The Password Saver

Installation and User Guide

Version 3.2
Release: April 12, 2014

Introduction

This program was created to store authentication data for applications, web sites, or anything that requires a pass code. The application/website/device can have multiple access values. Each of these values will be stored encrypted.

Design

The application was written in Java, version SE 1.7. It utilizes SQLite for the database. Additional jars used include:

sqlite-jdbc-3.7.2.jar

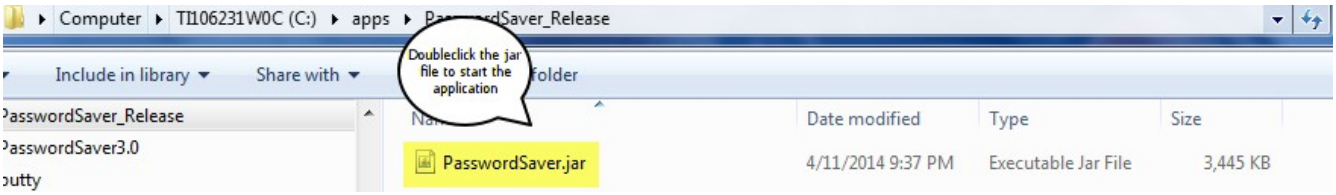
apache-commons-lang.jar

Installation

Download the zip file from http://www.spottedplaid.com/wp-content/uploads/2014/03/JPasswordSaver3-1.zip or get the source from GitHub – https://github.com/flashman71/flashys-stuff/tree/P2.

Create a directory and unpack the zip file. Double-click the jar file and the application will start.

Initial screen with the jar file.



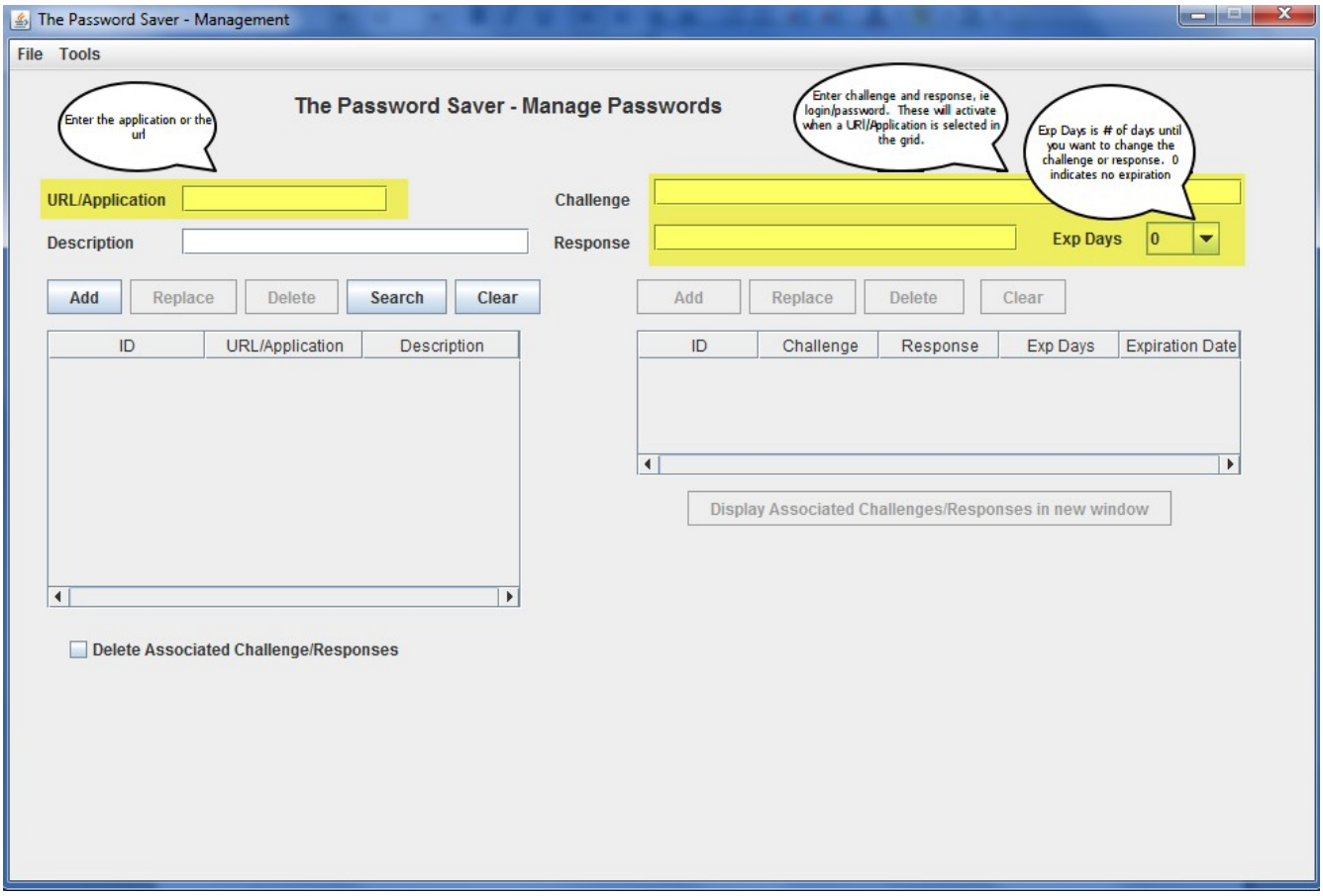
Intro screen. The current version is 3.2. Enter the pass code to open the database. If this is the first time this has application has been executed, enter the pass code that you want. When a value is entered the "OK" button will activate. If this is an existing database the application will validate the password and open the database, otherwise a failure message will be displayed.
Keystore File – This is where the password is stored. There can be multiple Keystore and Database files.
Database File – This is where the database is stored.


The Password Saver
Protected - Private
Copyright © Spotted Plaid Technologies, 2013.
Version 3.2
Pass code
Keystore File
keystore.kps
Database File
jpwdsaver.dbx
Button will activate once a Pass code is entered
Ok
Close

Once the database is open, the screen below will be displayed. This allows the user to maintain applications and authentication data. Applications/URLs must be entered first. Once this is done, the application needs to be selected in the grid, which will enable the Challenge/Response section.

Definitions:

URL/Application – This is the application/website/device/etc that has authentication.
Description – Description of the application
Challenge – This is the request from the application, ie login.
Response – This is the answer for the Challenge, ie your login for the application.
Exp Days – This sets an expiration for the Challenge/Response. This allows the user to manage passwords that need to be changed on a regular basis.
Delete Associated Challenge/Responses – If checked, when a URL/Application is deleted, the associated Challenge/Responses will also be deleted.
Display Associated... - This will display all Challenge/Responses for a selected URL/Application and display in a new frame. This allows the user to see the entire authentication.



This screen allows the user to change the password. Once a passphrase is entered all encrypted records in the database will be encrypted with the new code.