**Name:** Manage Authorization

**Goal:** Manage and control access to resources within a system based on user authorization levels.

**Actors:** Owner, Authorized User, Not Authorized User

**Preconditions:** The Owner has the necessary privileges to manage authorizations.

**Success End Condition:**

* The Owner successfully adds or removes authorizations for users.
* Authorized Users access and interact with resources according to their granted permissions.
* Not Authorized Users are denied access to restricted resources.

**Failed End Condition:**

* The Owner fails to add or remove authorizations for users.
* Authorized Users are unable to access resources according to their granted permissions.
* Not Authorized Users gain access to restricted resources.

**Trigger:** The Owner, Authorized User, or Not Authorized User attempts to access or manage resources within the system.

**Main Success Scenario:**

1. The Owner adds or removes authorization for a user.
2. The user's authorization status is updated accordingly in the system.
3. Authorized Users access resources according to their granted permissions.
4. Not Authorized Users are denied access to restricted resources.

**Extensions:**

1a. The Owner needs to modify the authorization level of an existing user.

1a1. The Owner updates the user's authorization level, granting or revoking specific permissions.

2a. Authorized User requests additional permissions.

2a1. The Owner reviews the request and decides whether to grant or deny the additional permissions.

**Sub-Variants:** None

**Related Information:**

* The authorizations are role-based.
* Periodic review of user authorizations to ensure they remain up-to-date and relevant.