

# Manual (original version)

## Feature 1 - Password Length

### How it Works

The application allows users to specify the desired length of the password. This length determines how many characters the password will contain. The `generate_password` function in `password_generator.py` uses this length parameter to construct a password of exactly the specified number of characters.

### User Expectations

Users can expect that the generated password will strictly adhere to the specified length. Shorter passwords are typically easier to remember but may be less secure, while longer passwords increase security at the expense of memorability.

## Feature 2 - Strength of Randomness

### How it Works

The randomness strength ("high", "medium", or "low") affects the predictability of the password. For "high" randomness, the application uses Python's `random.SystemRandom().choice` method, which is designed to be cryptographically more secure. For "medium" and "low" randomness, `random.sample` and `random.choices` methods are used respectively, with "low" randomness potentially repeating characters.

### User Expectations

With "high" randomness, each password is highly unique and secure, suitable for sensitive accounts. "Medium" randomness provides a balance between security and predictability, while "low" randomness might be more suitable for less critical applications where ease of remembering is prioritized.

## Feature 3 - Pronounceability

### How it Works

This feature determines whether the generated password consists of random characters or is a pronounceable sequence of letters. If pronounceable is chosen, the password is generated using a set of English words (`english_words_set` in `password_generator.py`), making the password easier to remember. The generated password will be a concatenation or truncation of these words to match the specified length.

### User Expectations

When the pronounceable option is selected, users should expect passwords that are easier to remember and might resemble actual words or phrases. However, it's important to note that

while pronounceable passwords are user-friendly, they may not always meet the highest security standards of completely random character strings.