



August 30, 2015 -- Rev 1.11

## What is CredLock?

CredLock (**C**red**en**tial**L**ock) is your digital file cabinet, a secure encrypted repository whereby you can create categories of information including: Website addresses, User Names, Passwords, Credit Card information, email addresses, insurance information, personal property details and much more.

What is your auto, home, umbrella or medical insurance policy number? How about your drivers license number? What is the serial number of your TV Set, computer, or other valuable pieces of electronic equipment? Are you unable to locate the purchase receipt, appraisal document or pictures of an article of personal property to prove its existence and claimed value to the insurance company? Can you remember a friends email address, home address, birthday, their various contact phone numbers or other specific personal details? If any of these pose an informational challenge, then you will really appreciate "DigiDex"<sup>TM</sup> which is CredLock's digital version of the stone-age Rolodex<sup>TM</sup> card system.

How about your frequently visited websites; do you have an easily accessible and manageable website directory, or more importantly, do you utilize User Names and Passwords that are complex enough to thwart the attempts of a would-be-hacker, either friend or foe?

We have designed all of the foregoing capability into the CredLock program which is based on a highly encrypted, password protected database. CredLock can be installed and executed from the primary hard-drive (not recommended) on your home computer, or as a preferred installation, from a USB Flash drive. The choice of a storage product for CredLock is very important and various options and features are put forward in the "CredLock System and Storage Media Considerations" section of this Operations Manual.

The CredLock system, through data encryption and password protection, is designed to keep your private data secure. It **MUST** however, when used on systems that are connected to the Internet, be used in conjunction with a current up-to-date firewall together with Malware and Spyware detection and removal software.

Without it, malicious software can, and will, infect and propagate itself throughout a computer system including USB drives that may be connected to it. While CredLock will keep your data secure and protect it from prying eyes, it cannot protect itself from malicious software within its operating environment that seeks to destroy its database and/or read and send out every keystroke you enter; forewarned is forearmed.

## Downloading and Installing the CredLock Demo Program

CredLock will run under all versions of Windows including Windows WinXP(SP2), Vista-32/64, Win7-32/64 and Win8-32/64, Win10-32/64.

A demonstration version of the CredLock program is available for download at [www.credlock.com](http://www.credlock.com). The demonstration program is full-featured and will remain active for a period of 30 days from the time of download. At the end of the 30 day period you must purchase, for a modest fee, a user license to continue to use the program.

When you arrive at the CredLock website scroll to the bottom of the page where you will find a section titled "Downloading the Credlock Demo Program". There you will find three pushbuttons labeled "External Media Demo", "Program Files (x86) Demo" and "Program Files Demo". Only one of these files needs to be downloaded based on your setup preference. The only difference between the files is where the "CredLock" system folder will be created. CredLock will run from wherever it is stored, however for security and portability purposes we recommend that you run CredLock from external media, preferring flash (Thumb) drive media.

The file names and their creation paths are as follows:

- a) **CREDLOCK\_DEMOVxxxEXTMEDIA.EXE** will create the CredLock system folder in the root directory of the media where it resides.
- b) **CREDLOCK\_DEMOVxxxPROGFILESX86.EXE** will create the CredLock system folder in the "\Program Files (x86)" folder of your primary hard disk drive. (Normally "C:")
- c) **CREDLOCK\_DEMOVxxxPROGFILES.EXE** will create the CredLock system folder in the "\Program Files" folder of your primary hard disk drive (Normally "C:").

Depending on the browser you are using (Usually Internet Explorer or FireFox) the process of downloading the demo file is somewhat different.

### FireFox

Click the pushbutton associated with the Demo File you wish to download. Firefox will open a window containing a "Save" button. Click that button and the file will automatically be directed to the "Downloads" folder on your primary hard drive. After the download has completed click the Firefox download arrow located in the upper right hand corner of the browser window. You should see the file that you just downloaded based on the list (a,b,c) above. Right-click on this filename, then left click on the "Open Containing Folder" button. This will launch Windows Explorer and select the file you just downloaded.

### Internet Explorer


Click the pushbutton associated with the Demo File you wish to download. Internet Explorer will open a window that contains a "Save" button with a pull-down arrow. Click the pull-down arrow and then left click on the "Save As" menu entry. When the Windows Explorer window is displayed, open the "Downloads" folder, then click the "Save" pushbutton.

## **Installing and Launching the CredLock Demo**

Locate the demo file you downloaded in the "Downloads" folder of your primary hard disk. If you elected to run the system from your hard disk and you downloaded either of the "Program Files" demo files, simply right-click on the filename then left-click the "Run as administrator" menu entry which will open the WinZip self-extraction window.

If you downloaded the external media demo file, right-click on the filename then left-click the "copy" menu entry. Select the root directory of your external media, right-click, then left-click the "Paste" entry, which will transfer the update file to the root directory of your external media. Next, right-click on the filename, then left-click the "Run as Administrator" menu entry which will display the WinZip self-extraction window.

The WinZip self-extraction window contains a field labeled "Unzip to Folder" which shows the path where the CredLock System folder will be created. This will vary based on the demo file you elected to download. The final installation operation is to left-click the "Unzip" button. A progress bar will be displayed followed by a confirmation message that 4 files have been unzipped successfully; click "OK", which will also launch the CredLock program.

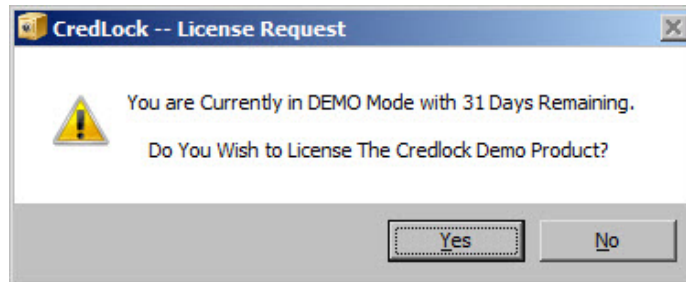
During the initial demo startup, the CredLock window (depending on how your screen has been configured), may be hidden behind other windows, so if you do not see the opening CredLock Window, check the taskbar for the CredLock ICON . Left-click the ICON to bring the CredLock main window to the foreground.

Because the demo program is not yet licensed, a window will be displayed indicating that you are in demo mode with an indicator of how many days there are remaining in the demo period.

As a final operation you should create a desktop shortcut to CredLock. To do this locate the CredLock system folder and open it. Within that folder you will find the CredLock.exe application file. Right-click on the file name then hover your mouse pointer over the "Send To" menu item, then left-click on the "Desktop (create shortcut)" sub-menu entry. This should place a CredLock shortcut on your desktop.

To ensure proper operation of CredLock, locate the desktop shortcut to CredLock and right-click on it. When the menu is displayed, left click on "Properties" (bottom of the menu) then left-click the "Compatibility" tab. At the bottom of the compatibility window, find the checkbox labeled "Run this program as an Administrator" and activate it, left-click "Apply", then left-click "OK". You should now be able to launch the CredLock program from the desktop shortcut ICON.

When you launch an unlicensed version of CredLock, the following window will be displayed.



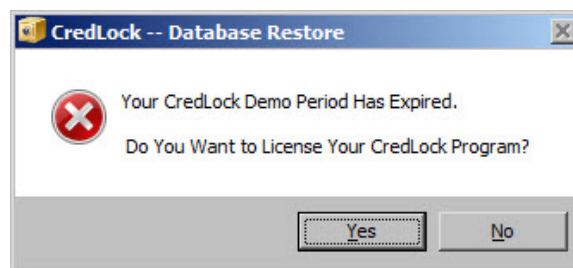
Clicking "No" will launch CredLock with no further questions.

Clicking "Yes" will display the following Window



Clicking "Place Order" will display the secure order form for purchasing your CredLock license.

After a period of 31 days has elapsed without a request to purchase the licensed version of the CredLock program, the following window will be displayed.

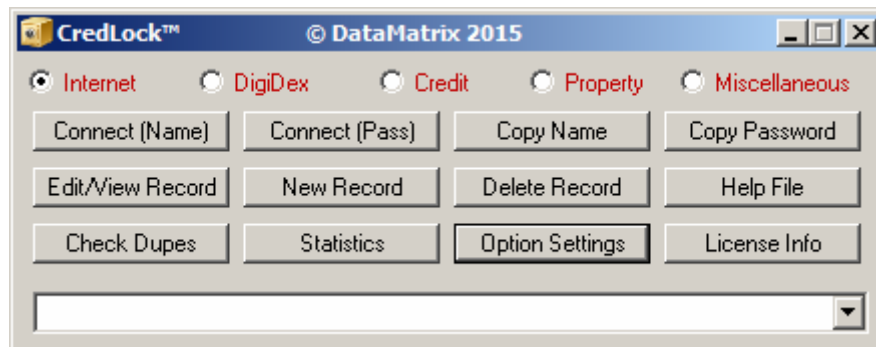


Clicking "Yes" will display the "License Product " window with instructions.

Clicking "No" will shutdown CredLock disallowing any further user interaction.

## Launching CredLock

Double-clicking the CredLock desktop shortcut will display the CredLock main window. Note: If you have activated CredLock's password protection, you will be prompted for your CredLock Master Password before the main window is displayed. Refer to Page 23 for details.



CredLock maintains your information in one of five record categories:

- 1) Internet -- Website addresses, Passwords and other relative information.
- 2) DigiDex™ -- Personal Contact (Email, Phone, Address) information.
- 3) Credit Card Information -- Issuing Bank, CC Numbers, Expiration Dates, PIN #, etc.
- 4) Property-- Personal Property, with detailed purchase information and Images.
- 5) Miscellaneous -- Information listed by user-defined categories with Images

The series of radio-buttons across the top line of the Credlock main window permit you to select the record category that you wish to access. Once a record category has been selected, the titles of the records that currently exist in that category will be listed in the pull-down list at the bottom of the CredLock main window. The middle row of pushbuttons are "Action" buttons that, with the exception of "New Record", permit you to Edit, View or Delete the record currently selected in the category title pull-down list. The "New Record" pushbutton permits you to create a new record within the selected record category.

From this point forward in the manual, use of the phrase "User Name and/or Password" will be replaced with the single word "Credential(s)".

## Internet Record Category

Do these character strings look familiar; "123456", "abc123", "password", "qwerty", "letmein"?

The foregoing list contains just a sample of the most frequently used credentials utilized by the Internet community. Then of course, there is the consistent use of dates relative to birthdays or other special occasion dates. Also, human-readable phrases like "openmyaccount" are easy prey for hackers. It is human nature for a person to use a sequence of letters and/or numbers that are meaningful to them and thus easy to remember.

To exacerbate an already bad situation, for convenience purposes, users continue to utilize the same, or a variation of the same credentials on multiple websites; yet another windfall for hackers. After all, with the numerous websites we utilize on a day-to-day basis, how can we possibly remember complex passwords like "\$#nNQt1+A!?!%FI&wP"?

With today's social media and other personal information websites, anyone, using a series of Google Searches, can gain access to your birth date, the city where you were born or now live, the names of your children and their birthdates, your favorite sports team, home address, license plate number and other assorted personal information. In other words, the type of information that you, like most, are likely to use as credentials on secure websites.

Most companies have turned to digital reporting and billing. To reduce costs, they are constantly urging us to move away from paper, and manage our affairs, both administrative and financial, using the internet. The personal convenience of it is a strong attraction and more-and-more we are utilizing the Internet to manage our banking, purchase merchandise, handle and pay for our Auto and Home insurance, our financial investments and a myriad of other tasks. Each of these secure websites require a user name and password, and most of us succumb to using easy to remember, relatively short credentials, that we repeatedly use from one website to another.

First, a guideline. The website will determine the minimum/maximum length and the types of characters you can use (some mandated) when creating your credentials. Before you create a credential, always make sure you understand the credential format that the website will accept. Some financial institutions and banks have been accused of restricting credentials to ridiculously short character lengths (8 characters) and restricting character types to uppercase, lowercase and numerical. A hacker, also knowing that restriction, using brute force methods, won't take long to crack a credential like "A1q9F7z2". As the website prompts us to enter our credentials, we are faced with entering an easy to remember, easily hacked credential or utilizing a lengthy complex character string that is almost impossible to remember, but provides a high "crack" resistance. Most of us take the easy route and use some easy to remember date like "May0190" which might be our birthday or anniversary. Understanding human behavior, these are the first types of credentials a professional hacker will try; after all, that information is easily available by doing a bit of research on social media or other public document websites.

A number of websites mandate that your "Name" credential be your email address and then allow you to create your own unique password, as mentioned earlier, within the format boundaries dictated by the website. When you must use your email address as your Name credential, you must make the password credential as strong as possible. Anyone with knowledge of your email address is already halfway to gaining access to your account, and your password credential is the final obstacle and it better be extremely hard to crack!

Previously we mentioned the use of the password "\$#nNQ1+A!?!%FI&wP". A credential of this complexity, consisting of a combination of uppercase, lowercase, numerical, and special characters, is almost unbreakable. Because of the mixed structure of this 17 character string, it would require years of processing time to break a credential of this complexity. A Strong Credential consists of the following attributes:

- 1) Use as many characters as possible.....and practical (15 minimum).
- 2) Vary the character types (Lowercase, Uppercase, Numerical and Punctuation).
- 3) Try not to duplicate any characters within the character groups listed in item #2.
- 4) The credential should not be human-readable and appear totally nonsensical.

Creating such a credential manually is somewhat of a chore, one that will keep you moving from one side of your keyboard to the other while attempting to create a credential that fulfills the four guidelines listed above. Avoiding character duplication is a particularly difficult process that will mandate the checking all of the previously entered characters to avoid repetition. When your minimum 15 character credential reads like complete gibberish, then you have achieved your goal of creating a strong credential. Strong yes.... easy to remember?....No!.

CredLock's Random Password Generator (RPG) reduces this chore down to a few entries and clicks. You simply select the characters types, the number of characters of each type, and then with a single click the credential string is randomized and created. You will probably say to yourself, "How will I ever remember that?" The truth is that you don't have to, all you should really care about is that this complex credential you have created will give you access to the website.

### Creating an "Internet" Record

With the "Internet" record category selected, left-click the "New Record" pushbutton. This will display the Internet Record form shown below.

**CredLock™ -- New Website Record**

Website Name:

Website URL:

User Name:

User Password:

Credit Card:  Exp:

PIN#-CCV#:

Challenge 1:

Challenge 2:

Challenge 3:

Phone Number:

Activation Date: 06/18/2015 Alert After: 0 Weeks

**Auto Generate User Name/Password**

Use  Uppercase Characters (A-Z)

Use  Lowercase Characters (a-z)

Use  Numerical Characters (0-9)

Use  Special Characters (! @ # \$ % \* { } [ ] + = ...etc)

Use  Control Characters (Values 1-31 -- Be Carefull!)

Use  Extended Characters (Values 128-255)

Note: The inclusion of Control and/or Extended Characters in a Name or Password, unless needed, is highly discouraged.

Avoid Character Duplication

Create Name Create Password

Check Dupes Save Copy Field Cancel

## Field Descriptions

**Website Name:** Use whatever name you feel describes this website "ABC bank", XYZ Insurance Co", "ABC Department Store", "Amazon", etc.

**Website URL:** The URL path to the website logon page usually "https://...."

**User Name:** Your User Name credential to access this website.

**User Password:** Your User Password credential to access this website.

**PIN--CCV:** If required, your User PIN for this website and/or the Credit/Debit Card CSV number.

**Credit Card:** A specific Credit/Debit Card number you might use on this website.

**Expiration Date:** Expiration Date of the Credit/Debit Card.

**Challenge 1-3:** Answers to challenge questions for this website.

**Phone Number:** Customer Service Telephone Number for the company.

**Activation Date:** The date this record was created. Used in conjunction with "Alert After".

**Alert After:** The number of weeks before alerting on a Credential Set. (See Text)

The first operation to perform in setting up a CredLock Internet Record is to give the record a title. The title can be anything you desire, the name of a bank, insurance company, department store etc. CredLock list title names alphabetically, so choose titles that will make it easy for you to locate, select and access the record. This is the name that will appear in the category name pull-down list at the bottom of the CredLock main window.

First, launch your Internet browser (FireFox, Internet Explorer, etc.) and navigate to the sign-on page of the website where you wish to link. Next, go to the URL "https" address string, right-click on it, then left-click the "Copy" menu entry. Next, return to the CredLock Internet Record, right-click in the "Website URL" data field, then left click the "Paste" menu entry. This will place the sign-on URL path into the Internet Records "Website URL" field.

## Auto Generate User Name/Password Panel

In a prior section we outlined what constitutes a strong credential. For reference:

- 1) Use as many characters as possible.....and practical (15 minimum).
- 2) Vary the character types (Lowercase, Uppercase, Numerical and Punctuation).
- 3) Try not to duplicate any characters within the character groups listed in item #2.
- 4) The credential should not be human-readable and appear totally nonsensical.

As mentioned earlier, Credlock makes the entire process of creating a strong credential a very simple procedure using the "Auto Generate" functionality built into the Credlock system.

Let's assume that you are setting up credentials on a website that will permit a credential length of up to 25 characters, permitting the use of uppercase, lowercase, numerical and punctuation characters. Given that scope, you elect to create a 20 character credential that will consist of 5 characters of each type. CredLock makes this task effortless; simply enter a '5' in the field adjacent to the character type, then click either the "Create Name" or "Create Password" pushbutton. Automatically, CredLock will randomly select a character from each type, then fully randomize the entire 20 character credential, placing the result into the appropriate credential field (Name or Password).



### **"Avoid Character Duplication" Checkbox**

Item #3 relative to creating a strong credential states that you should, if possible, try to avoid using the same character more than once in a credential string. If you activate the "Avoid Character Duplication" checkbox, CredLock will attempt to meet that credential criteria. Obviously, if you attempt to create a 15 character credential that consists solely of numerical characters, it will be impossible to avoid duplication. Should that situation exist, CredLock will display an error message notifying you that duplication is unavoidable given the selected character type and the requested credential length. This error message will continue to be displayed until you deactivate the "Avoid Character Duplication" checkbox.

### **"Activation Date" and "Alert After" Field Descriptions**

Regardless of the credential strength, the longer the period of time a given website credential is retained, the more susceptible it becomes to being compromised. In fact, if you are using credentials that are based more on your ability to remember them, than a concern for strength, the chances are that the credential length is short and consists of only a few letters and numbers. Because of that, the inconvenience of changing the credential on a regular basis may not be of concern, that is, until the inevitable happens.

Frequency of credential change is important and because of that, CredLock has an alert feature that will remind you to change your website credentials at periodic intervals. When you first create an Internet Record, the 'Activation Date' field will contain the creation date. If you wish to be reminded to change your credentials, let's say on a monthly basis, place a number in the "Alert After" data field; this number represents the number of weeks between alerts. For example, if you want to be reminded each month enter '4' in the "Alert After" data field. Entering a '0' in the field will disable the credential alert function.

Now, whenever you access a website where an alert period has been defined, if the activation date plus the alert period is greater than the current date, an alert message will be displayed notifying you that your credentials for that website have been in use for some number of days since the activation date. The process for modifying your credentials will be described in an upcoming section of this document.

### **"Check Dupes" Pushbutton**

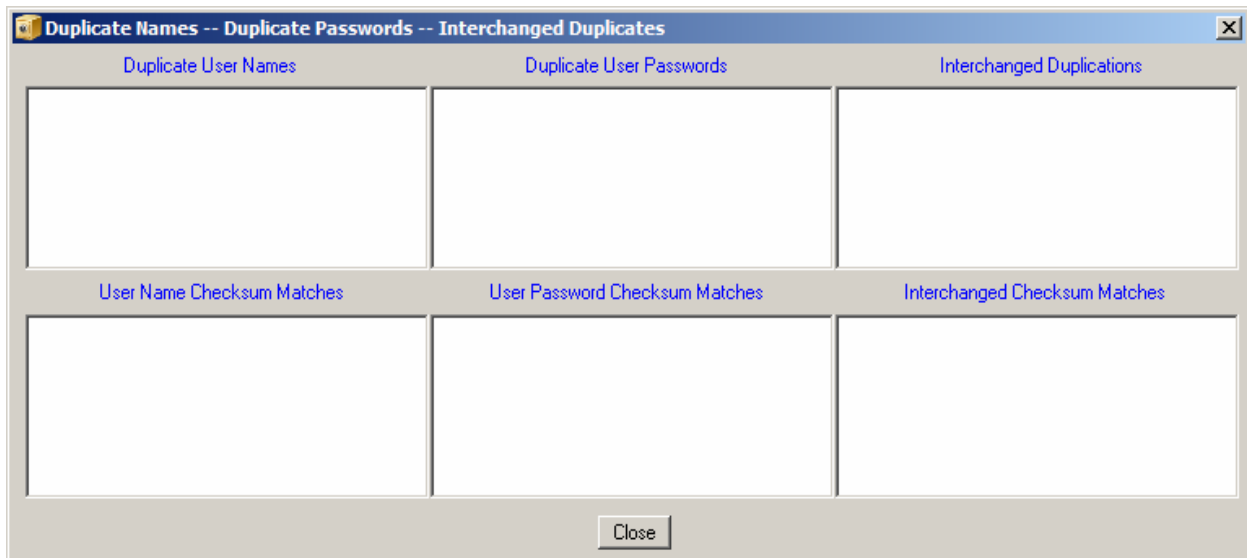
One bad credential trait users repeat, once again for convenience, is the use of the same characters, either in the same sequence, or rearranged slightly on multiple websites.

One of CredLock's many features is to bring to the forefront those websites where that situation exists. It does this in three ways: first CredLock scans all of your Internet records checking for the use of identical Names, Passwords and also websites where you have interchanged the same credentials on multiple websites. That is where a User Name on one website has been used for the password on another website.

Also, it performs an additive sum check as well. If you use "ABC123" on one website, then on other websites you use "abc123", "A1B2C3", "a3b2c1", to you they may be visually different, however, from a computational point of view they all have the same additive checksum because the characters that make up the credential are all the same.

You might say "Wait a minute, all the characters might be the same but some are uppercase and some are lowercase; doesn't that make them different?". Well in a binary sense you are correct, however from a strictly language point of view, they are all the same. This is one of the first places a hacker will prey on your habit of creating credentials with, although rearranged, identical characters. Easy for you to remember, but once one of your websites has been compromised the rest will soon follow. The hacker will perform a check, first in uppercase, then lowercase cross checking for the same additive sum that you have used on other websites.

To put all of this into action, select the "Internet" record category, then click the "Check Dupes" button on CredLock's Main Window which will display the window shown below. Websites having identical credentials are listed in the first two segments. The third segment "Interchanged Duplications" shows websites that have identical credentials that have been interchanged. That is, you have a password on one website that is also used as a User Name on another website. Ideally, you want to see the word "None" in each of the upper segments. If any website duplications are indicated, for security reasons, you should edit the credential(s) on those websites to eliminate the duplication.



The lower segment of the "Check Dupes" window contains identical checksums of User Names, passwords and interchanged credentials. As mentioned earlier, additive checksums are the cumulative checksum of the characters that make up the credential(s). The display of websites in this segment is not necessarily a problem indicator. In the worst case it indicates that the credentials are completely identical or are comprised of the same characters in varying sequences. In the best case, it indicates that a series of characters in the credential are additively the same, though they can be totally different, having no similarity, they just happen to have an additive value that is the same.

Whether you elect to change one or both of the credentials to eliminate this additive value error is up to you. It really depends on the similarity of the strings. As mentioned above, if the characters that comprise the credential(s) are quite similar, than consider modifying one or more of the websites. If however, the credential, to a great degree, meets the four guidelines of credential strength, than you may retain the existing credentials as originally entered.

One caveat: most websites do not allow you to modify your existing User Name because it is tightly coupled to your personal account. Of course where some websites by default use your email address as your User Name, CredLock will most certainly list those websites as having duplicate or possibly interchanged user names. When you create a new account on a website, if it's allowed, try to create unique user names. Once the User Name is registered with the website, the security of your account will for the most part, lie with password strength.

### **"Challenge 1-3" Data Fields**

A number of websites will require you to enter the answers to challenge questions such as: what High School or college did you go to or what was the name of your first pet? etc. These challenge questions, are to some degree, as important as your sign-on Credentials, and like sign-on credentials it is in your best security interest not to use the same challenge questions and answers across multiple websites.

Most websites will ask you slightly different questions and normally there not be a conflict. However, a site may ask you the same challenge question, for example a common question is "What was the name of your First Pet?". Let's say you have previously answered this question on another website and that you entered the name "Spot". If you now enter the name "Spot" on this new website, you will have compromised the challenge question for all of the sites where you have used that challenge answer. You have to modify your answer with something else about "Spot", maybe Spot's pedigree, color, favorite toy, etc. Don't feel compelled to answer the question honestly; use another name or for that matter anything you want, for example "Never Had a Dog". The important thing is that you enter the challenge answer, then copy and paste that information back into one of CredLock's Challenge data fields. Let CredLock remember your challenge answer so when a website does challenge you with a personal question, you can quickly copy-and-paste the answer from the CredLock web-record directly to the answer field.

### **Saving the Internet Record**

Once you are satisfied that all of the web-record information has been correctly entered, click the "Save" pushbutton. A message will be displayed confirming that your record has been encrypted and saved to the CredLock database. The entry form will clear in preparation for the next entry. If you are finished, click "Cancel" to return to the CredLock Main Window.

### **Connecting and signing on to a Website**

From the CredLock main window, pull-down the alphabetically ordered website list at the bottom of the window and select the website you want to visit.

There are two pushbuttons in the upper-left-hand-corner; one labeled "Connect (Name)", the other "Connect (Pass)". Either of these pushbuttons will launch your preferred browser and automatically connect to the URL path you have placed in the Internet record for that website. Which pushbutton you utilize depends on whether you want to transfer the User Name or the User Password to the clipboard. Most websites want both credentials, usually User Name first, then the password. So, in the majority of connections, you would click the "Connect (Name)" pushbutton.

Websites have two types of sign-on panels. Some contain both the User Name and the Password fields together with a single "Log On" button while others have two separate panels, one for the User Name, and one for the Password. You already have your User Name in the queue from the "Connect (Name)" operation, so simply right-click and "Paste" to transfer your User Name. If the Password field is not displayed click the "Log On" (or similar) button to display the password field. Next, click the CredLock taskbar ICON, then left-click the CredLock "Copy Password" pushbutton. Return to the website sign-on page, right click in the password field, then "Paste". Complete the sign on operation by clicking the website "Finish", "Sign On" or "Log On" button.

One caveat worth mentioning; for your convenience, most browsers will ask if you want to save your User Name and/or password for the website. We strongly recommend that you always click "NO" to this request. If you click "Yes", you are leaving your confidential credentials within the browser system permitting a secure piece of data to be viewed by those possessing the knowledge of how to access and view this browser information. Always retain your credentials solely within the confines of the CredLock system database, and always refuse the browsers request to retain these sensitive credentials outside of the CredLock system environment.

### **CredLock System and Storage Media Considerations**

Although you can install CredLock on your primary 'C' drive, we suggest that you install and run the system from a removable flash drive. The primary benefit of doing this is that it permits you to physically and digitally disconnect your CredLock system from any computer. As mentioned earlier, the CredLock system leaves no data remnants on the computer, so once you have shutdown CredLock and disconnected the flash drive, your credentials are securely in your physical possession, safe from prying eyes.

CredLock can be used on any computer, be it a desktop, laptop or notebook, whether it be at your home, business, or a public location. How you intend to utilize your CredLock system, will to a great degree, determine the type of flash drive media you should select. If you will be using the system solely at home, in a virus protected environment, where security is not a major concern, then just about any flash drive will work. If your home computer(s) is utilized by multiple individuals, and you wish to ensure the privacy of your credentials, you should always password protect CredLock, shut it down after each use, and if you feel the need to, safely close down the device and remove the flash drive from the computer.

If you intend to use your CredLock Flash Drive in a business or public environment, that is, across multiple computers of unknown composition, the choice of storage media becomes more critical, primarily because of malware and other malicious software. Some of this nefarious software propagates itself using plug-in media like a flash drive. When a virus-free flash drive is plugged into an infected computer, the virus installs itself on the flash drive. Your previously virus-free Flash Drive has now become a virus "Carrier" which will attempt to infect the next host computer that you plug it into, including your home computer. Hopefully your anti-virus will pick up this activity and eradicate the virus....hopefully!!

If portable operation of CredLock is anticipated, for the reasons listed above, you are well advised to purchase a device that is equipped to present the flash drive to the system as a read only device. When configured in this mode, the drive is write-protected and nothing can be written to the device including any malicious software that might attempt to install itself on to the media. Write-protection will allow you to plug your CredLock system into ANY computer, launch and use it in read-only mode, and when you are finished, remove the flash drive without concern that the drive has been compromised by malicious software.

The availability of flash drives that possess write-protect capability are limited. Devices that incorporate this feature use either a mechanical switch on the side of the device or a software selectable checkbox that permits you to configure the device in a Read-Only mode as a part of the sign on process. We personally prefer the software method to the mechanical switch, primarily because we have found that these mechanical switches do not have detents, and as such, are easily moved to the write-enable mode during insertion or removal from the computer.

One software based model that we like in particular is the "Data-Traveler"<sup>™</sup> series of flash drives that are manufactured by Kingston. These drives are quite unique in that they use dual-partitioning to shield the contents of the drive by initially presenting the drive as a read-only CDROM device that displays a window requesting a User Password. Once the correct password has been entered, a secondary drive partition, with a separate drive letter (usually the next sequential letter, but not always) is activated, permitting it to operate as a standard flash drive. The secondary partition is where your CredLock System and database are located.

Flash drive storage space is another consideration. In 99% of the situations, if you are using the drive only for the CredLock system, a 4GB device will suffice. The primary consideration is the number of image files you will be storing to the database. Image files are associated with CredLock's Property and Miscellaneous records (more on this in a subsequent section). If you foresee that a number of image files will be required, you might want to consider moving up to an 8GB device. Given today's USB Flash Drive pricing, the cost of doubling the storage from 4GB to 8GB is minimal.

Now to the question of security and pricing. In a minimal security situation where the flash drive will never leave your home, the purchase of a standard 4GB-8GB flash drive, together with the utilization of CredLock's built-in password protection should be sufficient. For example, the price of a Kingston G4-8GB device, at the time of this writing is \$5.50 on Amazon.

One caveat: when a simple device of this type is plugged into a host computer, because the device is not password protected, and CredLock's Image files are stored in their native format, they may be directly viewed by anyone by directly accessing the drive folders using Windows Explorer. However, the most secure components of CredLock: Website User Names and Passwords, all data records and the content therein are fully encrypted by CredLock and cannot be viewed intelligibly unless a CredLock Master Password is correctly entered. When using a simple Flash Drive such as this, ALWAYS password-protect your CredLock system.

The next step-up in security would be the Kingston "Data Traveler Locker+G3". This flash drive outlined earlier, actually shields your entire CredLock system including the image files unless a user defined password is provided to open the secondary partition where the CredLock system is located. Once the password has been entered, the device operates as a standard flash drive in an identical fashion to the G4 mentioned in the previous paragraph. A nice security feature of this device is that if you should lose it, and someone plugs it into their computer, and they exceed 10 attempts at entering a password, the device automatically erases all of the data on the drive. CredLock has a similar feature that will be described in more detail in the "CredLock Options Window" section of this manual.

Other than the CredLock data encryption, the "Locker+G3" offers no additional hardware data encryption. The 8GB device has a slight step-up in price at \$11.94 on Amazon (at the time of this writing). Remember though, this drive does not offer a read-only mode and you run the risk of malicious software infection if it is plugged into a computer of unknown composition.

If you intend to use any flash drive in a portable mode, that is, the device will be plugged into computers of unknown composition, than the use of a write protected device to avoid malicious software is mandatory. If you prefer a device that utilizes a mechanical switch, then the "Kanguru Flash-Blu 30™" 8GB unit will fit the need. At this time, it is listed on Amazon for \$22.65. Truth be told though, this unit is basically a Kingston G4-8GB with the addition of a write protect switch and paying 4 times the price for the mechanical write-protect switch seems like a steep price to pay. In addition, it also retains the G4 caveat of other person's being able to view the image files even though they have not entered a password into the CredLock system.

We all know that situations change, and although the basic flash drive may presently fulfill your needs, a change in circumstances may dictate that you seek out a device with additional security for your CredLock System and the data therein. The question is should you just accept this possibility and purchase the most secure device at the start? The most secure device as we see it, would be one that possesses the partition shielding of the "Data Traveler Locker+G3" coupled with a software selectable read-only mode, plus 256 bit AES encryption.

Such a device does exist and it is the Kingston "Data-Traveler Vault Privacy 3.0". This unit is USB 2.0/3.0 compatible, has dual-partitions, password protection, a software selectable Read-Only mode, and utilizes 256 bit AES hardware data encryption. With all of these features and security, it does come in at a higher price. However, at a current Amazon price of \$22.74 for the 4GB Model and \$29.96 for the 8GB unit it won't break-the-bank, and will give you worry-free security. The only negative operational aspect of the "Privacy 3.0" is that when the password window is presented, the Read-Only checkbox is defaulted to Read-Write (unchecked). Because of the dual-partitioning protection, this does not compromise the integrity of the device because the device remains in Read-Only mode until the user-assigned password has been entered and accepted. Just remember, if you are inserting it into a computer of unknown composition to ALWAYS activate the Read-Only mode checkbox before you enter your password.

It is important to emphasize that a write-protected device will protect your flash drive and your CredLock system from infection, however it does not prevent an already running virus from capturing your data and/or keystrokes. Launching CredLock using computer of unknown composition is just asking for trouble and we highly discourage the use of your CredLock system in such an environment. At the very least, the computer should have an active up-to-date anti-virus program in place and if the system allows for it, you should perform a complete virus scan on the computer BEFORE you plug in your CredLock Flash Drive.

Although we have mentioned their company a lot in this section of the manual, we want to say that DataMatrix is not affiliated with, or derives any remuneration from the Kingston Company. The reason is that we have developed the CredLock system using their devices, and as such, we feel very comfortable recommending their products. If however, you find other devices that meet your needs and pricing, by all means purchase them, CredLock is not device specific.

### **Modifying your Website Credentials**

Earlier, we mentioned that CredLock can notify you when a website's credentials have been in use for a specific period of time. If you activated this feature, each time you make a request to sign-on to that website, CredLock checks to see if the alert period has expired. If the alert period has been exceeded CredLock notifies you of this fact so you can modify the credential(s) associated with this website.

To begin the credential change process, first sign-on to the website using your current credentials, then navigate to the website page where the existing credentials can be modified. Procedurally, get to the point where the website is ready to accept your new credential(s).

Next, return to CredLock and click the "Edit/View Record" pushbutton to display the data fields associated with this website's Internet record. Next, in the Auto Password generation panel select the counts and composition of the new credential and click "Create Name" or "Create Password". Remember, when composing new credentials, you must follow the character guidelines (Type and Length) that have been established by the sites Webmaster.

When the credential has been created, position the cursor into either the CredLock name or password field and click the "Copy Field" pushbutton. Switch back to the website, select the appropriate credential field (usually Password), right-click then left-click the "Paste" menu entry. This will place the newly created credential into that field. If you are changing both the name (see note below) and the password, return to CredLock, re-position the cursor to the other credential field and once again left-click CredLock's "Copy Field" pushbutton. Return back to the website page, right-click in the other credential field, then paste the information from CredLock into that field. Lastly, save your new Credential(s) on the website page.

Note: As mentioned earlier, most websites will not permit you to change your existing User Name due to the tight-coupling of the name to your account. That said, in the majority of cases the password will be the only credential that can be modified after the initial setup.

If you are utilizing, and we hope you are, CredLock's name/password generator to create your credential(s), you have to be careful when you elect to include special characters as a part of the credential. Before creating any credential, always make sure that you understand the websites guidelines for credential creation. The maximum length is the first consideration, followed by the types of characters that are allowed or mandated for the credential construction.

For most websites, a credential consisting of a combination of uppercase, lowercase and numerical characters are normally accepted and occasionally punctuation and other special characters are allowed or may in fact be mandated; a maximum length is normally imposed.

Special characters within a credential, may at times be problematic primarily because even though the website indicates that they can or must be a part of the credential, some characters may be rejected. If the website accepts or mandates one or more special characters (\$, #, &, !), to avoid rejection, use them sparingly. As a general guideline, always try to use the maximum credential length possible and utilize all of the character types that are allowed while minimizing but not eliminating, the use of special characters.

If you keep the count of special characters to a minimum, and the website rejects the credential, regenerate the credential and retry the field-copy-and-paste operation. If the website continues to reject the password, gradually reduce the count of special characters until the website accepts the credential.

After the website has accepted your new credential, return to CredLock, and if you are running with alerts, as a final operation, double-click in the "Activation Date" field which will display the current date. When the date is displayed, click the "Apply" button. This will reset the beginning alert activation period to the current date. If you want, you can modify the "Alert After" period number. Finally, click the "Save" pushbutton to encrypt and store the edited Internet record back to the CredLock database. As a final test, sign-off the website, then use CredLock to re-connect and sign-on using your new Password credential.

## DigiDex™ Records

As mentioned at the beginning of this document, CredLock's "Digidex" is a digital version of the old-style Rolodex™ card system but with a lot more functionality. First, CredLock's "Digidex" record can provide much more information and also includes a built-in Email address manager and router. The data fields above the Email Group panels are self explanatory, and there is no reason to describe them with any more detail than the field labels themselves provide, just utilize them for the intended data.

The screenshot shows a dialog box titled "CredLock™ -- Add DigiDex Record Information". It contains the following fields and controls:

- Input fields for: NickName, Last Name, First Name, Department, Title, Birthday, Home#, Business#, Cell#, and FAX#.
- A Note text area.
- Three checkboxes for "Email Group 1", "Email Group 2", and "Email Group 3". "Email Group 1" is checked.
- Three large empty rectangular panels, each with a "Primary ---->" label to its left.
- A "Address Divider" section with radio buttons for "ENTER", "TAB", and "CHAR", and a small text input field.
- A row of buttons at the bottom: "Email Primary", "Email Group", "Copy Primary", "Copy Group(s)", "Copy Field", "Save", and "Cancel".

The Email Group panels (1,2,3) are used for email addresses. Each group panel can accept up to 10 email addresses. The first address within each group is called the "Primary" address. These panel groupings are most effective when you communicate with members of the same business, organization, or club group.

You might ask, why three groups? When you initially setup these panels with Email addresses, give consideration to the possible email situations: for example topics and interests where you might want to selectively send an email only to Group 1 and exclude those addresses in Groups 2 and 3. Another example would be where Group-1 contains the primary addressee's and Group-2 contains the Cc or Bcc addressee's. Also, within each group the primary address could be a Group Leader and you might want to send the email correspondence to only the Group Leaders within each group.

The two leftmost buttons at the bottom of the window are used to connect to and launch your default email program. If you left-click "Email Primary" your default email program will be launched with only the primary email addresses of activated groups as the addressees. If you click the "Email Group" pushbutton your default email program will be launched, and the addressee field will contain all of the email addresses (including primaries) contained in the group panels that have their associated checkbox activated.



When an email contains more than one addressee, each address is separated by a delimiter character. Because email addresses are variable in length, the delimiter character permits the email program to properly separate out the individual email addresses. Although most email programs accept a comma or semicolon as the delimiter character, other programs may require some other special character like an 'Enter' or 'Tab' key or possibly a slash bar.

CredLock permits you to select the address delimiter character via a series of radio-buttons positioned below the email group panels. You can choose between "Enter" or "TAB", or if a special character is required, select the "CHAR" radio-button and place the address delimiter character (usually a comma or semicolon) into the adjacent data field.

Up to this point, we have been discussing local email programs, those that reside on and are launched from your computer which then connects to your ISP (Internet Service Provider). A number of ISP's provide their own web-based email programs such as RoundCube, Squirrel-Mail or Gmail. When using these programs, there is really no program to launch locally as these programs are web-based applications and as such are already resident and operational when you sign-on to your ISP. Because no local email client program exists, the "Email Primary" and "Email Group" pushbuttons which launch local email programs, cannot be used.

When using a web-based email program, the "Copy Primary" or "Copy Group(s)" pushbuttons should be used to transfer email addresses to the addressee, Cc or Bcc fields of web-based email applications. "Copy" buttons, still retain the full functionality of group and delimiter character selection as described for localized email programs except that addresses for web-based programs must be passed via the clipboard. This necessitates that once the "Copy Primary" or "Copy Group(s)" button is left-clicked, you must return to the web-based email program, select the desired addressee field, then right-click and paste the clipboard contents.

The "Copy Field" pushbutton will copy the contents of the selected data field to the clipboard. That information may now be passed to any program via the Windows "Paste" function. It is important to note that if you place the cursor into one of the email group fields and then left-click "Copy Field", all of the addresses therein are copied to the clipboard, however the divider character between address will always default to a new line code. That is, each address will appear on a separate line.

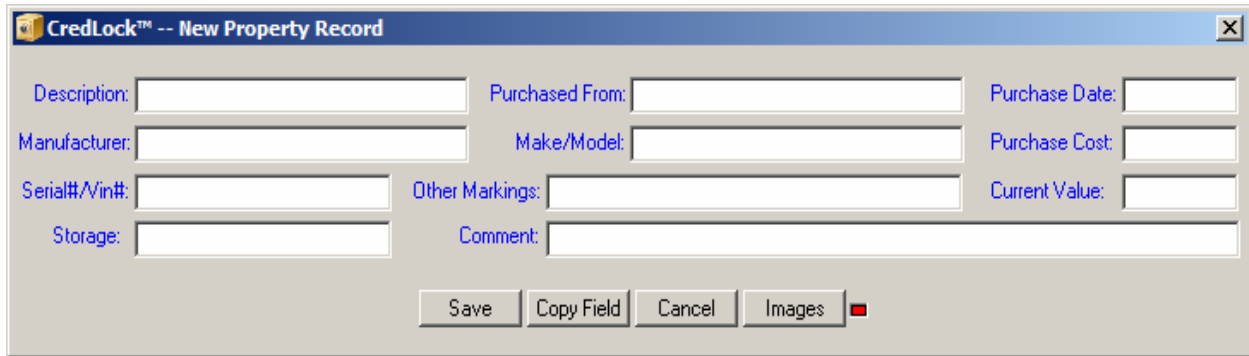
### Credit Card Records

Card Provider:	Master Card	Last Name:	Smith	First Name (MI):	Joseph		
Card Number:	1234-5678-8765-4321	Expiration:	11/16	Security Code:	389	PIN#:	
Bank Name:		Tel#:		Account#:			
Comments:							

Save Copy Field Cancel

CredLock will also maintain your Credit/Debit card information. No need for further explanation here, as the data field labels are self explanatory. If you need to copy the information from the record to another program, position the cursor in the field and click the "Copy Field" pushbutton.

## Property Records



Administratively keeping records of your personal property seems like a lot of work, that is, until tragedy strikes either in the form of a house break-in or a weather disaster. Some of this property may be covered by home owner's insurance, some not, Police Reports on stolen property often ask for serial numbers on electronic or other equipment. Just to keep the honest people honest, Insurance companies are always about appraised value, receipts and pictures. Without supporting paperwork and pictures, claims can and usually do take forever. CredLock's Property Record endeavors to make the entire job of administrating personal property a whole lot easier. No need to detail the record contents, the data field labels are self explanatory.

One item requiring explanation is the "Images" button. As mentioned earlier, pictures and receipts are important documents that substantiate to the insurer, that you in fact purchased and/or possessed the equipment or item that may have been stolen or destroyed. When an item of any real value is purchased, the first thing you should do is to record the serial number (if available) then take a picture of both the item and the receipt. With smart-phones so prevalent today, just about everybody has a camera available.

After you have written down the administrative information and imaged the item and receipt, create a new CredLock Property document and fill in the appropriate data fields. Next, transfer the images from your phone/camera to the computer, then click the CredLock Property Record "Images" pushbutton which will open Microsoft's WordPad program. Unlike Microsoft Word (and its hefty price), WordPad comes standard and free with every version of Windows from Windows-XP to Windows-8. The primary format handled by the WordPad program is "RTF" (Real Text Format). **Note: For proper operation of CredLock, it is important that you associate ".RTF" files with the WordPad program. You accomplish this by activating the .RTF checkbox in the Windows "Default Programs" settings.**

Clicking the "Images" pushbutton will open a blank or existing RTF file. At the top of the page will be the text from the CredLock "Description" field. You may now enter text, insert pictures, or scanned images into the RTF image file. When you have completed your editing of the Image file you must click the WordPad "Save" button prior to saving the property record itself. If you attempt to close the property record prior to closing the RTF image file, an error message will be displayed requesting that you do so. Once the image file has been saved, click the property record "Save" button to store the record back to the CredLock database. When you access an existing Property Record, the "Image" LED will indicate if there is an associated image file (Green) or not (Red). If the LED is Green you may view, edit text or add images to the existing Image File.

Because it is so subjective, we have not detailed to any great degree the process, of inserting the images into the WordPad file. However, in the WordPad Help File there is an excellent topic on Inserting Pictures into WordPad Files titled "Working With Digital Pictures" The WordPad help file can be accessed by clicking the '?' in the upper right hand corner of the main window.

## Miscellaneous Records

Specific Item PDL	Description
▼	
▼	
▼	
▼	
▼	
▼	
▼	
▼	
▼	
▼	

The Miscellaneous record is somewhat of a catch-all from an information point of view. You specify the primary category of the record in the "Miscellaneous Category" data field and then you can list 10 specific items within that specified category. Each item entry has a description field that can contain up to 100 characters. Each item within a category can have a specific Item name that is listed in the "Specific Item PDL" pull-down list.

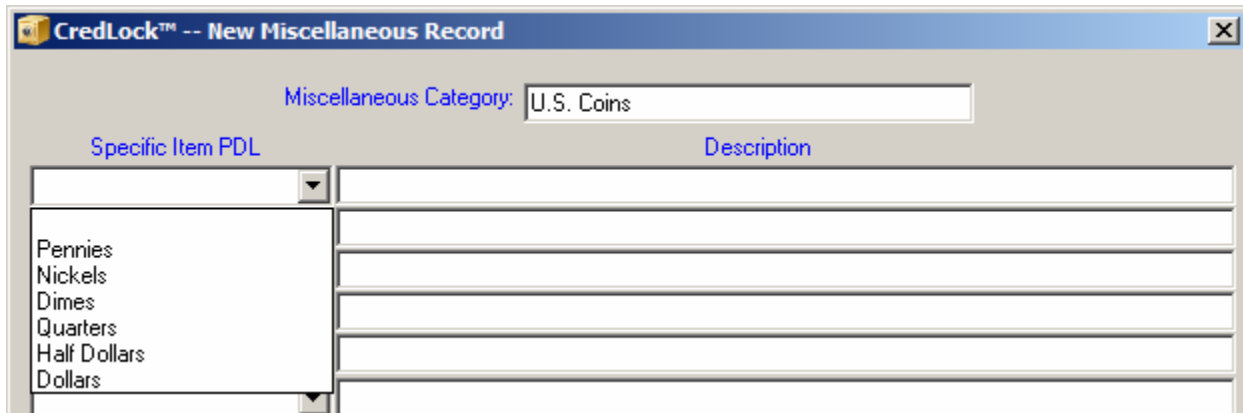
The "Specific Item PDL" can contain up to 255 separate entries (the number of items is a system-wide count and not by each category). As an example, let's say you have a collection of US coins and you want to list the dates of the various coins in your collection. You would first create a primary category of "U.S. Coins" and then items with the labels "Pennies", "Nickels", "Dimes", "Quarters", "Half Dollars" and "Dollars".

Setting up the Item list is quite easy. There are two buttons at the bottom of the record display labeled "Edit PDL" and "Add to PDL". In this case, to add the coinage items, click the "Add to PDL" pushbutton which will display the dialog box below.

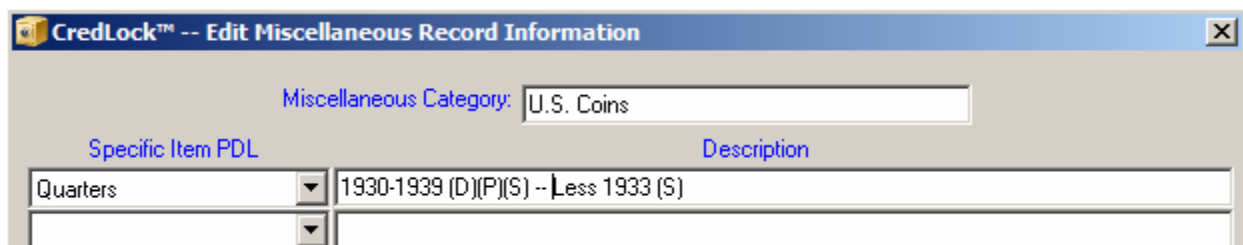
Pennies	
Apply	Cancel

Enter the word "Pennies", then left-click the "Apply" button. A confirmation message will be displayed that the item label has been added to the list. Once you acknowledge the confirmation message, the data field will clear in preparation for your next entry. Once you have added the rest of the coin items, click the "Close" button to exit the entry window. (The "Cancel" button label changes to "Close" after you have added your first item)

After making the additions to the Item list, if you pull-down the list it will display as:

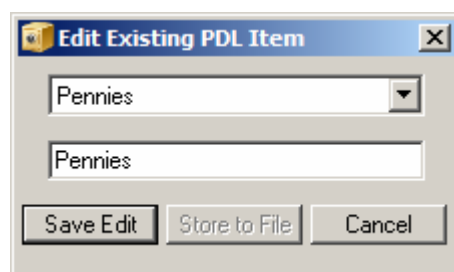


Once you have your item list, you can add some descriptive information about the item. Let say, you have all the quarters from 1930 to 1939 with all mint marks D, P and S, except the 1933(S) quarter you might add in the description segment.



Anyway, you get the general idea. The Miscellaneous Record can be quite useful in categorizing just about anything, with the additional ability to add descriptive information for each item. When you enter data into the "Description" field and you exceed the physical width of field, the data in the field will automatically scroll to the left to make room for additional characters.

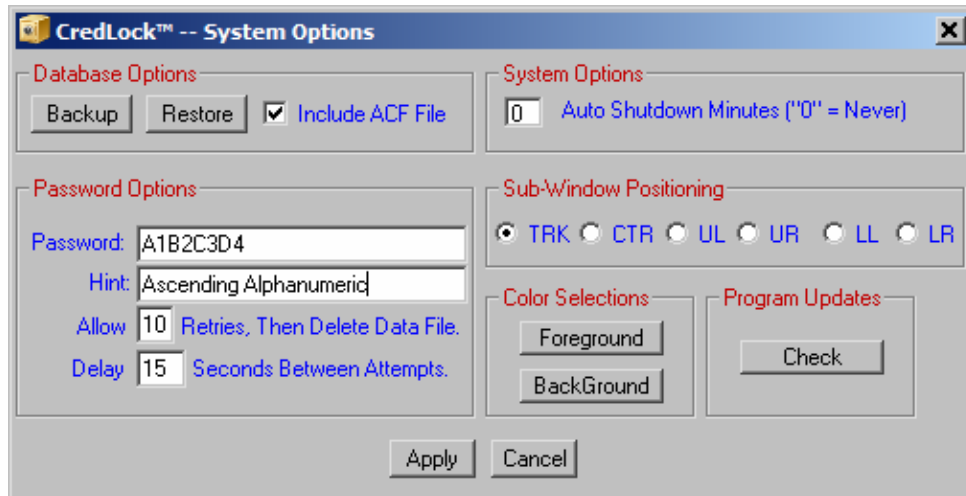
If you notice any spelling errors, or wish to modify an existing label in your item list you can edit them at any time by clicking the "Edit PDL" button. This will display the following Window:



The top field contains the entire item list. First, pull-down and select the item that needs to be modified, then edit the content in the lower window, and click the "Save Edit" button. In the window above you'll notice that the "Store to File" pushbutton is deactivated. It will activate after you click the "Save Edit" button. CredLock saves all of your item edits in a temporary buffer and only stores them permanently when you click the "Store to File" button. You may at any point click "Cancel" to discard any previous edits. Doing this will of course discard all of your edits, retaining the original file contents.

## CredLock Options Window

The CredLock options window allows you to control the way your CredLock system operates. If you click the "Option Settings" pushbutton in the CredLock Main Window, the following window will be displayed:



### **"Database Options" Panel**

The "Backup" button permits you to backup your entire CredLock database including images onto backup media. It is STRONGLY suggested that the backup media be removable, such as another flash drive, preferably one with password protection and separate partitions. These types of drives were discussed in detail in an earlier section of this manual.

With security in mind, backing up your CredLock files onto your primary hard drive is like leaving the key to your house on top of the doormat. Even though the database files are highly encrypted, the image files are not and are viewable by anyone with access to your computer.

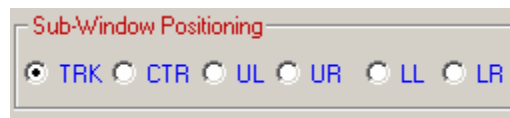
Backing up is easy. Left-click "Backup" and navigate to the destination folder where you want to store the files. For normal operation, the ACF file checkbox should always be activated. Once the files have been backed up, remove the media and store it in a safe and secure place.

Flash drives are not impervious to damage or failure, so if your flash drive should fail and you can no longer access your CredLock system, simply purchase another drive, then download and install a new CredLock system. Next, launch CredLock, which will open in Demo Mode, and then click the "Option Settings" pushbutton. Next, plug in your backup media, and click the "Restore" pushbutton. A message will be displayed asking you to confirm that you want to restore your CredLock database; answer affirmatively and a window will be displayed permitting you to navigate to your CREDLOCK.INF backup file. Once you locate the INF file, click the "Open" button and your CredLock database will be restored. In addition, if you were a licensed user at the time of the backup, the file restoration process will also restore your CredLock operational status from Demo to Licensed mode.

## **"System Options" Panel**

Your CredLock database contains many records filled with secure information. Most CredLock users will utilize the program throughout their day, minimized on the taskbar ready for immediate operation. If your computer is in an environment where others have access to it, and that is something of concern, you might want CredLock to automatically shutdown after a fixed period of inactivity. This is easily accomplished by entering the period in minutes in the "Auto Shutdown" data window. When CredLock closes due to an auto-shutdown, you will have to re-launch it and re-enter your CredLock Master Password to gain access to the system. If you wish to disable the auto-shutdown feature, which we discourage, enter '0' (default) in the "Auto Shutdown" field.

## **Record Window Positioning Panel**



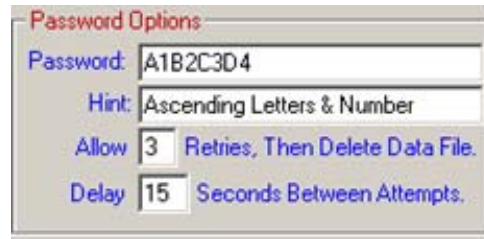
The "New" and "Edit/View" pushbuttons in the CredLock main window display a sub-window containing the data associated with the category record that has been selected in the main window category pull-down list. The "Checkdupes", Statistics, and "Option Settings" pushbuttons also produce their own data sub-windows. With the exception of the "Statistics" sub-window, all of the aforementioned sub-windows are larger in size than the CredLock main window.

These data sub-windows normally track with, and are centered on the CredLock main window when they are displayed. The tracking methodology works fine as long as the main CredLock window remains away from the screen edges and well above the task bar. However, some users may prefer to position the CredLock main Window at desktop locations where the centering of the sub-window results in considerable clipping of the window geometry and the data therein.

The "Sub-Window Positioning" panel in the Option Settings window permits the user to place the sub-window at selected fixed location on the desktop. The default setting for positioning is "TRK" meaning that Credlock will always center any sub-window over the main window regardless of where the CredLock main window is positioned on the desktop.

If you find that your preferred location for the CredLock Main window causes sub-window clipping, then you can instruct CredLock to disable main window tracking and place the sub-windows at a fixed location on the desktop. The choices are "CTR"(Center), "UL"(Upper Left Corner), "UR"(Upper Right Corner), "LL"(Lower Left Corner), and "LR"(Lower Right Corner). Selecting one of these non-track modes will fix the placement of the sub-window to the chosen location, independent of the positioning of the CredLock Main Window. This setting will apply to all data records as well as the Option Settings, Check Dupes, and Statistics sub-windows as well.

## "Password Options" Panel



Credlock does its best to protect your private information in many ways. You can bypass them if you wish, but that is strongly discouraged.

The first is password protection. You can disable it by leaving the password field blank, but that will allow anyone to access your CredLock system and the information therein. Even with a password protected Flash Drive, a CredLock password offers yet an additional level of security. The password shown above is very simple and also very easy to crack. You would certainly want to create a character string that is a bit more complicated, a string based on the measurements of password strength outlined earlier in this manual. In fact, you could use the CredLock Password generator to create the master password for your CredLock System.

Throughout this manual we have continually stressed that you really shouldn't care about the sequence of characters or complexity of your password; the automation of CredLock removes that burden. Strength of a credential is important and is determined by length and character variance.

Here though, with respect to the CredLock master password, is a situation where you do have to remember the exact content and sequencing of a credential. This is where most people choose the easy way out and start using passwords that are familiar and easy to remember...don't do it. Make it just as complex as the automated credentials generated by CredLock. Just make sure that you record the credential on a business card or piece of paper and put it somewhere safe. A good place is to keep it in your wallet with your driver's license. If you use a business card, cover the credential with clear tape to avoid erosion of the characters due to frequent use.

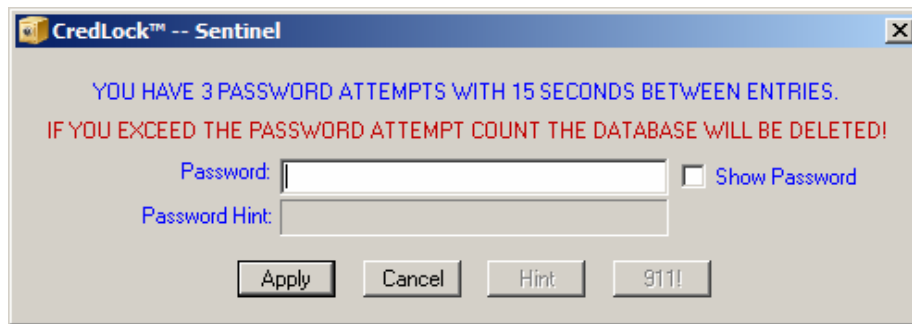
Below the Password field is the "Hint" field. Enter whatever information, up to 27 characters, that will help you to remember the password credential. Use a hint that will make sense only to you and no one else. Using a hint like "My Birthday" is almost like giving your password to anyone that views the hint by itself. Of course you could use that and make your password something entirely different...it's an interesting approach, but if you ever need the hint to truly remember your password, it can become a problem.

The next level of security in CredLock is the retry count field. In this field you place the number of password retries that CredLock will allow before it shreds the entire CredLock database. Most hackers like to automate cracking by running programs on data fields that employ brute-force methods by continually running random strings through the password data field. With a retry count of '3' they can only do that three times and then there will be no data to hack; it will have been digitally shredded. The lower you set the retry count, the better. Obviously '1' is not a good choice but something in the '3' to '6' range is appropriate. If, for whatever reason, your database files are shredded, you can always restore them from your backup copy....you did make a backup, right?

Of course, the foregoing are only suggestions; you have to determine the level of security you want, and with that, the level of inconvenience you are willing to tolerate to achieve it.

The remaining security protection in CredLock is the retry delay. As mentioned earlier, brute-forcing a program for a password requires that a password cracking program continually pass random strings through the password field. A computer hacking program can run thousands of passwords per second through the field. CredLock's retry delay prevents that from happening. With '15' in the retry delay field, the system will only process passwords at 15 second intervals. This feature, coupled with the maximum retry count outlined in the previous paragraph, should thwart most attempts at gaining access to your CredLock System.

So, with password protection activated together with an established retry count and delay, when you launch CredLock the following window will be displayed:



Notice that the "Hint" button is deactivated; there is no need to give an unauthorized person your hint up-front. The "Hint" button will activate only when you have 2 password retries remaining. Normally, as you enter the password, only asterisks will be displayed. If you desire to view the characters you are entering, then activate the "Show Password" checkbox.

I'm sure you are curious about the "911!" button. If for any reason you cannot remember your password, even given the hint, and you are down to 2 retries, both the "Hint" and the "911!" buttons will activate. This is your last resort to recovering a password that you cannot remember but it involves some back-and-forth emailing between you and CredLock's author company DataMatrix. This level of support is available only to licensed users of CredLock.

Clicking the "911!" button, instructs CredLock to assemble an encrypted file that contains information regarding your CredLock license. Rest assured that no data records are included in this file. After the file has been generated, close the CredLock password request window. Next, go to your CredLock folder and find a file with a name consisting of your phone number and the suffix ".hdr". i.e. "2011234567.hdr". This is the file you must send as an email file attachment to credlock@prologsystem.com. The email subject title should be "CredLock 911 Request".

When you licensed your copy of CredLock, you were supplied with a license registration file and a customer number. The instructions suggested that for future reference you print that email and place it in a secure and easy to remember location.

We mention this because along with the "911" file attachment you MUST include your customer number. For security purposes, we will not provide any information to a "911" customer request without their customer number. It accomplishes two purposes: it validates you as a licensed user, and if you have kept that number private, that you are in fact, the licensed user of the system.

Once we have verified the information in the email file attachment and your customer number, we will send you a return email with the title "Your Request". The textual portion of that email will contain your current password and nothing else. Launch CredLock, enter the password from the return email, and CredLock should be back to normal operation.



## "Color Selections" Panel

The foreground and background coloring of data fields are important in creating an effective user interface. Most of us, to place more information on the desktop, choose a high resolution setting. While this does create more desktop space, it also reduces the physical size of the information within the data fields that comprise each window. Subjectively the default black-on-white color combination may not provide sufficient contrast for ease of reading. To deal with this potential issue, CredLock provides via the options Color Selections Panel, the ability to modify the color combination of the foreground and background colors.

To change a color, simply click either the "Foreground" or "Background" pushbutton which will display the standard Windows-Color-Picker display. Choose your color then click the color-picker "OK" button. This will immediately change the color combination of all the data fields that comprise the Options window. You may continue to experiment using different Foreground and Background color combinations until the contrast is to your liking. Once you reach that point, click the "Apply" button which will save your color selections throughout all of CredLock's display windows. If you click the "Cancel" button, any color changes you have made will be discarded and the original color combinations will be restored.

## "Program Updates" Panel

The "Check" pushbutton in the Program Updates panel permits you to check for any CredLock program update files. Clicking the "Check" pushbutton, instructs CredLock to compare the program version number you are currently using against the CredLock website resident update file version number. If the versions compare, a message will be displayed that your current version is up-to-date.

If the website version is more current than your local version, a message window will be displayed alerting you that a program update file exists, and, based on where your CredLock system is located, which update file you should download. You will also be asked if you wish to connect directly to the Update Files Section of the CredLock website. There you will find a series of filenames and associated pushbuttons presented as:

**CREDLOCK\_UDVxxxEXTMEDIAV.EXE**

External Media Update

**CREDLOCK\_UDVxxxPROGFILES.EXE**

Program Files Update

**CREDLOCK\_UDVxxxPROGFILESX86.EXE**

Program Files (x86) Update

Operationally, there is no difference between the update file associated with each of the update buttons. The choice of which file you download only determines where the update files will be stored when the self-extracting file is expanded. The "xxx" in the update filename contains the 3 digit version number of the update.

If your CredLock system folder is located on external media (Flash or Hard Drive), then you should click the "External Media Update" pushbutton and download the file directly to the root directory of the media where the CredLock folder is located.

If your CredLock system folder is located in the "Program Files" folder, then you should click the "Program Files Update" pushbutton and download the file to the "Downloads" folder on your primary disk drive.

If your CredLock folder is located in the "Program Files (x86)" folder, then you should click the "Program Files Update (x86)" pushbutton and download the file to the "Downloads" folder of your primary disk drive.

Once the update file has been downloaded, if CredLock is running, shut it down. Next, locate the update file, and right-click on the update file name, then left click the "Run as administrator" menu entry, which will display a WinZip extraction window. Click the "Unzip" button to begin the extraction and routing process of the update files to your existing CredLock folder located in the root directory of external media or the "Program Files" or "Program Files (x86)" folder on your primary hard drive. Files contained in the update packet will automatically overwrite the existing files in your CredLock folder. Following installation of the update, you should click the "License Info" pushbutton to ensure that the displayed version number is the same number listed in the update file name. The update process does not modify your database files in any way.

### **Other CredLock Main Window Pushbuttons**

#### **"Statistics"**

The "statistics" pushbutton will display the count of active records within each record category.



#### **"Delete Record"**

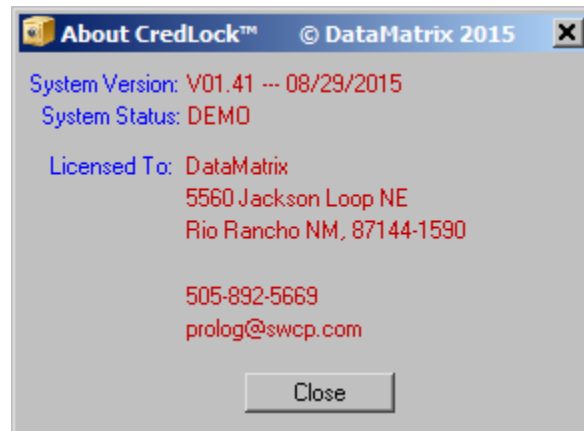
To remove a record from the CredLock database, first, at the top of the main window select the record Category, then from the list at the bottom of the main window select the record to be deleted, which will automatically display the contents of the record to be deleted. Once you have verified that the data contents reflect the record that you want to delete, close the view record window, then click the "Delete Record" pushbutton. A delete confirmation message will be displayed, and if you answer affirmatively, the selected record will be shredded from the CredLock database. In the case of Property and Miscellaneous records any associated Image file will also be shredded. It is important to note the use of the word "Shredded". Shredding is much more than just the deletion of a file. It involves multiple passes on each character of the file before it is finally deleted. What's left after shredding and deletion is a sequence of incoherent data characters that have no resemblance to the original contents of the file.

## **"Check Dupes"**

On page 9 of this document we described the operation of the "Check Dupes" button as it applied to an Internet Record. In that context, the search applied only to the User Name and Password for the displayed record. Clicking the main window "Check Dupes" button initiates a scan of all Internet records for duplications of User Names and Passwords. The scan results display is the same as shown on Page 10 of this document. For a detailed description of how to interpret, and apply the results refer to the "Check Dupes Pushbutton" section on page 9.

## **"License Info"**

The "License Info" pushbutton will display the license information associated with the CredLock system. The window below shows the current version together with the system status which for this product is "Demo", and because it is a "Demo" version of the CredLock product it is licensed to our company "DataMatrix". Once the product is registered, the "System Status" will change from "Demo" to "Licensed" and your Name, Address, Telephone Number and Email Address will be displayed in place of our company information.



## **"Help File"**

CredLock is supplied with a built-in Help File in PDF format. You must have the Adobe Reader program installed on your computer to view this file. Left-clicking the CredLock main window "Help File" pushbutton will launch Adobe reader displaying the CredLock Help File. The name of the file is "CredLock\_Help.PDF" and is located in your CredLock system folder.