## Main roles:

User – guest who is not logged in

Registered User – logged user

Administrator??? - Client

## Product Functions

|  |  |  |  |
| --- | --- | --- | --- |
| CLASS OF USE CASES | № | USE CASES | DESCRIPTION OF USE CASES |
| Related to System Authentication | 1 | **Register** | *Register in the Reminder* |
| 2 | **Log in** | *Login in the Reminder* |
|  | 3 | **Forgot Password** | *User enters email he used for registration and receives new password on that email* |
|  | 4 | **Change Password** | *Changes the login password* |
|  |  |  |  |

## Functional Requirements

*Use cases related to System Authentication:*

*Use Case №1:* Register  
*Primary Actor*: User/Registered User  
*Pre Condition*: Installed browser and active internet connection. User hits Reminter ulr in the address bar. User is redirected to Reminder main page. From there user hits “Register” (Refer to prototype)

*Valid Format for different Fields:*

*“Username”* field:

* Username is a sequence of letters and digits, where '**.**', '**-**' and '**\_**' can appear between them
* Small and capital letters from Latin alphabet
* Special symbols “\_ . -”
* Digits 0-9
* Each username must start with small or capital letter
* Two symbols can’t be used one after the other

*“Email address”* field:

Emails are considered to be in format **<user>@<host>**, where:

* **<user>** is a sequence of letters and digits, where '**.**', '**-**' and '**\_**' can appear between them.
* **<host>** is a sequence of at least two words, separated by dots '**.**'. Each word is sequence of letters and can have hyphens '**-**' between the letters

*“Password”* field:

* A minimum of 6 characters is required.
* Small and capital letters from Latin alphabet
* Punctuation marks
* Digits 0-9
* Password must be mix of uppercase and lowercase characters, numbers and punctuation.
* If you change an existing password, the new one must be different from the last password

*“Confirm password”* field:

* Exact match with “Password” field

*Main scenario*:

1. User types his desired username in “Username” filed
2. User types his email address in “Email address” filed
3. User types his desired password in “Password” filed
4. User confirms his desired password in “Confirm password” filed
5. System does authentication
6. User is redirected to new page with message: ”To complete the registration, please confirm you details send on your email address.”
7. Once he click on the link from the message send to email address upon registration he will be redirected to his Dashboard. In this email will be described the T&C that he accept upon hit.

*Alternate scenario:*

1. Authorization fails – User hits the “Register now” button with blank:

* “Username” field
* “Email address” field
* “Password” field
* “Confirm password” field
  1. System does Authentication
  2. Prompt the user error messages
* “Enter username”
* “Enter email address”
* “Enter password”
* “Confirm password”
  1. User is allowed to enter all details

1. Authorization fails – User hits the “Register now” button with one or more blank fields
   1. System does Authentication
   2. Prompt error message to enter the data where fields are left blank
   3. Information in “Username” and “Email address” fields if there is such provided is been saved
   4. Information in “Enter password” and “Confirm password” fields if there is such provided in been deleted
   5. User is allowed to enter the details
2. Authorization fails – User hits the “Register now” button with details in all fields.
   1. System does Authentication
      1. If one or more fields are not in the right format
         1. Prompt error messages for incorrect credentials
         2. Information in all field where data is not in the right format is deleted including the “Enter password” and “Confirm password” fieldsno matter if they are in the right format
         3. User is allowed to enter new details
      2. If there is a registration with both the username typed in “Username” and the email typed in “Email address”
         1. Prompt error messages “Username is already taken” and “Email address is already used for registration”
         2. Information in “Username” is deleted.
         3. Information in “Email address” field is deleted
         4. Information in “Enter password” and “Confirm password” fields is deleted
         5. User is allowed to enter new details
      3. If there is a registration with the username typed in “Username” and all other fields are completed correctly
         1. Prompt error messages “Username is already taken”
         2. Information in “Username” is deleted.
         3. Information in “Email address” field is deleted
         4. Information in “Enter password” and “Confirm password” fields is deleted
         5. User is allowed to enter new details
      4. If there is a registration with the email typed in “Email address” field and all other fields are completed correctly
         1. Prompt error messages “Email address is already used for registration”
         2. Information in “Username” is kept.
         3. Information in “Email address” field is deleted
         4. Information in “Enter password” and “Confirm password” fields is deleted
         5. User is allowed to enter new details
   2. Authorization fails – User hits the “Register now” button with different passwords in “Password” and “Confirm password” fields
      1. If information in “Username”, “Email address” and “Password” fields is valid
         1. Prompt error message “Password not match”
         2. Information in “Username” is kept.
         3. Information in “Email address” is kept
         4. Information in “ “Confirm password” field is deleted
         5. User is allowed to enter new details
      2. If information in one or more of “Username”, “Email address” and “Password” fields is not valid
         1. Prompt error messages for incorrect fields
         2. Information in “Username” is deleted if not valid.
         3. Information in “Email address” is deleted if not valid
         4. Information in “ “Confirm password” field is deleted
         5. User is allowed to enter new details
3. User select the “Log in” button
   1. User is redirected to “Log in” page from where he can enter the system

*Use Case №2:* Login  
*Primary Actor*: User/Registered User  
*Pre Condition*: Installed browser and active internet connection. User hits Reminter ulr in the address bar. User is redirected to Reminder main page. User select the “Log in” button and is redirected to “Log in” page (Refer to prototype).  
*Main scenario*:

1. User types valid username or email address in “Username or email address” field and valid password in “Password” field
2. User hits the “Log in” button
3. System does authentication
4. Reminder Dashboard is displayed

*Alternate scenario:*

1. Authorization fails – User hits the “Log in” button with blank “Username or email address” field and blank “Password” field.
   1. System does authentication
   2. Prompt the user error messages “Enter username” and “Enter password”
   3. User is allowed to enter username or email address and password
2. Authorization fails – User hits the “Log in” button with blank “Username or email address” field and any password typed in “Password” field.
   1. System does authentication
   2. Prompt the user error message “Enter username”
   3. Typed in the “Password” field is deleted and field is returned to its initial state - blank
   4. User is allowed to enter username or email address and password
3. Authorization fails – User hits the “Log in” button with typed registered/not registered username or email address in “Username or email address” field and blank “Password” field.
   1. System does authentication
   2. Prompt the user error message “Enter password”
   3. User is allowed to enter password. “Username or email address” field keeps the information
4. Authorization fails – User hits the “Log in” button with typed not registered username or email address in “Username or email address” field and any password typed in “Password” field.
   1. System does authentication
   2. Prompt the user error message “Incorrect username”
   3. Typed in the “Password” and in “Username or email address” fields is deleted and fields are returned to their initial state - blank
   4. User is allowed to enter password. “Username or email address” field keeps the information
5. Authorization fails – User hits the “Log in” button with typed registered username or email address in “Username or email address” field and incorrect password typed in “Password” field.
   1. System does authentication
   2. Prompt the user error messages “Incorrect password”
   3. User is allowed to re-enter password. “Username or email address” field keeps the information
   4. If user tried 5 times with wrong passwords, the account will be closed for log in and email will be send to users email address. He will be redirected to different page with information about that.
6. Authorization fails – User hits the “Log in” button with typed correct password for some registered user or for the user entered in “Password” field in “Username or email address” field and valid registered username or email address typed in “Password” field.
   1. System does authentication
   2. If typed in “Username or email address” doesn’t match any registered username or email address
      1. Prompt the user error messages “Incorrect User”
      2. Typed in the “Password” and in “Username or email address” fields is deleted and fields are returned to their initial state - blank
      3. User is allowed to re-enter username.
   3. If typed in “Username or email address” matches registered username or email address
      1. Prompt the user error messages “Incorrect Password”
      2. Typed in the “Password” field is deleted and field is returned to its initial state - blank
      3. User is allowed to re-enter username.
7. User select the “Back to Register” button
   1. User is redirected to “Register” page from where he can register
8. User select the “Forgot password” button
   1. User is redirected to “Forgotten password” page from where he can fill in his email address in order to receive new password

*Use Case №3:* Forgot password  
*Primary Actor*: User/Registered User  
*Pre Condition*: Installed browser and active internet connection. User hits Reminter ulr in the address bar. User is redirected to Reminder main page. User selects the “Log in” button and is redirected to “Log in” page. User selects “Forgot password” label and is redirected to “Forgotten password” page (Refer to prototype).  
*Main scenario*:

1. User types valid email address in “Email address” field
2. User hits the “Send new password” button
3. System does authentication
4. User is redirected to different page that confirms a new password is sent to his email.

*Alternate scenario:*

1. Authorization fails – User hits the “Send new password” button with blank “Email address” field
   1. System does authentication
   2. Prompt the user error message “Enter email”
   3. User is allowed to enter email address
2. Authorization fails – User hits the “Send new password” button with email in invalid format written in “Email address” field
   1. System does authentication
   2. Prompt the user error message “Invalid email format”
   3. User is allowed to enter email address
3. Authorization fails – User hits the “Send new password” button with not registered email written in “Email address” field
   1. System does authentication
   2. Prompt the user error message “Not registered email”
   3. User is allowed to enter email address

*Use Case №4:* Change password  
*Primary Actor*: Registered User  
*Pre Condition*: User is logged in in the Reminder. User selects “Account” menu. User selects “Change Password” option. A pop-up window displays the “Change password” panel (Refer to prototype).  
*Main scenario*:

1. User types his current password in “Current password” field
2. User types his desired new password in valid format in “New password” field
3. User confirms his new password in “Confirm new password” field
4. User hits the “Change password” button
5. System does authentication
6. A password conformation message is shown on the same pop-up window

*Alternate scenario:*

1. Authorization fails – User hits the ““Change password” button with blank one or more of the fields “Current password”, “New password”, “Confirm new password”
   1. System does authentication
   2. Prompt the user error message where field/s is/are blank
   3. Information in all fields is deleted
   4. User is allowed to enter email address
2. Authorization fails – User hits the ““Change password” button with password in invalid format in or more of the fields “Current password”, “New password”, “Confirm new password”
   1. System does authentication
   2. Prompt the user error message where field/s is/are not in the right format
   3. Information in all fields is deleted
   4. User is allowed to enter email address
3. Authorization fails – User hits the ““Change password” button with password that doesn’t match his current password in “Current password” field, and any or bland information in or more of the fields “New password”, “Confirm new password”
   1. System does authentication
   2. Prompt the user error message “Invalid password” for “Current password” field
   3. Information in all fields is deleted
   4. User is allowed to enter email address
4. Authorization fails – User hits the ““Change password” button with password that matches his current password in “Current password” field, and password in invalid format in “New password” and “Confirm new password” fields
   1. System does authentication
   2. Prompt the user error message “Invalid password format” for “New password” field and/or “Confirm new password” field
   3. Information in all fields is deleted
   4. User is allowed to enter email address
5. Authorization fails – User hits the ““Change password” button with password that matches his current password in “Current password” field, and different passwords in valid format in “New password” and “Confirm new password” fields
   1. System does authentication
   2. Prompt the user error message “Password not match” for “Confirm new password” field
   3. Information in all fields is deleted
   4. User is allowed to enter email address
6. User hits the ““Change password” button with password that matches his current password in “Current password” field, and same password for “New password” and “Confirm new password” fields
   1. System does authentication
   2. Prompt the user error message “Incorrect password”
   3. Information in all fields is deleted
   4. User is allowed to enter email address

More cases to be tested. To be added in test cases:

1. User hits the ““Change password” button with password that doesn’t match his current password in “Current password” field, his current password in “New password” and “Confirm new password” fields
   1. System does authentication
   2. Prompt the user error message “Invalid password”
   3. Information in all fields is deleted
   4. User is allowed to enter email address