INTERNATIONAL
POINT OF SALE

CornerStorePOS

PA DSS Implementation Guide

Version 1.0 – January 9, 2010

1. Introduction

a. What is PA-DSS

i. The (PA-DSS) Payment Application Data Security Standard (PA-DSS) is a set of security standards created by the PCI SSC to guide payment application vendors to implement secure applications.

ii. The Purpose of this PA-DSS Implementation guide is to instruct merchants, resellers and integrators on how to implement CornerStorePOS and any other software provided by International Point of Sale (Hereby known as "CORNERSTOREPOS") into their store, network or system; in a PA-DSS compliant manner. This guide is not for use as a CornerStorePOS installation guide.

b. CornerStorePOS and PA-DSS Implementation

i. CORNERSTOREPOS provides the information about its software and how it follows the rules and guidelines of the PA-DSS to be PCI Compliant.

2. Do not retain full magnetic stripe, card validation code, or value.

a. CornerStorePOS and card data

i. CORNERSTOREPOS does not store any cardholder data whatsoever. The only data that is read is immediately encrypted, sent to the processor, then discarded. Reading the accountholder's name, Primary Account Number (displaying the last 4 digits on a receipt), expiration Date, and Service Code. Any attempt to reprint the receipt would result in the information not being shown. [PA-DSS Requirement 1.1.1, 1.1.2]

ii. CORNERSTOREPOS does not save any user's Personal Identification Number (PIN) or the encrypted PIN block. Any PIN is immediately encrypted, sent, then discarded. [PA-DSS Requirement 1.1.3]

iii. Because CORNERSTORE does not and has not saved cardholder data, when CORNERSTOREPOS is installed onto a user's computer, it does not need to delete any previous cardholder data. [PA-DSS Requirement 1.1.4]

iv. CORNERSTOREPOS does not save any test cardholder data used for debugging and testing purposes. When a user first installs CORNERSTOREPOS however, a default test merchant ID is provided. [PA-DSS Requirement 1.1.5]

3. Protect Stored cardholder data

a. CORNERSTOREPOS and stored cardholder data

i. CORNERSTOREPOS does not save any user information; therefore one does not need to purge any information stored. [PA-DSS Requirement 2.1, 2.3]

4. Provide secure authentication features

a. CORNERSTOREPOS and security

i. CORNERSTOREPOS provides the user with an administrative account already created. The default username is "admin" and the default password is "admin123". It is highly advised of the user to give a more unique password to

their software. In addition, it is also advised to give all users their own unique username and password using employee maintenance (as explained in the CornerStorePOS Getting Started Manual). Employees are either forbidden or allowed access of administrative settings, based on the administrator's choice and employee position. [PA-DSS Requirement 3.1]

1. A user who logs in for the first time is urged to change the admin password.
2. A user who installs CornerStorePOS has to implement the following
    a. Set system Idle time to 15 min and password protection as shown below
        i. Right Click Anywhere in the window and click properties
        ii. Go to Screen Saver Tab and choose Wait time 15 min, and check on resume, password protect
        iii. Click Apply and then OK

ii. In addition to [PA-DSS Requirement 3.1] It is the user's decision, however recommended to implement user account settings in Windows. The following are recommended settings to use for users.

iii. CORNERSTOREPOS provides a default user account for the software. CORNERSTOREPOS also provides a username for the database, defaulted at username "sa" and password "Intlp0s". It is recommended that the user creates a username and password for the windows system for additional security. [PA-DSS Requirement 3.2]

iv. CORNERSTOREPOS encrypts all passwords using an algorithm recommended by the PA-DSS. [PA-DSS Requirement 3.3]

5. Log payment application safety

a. CORNERSTOREPOS and log activity

i. CORNERSTOREPOS keeps an event log of all accounts in CornerStorePOS. Whenever an account logs in, logs out, makes a sale, changes an item, is created/deleted, or any other setting change in CornerStorePOS; it creates a log for it. [PA-DSS Requirement 4.1, 4.2] (**To see how to view the log data, see Section: 12**)

6. Develop secure payment applications

a. CORNERSTOREPOS and secure payment applications

i. CORNERSTOREPOS does not process any credit card information. It is encrypted and processed through Mercury's TranSentry program. The TranSentry program encrypts and send it to the payment processing Server. TranSentry uses all current standards following the PCI Compliance. [PA-DSS Requirement 5.X, 7.X 9.X, 12.X, 13.X]

7. Protect wireless transmissions

a. CORNERSTOREPOS and wireless networks

i. TranSentry is able to use networks with encrypted transmissions (such as WPA, WPA2, SSL/TLS, IPSEC VPN, OR WEP)
    1. If WEP is used, it is highly suggested to do the following to create a safe protected network [PA-DSS Requirement 6.1, 6.2]
        a. Use with a minimum 104-bit encryption key and 24 bit-initialization value
        b. Use ONLY in conjunction with secure encrypted transmission technology (Such as IPSEC, VPN, or SSL/TLS)
        c. Rotate shared WEP keys quarterly (or automatically)
        d. Rotate shared WEP keys whenever there are changes in personnel with access to keys
        e. Restruct access based on media access code (MAC) address.

8. Facilitate secure network implementation

a. CornerStorePOS and Networks.

i. CORNERSTOREPOS can exist in a secure network; however Mercury heavily suggests that you use a wired network for security purposes. **(If you would like to set up the network in accordance to Mercury and PCI Standards, follow the section below Section: 13)** [PA-DSS Requirement 8.1]

9. Facilitate secure remote software updates

a. CornerStorePOS and updating

i. CORNERSTOREPOS does not have any method for allowing an automatic or a remote update. It does not have any method of checking for updates. CORNERSTOREPOS does send information using Twitter to alert customers that there is an update in Versions 2.0.9 and later. In order to upgrade CornerStorePOS, a user must willingly download CornerStorePOS or the user allow a technician to log onto the user's computer and download the patch or new file to install. The CornerStorePOS file will be replaced but the Database will remain intact. It is suggested practice to take a backup of your database before an installation in the event of accidental deletion or failure. [PA-DSS Requirement 10.1]

10. Facilitate secure remote access to payment application

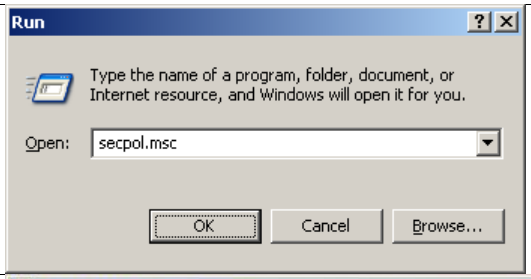
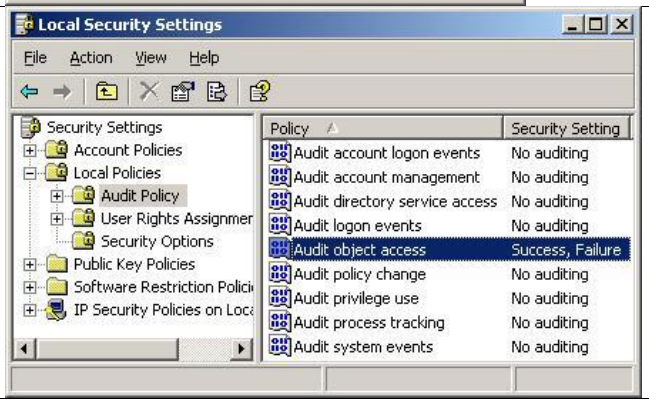
a. CornerStorePOS and Secure Remote Access

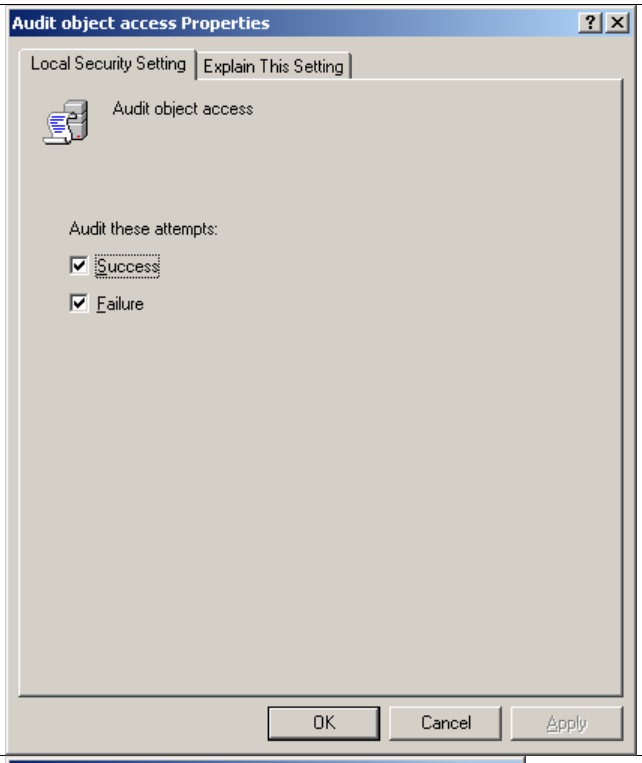
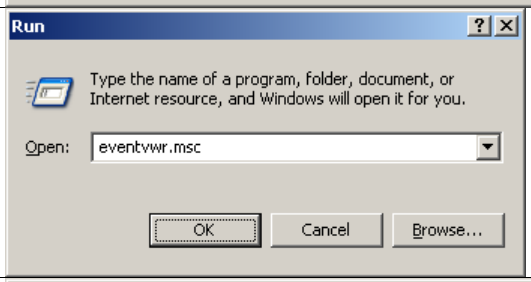
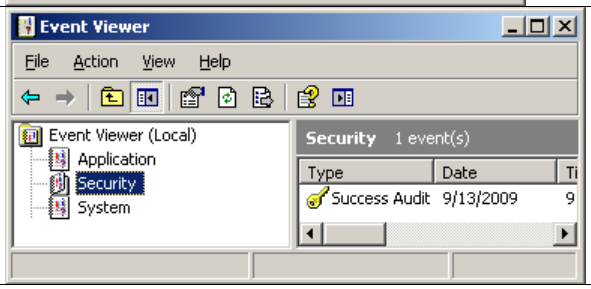
i. CORNERSTOREPOS does not have any method of remote access. CORNERSTOREPOS uses an external program that can be called through the CornerStorePOS software. ShowMyPC is the software of choice, as it is the most secure. A person ("client") cannot access the PC for longer than 1 hour a session and must have a code and consent from the owner of the software ("host"). The host allows access to a client by providing that client a "ShowMyPC password" generated by the host. [PA-DSS Requirement 11.1, 11.2, 11.3]

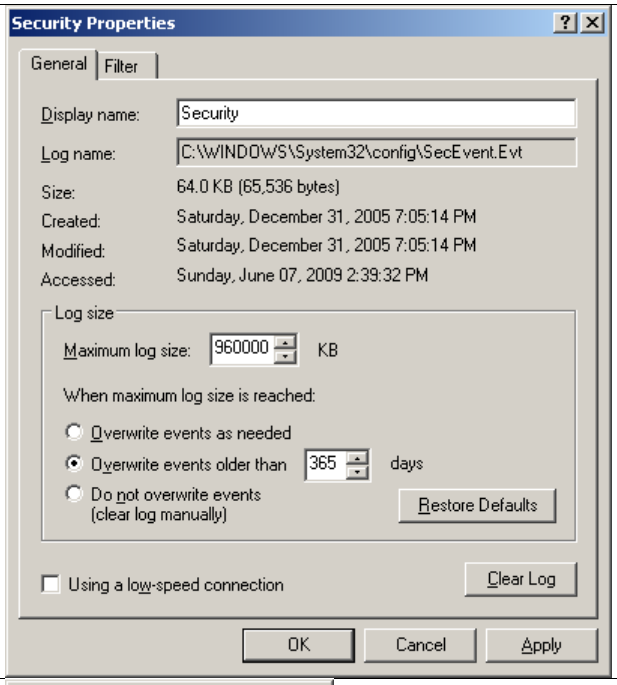
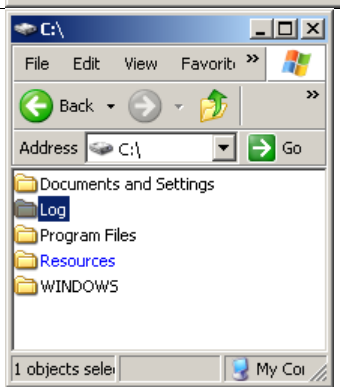
11. Maintain instructional documentation and training programs for users.

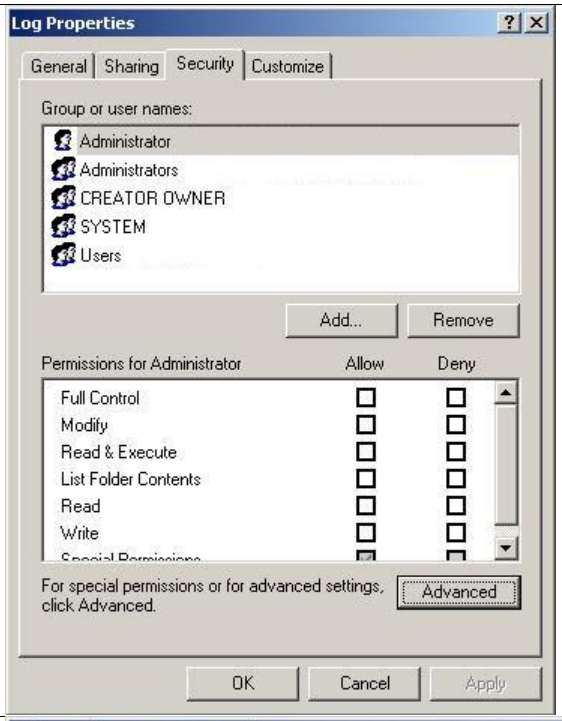
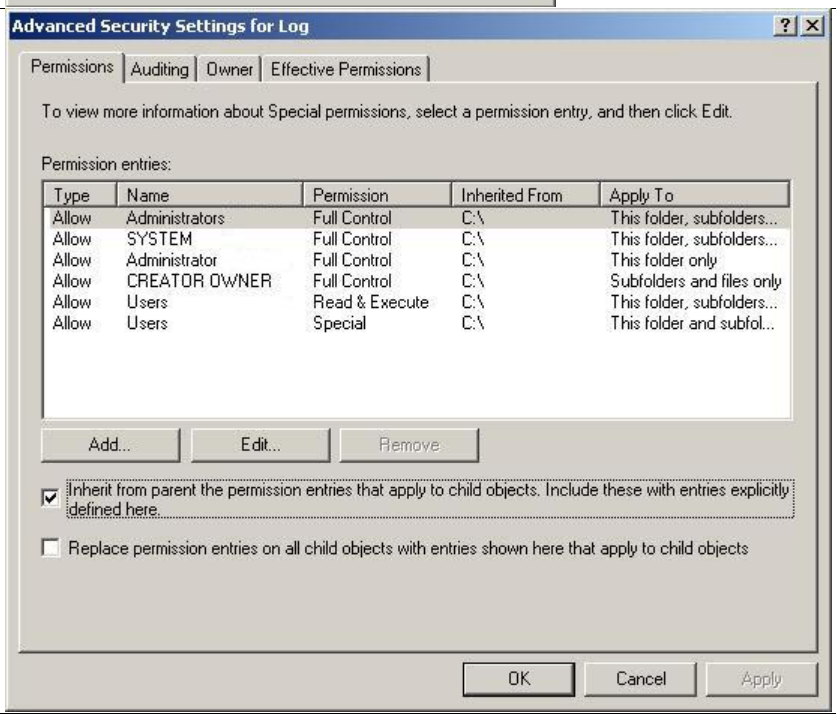
i. CORNERSTOREPOS has created this user guide for users and resellers to understand the requirements for the PA-DSS and how CornerStorePOS meets those requirements. [PA-DSS Requirement 14.1]

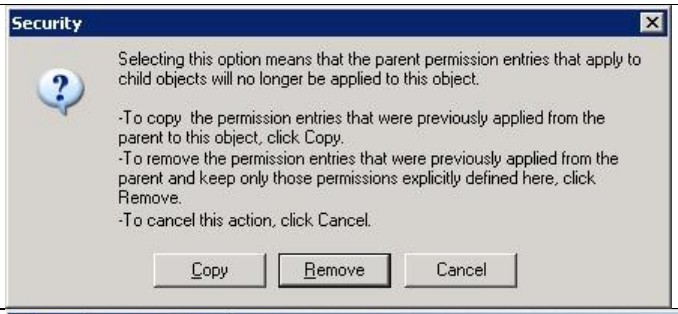
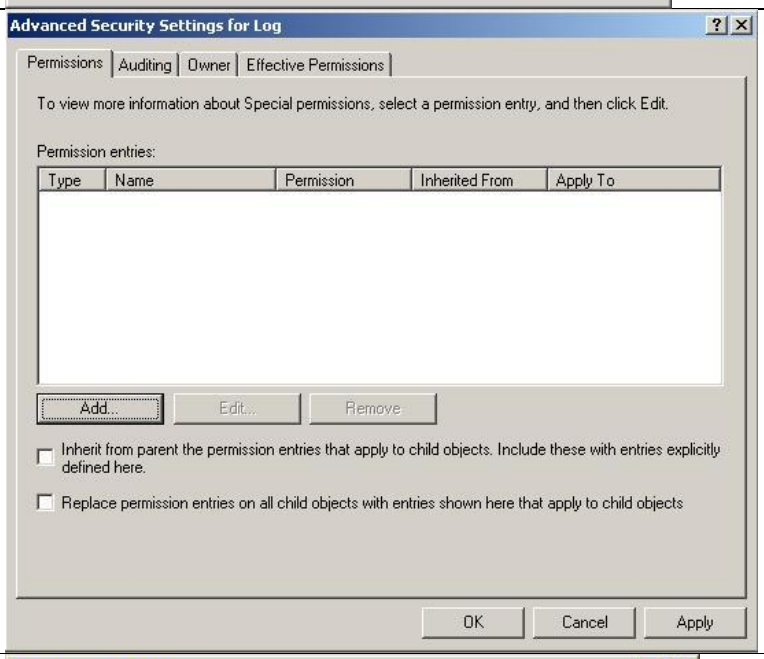
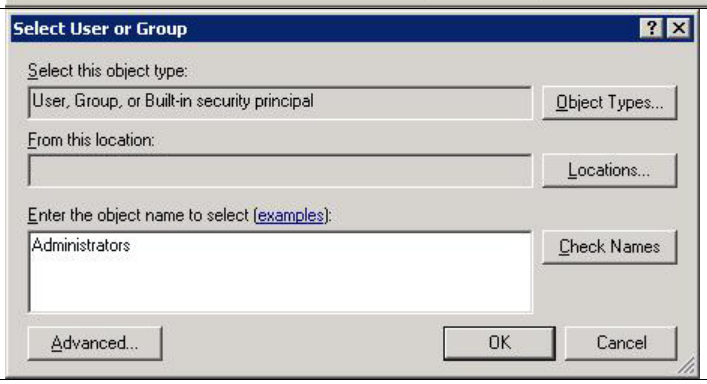
12. Log File Security Settings

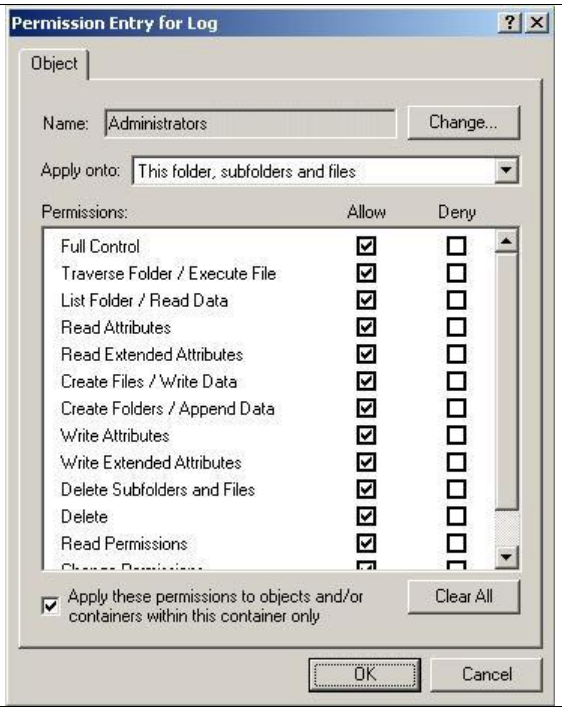
Go to the Run line in your Start menu. Type secpol.msc and hit the OK button.	
Under Local Policies, Audit Policy, double click on "Audit object access".	

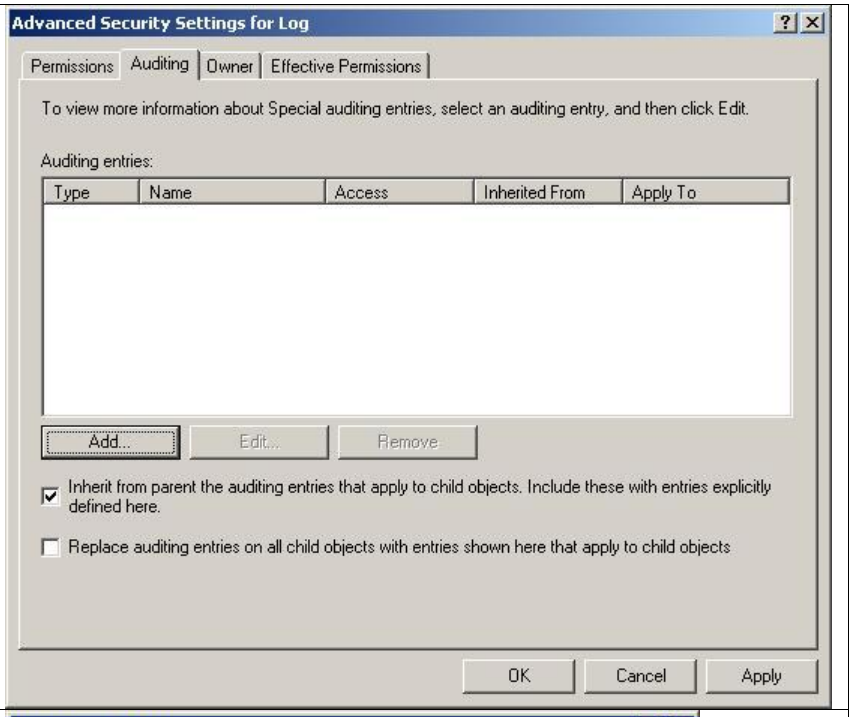
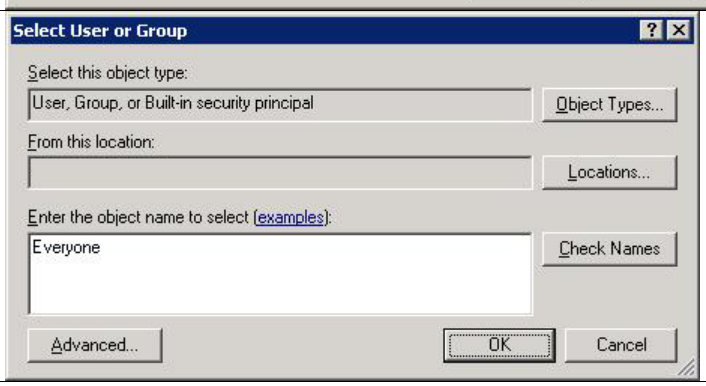
Enable success and failure then hit OK. Close out of the Local Security Settings window	
Go to the Run line in your Start menu. Type eventvwr.msc and hit the OK button.	
Right click on Security and choose “Properties”.	

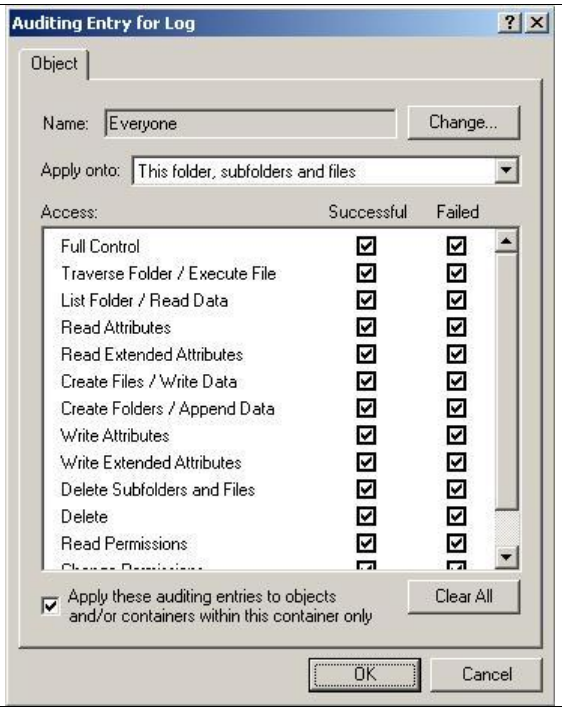
Change the maximum log size to 960,000 KB. Configure to overwrite events older than 365 days. Hit OK.	
Navigate to the parent folder of the log file location. The default log file location is "C:\Log", so you would navigate to "C:\" Right click on the log folder and choose Properties.	

Switch to the Security tab and click on Advanced	
Uncheck the box that says “Inherit from parent the permission entries…”	

Click the Remove button.	
Click the Add button	
Type “Administrators” and hit the OK button	

Check the box to Allow Full Control. All the boxes below will automatically be selected Check the box at the bottom, "Apply these permissions to objects…" and hit the OK button.	
Repeat steps 12-15 for any additional accounts that need access. If you run ***CornerStorePOS*** under non-administrative Windows user accounts, they'll need to be added as well.	

Switch to the Auditing tab and click the Add button	
Type “Everyone” and hit the OK button	

Check the Full Control Successful and Failed boxes. All the boxes below will automatically be selected Check the box at the bottom, "Apply these auditing entries to objects…" and hit the OK button	
Hit OK on the remaining dialogue boxes to close them all. Close any windows left open from this procedure	

13. Steps to Ensure that your POS system is secure

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.
- Perimeter firewalls must deny or control all traffic from the wireless environment into the cardholder data environment.
- Wireless networks attached to your payment processing network MUST meet the following PCI DSS requirements:

1. As of April 1, 2009, all newly deployed wireless networks must be using WPA2 encryption. **Note: The use of WEP as a security control was prohibited as of 30 June 2010.**
2. Existing wireless setups must use WPA2 encryption
3. The default WPA2 encryption key must be changed to a unique strong key.
4. The default password for accessing the Wireless Access Point's settings must be changed to a unique strong password.
5. Change default SNMP (Smart Network Management Protocol) community strings on Wireless Access Points if SNMP is supported or disable SNMP altogether.
6. Synchronize the access points' clocks to be the same as your computers to ensure logged timestamps match.
7. Update firmware to support strong encryption for authentication and data transmission.

- If you have a wireless network attached to your payment processing network, the following steps must be satisfied to enable additional security:
    1. 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.
    2. Disable SSID Broadcast to make your wireless network less visible to unauthorized users.
    3. Use MAC address filtering so that only authorized computers are allowed access to the wireless network.
    4. When configuring WPA2, use the AES option. Only use TKIP when AES is not an available option. Although not severe, there are known weaknesses in TKIP.

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.

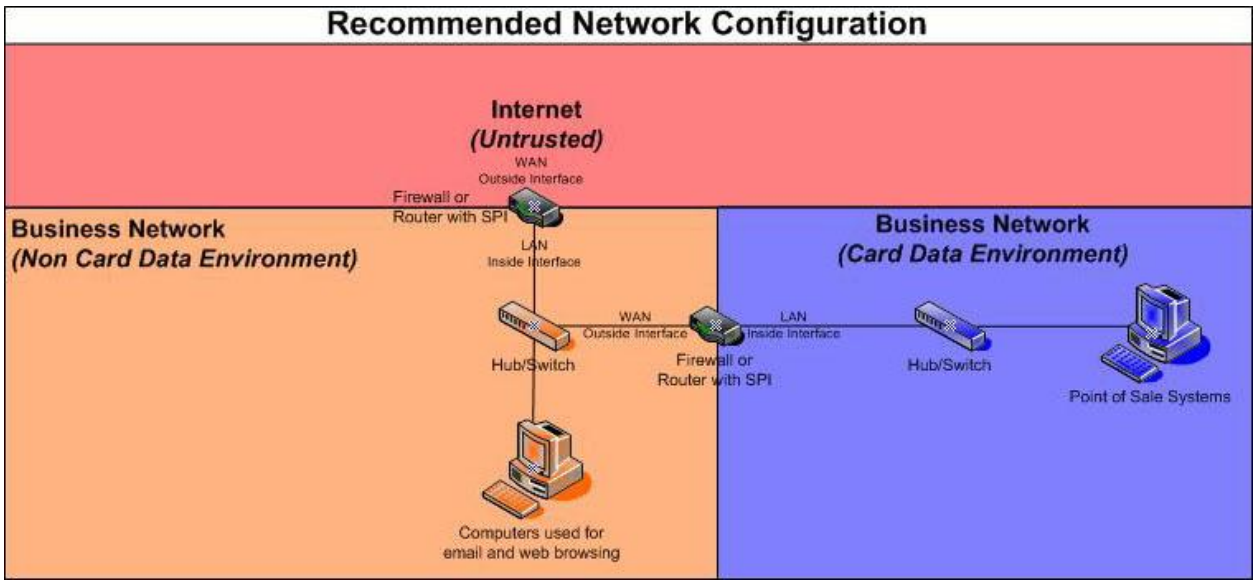
Untrusted Environment – Network connections that anonymous people have access to are considered "untrusted." They should have no network access to your business computers and POS equipment. Business computers should never be connected directly to this zone. Common untrusted networks are the internet 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.

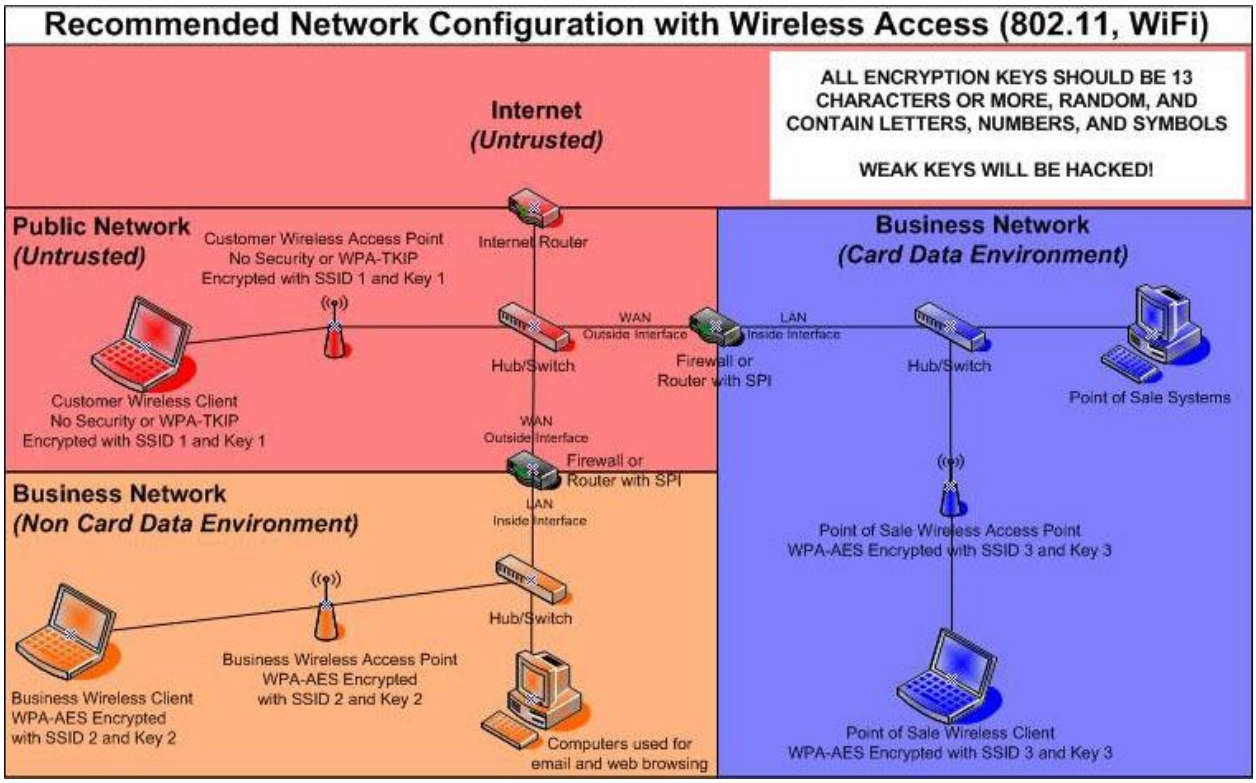
Non Card Data Business Environment – Systems not used for payment processing, but are still business owned fit into this segment. These are systems that can be used for email, web browsing, and other higher risk activity that you would never want to perform on your payment processing systems. On occasion, 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:

- Protect both business environments from the untrusted environment
- Protect your card data business environment from the non card business environment


Recommended Network Configuration
Internet
(Untrusted)
WAN
Outside Interface
Firewall or
Router with SPI
LAN
Inside Interface
Business Network
(Non Card Data Environment)
Business Network
(Card Data Environment)
WAN
Outside Interface
LAN
Inside Interface
Hub/Switch
Firewall or
Router with SPI
Hub/Switch
Point of Sale Systems
Computers used for
email and web browsing


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!
Internet
(Untrusted)
Public Network
(Untrusted)
Customer Wireless Access Point
No Security or WPA-TKIP
Encrypted with SSID 1 and Key 1
Internet Router
Business Network
(Card Data Environment)
WAN
Outside Interface
LAN
Inside Interface
Hub/Switch
Firewall or
Router with SPI
Hub/Switch
Point of Sale Systems
Customer Wireless Client
No Security or WPA-TKIP
Encrypted with SSID 1 and Key 1
WAN
Outside Interface
Firewall or
Router with SPI
Business Network
(Non Card Data Environment)
LAN
Inside Interface
Point of Sale Wireless Access Point
WPA-AES Encrypted with SSID 3 and Key 3
Hub/Switch
Business Wireless Access Point
WPA-AES Encrypted
with SSID 2 and Key 2
Business Wireless Client
WPA-AES Encrypted
with SSID 2 and Key 2
Computers used for
email and web browsing
Point of Sale Wireless Client
WPA-AES Encrypted with SSID 3 and Key 3