Use Case

**Use Case: User Authentication**

**Actor:** User

**Description:** This use case describes the process by which a user authenticates themselves to access the Security Town System.

**Preconditions:**

The Security Town System is accessible and running.

The user has an account registered with the system.

**Postconditions:**

Upon successful authentication, the user gains access to the system's functionalities.

Upon unsuccessful authentication, the user is denied access and may be prompted to try again or reset their password.

**Main Flow:**

1-The user navigates to the login page of the Security Town System.

2-The system presents the user with input fields for username/email and password.

3-The user enters their username/email and password.

4-The user submits the login form.

5-The system verifies the entered credentials:

**--If the credentials are valid:**

-The system authenticates the user.

-The system grants access to the user's account and associated functionalities.

-The system logs the user's access activity.

**--If the credentials are invalid:**

-The system denies access to the user.

-The system may display an error message indicating that the credentials are incorrect.

6-The use case ends.

**Alternate Flows:**

**Invalid Credentials:**

**If the entered credentials are invalid:**

-The system denies access to the user.

-The system may display an error message indicating that the credentials are incorrect.

-The user may choose to try again or initiate a password reset process.

**Exceptions:**

**1-Technical Failure:**

**If there is a technical failure during the authentication process:**

-The system notifies the user of the failure.

-The user may retry the authentication process later.

**2-Account Lockout:**

**If the user exceeds a certain number of failed login attempts:**

-The system locks the user's account temporarily.

-The user may need to contact support or go through a password reset process to regain access.