Solar Size

Role Based Access Control (RBAC)

April 9, 2022

About this document:

Role based access control is a breakdown of the authorization of the users of a software solution. Each role is assigned functionality, which can alter the use-cases of the service. Roles are assigned in a hierarchy, with certain sub-roles enabling further functionality separate from their parent class. This document breaks down the permissions of each type of user, as well their envisioned use cases.

Current Status:

With this project, we utilize a front-end dashboard that is open to anyone with access to the web page. Greenwave envisioned this tool as an internal service that they would utilize to show to their customers. Greenwave indicated that permission control was not a crucial aspect of the service to them, as they would socially enforce the limitations on who can use the tool.

We realize the importance of customizing an experience, and allowing for permissions to be granted and denied as to better serve the tool. Being able to limit who can request API calls, perform CRUD operations, and access the tool, would undoubtedly help create a better and more secure experience. At the time of this MVP, the SolarSize service has a single primary role:

1. **User** - The user is able to make calls to the API. The API calls include
   i. Getting an estimation based on inputs
   ii. Getting latitude and longitude values from the address
   iii. Sending a CSV file to the server
   The user is able to submit inputs and view the summary freely. They are not limited in their ability to perform actions if they have access to the web page.

Envisioned Status:

Our envisioned roles are as follows:

1.
   Registered User - A user would be required to make a login. With this login, they will be able to use the website. When they make calls to the API, their account grants them access by utilizing a unique API key. Users can save their locations and results. The user role can also submit support requests to the

website. They can also submit bug reports or inaccuracies.

   a. **Residential** - Residential users would have simplified inputs. There would be more plain language used, for example, excluding module efficiency, and using only panel wattage, which is more clearly viewed when buying a solar panel.

   b. **Industrial** - Industrial users would have more advanced inputs. They would have access to special APi calls, such as more detailed summary pages. For example, the page could include peak KV usage analysis using the spikes of power usage.

2. **Non-registered user -** A non-registered user would have access to a login page and a signup page. They would not have access to the API or tool until they signed up.

3. **Admin** - An admin role would have access to all the privileges that a normal User account has. Admin accounts can also view support tickets based on their subrole. Admins could also have special access to the API to allow for CRUD actions to occur.

   a. **Business Admin:** A business admin would have access to user inquiries and business problems. They would be informed of a user's personal information and their previously entered inputs.

   b. **Developer:** A developer would not have access to a user's personal information. Once logged in, they would be able to see special debugging information on the webpage. They would also have access to bug reports and technical questions.