PA-DSS Implementation Guide:
Steps to ensure that your POS system is secure

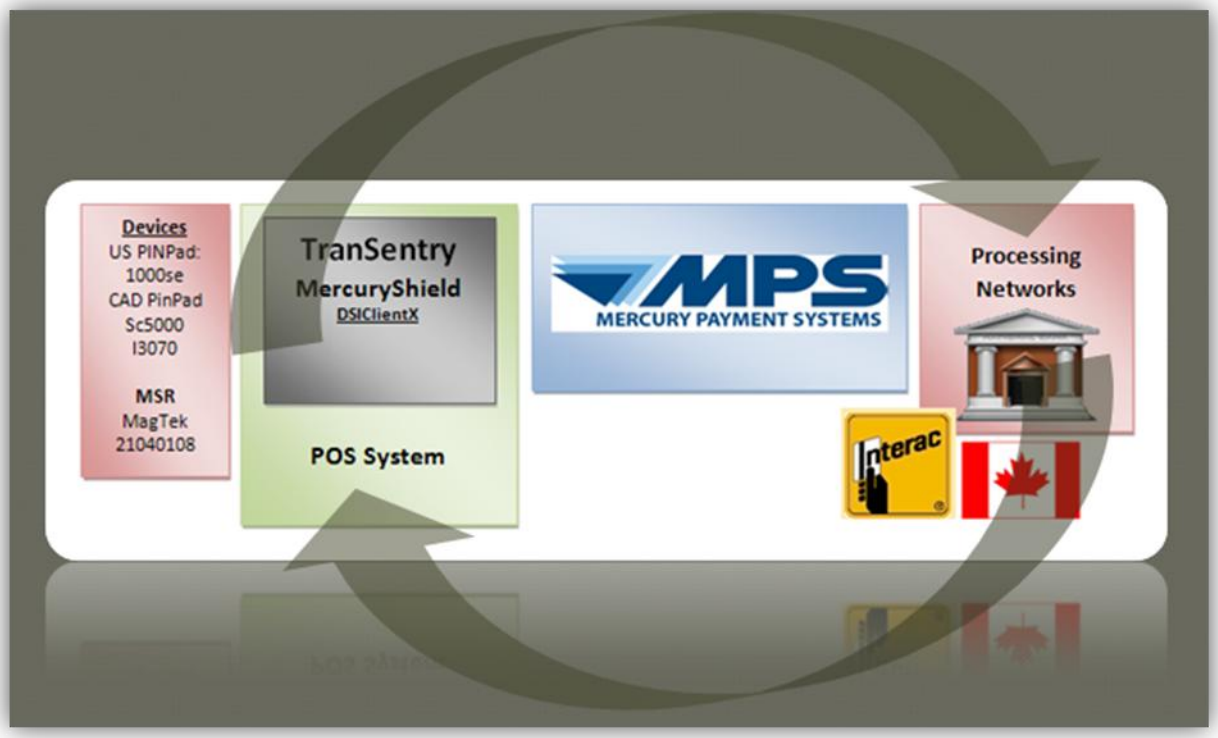
About the PCI Security Standards

The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including: the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and PIN-Entry Device (PED) Requirements. All of the five founding credit card brands have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs. Each founding member also recognizes the QSAs and ASVs certified by the PCI Security Standards Council as being qualified to validate compliance to the PCI DSS.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. All businesses handling credit and debit cards are required by the card brands to maintain PCI DSS compliance.

The PA-DSS is a security standard designed to help software vendors develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI Data Security Standard. All payment applications handling credit and debit cards are required by the card brands to maintain PA-DSS compliance.

For more information on the PCI standards, visit http://www.pcisecuritystandards.org



Implementation Guide

Welcome to TranSentry™ and Mercury Payment Systems Secure Payment Processing

TranSentry is a PA-DSS validated payment application that has been directly integrated into your Point of Sale system. This direct integration gives your system the PA-DSS compliance required by the card brands while maintaining the familiar end-user functionality of your POS. When used in your PCI DSS compliant business, TranSentry also gives you and your customers' peace of mind knowing card data is safe from theft.

TranSentry eliminates the need for your POS application to handle sensitive cardholder data. Once a transaction is ready to be tendered on your POS, TranSentry seamlessly takes over the transaction flow and initiates the swipe or manual entry of the card information using its own easy to use screen. TranSentry's powerful engine then handles the processing of the transaction directly to Mercury Payment Systems' secure network, passing back to your POS all the necessary non-sensitive transaction response information.

Implementing Your Point of Sale and TranSentry Securely

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

TranSentry will never store sensitive card data. There are no debugging or troubleshooting settings that permit sensitive data 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, the card data must be properly encrypted and protected as defined by the PCI Data Security Standard.

RocketPOS stopped storing cardholder data several years ago in previous versions if you are upgrading from an older version the update process will if any cardholder data is present automatically shrink and empty those fields. The cardholder data if present would be found in the c:/Nickel/CCHist.dbf on main POS station.

Encrypt Sensitive Traffic over Public Networks

TranSentry uses the Datacap DSIClientX to send transactions containing card data over the internet to our servers for payment processing. The DSIClientX is the client component of the Datacap NETePay solution, a PABP 1.3 validated product. The transmission is encrypted using SSL and an approved strong encryption protocol.

Attempting to send 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 send sensitive card data for a valid business reason, you must ensure you're sending it encrypted using secure encryption transmission technology (*e.g.* IPSEC, VPN, SSL/TLS).

Remote Access

TranSentry does not require the use of remote access or any other form of remote administration (*e.g.* Telnet).

If you use an alternate administration interface over the network (*e.g.* administrative web page, telnet) 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 vendors, resellers/integrators, or customers can access customers' payment 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 reseller/integrator personnel
- Establish customer passwords according to PCI DSS requirements 8.1, 8.2, 8.4, and 8.5

Mercury has evaluated several remote access solutions, comparing cost, convenience and security features that meet PCI compliance requirements for remote access. Mercury recommends the use of LogMeIn Central with free or professional client packages. LogMeIn accounts need to be configured for two-factor authentication.

For more information, visit LogMeIn at: http://www.LogMeIn.com

Wireless Networks

TranSentry does not require the use of a wireless network and Mercury 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 payment processing systems, make sure that a firewall prevents access to the payment processing systems.

- Wireless networks attached to your payment processing network MUST meet the following PCI DSS requirements:
  - As of April 1, 2009, all newly deployed wireless networks must be using WPA or WPA2 encryption.
  - Existing wireless setups must use WPA or WPA2 encryption when it's an available option. Some older wireless equipment lack WPA support, but almost all can be updated through firmware and driver updates made available on the manufacturer's web-site.
  - 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 so 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 POS 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 POS 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

RocketPOS when first installed uses a default administrator account with the username: *TEMP* and a default password: *Temp123* When a user first logs in she/he is prompted to change the default administrator password. Users are advised to change all default user IDs and passwords since they're easily guessed and usually documented in product manuals (*e.g.* User: Admin Password: password).

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.

It is highly recommended to disable or delete inactive or terminated user accounts immediately to prevent access. Although immediate action is recommended, for PCI compliance, this absolutely must be done within 90 days.

These requirements are for PA-DSS compliance and automatically maintained by **RocketPOS**. They apply only to user accounts with administrative level access.

- Passwords must be at least seven characters
- Passwords must contain at least one upper case and one lower case letter
- Passwords must be changed at least every 90 days
- Passwords must not be the same as the last four 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
- After a user idle time of 15 minutes, the password must be re-entered

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

Logging

TranSentry logging is enabled upon startup and cannot be disabled. It logs the following information for every credit or debit transaction.

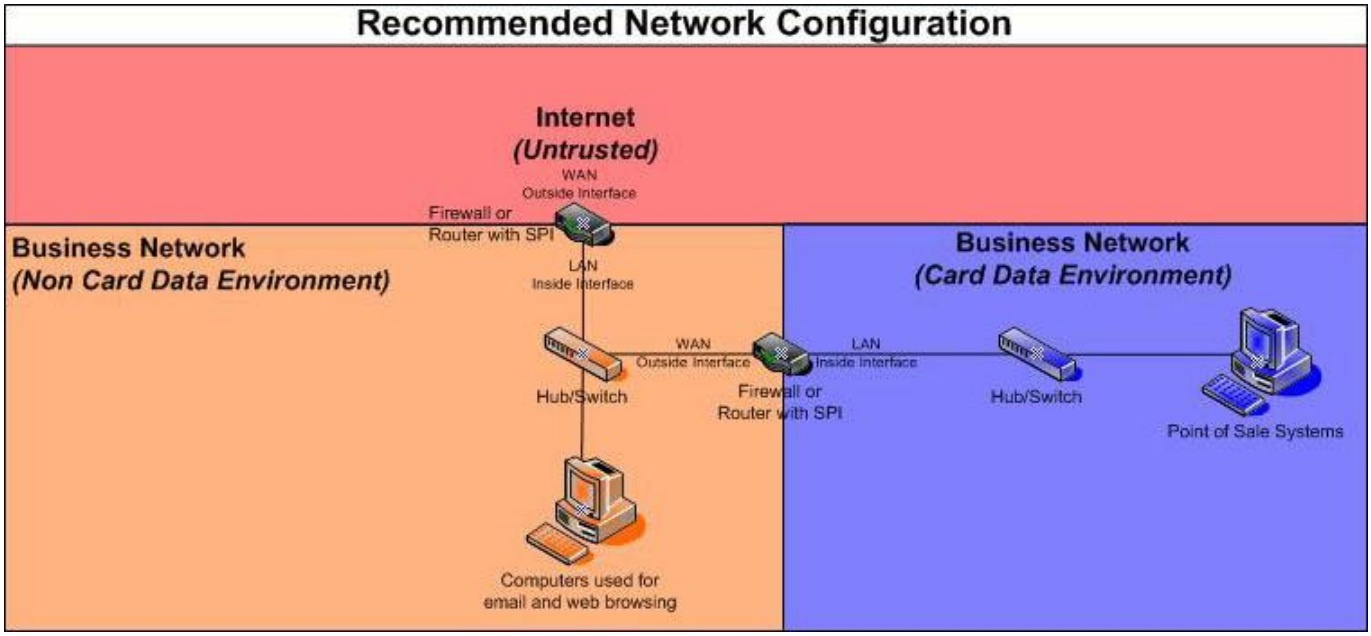
- Date and time
- Type of transaction
- Success or failure indication
- Username
- Origination of event

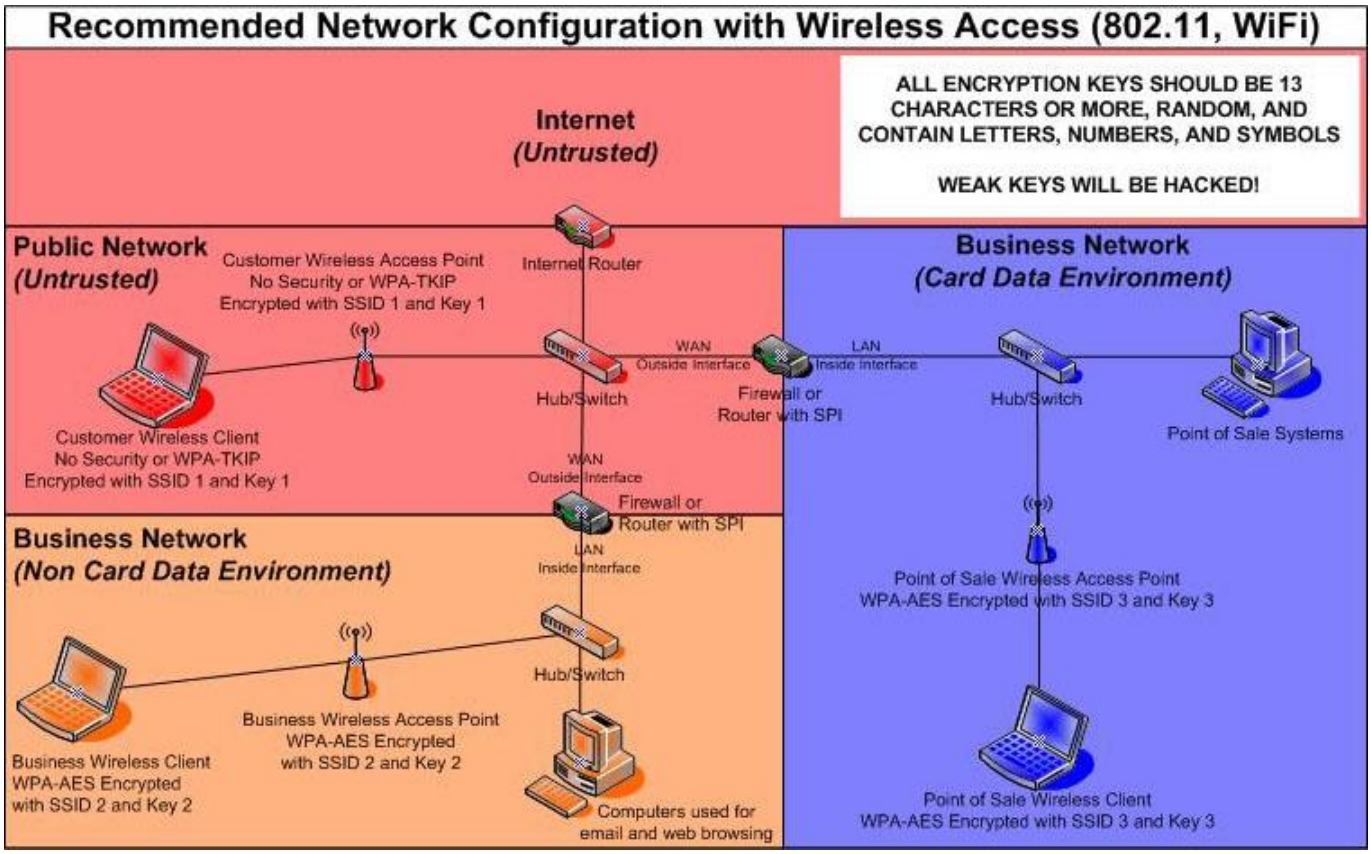
The location of the TranSentry logging directory is configured in MPS.POS.UTILS.DLL.config and defaults to: "C:\Log\TranSentry\". Log files are created using the following naming convention: TranSentryLogYYYYMMDD.log

RocketPOS logging is enabled upon startup and cannot be disabled. It logs the same information shown above for administrative level access and every credit or debit transaction. The location of the *RocketPOS* logging directory is *C:\Nickel*.

For PA-DSS compliance, log files must have access controls applied so that only authorized users can modify them. Additionally, the Windows Security Event Log will need to be configured to log access to the TranSentry and *RocketPOS* log files. To enable these settings, follow the steps provided in Appendix B, Log file Security Settings. Not applying these settings or disabling them can result in non PCI DSS compliance.

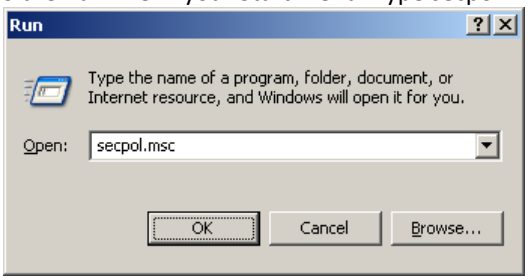
Appendix A:
Recommended Network Configurations



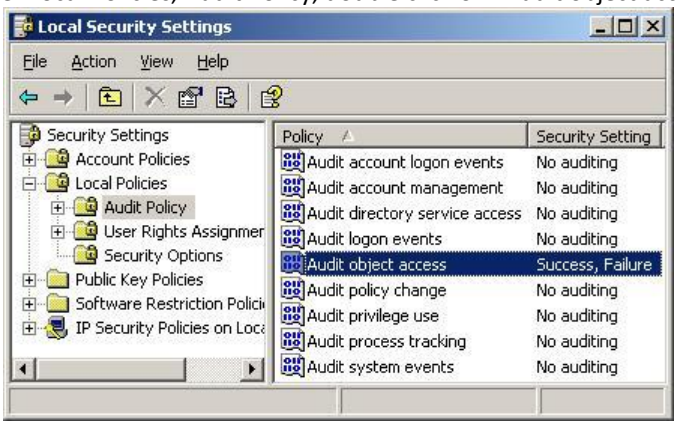


Appendix B:
Log file Security Settings

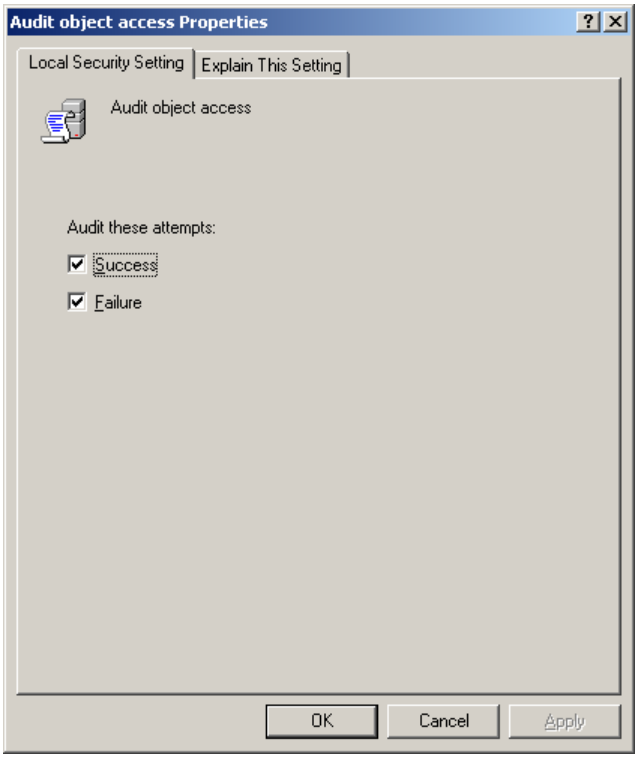
1) Go to the Run line in your Start menu. Type secpol.msc and hit the OK button.



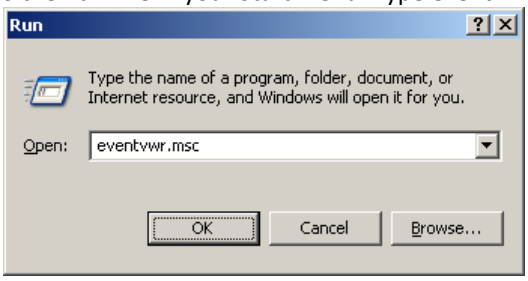
2) Under Local Policies, Audit Policy, double click on “Audit object access”.



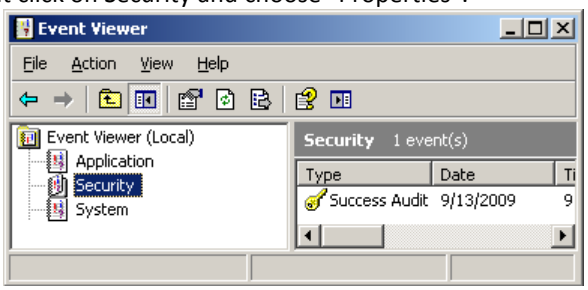
3) Enable success and failure then hit OK. Close out of the Local Security Settings window.



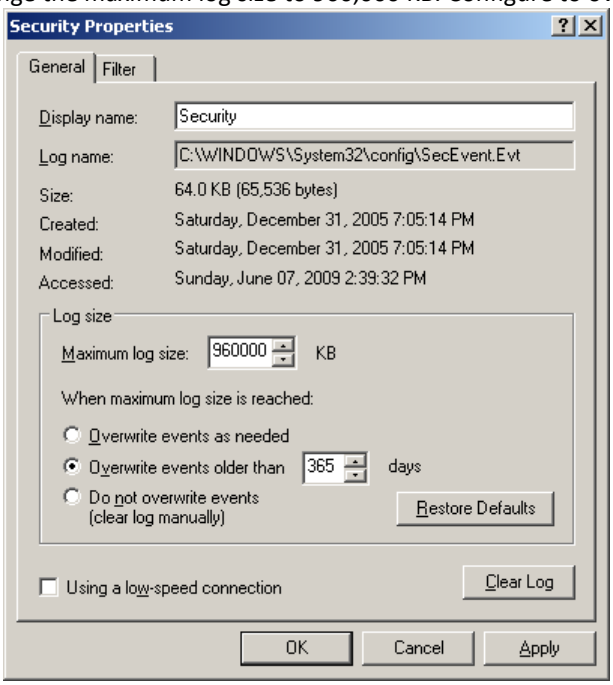
4) Go to the Run line in your Start menu. Type eventvwr.msc and hit the OK button.



5) Right click on Security and choose “Properties”.

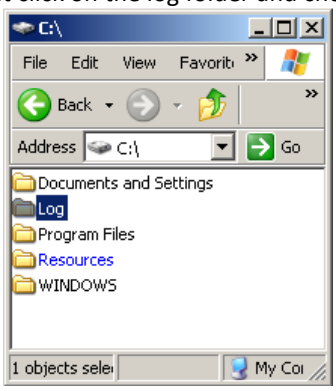


6) Change the maximum log size to 960,000 KB. Configure to overwrite events older than 365 days. Hit OK.

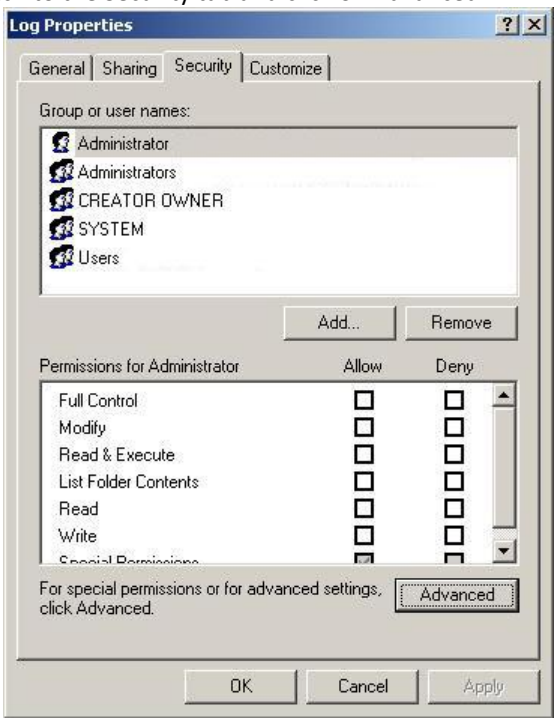


7) Navigate to the parent folder of the log file location. The default log file location is “C:\Log”, so you would navigate to “C:\”.

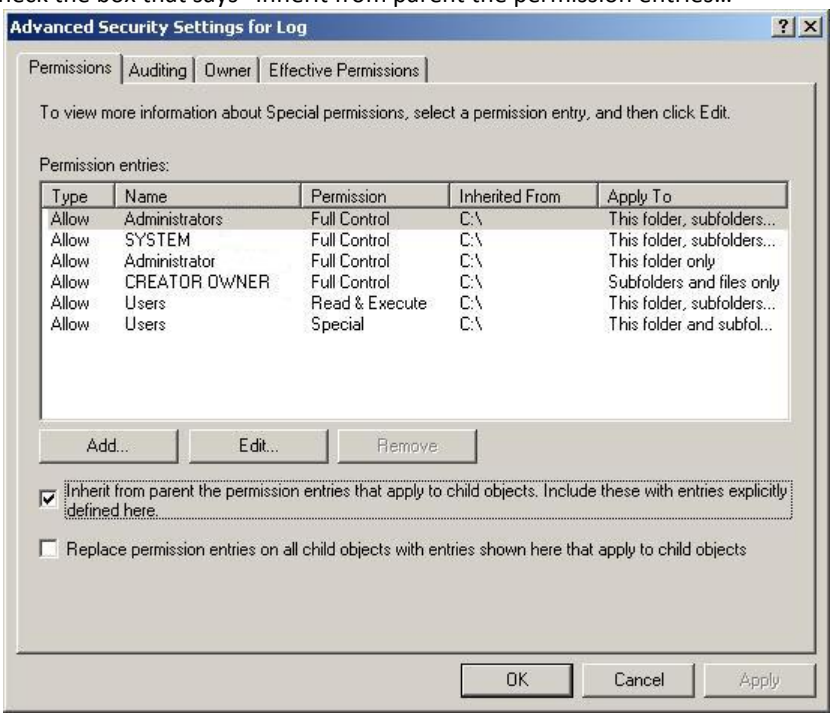
8) Right click on the log folder and choose Properties.



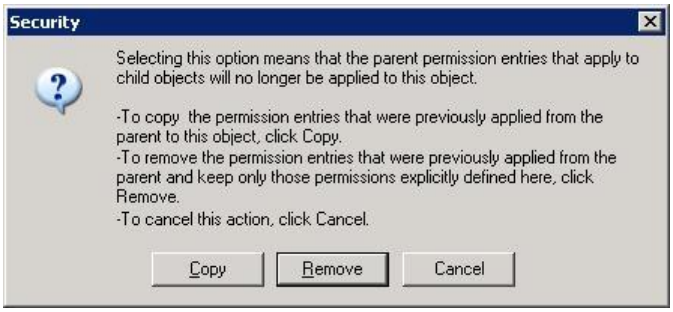
9) Switch to the Security tab and click on Advanced.



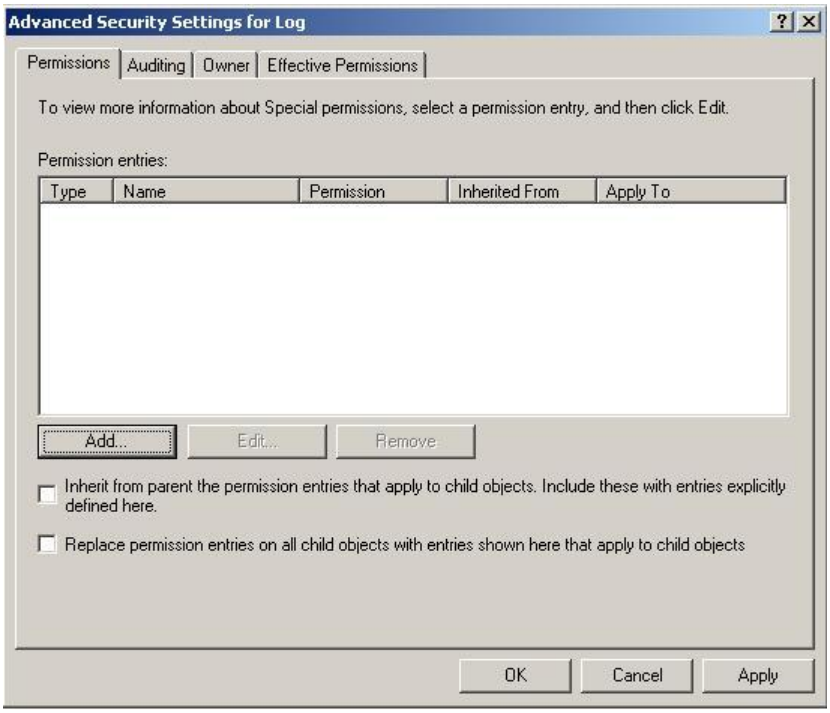
10) Uncheck the box that says "Inherit from parent the permission entries…"



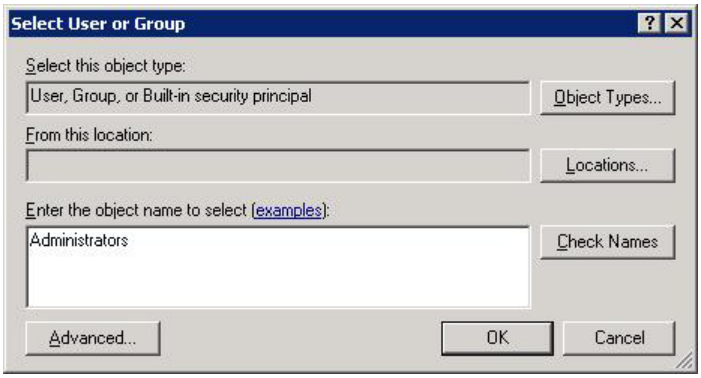
11) Click the Remove button.



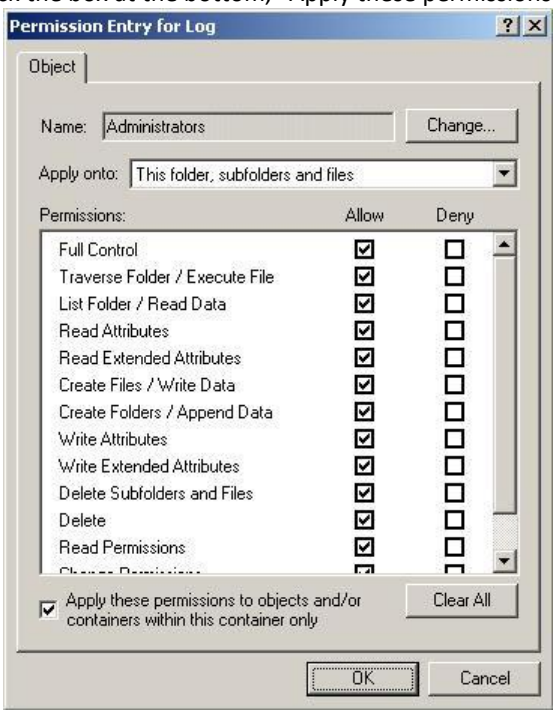
12) Click the Add button.



13) Type “Administrators” and hit the OK button.

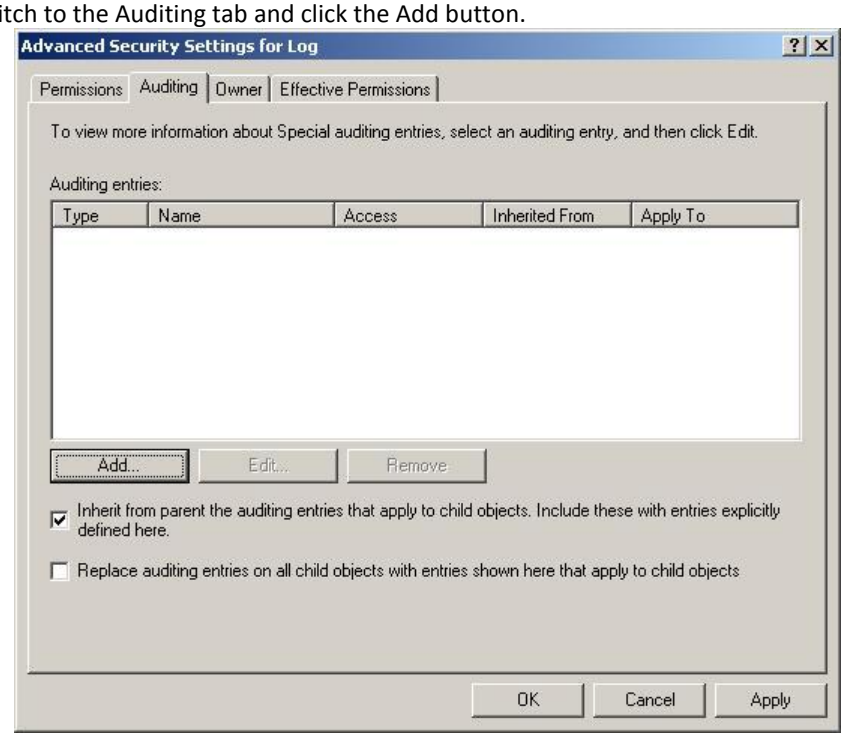


14) Check the box to Allow Full Control. All the boxes below will automatically be selected.
15) Check the box at the bottom, "Apply these permissions to objects…" and hit the OK button.

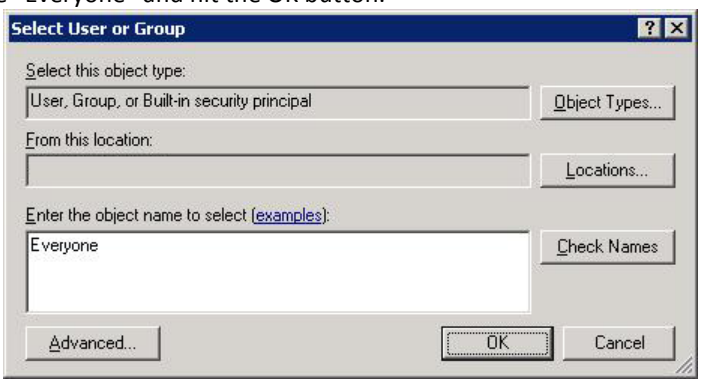


16) Repeat steps 12-15 for any additional accounts that need access. If you run *RocketPOS* under non-administrative Windows user accounts, they'll need to be added as well.

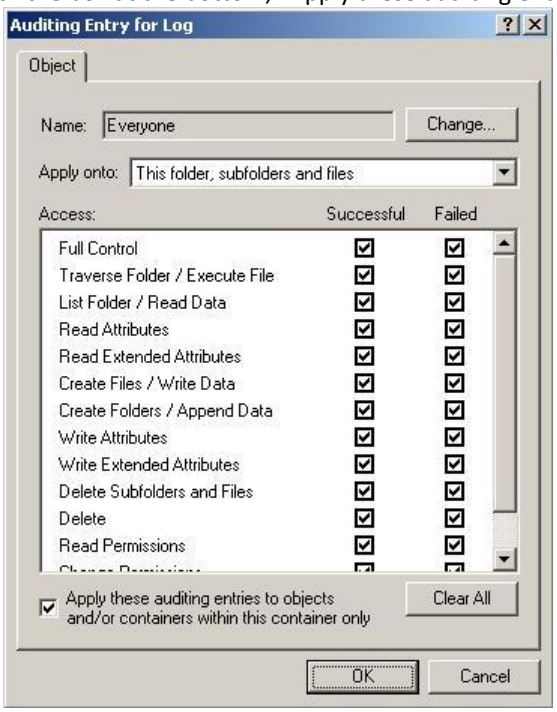
17) Switch to the Auditing tab and click the Add button.



18) Type “Everyone” and hit the OK button.



19) Check the Full Control Successful and Failed boxes. All the boxes below will automatically be selected.
20) Check the box at the bottom, “Apply these auditing entries to objects…” and hit the OK button.



21) Hit OK on the remaining dialogue boxes to close them all.
22) Close any windows left open from this procedure.