# MasterPass User Manual


# Zamithal

Submitted by: Skyler Swenson

Submitted to: David Bishop

Email: Skyler.Swenson@oit.edu

Date: 3/18/2017

Version: 1.0

# 1. Table of Contents



# 2. Introduction

MasterPass is a password management software designed derive secure passwords of any length and requirement from a single password. The passwords can be used in any system requiring a log in without fear that the password leak may affect other accounts. This is accomplished by hashing the user's master password and using that hash as a base for creating unique passwords. MasterPass is intended to be completely offline and never store a copy of the users non-hashed password anywhere.

## 2.1. Problem Statement

Password leaks happen. Eventually someone, somewhere slips up. Be it a phishing attack, or a cracked algorithm, creating a perfect security system is nearly impossible. While no database should store passwords unhashed, a typical user has no way to know for sure if their password is secure with the website or application they trusted their password to. The more websites a user uses the same password on, the more likely their password is to be leaked.

## 2.2. Problem Addressment

MasterPass addresses this issue by never giving any website the same password. All passwords are hashed versions of the master password manipulated to fit the websites criteria. While MasterPass stores many passwords, the user still only must remember a single password. The single password can be used repeatedly with no risk to security. Passwords are stored completely offline in an encrypted file. The encrypted file does not contain the master password so, even if the encrypted file was cracked, the user's master password is still safe.

## 3. Login Page

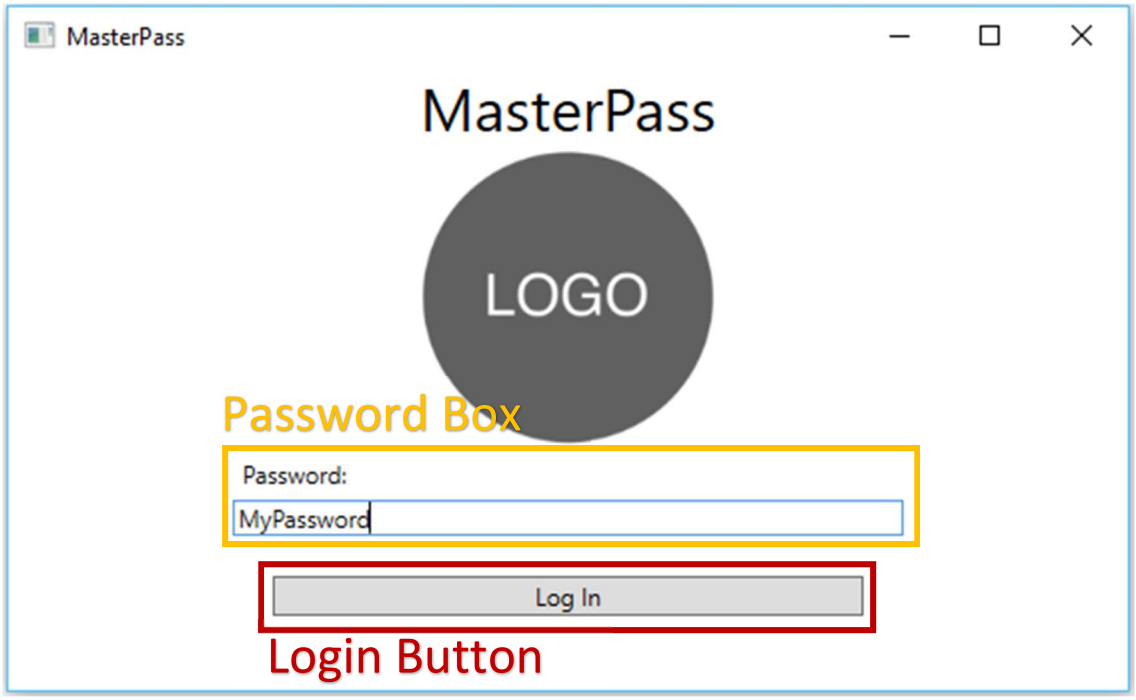
When the application is launched, the user will land on the login page. The login page has only a single text field and a single button.

**Password Box:**

Here the user enters their master password that all application passwords are derived from.

**Login Button:**

Attempts to restore any data for the given password. If there is no data, new data is created for that password. The user is then taken to the password viewing page.



## 4. Password Viewing Page

This is the main page of the application. From here the user can copy, view, and add passwords. Additionally, they can add applications to keep passwords for.

**New Application Button**

Allows the user to generate new applications to keep passwords for. Opens the application creation page.

**New Password Button**

Creates a new password for the application.

**Application Name**

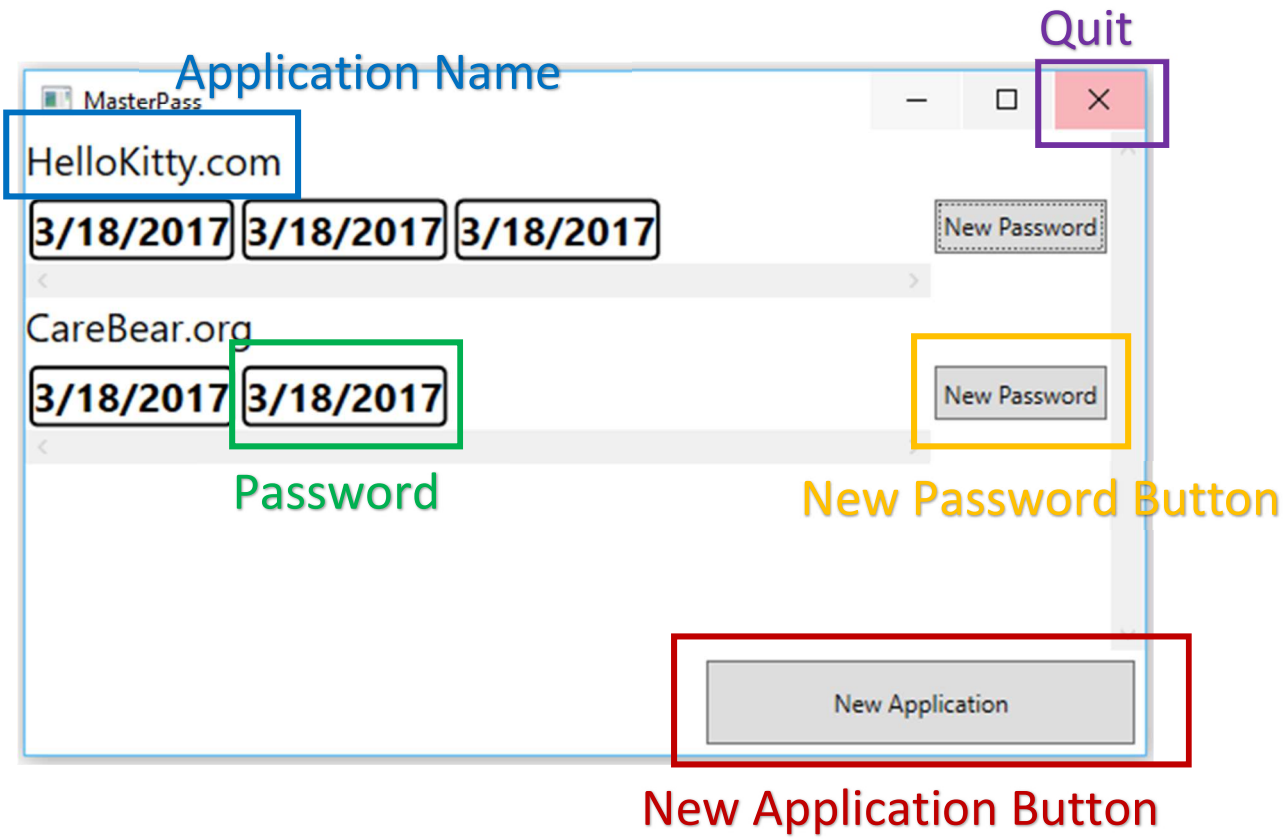
The name of the application passwords are being kept for. Right click this to delete the application.

**Password**

The stored password for the website. Left clicking the date box will copy the password to the clipboard. Right clicking it will open up the password details window.

**Quit**

Prompts the user for an optional save and quits the application.



## 5. Create Application Window

This window allows the user to create a new application definition and define the rules for making passwords.

**Application Name**

The name of the application name the user wishes to create rules for. This is factored into the unique password generation.

**Password Length**

The length of passwords to generate. All passwords will be exactly this length.

**Seed**

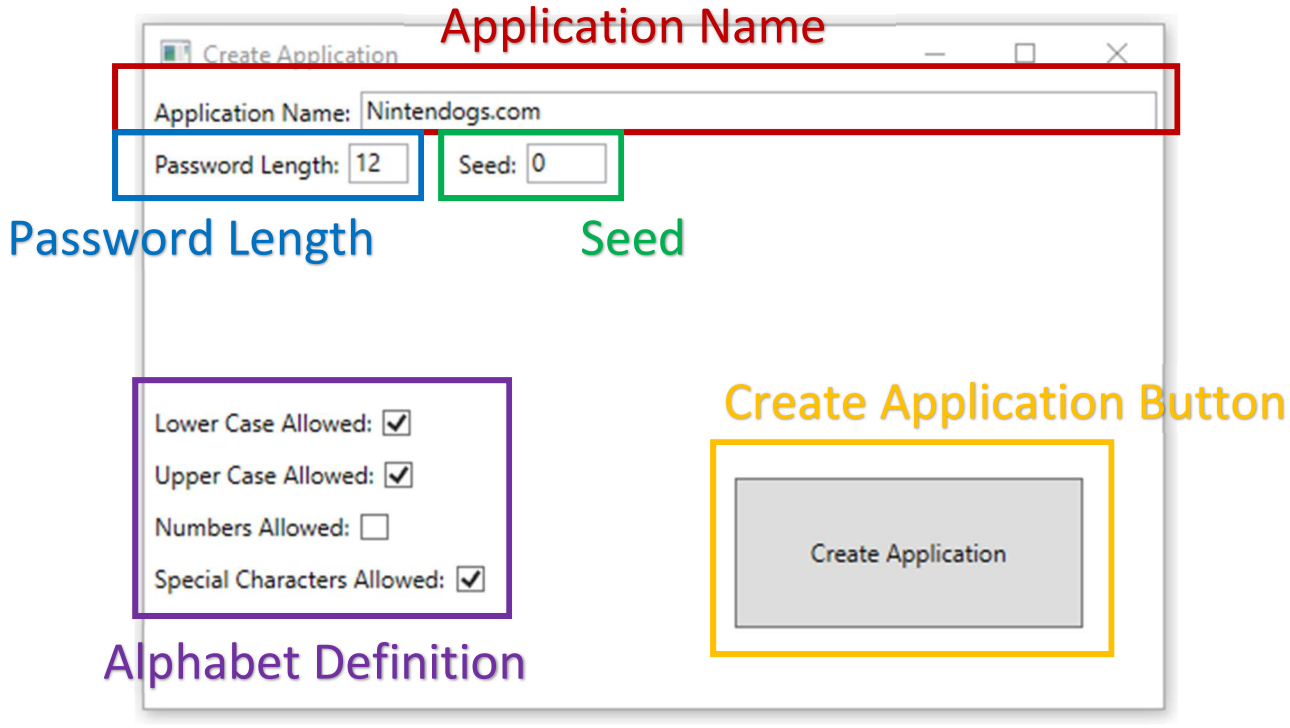
The unique seed that makes each password different from passwords for the same application. This will most likely need not be changed.

**Alphabet Definition**

These check boxes are used to define the rules for creating a password.

**Create Application Button**

Finalizes the creation of the application.



## 6. Password Information Window

This window allows the user to view details about the password and delete it.

**Password**

The password.

**Creation Date**

The date this password was created.

**Seed**

The unique seed that differentiates this password form other passwords for this application.

**Delete Button**

Causes the password to be deleted.