is recommended that you first verify that the user has an email address entered, before adding or entering Keycloak roles.
7. In the Keycloak Roles list, select one or more roles to assign to the user. Click **Update** when finished.



The following are the available Keycloak roles:

- **Access AFIX** – Allows the user to access the SMaRT AFIX application
- **Access Manage Users Page** – Allows the user to access the Manage Users page in SMaRT AFIX
- **Access iQ** – Allows the users to access the STC | iQ application
- **Access IWeb** – Indicates that the user is an IWeb user
- **Access PHC-Hub** – Allows the user to access the PHC-Hub application
- **Access VOMS** – Allows the user to access the VOMS 2.0 application
- **Access STC|U** - Allows the user to access the STC|U learning management application
- **Organization Provider Content (data) Security** – Allows the user to access organization and facility data, as well as access to organizational functions. Note: Provider Level Permissions should also be assigned with this role
- **Provider (Org and Fac) groups Content (data) Security** – Allows the user to beaded to provider groups in SMaRT AFIX
- **Provider Interface Profile Form** – Allows the user to access the organization and/or facility functions in STC | iQ, depending on access level, including the Provider Interface Profile Form
- **Provider Level Permissions** – Allows the user access to facility data and functions
- **State Level Permissions** – Indicates the user has Registry Client access for any STC application