RBAC VISION

Copy-Waste

Importance of RBAC

Role Based Access Control (RBAC) is an important aspect of software development as it allows the software to control and authorize the various actions a user can make in order to manipulate and view information presented to them. Specifically, it provides the ability for the software to attach permissions to users in order to authorize any create, read, update, and delete actions they perform as they interact with the interface. This provides security to the information, as well as ensuring the information is accurate and curated for the given user.

Current State of RBAC

In its current state, RBAC for this project is handled by the Streamsight API, which is implemented and managed by Prairie Robotics. Our dashboard communicates with the Streamsight API to request information required for the components on the dashboard. In this communication process, the API is responsible for authorizing any requests prior to fulfilling them. This is achieved by taking advantage of the login process which activates a session token containing the user's username. This username is first authenticated through an Amazon Web Service (AWS) called Cognito to ensure the user is valid. Then this username is queried within the database to validate any required permissions to access information requested in the future.

As the Green Screen dashboard is currently a read-only interface, the information displayed is primarily related to the service events which are recorded, and the contaminants that were identified for a specific organization. In order to effectively view this information on the dashboard, the users are required to have the following read permissions:

1. serviceEvents **2.** serviceEventContaminants

3. contaminants **4.** organization

If the user does not have these permissions, their request will not be authorized to read this information. To indicate this, they will be provided a "Forbidden Request" message from the API.

Future Developments

In future iterations of the dashboard, it would be useful for users to communicate and create threads to identify issues, and converse with their peers to drive improvement within their local recycling streams within their municipalities. However, this would require the creation of additional permissions for users to not only read, but be able to create, update, and delete messages and conversations.

The permissions that should be added when this functionality is implemented would include:

1. createMessage
2. readMessage
3. updateMessage
4. deleteMessage

These permissions will be important so that an average user does not have the ability to update or delete another user's message unless they are an administrator for the municipality. Additionally, every user should be able to create and read messages within their organization, while not being able to create / read messages from other municipalities. These additions will be significant when scaling up the reach and use of the Green Screen dashboard.

Definitions:

Service Event: occurs when recycling is collected from a bin