**Use Case Description**

|  |  |  |
| --- | --- | --- |
| Use case name: | Log In | |
| Scenario: | User is logging in to their account to view or modify information.  Admin user is logging in to their account to create new users, delete/disable users, and update member information. | |
| Triggering event: | User clicks “Log In” | |
| Brief description: | See “Scenario” | |
| Actors: | Admin User, Regular User | |
| Related use cases: | Create Account | |
| Stakeholders: | User | |
| Preconditions: | Account is created, directory not accessible | |
| Postconditions: | Directory is accessible according to permissions OR access is denied | |
| Flow of activities 1: | Admin User:   1. Admin user inputs account user name and password, and clicks “Log in” 2. Admin user clicks “Update Directory” | System:   1. Validates administrative account information 2. Grants access to user with admin rights 3. System presents member directory access control list (ACL) interface |
| Flow of activities 2: | Admin User:   1. Admin user inputs account user name and password, and clicks “Log in” 2. Repeat for a total of 3 times 3. Repeat 1 with added captcha information | System:   1. Validates administrative account information 2. Denies access to user 3. Display a captcha 4. Repeat 1 5. Grant access to user |
| Flow of activities 3: | Regular User:   1. User inputs account user name and password, and clicks “Log in” | System:   1. Validates account information 2. Grants access to user |
| Flow of activities 4: | Regular User:   1. User inputs account user name and password, clicks “Log in” 2. Repeat for a total of 3 times 3. Repeat 1 with added captcha information | System:   1. Validates account information 2. Denies access to user 3. Display a captcha 4. Repeat 1 5. Grant access to user |
| Exception conditions: | User does not input valid account security information | |