Test Cases
Group 5 - Adila Biswas, Brina Chahal, Ethan Trant, Shefat Rahman, Zeba Karobi

Test Case 1: Configuration for Length - Set Length

Input:

1. A password configuration rule that states that the password length should be a specific number (e.g., a set length of 12 characters).

Tests:

1. Test to check if the input is less than the minimum length for the password generator.
2. Test to check if the input is greater than the maximum length for the password generator.
3. Test to check if the input is within the generator's default maximum and minimum password character limit.

Output:

Pass: Carry on with all other password configuration tests. Once all tests are passed, the latest valid password is displayed and added to the session history.

Fail: Error message indicating an invalid given length.

Test Case 2: Configuration for Length - Set Length

Input:

1. A password configuration rule that states that the password length should be within a range for the length (e.g., minimum length of 8 characters and maximum length of 12 characters).

Tests:

1. Test to check if the maximum or minimum input is less than the minimum length for the password generator.
2. Test to check if the maximum or minimum input is greater than the maximum length for the password generator.
3. Test to check if the inputted range is within the generator's default maximum and minimum password character limits.

Output:

Pass: Carry on with all other password configuration tests. Once all tests are passed, the latest valid password should be created with a randomly generated number within the range as the length.

Fail: Error message indicating an invalid given length range.

Test Case 3: Configuration for Special Characters

Input:

1. A password configuration rule that states that the password should or shouldn't include special characters (e.g., include at least 1 special character from default special character list for passwords).

Tests:

1. Test to check if the special characters list is valid.
2. Test to check if the chosen configuration conflicts with any other chosen configuration rule.

Output:

Pass: Carry on with all other password configuration tests. Once all tests are passed, the latest valid password should be created with or without special characters to the rule's specification.

Fail: Error message indicating an invalid special characters rule.

Test Case 4: Internal Password Check Against Configuration Rules

Input:

1. Password is generated.

Tests:

1. Test that password meets the specified length, or falls within the specified length range.
2. Test that the password meets the specified special characters requirement according to the set rule.
3. Test that the password meets the upper and lowercase requirement according to the set rule.
4. Test that the password meets the number requirement according to the set rule.
5. Test that the password meets the minimum strength requirement according to the set rule.

Output:

Pass: Password is successful in generation, added to the session history, and displayed for the user.

Fail: Password is regenerated, not added to session history, and not displayed for the user.

Test Case 5: Request to Regenerate Password Using Same Rules

Input:

1. Regenerate password button is pressed.

Tests:

1. Test that previously specified rules are still valid.
2. Test that newly generated password meets strength requirements.
3. Test that newly generated password meets all configured rules requirements.

Output:

Pass: Password is successful in regeneration, added to the session history, and displayed for the user.

Fail: Password is regenerated, not added to session history, and not displayed for the user.

Test Case 6: History Clearing - On Request

Input:

1. Clear history button pressed.
2. User confirmation: ‘Yes’ or ‘No’.

Tests:

1. Test to check if the clear history button is pressed.
2. Test to check if the User response is ‘No’ to clearing generated password history.
3. Test to check if the User response is ‘Yes’.

Output:

Pass: If user response is yes, clear history. If no, abort clearing history. The result matches the user’s response.

Fail: Error message indicating that there was an error, and that history will be cleared.

Test Case 7: History Clearing - On Session End

Input:

1. User ends the session.

Tests:

1. Test to check if the session is ending.

Output:

Pass: Session history is cleared without additional user confirmation.

Fail: Error message indicating that there was an error with ending the session, and that history will be cleared.

Test Case 8: Session History Update with Latest Generated Password

Input:

1. A new password is successfully generated.

Tests:

1. Test that the newest generation was added successfully to the session history.

Output:

Pass: Latest generated password is added to session history with no other input.

Fail: Error message indicating that there was an error with updating the session history, and that history will be cleared.