

Implementing Your Point of Sale and CCEngine

Of the PA-DSS and PCI DSS criteria that determine the security level and ultimate compliance of your POS system, six areas stand out as requiring particularly close attention: Storing Card Data, User Management, Logging, Wireless Network Considerations, Remote Access and Encryption over Public networks.

Storing Sensitive Card Data

VRP will never store sensitive card data in clear text and will not store any magnetic card data, VCC2, and entered debit pin codes at all. There are no debugging or troubleshooting settings that permit magnetic track data or pin entries to be stored. Storing sensitive card data through alternate means should be avoided whenever possible to avoid risk of theft and to minimize PCI compliance requirements. If you must store sensitive card data for a valid business reason, you must ensure you're not storing information deemed prohibited for storage by PCI such as full magnetic stripe, CVV2 or PIN data. If you are storing full account numbers not using the VRP CC Engine, the card data must be properly encrypted and protected as defined by the PCI Data Security Standard.

If you are upgrading from a prior version of VRP, the automatic upgrade procedure will convert all sensitive data, encrypted or not, to a secure encrypted data as required by PCI

We recommend not to store sensitive data unless it is needed for running your business. Use the "purge CC Info" utility on a regular basis to erase old credit card data that is no longer needed.

Encrypt Sensitive Traffic over Public Networks

Use only the CC engine to process credit card payments. The CC engine is secure and uses technologies approved by PCI. Do not use remote control programs such as PC Anywhere or VNC to process credit cards on a remote computer. See the "remote Access" section for further instructions.

Remote Access

The CC engine of VRP does not require the use of remote access or any other form of remote administration.

If you use an alternate administration interface over the network (*e.g.* Remote desktop or LogmeIn) to access your payment processing environment, the traffic must be encrypted with a secure encryption technology (*e.g.* SSH, VPN, or SSL/TLS) to maintain PCI DSS compliance.

If you require the use of traditional remote computer or network access, it must meet the following requirements to maintain PCI DSS compliance.

- Do not use remote access solutions requiring "port forwarding" such as VNC and PCAnywhere.
- Incorporate two-factor authentication for remote access. Use technologies such as RADIUS, TACACS with tokens, or VPN with individual certificates assigned to each user.
- Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these

technologies for all employees and contractors. Ensure these usage policies require the following:

- Explicit management approval.
 - Authentication for use of the technology.
 - A list of all such devices and personnel with access.
 - Labeling of devices with owner, contact information, and purpose.
 - Acceptable uses of the technology.
 - Acceptable network locations for the technologies.
 - List of company-approved products.
 - Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.
 - Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use.
 - When accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media.
- If e-commerce integrators access the database applications remotely, the remote access must be implemented securely.

Examples of remote access security features include:

- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).
- Allow connections only from specific (known) IP addresses.
- Use strong authentication and complex passwords for logins. Refer to PCI DSS requirements 8.1, 8.3, and 8.5.8–8.5.15
- Enable encrypted data transmission according to PCI DSS requirement 4.1
- Enable account lockout after a certain number of failed login attempts according to PCI DSS requirement 8.5.13
- Configure the system so a remote user must establish a Virtual Private Network (“VPN”) connection via a firewall before access is allowed.
- Enable logging functions.
- Restrict access to customer passwords to authorized integrator personnel.
- Establish customer passwords according to PCI DSS requirements 8.1, 8.2, 8.4, and 8.5.

VRP evaluated several remote access solutions, comparing cost, convenience and security features that meet PCI compliance requirements for remote access. VRP recommends the use of LogMeIn with two factor authentication.

Wireless Networks

VRP does not require the use of a wireless network and VRP advises against using one. If you set up or have a preexisting wireless network, take the following precautions to remain PCI compliant.

- If the wireless network is not used by your CC engine, make sure that a firewall prevents access to the CC engine and / or to the database.
- Wireless networks attached to your in store network MUST meet the following PCI DSS requirements:
 - Use WPA or WPA2 encryption.

- In the rare case when there are no available updates from the manufacturer that add WPA or WPA2 support, WEP must be used. Those devices must be replaced with newer equipment and the encryption changed from WEP to WPA or WPA2 encryption by July 1, 2010.
 - The default WPA/WPA2 encryption key must be changed to a unique strong key.
 - The default password for accessing the Wireless Access Point's settings must be changed to a unique strong password.
 - Change default SNMP (Smart Network Management Protocol) community strings on Wireless Access Points if SNMP is supported or disable SNMP altogether.
 - Synchronize the access points' clocks to be the same as your computers to ensure logged timestamps match.
- Wireless networks attached to your payment processing network are HIGHLY RECOMMENDED to enable additional security:
 - Do not wait for the July 2010 deadline to update from WEP to WPA. WEP is extremely insecure. Easy to use tools are readily available that only take minutes to discover the WEP key. These tools have been employed for the last several years by criminals to access business networks, leading to several data breaches.
 - Use wireless keys of 13 random characters containing letters, numbers, and symbols. Keys comprised of words or names are quickly found by criminals using readily available, easy to use tools.
 - Disable SSID Broadcast to make your wireless network less visible to unauthorized users.
 - Use MAC address filtering so that only authorized computers are allowed access to the wireless network.
 - When configuring WPA or WPA2, use the AES option. Only use TKIP when AES is not an available option. Although not severe, there are known weaknesses in TKIP.

More information on network segmentation can be found in the section, Network Basics and Segmentation. Recommended network configuration diagrams are available in Appendix A, Recommended Network Configurations. For a more thorough explanation regarding setting up wireless networks, review the PCI DSS Wireless Guidelines document listed on the PCI Security Council's website: https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

Network Basics and Segmentation

Switches are network devices that allow you to connect together multiple computers, routers, and wireless access points, firewalls, etc. Switches have multiple network ports, one for each item connected using a network cable. All devices connected to the same switch can communicate with each other unobstructed.

Firewalls are network devices that allow you to protect a network segment on the LAN side from the network segment on the WAN side. Although they can cost up to \$70,000, there are inexpensive (\$40-\$100) small routers containing firewall functionality that can be found at any store containing computer equipment. These inexpensive routers will work sufficiently as long as they support Stateful Packet Inspection (SPI).

Network segmentation is a strategy intended to simplify PCI compliance of your network and to help you protect your business from hackers. At the most basic level, there are three zones representing three levels of risk.

Untrusted Environment – Network connections that anonymous people have access to are considered “untrusted.” They should have no network access to your business computers and

point of sale equipment. Business computers should never be connected directly to this zone. Common untrusted networks are the internet connection itself, customer wireless internet access, and visitor network connections. This is the highest risk zone because anybody can connect to it anonymously. Systems connected to this zone are commonly hacked or get infected with malware and viruses.

Non Card Data Business Environment – Systems not used for payment processing, but are still business owned fit into this segment. These are systems that can be used for email, web browsing, and other higher risk activity that you would never want to perform on your payment processing systems. On occasion, these systems will almost certainly become infected with malware and viruses. Once a computer in this zone is infected, the hacker or infection will spread to other systems if they're not protected by a firewall. Note that if any systems in this zone handle credit card data, that data is being put at risk. This is a medium risk zone due to risk of occasional infection. By segmenting these systems into their own zone, the breach is contained. The hacker, malware, or virus doesn't reach your firewall protected payment processing zone.

Card Data Business Environment – Systems used for payment processing fit into this segment. These systems should only be used for Point of Sale activity and should NEVER be used for any other reason. Should these computers become infected with malware or viruses, sophisticated hacking tools can potentially steal sensitive data such as credit cards. The average cost of a breach for a small merchant is \$36,000. This is a low risk zone because it's protected from the other two zones and high risk activities such as web browsing and email do not occur inside it. The chance that hackers, malware, or viruses spread to these systems is minimal.

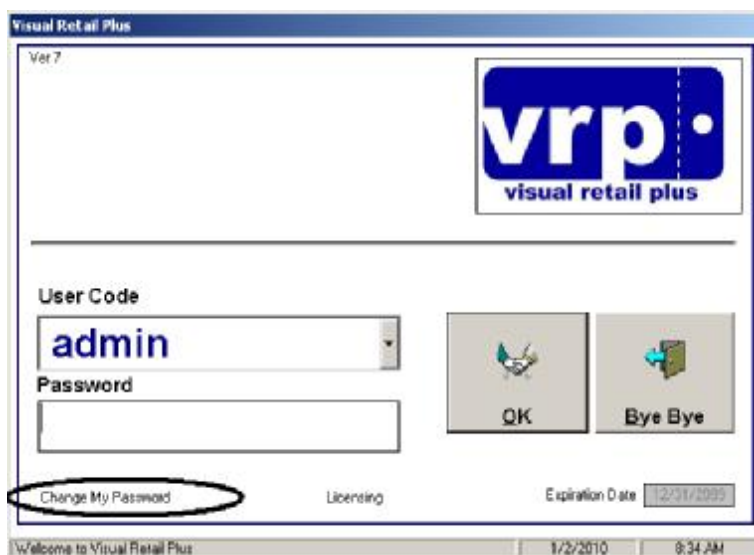
In summary, to segment your network for security you should:

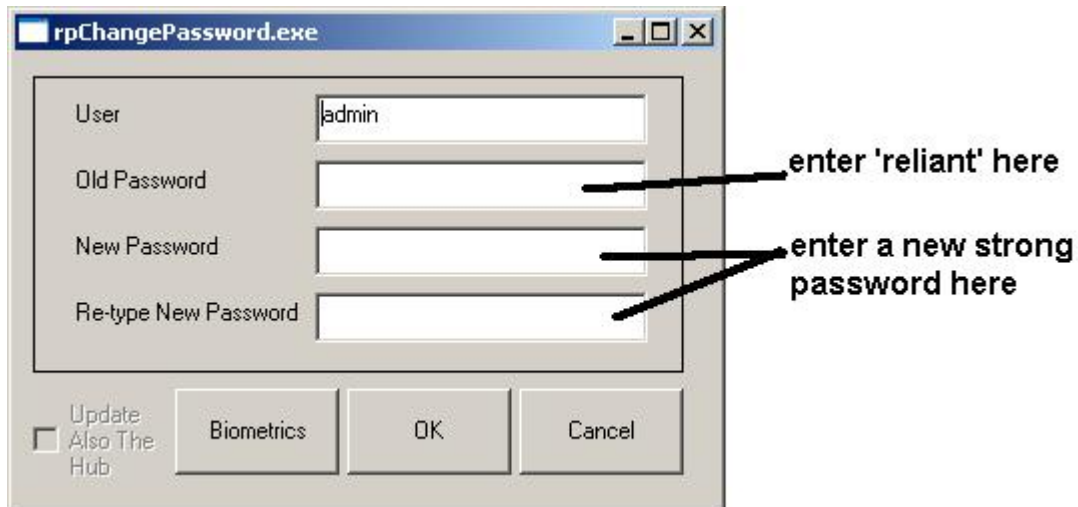
- 1) Protect both business environments from the untrusted environment.
- 2) Protect your card data business environment from the non card business environment.

For simple network diagrams to help guide your network configuration, see Appendix A, Recommended Network Configurations.

User Management

VRP when first installed uses a default administrator account with the username: *admin* and a default password: *reliant*. When a user first logs in she/he must change the default admin password. From the first login screen click on "Change my password" and follow the instruction on the screen.





Each user must have a unique user ID and password. Do not use group, shared or generic accounts or passwords. Users should never share their passwords with anyone else.

These requirements are for PA-DSS compliance and you must maintained them. They apply only to user accounts with administrative level access.

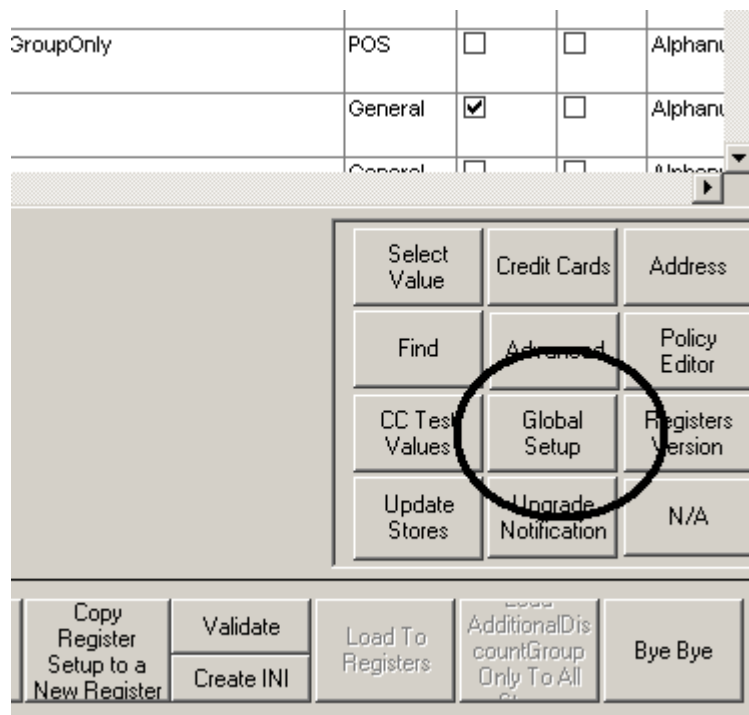
- Passwords must be at least 7 characters
- Passwords must contain at least 1 upper case and 1 lower case letter
- Passwords must be changed at least every 90 days
- Passwords must not be the same as the last 4 used
- Failure to login six times in a row will result in the account being locked out for 30 minutes or until unlocked by another administrator
- Change in setup the idle time to a maximum of 15 minutes, after the timeout the password must be re-entered.
- VRP recommends to apply auto Logoff after each sale transaction.
- VRP recommends to use fingerprint device to disable the manual login option to cashiers who handle credit and debit cards.

See Appendix C for instruction how to create users security levels

Changing the main encryption key

VRP's database is storing sensitive data in an encrypted format. The password related to decryption is stored in an encrypted mode in the database as well. Upon startup of the system at the first time, you will be prompted to enter a password that VRP will use to create the encryption certificate. If you choose not to enter a password, credit cards will not be processed by the CC Engine. Administrators can change that password, but upon change all previously entered sensitive data will no longer be readable.

To change the password creating the certificate, go to the global setup and create a new key as follow:





When you press “Create certificate” you are asked to enter the encryption password.

Note: Choose a strong password that is at least 7 characters long, contains numbers and both upper and lower case letters. The more complicated it is the better. Select a password that has no relationship to personal or company data.

Example for a good password is a56\$Qkk!2

Example for a medium strength password is John2010

A bad password is Galaxy (especially if your company name is Galaxy)

Remember or save the password in a secure place, you will need it in case that the SQL server is recreated or the database must be restored from backup.

Additionally, Windows accounts should be configured to meet these secure authentication requirements for PCI DSS compliance.

Logging

VRP logging is enabled upon startup and cannot be disabled. It logs the following information:

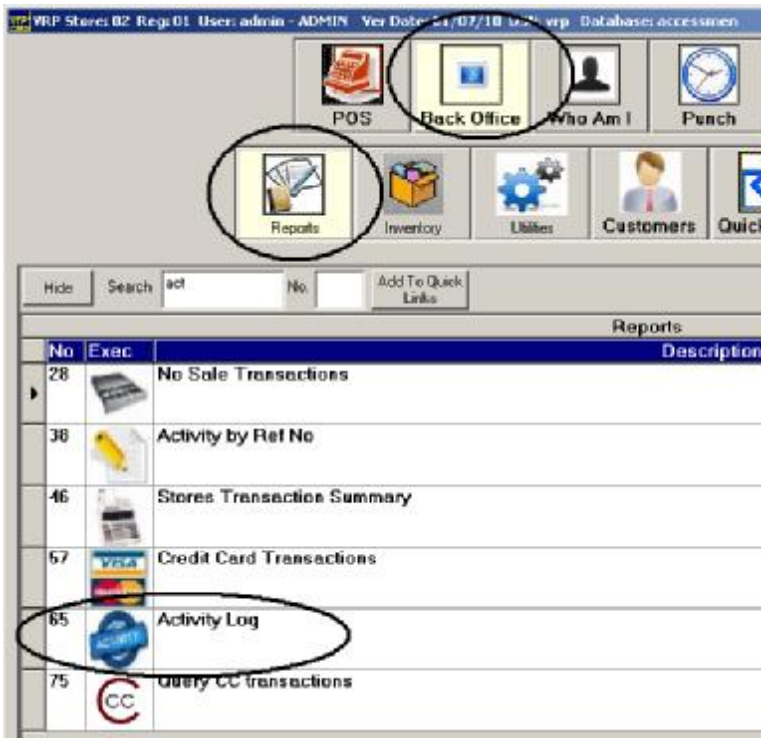
- User login time into to VRP
- Date and time of any transaction, credit card transactions are logged for both request time and finalize time.
- Type of transaction
- Transaction amount
- Register number
- Success or failure indication
- Username

The SQL transaction log including card payment transactions is automatically maintained by the database and is accessible only by the SQL service. The data must be protected using the SQL security.

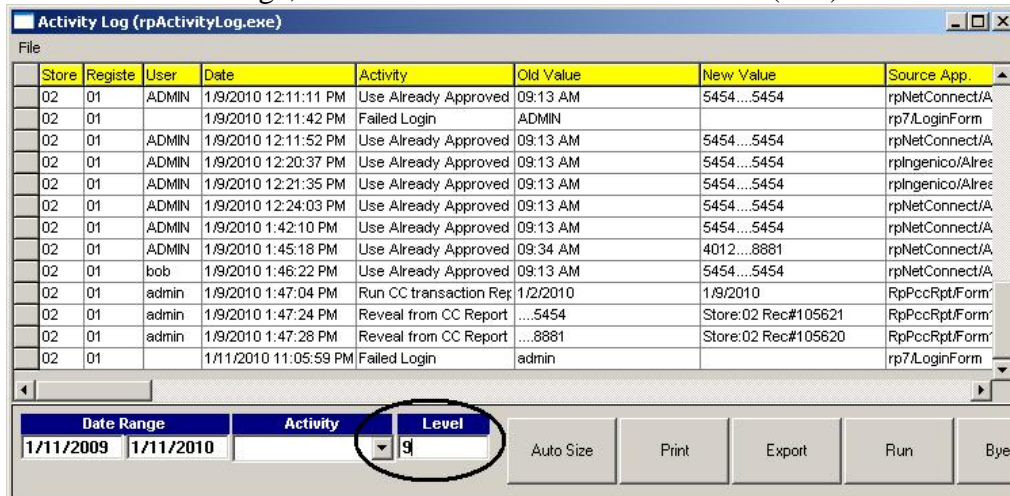
Create an SQL user instead of the standard sa that is allowed to use the VRP database.

See Appendix B

To Access the compliance logs use the activity log program:



Choose the date range, enter 9 for credit card related issues (PCI) and click “Run”



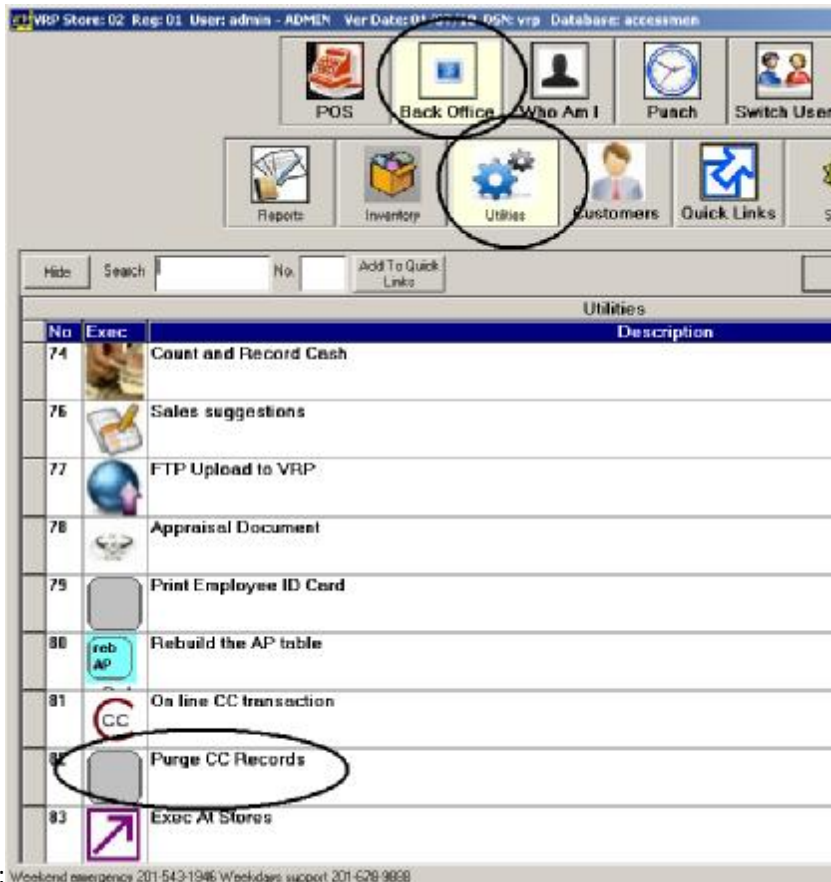
Purging Sensitive Data

The best way to protect your customers is not to keep any sensitive data. It is required to destroy any sensitive data that is no longer needed for the normal course of running the business.

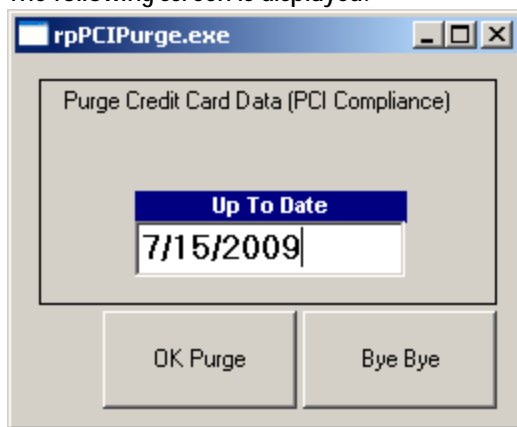
A typical merchant will not need credit card information beyond a week or two, and VRP recommends to purge sensitive card data as soon as it is no longer needed.

To purge card data use one of the 2 following methods:

1. Manual purge



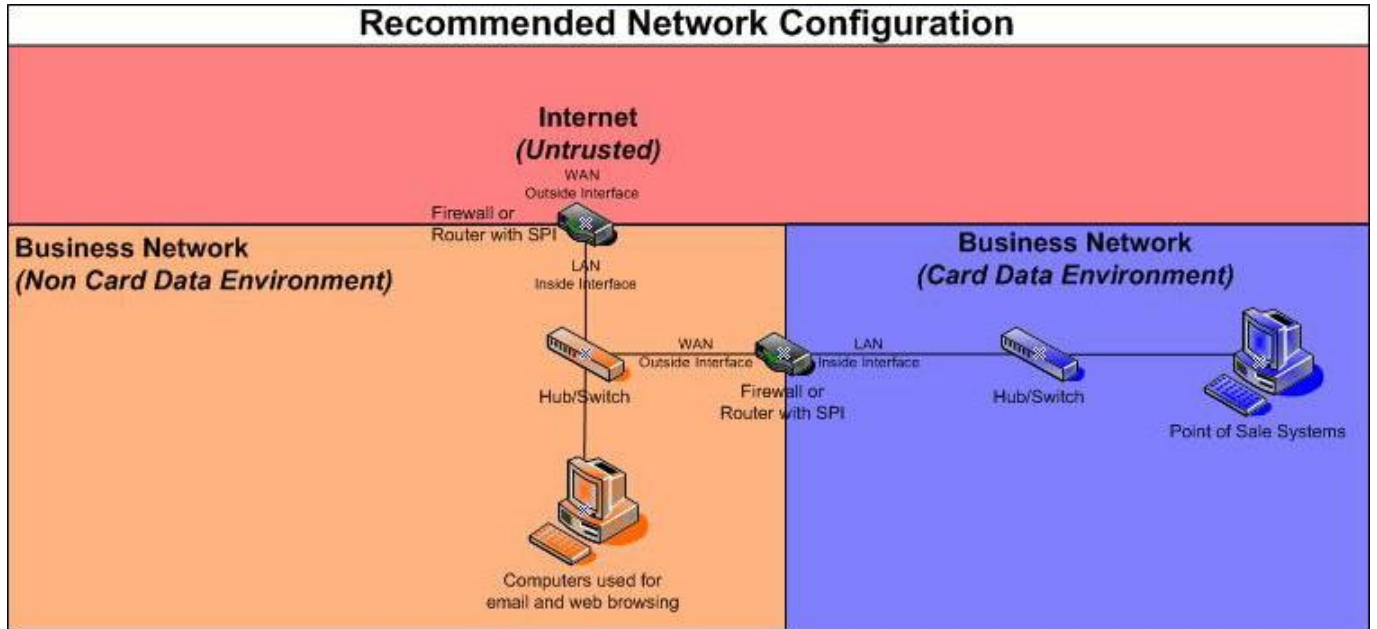
The following screen is displayed:



Enter a late as possible date and click OK Purge

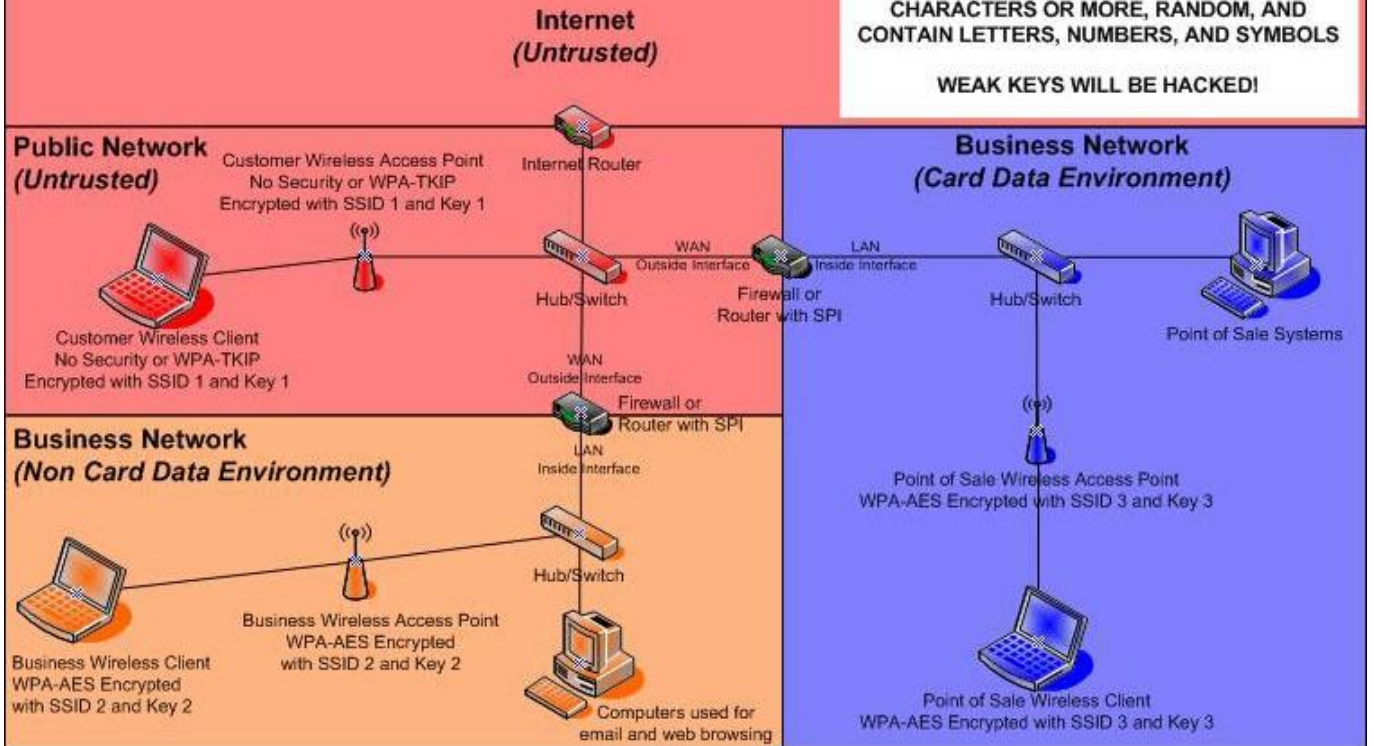
- Automatic purge of data – Consult VRP how to setup the scheduler to perform a daily purge of data older than a selected number of days old.

Appendix A: Recommended Network Configurations



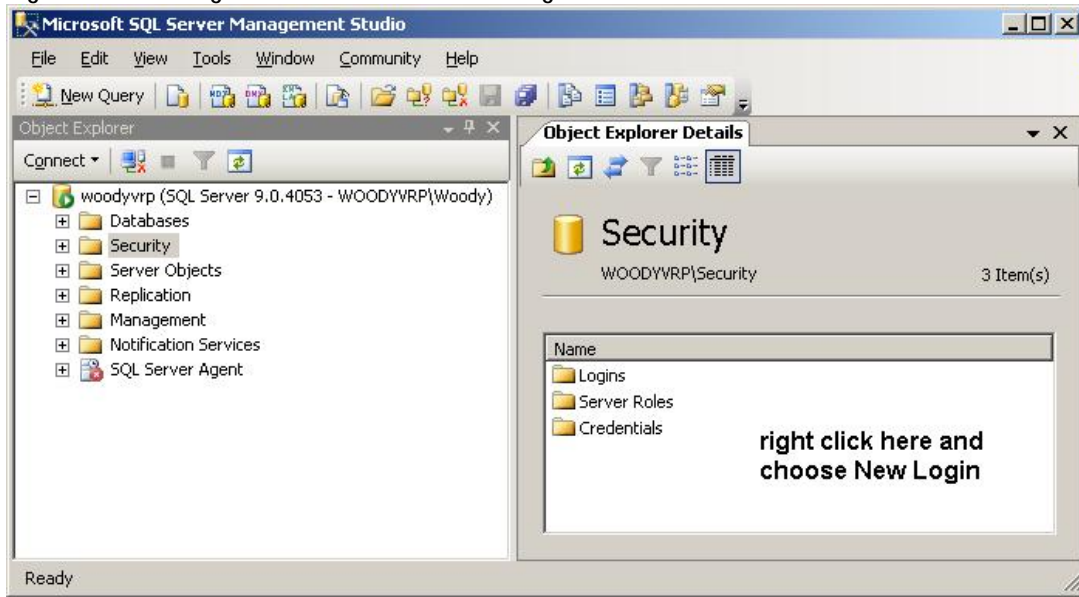
Recommended Network Configuration with Wireless Access (802.11, WiFi)

ALL ENCRYPTION KEYS SHOULD BE 13 CHARACTERS OR MORE, RANDOM, AND CONTAIN LETTERS, NUMBERS, AND SYMBOLS
WEAK KEYS WILL BE HACKED!

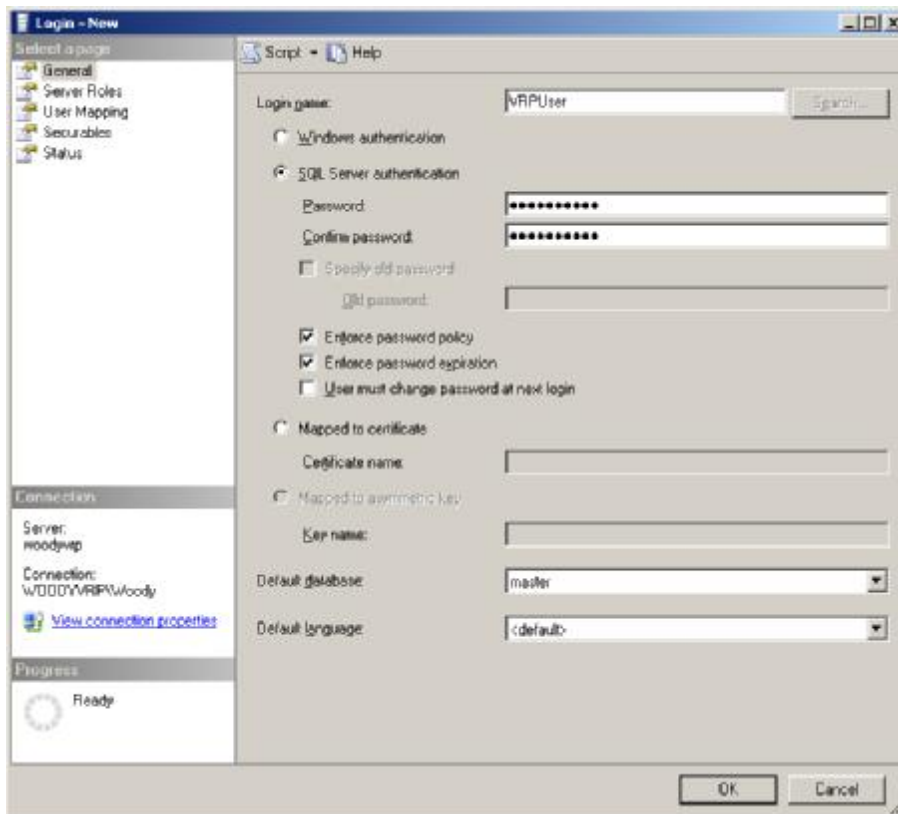


Appendix B

Open the Microsoft SQL Server Management Studio, login as sa and navigate to the security. Right click in the logins screen and chose "new Login"



Create a new login , choose SQL server authentication and provide a strong password Check the screen boxes as below

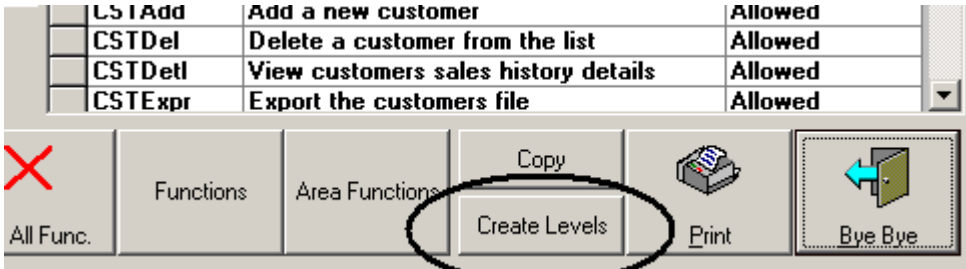


Appendix C Users Security Level

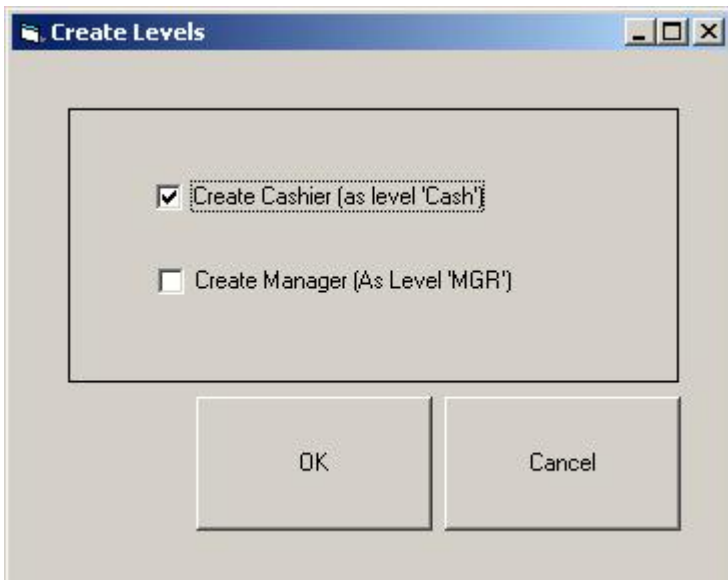
Login as admin, click on Back Office then Security



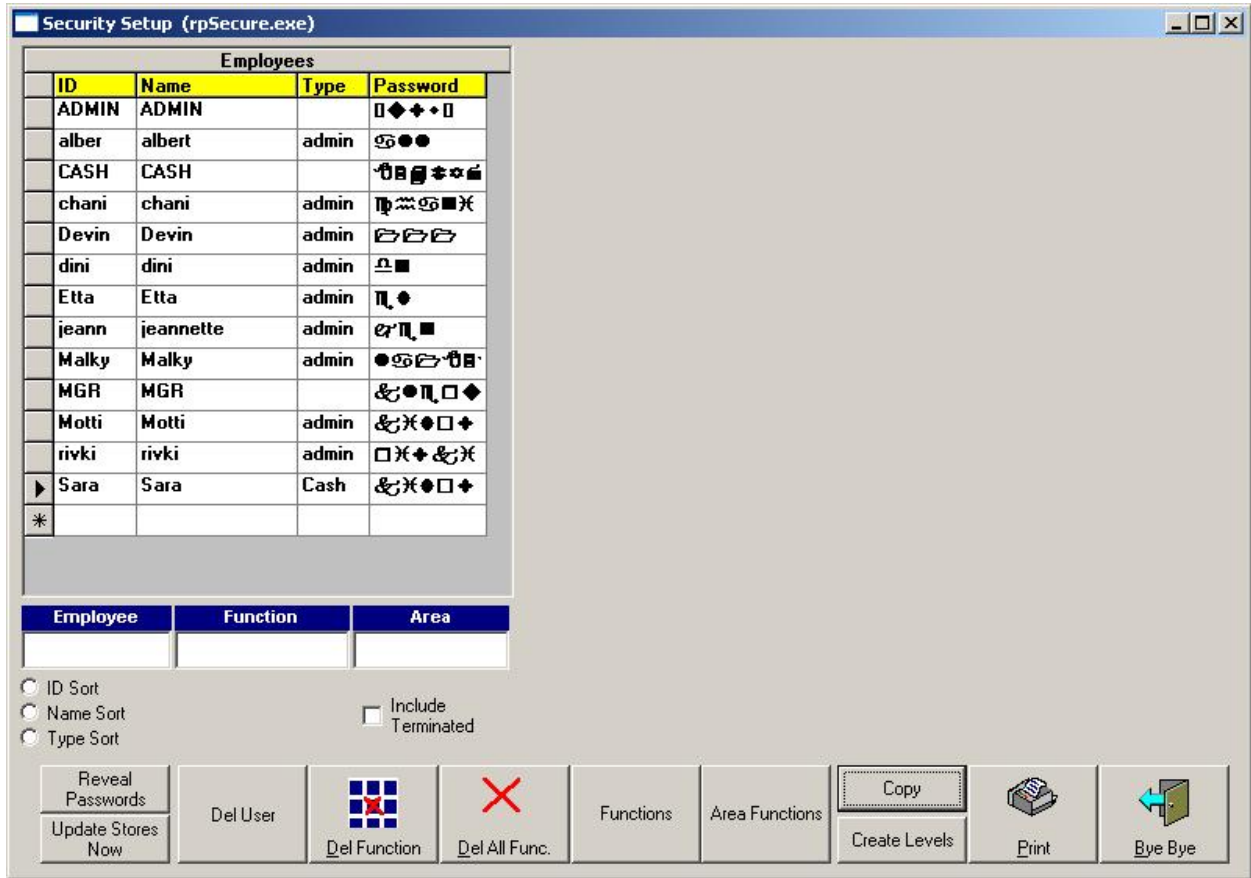
Click on "Create Levels"



Check the "Create Cashier checkbox and click OK



Select the user for which you want rights to be restricted and change it's "Type" to "Cash". In the example below Sara is a cashier with limited access to any function that reveals sensitive data.



View the full training video <http://www.posplus.com/tracy/security.wmv> regarding security on how to maintain more detailed security levels.