

Installation and Upgrading the New PCI-Compliant POS

The new **Version 11** of Rocket POS will meet all current requirements of the PCI-DSS compliance at the time of issue. The whole purpose of the PCI compliance is to safe-guard credit card information. This includes NOT storing any credit card information electronically that can be used to do charges at a later date.

We recommend you read and print this entire document before starting your upgrade. There are many steps that must be followed in order to successfully upgrade your existing POS software. You may **lose your data** if these steps and procedures are NOT followed.

A Few Things You Need to Know Before Proceeding

Three (3) of the invoicing screens have been removed from the Point of Sale leaving ONLY the Pro-Invoice Screen. This was done to simplify code maintenance and PCI-Compliance.

If you are using Mercury, you need to contact **Your Primary Business Contact**, Toll Free **(800) 846-4472** at Mercury before doing the upgrade. Mercury will assign you a new account number to work with the new Mercury routines found in this new version. If you install version 11 without contacting Mercury and getting your new account number, you will NOT be able to accept credit cards until your new account number is installed.

At this time, this version is NOT compatible with the SQL Multi-Store. We expect changes made to the SQL Multi-Store soon to be compatible with version 11.

If you are going to order a new Magtek card scanner, only the NON-signature capture model is supported. Signature capture is supported with our Topaz interface at this time.

We cannot stress enough, missing a step below will make your POS useless

Summary of Upgrade Steps

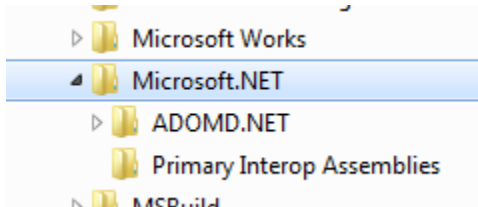
- Make a copy of the Nickel Folder
- Test existing data for flaws
- Install the Upgrade
- Unlock the upgrade with your new NSI unlock file
- Update the additional stations on your network.

If you feel like you need phone support for help in this installation, please go to the link below, fill out the form and fax it in.

http://www.rocketpos.com/Order/EU_Support.pdf

Email support is free and answered on a first come, first served basis. We do expect heavy volume over the next few weeks. If we can't answer your question by email within three tries, you will have to send in a support agreement.

You want to make sure .NET 3.5 is installed on your computer. If you are using VISTA or Windows 7 – chances are you have .NET installed already. If it is there, you should see a folder similar to the below under the folder **C:\Program Files\Microsoft.NET**



If you do NOT have .NET on your computer, go to the link below to install it from Microsoft.

<http://www.rocketpos.com/VU.asp>

The very first step we want to do is make a copy of the NICKEL folder. This is in case something does not go as expected and you can copy it back to start over.

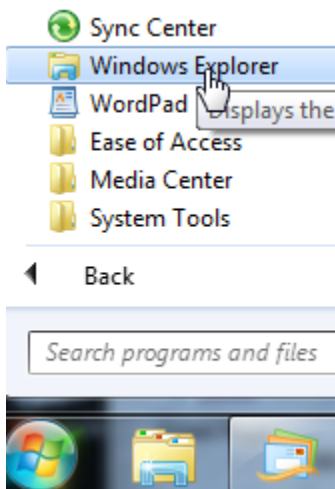
Make SURE you are the Only one on the Network or PC while doing the below steps.

The below steps are for the DATA computer. In other words, the computer that holds the POS data that it uses every day.

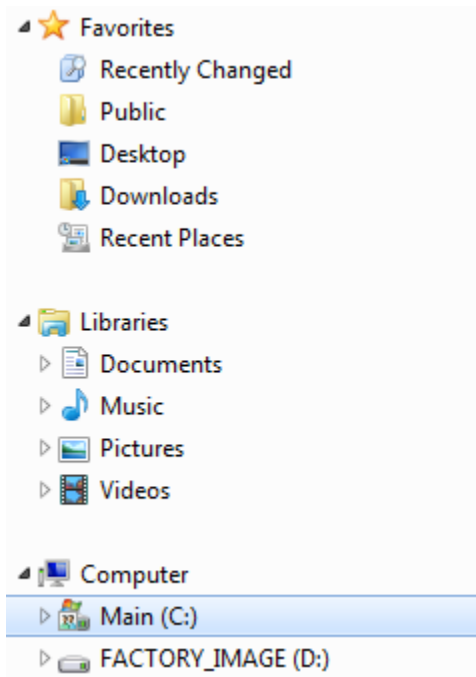
Reboot your Computer to make sure all programs are closed and all other users are off the system.

We are using Windows 7 in our example screens here, your may be different but the functionality should be the same.

Bring up Windows Explorer (not Internet Explorer)



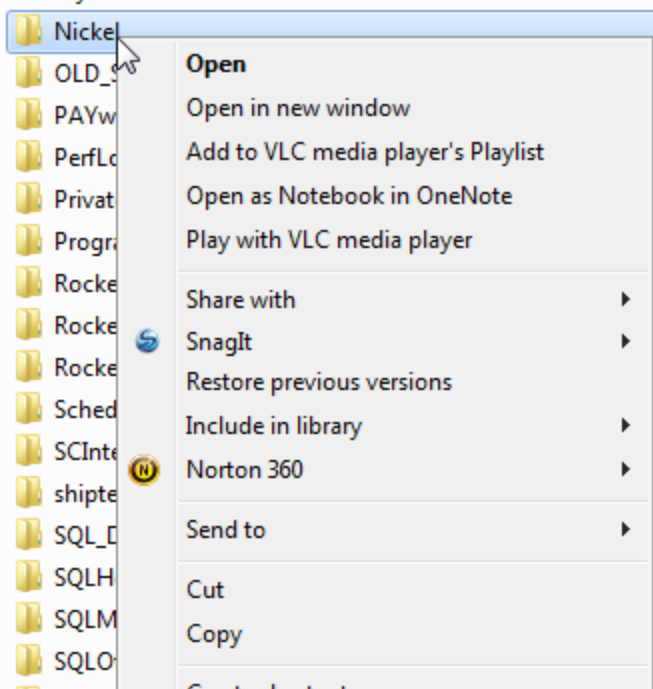
Find C: drive or the Drive containing the NICKEL folder with the POS data



Now Open the C: Drive by clicking on it and finding the NICKEL folder.



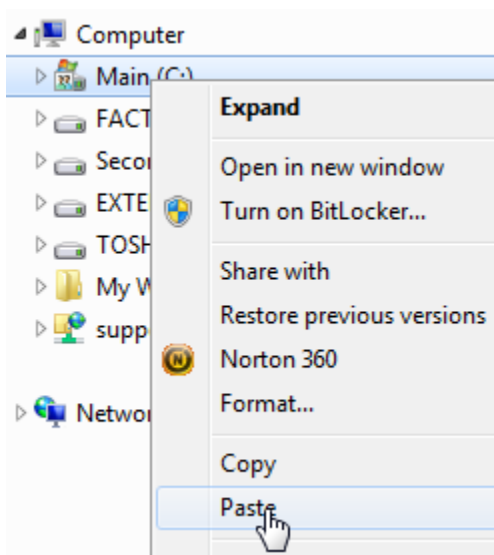
Right Click on the NICKEL folder and the below screen will come up



Click on the **Copy** option

Now go click back on the C:

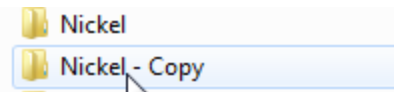
Right click on the C: drive



Click on the Paste option

Give your PC a few seconds to copy the folder

You should now have two exact copies of the NICKEL folder



Note: some versions of Windows rename the **Pasted** copy as a different name other than shown above.

Okay, now we have a Fall-Back copy of our data.

We want to now check that our existing data is aligned properly and has no missing sections or corruption

Go back to the C: drive and click on the NICKEL folder again. All the Files in the NICKEL folder should now show on the right-hand window of Explorer.

Click on the Type header until you see a file called dbcmake.exe (or dbcmake)

Name	Date modified	Type	Size
_uninstall	1/6/2010 10:36 AM	File folder	
dbcmake.exe	6/30/2009 5:34 AM	Application	961 KB
nposwiz.exe	5/26/2004 7:13 AM	Application	873 KB
tracker.exe	1/6/2010 9:16 AM	Application	15,942 KB

Double click on this file.

You should see the following



Click the **Create DBC And Tables** button, you will be asked to continue, say yes.

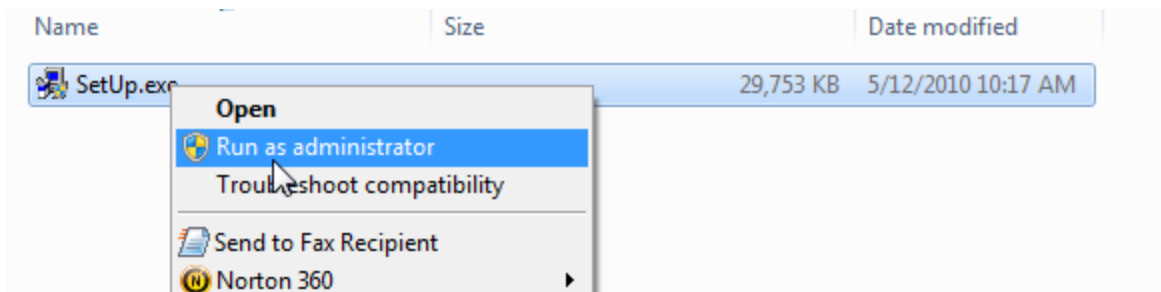
If this routine ERRORS-out – you have corrupted data and may have to send your data to us for repair. See our website and support agreement for pricing on this service.

If this routine completes with no problem, you are ready to continue with the upgrade.

Download the Upgrade from our website download area. Place this in a folder or on your desktop so you may do the install from it. We strongly suggest keeping a copy of this file for the future in case your system should crash or you need to install the exact same version on another computer.

After Downloading the Update

THIS IS IMPORTANT – With the new Windows Operating Systems from Microsoft – you will need to do the following; After downloading the file called UnZipMe.zip from our webpage, open the ZIP file and then RIGHT CLICK on the file inside called Setup.exe. The screen below will open up and then click on **Run as Administrator**. This is necessary to overcome all the security locks in the newer versions of Windows. You may also have to do the same procedure in running dbcmake and Tracker and the batch files until you have your security levels at the correct settings within your copy of Windows.



The download will be a zip file; you should be able to double click on it to expose the SETUP.EXE file inside the zip file. Double click on this file. This should start the install routine. Follow the on screen prompts.

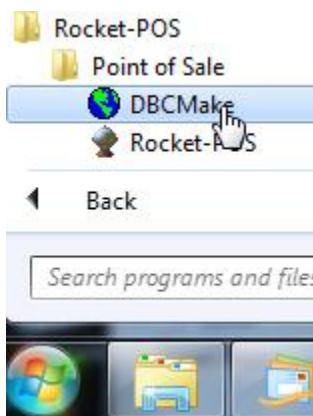
The password for the new install is: **superpos** (*all lower case - case sensitive*)

After installation is complete, reboot your computer.

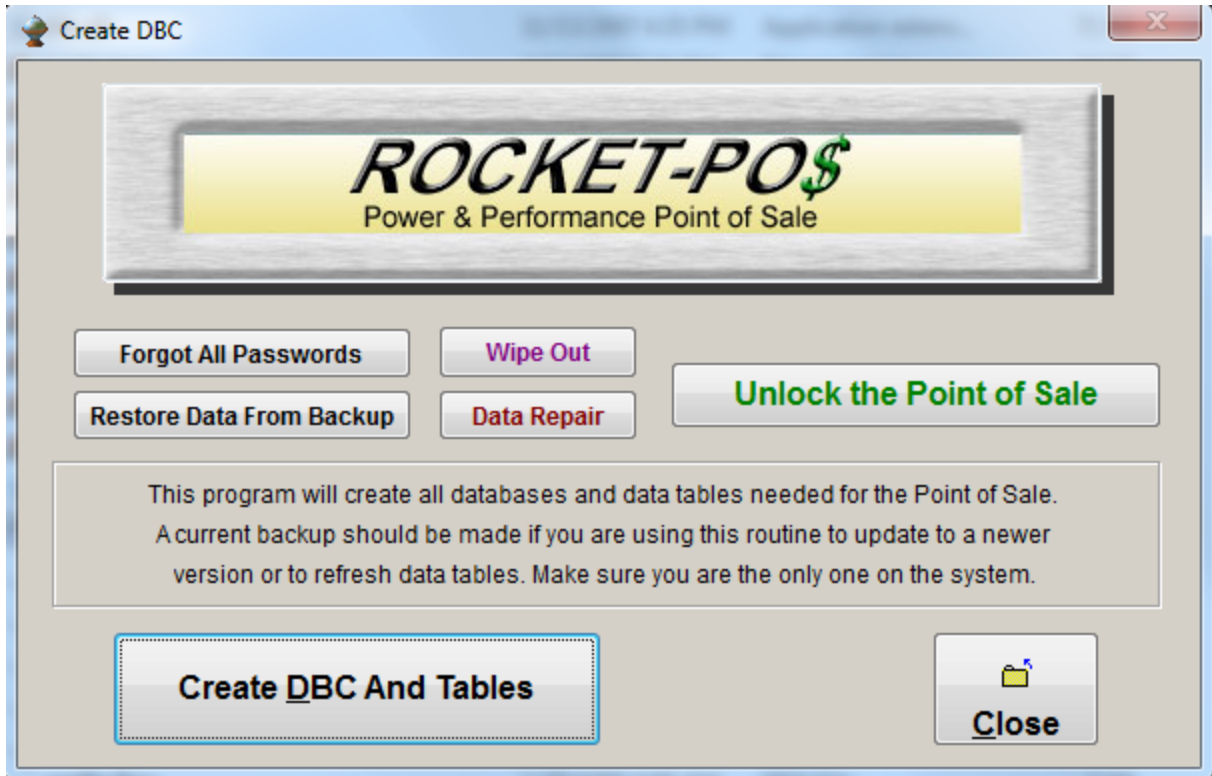
To make sure the new install took effect, go into the Windows Explorer again and check the dates on these two files; TRACKER.EXE and DBCMAKE.EXE – their dates should be December, 2011 or later. If not, erase these files and then do the install again.

Now we need to bring the POS data files up to the new specifications and verify the new libraries loaded.

Go to your start button in Windows (*See above about running as an Administrator*)



And click on dbcmake again.

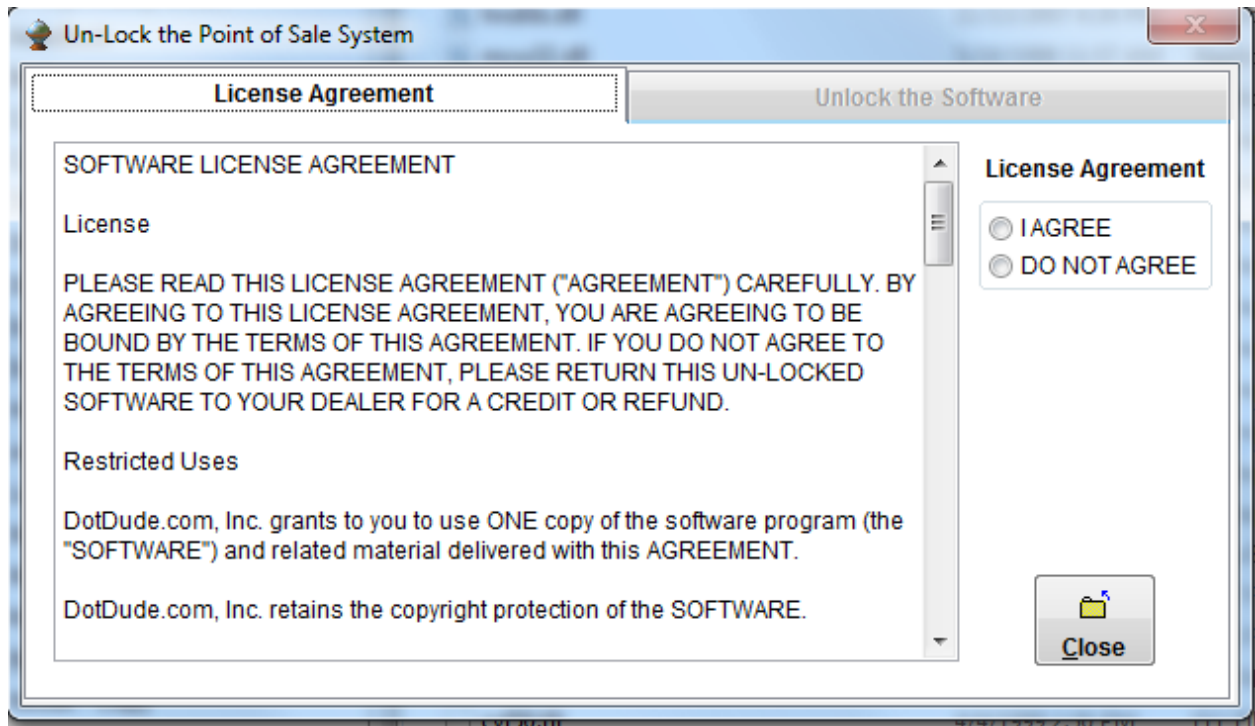


Click the Create DBC And Tables button again, say Yes to the prompt and let the dbcmake up data your files and structures. If this routine errors out, you may have corrupted data and will need us to fix your data files. Go to our website under the Support area for pricing and the Support agreement.

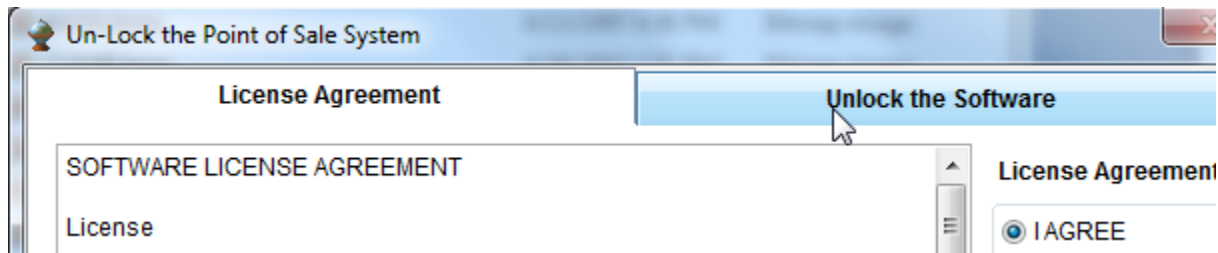
We now need to Unlock the POS with our new NSI file, this file should have been given to you by your dealer or emailed directly to you.

Place this file in the NICKEL folder.

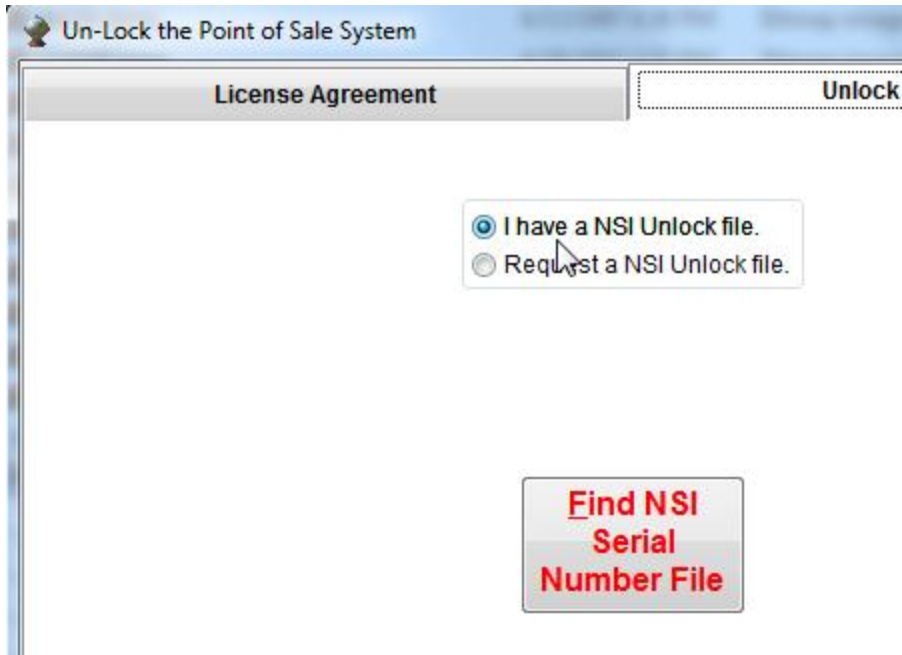
Click the Unlock button showing above. You must Agree to the License Agreement before going any further.



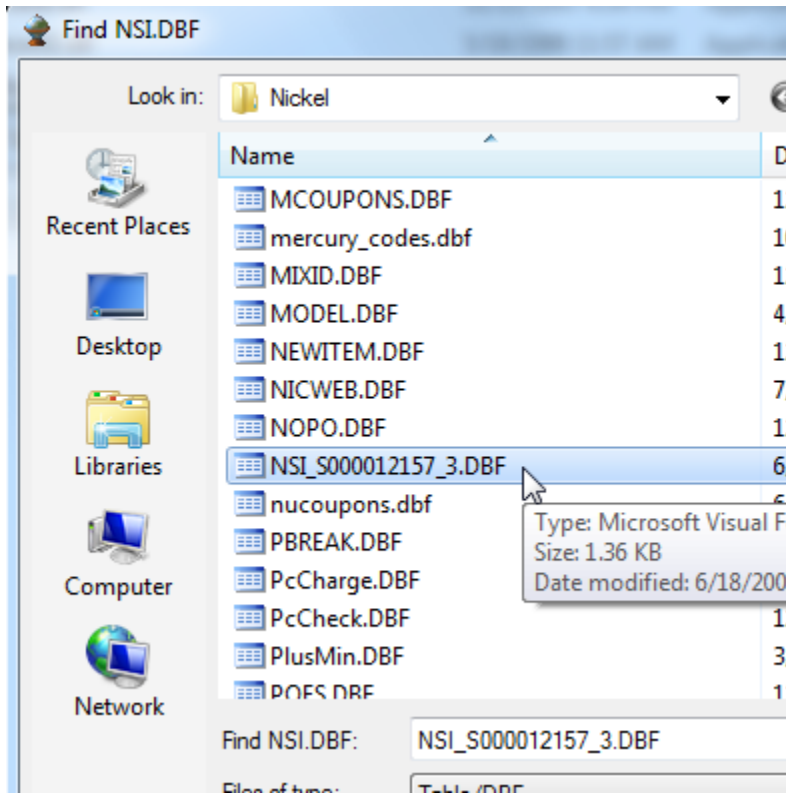
Once you Agree, click the Unlock Tab



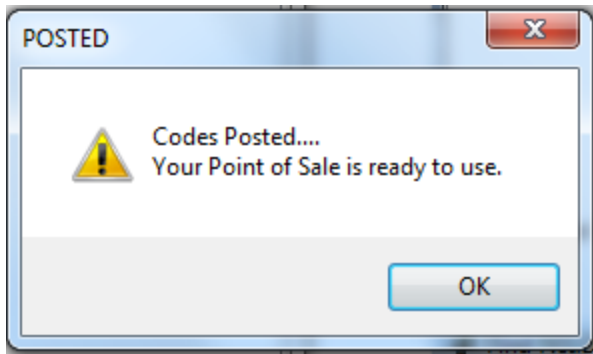
Click the I Have a NSI Unlock File



Then click the **Find NSI Serial Number File**, the below window will open up. Select your NSI file and then click **Select**.



You should now get the following window



You can now Exit the dbcmake program.

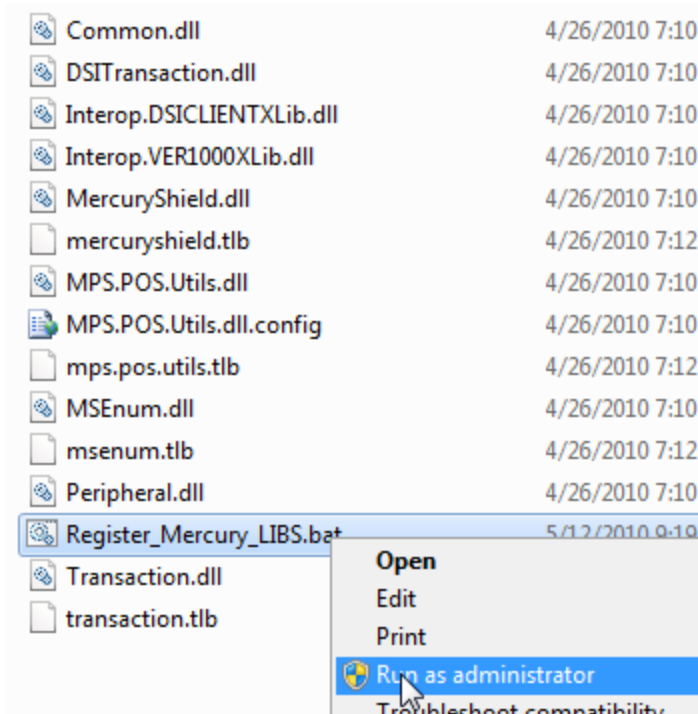
Please NOTE; Sometimes our code generator will mess-up and generate an invalid code, if this appears to happen to you, email use and let us know. You will be able to tell if this happens when you enter the Point of Sale and you get a message, Invalid Codes.

If you are using Mercury – **you must download and Install the latest DSIClient** from their website

You must install Microsoft .Net 3.5 for either Mercury or pcCharge to work correctly – see our web page for the link to this.

The next steps are necessary to register the Mercury and VeriFone Libraries.

In Windows Explorer, find the folder called C:\Mercury_Shield, inside of this folder you will find a file called, **Register_Mercury_LIBS.bat**, right click on this file and then run as an administrator as shown below;



You will see an old style DOS window open and run an internal program. You will have to press your Enter key four times (once after each pause) to get the pause to run the next command. Make sure before hitting your Enter key that command ran successfully.

You must now do the same thing for pcCharge. Find the folder called C:\Verifone, inside of this folder you will find a file called **Register_pcCharge.LIBS.bat**, right click on it, and run as an Administrator as above and you will have to click your Enter key three times here.

Note: We used pcCharge 5.7.1 to test against and it worked fine so any version of pcCharge 5.7.1 or greater should work.

Make sure to run the install above on all work stations, you just do NOT have to run the dbcmake program on the stations connecting to your data.

You are now ready to use the POS

Here are some things that have changed and will affect you because of PCI;

A manager password is now mandatory for Managers.

Salespeople

Salesperson Security Rights Account

Name: My Favorite Clerks Name

Street: Main Street

City: Emmitsburg

State: MD Zip: 21727

Phone: (410) 324-2342 No

Active Clerk

This clerk can be a Line-Item Clerk

Is A Service Tech

Use A Cash Drawer

Sign On Code: 001

Password:

Admin Password: Optional

Admin PW must be min of 7 characters and contain 1 Upper and 1 Lower Alpha Character and a Numeric Character

Department:

Listed As An Admin

Prev Next Add

A Default Manager Password was made for any Managers in your POS system of **Temp123**

Point of Sale User Management Requirements

Rocket POS supports unique user accounts. No two individuals can share an account. Any out of the box default accounts must be prompted to change the password at first login. Depending on the type of access a user account has, two different levels of security requirements apply.

1. Administrative Users

Administrative users are those that have access to administrative functions as defined below. Access to create, edit, or delete users Alter user privileges Password resets or account lockout resets Access to configuration screens Access to delete the logs if such a function is available Creation and deletion of system level objects (drivers, system services) if such a function is available

Security requirements for administrative users: Required to log in at the beginning of their shift and sign out at the end of their shift. Managers must have both a username and a password. The password must meet the following requirements.

- Contains both numeric and alphabetic characters
- Minimum length of seven characters
- Must be changed every 90 days
- A new password cannot be the same as the prior four passwords Six consecutive incorrect passwords submitted for a user login results in that user account being “locked out.” During account lockout, not even the correct password can grant them access. Locked out accounts must remain locked out for at least 30 minutes or until another administrator resets the lockout. If the user is idle (no activity has been performed by that user) for 15 minutes, the user must re-enter their password to continue their session.

2. Basic Users

Basic users are those that do not have access to any administrative functions.

Security requirements for basic users: Required to log-in at the beginning of their shift and sign out at the end of their shift. Basic Users must have both a username and a password or PIN. No complexity requirements apply.

Card Changes

If you are using pcCharge – the Credit Cards screens are not drastically changed but will have PCI-Compliant at the top of each screen.

If you are using Mercury – the screen changes are totally new.

How the new PCI routines work within the POS – essentially when a card is scanned now or hand entered, it is actually being scanned or entered into the pcCharge SIM module or the Mercury Mercury-Shield module. This keeps the Credit Card data from ever “Touching” our POS. If our POS never touches the credit card data, there is no way to store the data.

You will find two new folders on your C: drive.

For Mercury it is called – C:\Mercury_Shield

For pcCharge it is called – C:\Verifone

Without these folders, the new credit card routines will not work.

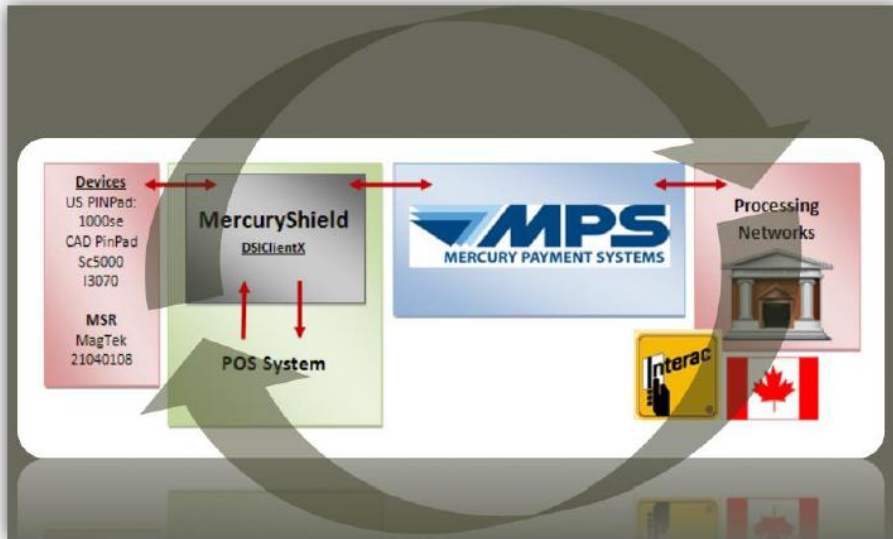
Do NOT erase these folders.

Inside of these two folders are a BATCH file that will be required to be run by you.

Particular note to pcCharge users, the Everest Plus pin pad is no longer supported as it is NOT PCI compliant. **Only the Peripherals listed in our POS are supported** and not all peripherals listed in the VeriFone SIM flyer.

Mercury now ONLY supports the VeriFone 1000se Pin Pad and **will soon** support the Ingenico i3070 pin pad.

How Mercury Shield Works



MercuryShield™

PA-DSS Compliance Benefits and Ease of Integration

Mercury Payment Systems' MercuryShield provides software vendors with the ability to deliver fully integrated payment solutions without the need to store, process, or transmit cardholder data. As a PA-DSS validated payment application, MercuryShield is an easy way for point of sale (POS) developers to integrate to a processing solution that removes their payment application software from the need to contact cardholder data. As a result, this frees the POS developer to focus on the advantages of their other functions and features and eliminates the untold time and expense which would be required to achieve and maintain PA-DSS compliance.

With MercuryShield, a developer's application is responsible only for an exchange of non-sensitive payment transaction data. Using a set of easy to implement .NET assemblies, MercuryShield securely handles all of the sensitive cardholder data throughout the transaction flow. MercuryShield encrypts, sends, and receives the transaction information and passes back to the POS application only non-sensitive transaction data. In other words, by shifting the responsibility of handling sensitive cardholder data to Mercury®, MercuryShield removes the developer's software application from the most significant portion of PA-DSS compliance: your system no longer needs to store, process or transmit sensitive cardholder data.

Additionally, by following the procedures outlined in this integration guide, Mercury's developer partners will benefit from:

- reduced programming time
- a simple integration process
- step by step instructions designed and tested internally
- easily accessible .NET assemblies (COM accessible available)
- peripheral support built in to MercuryShield
- Canadian Debit functionality and an uncomplicated remote Interac certification process

How pcCharge SIM Works

