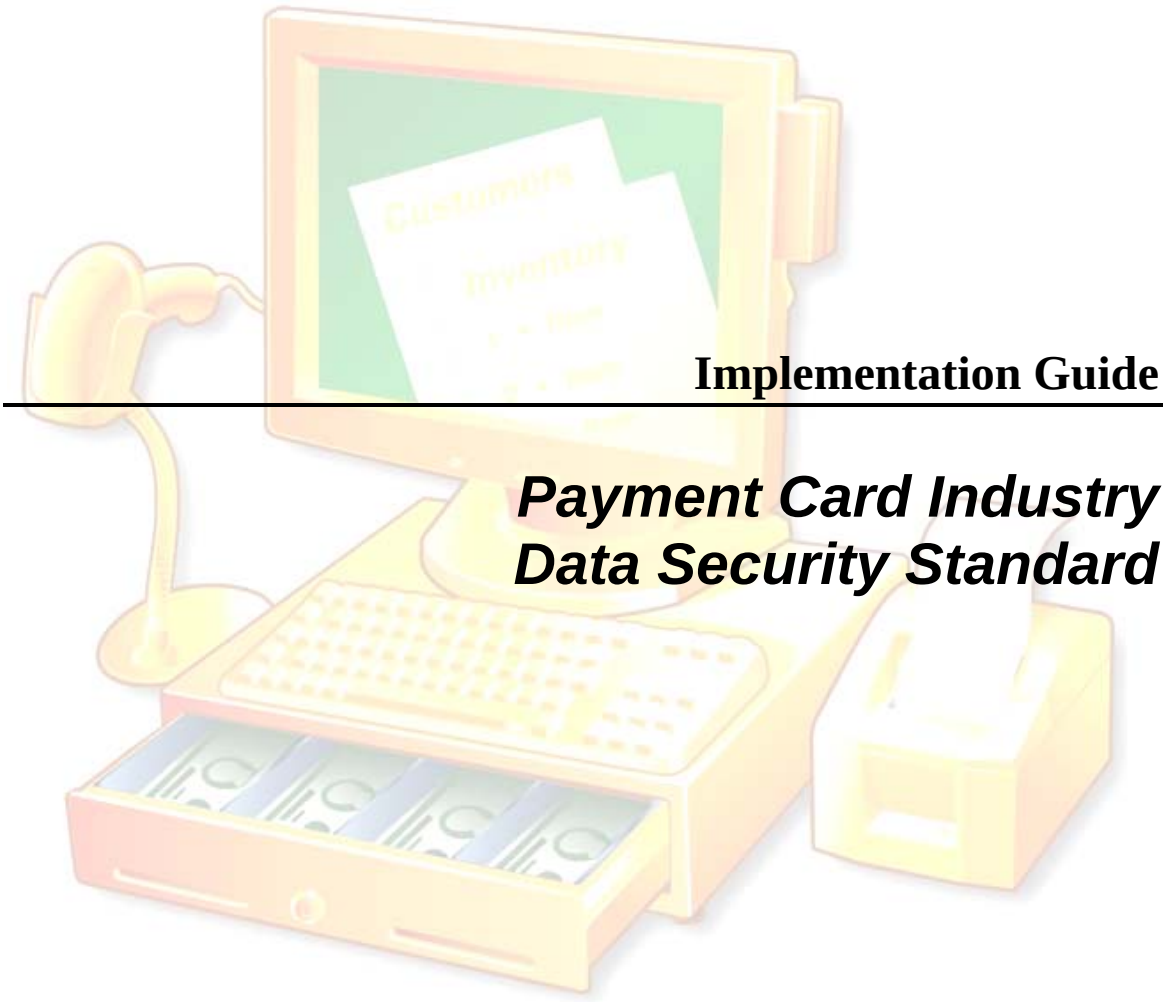
QuickBooks

Point of Sale

Versions 8.0, 9.0



Implementation Guide

Payment Card Industry Data Security Standard

intuit

Copyright and Trademarks

Table of Contents

Click the entries or page numbers below to jump to that section

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) includes requirements for the configuration, operation, and security of payment card transactions in your business.

When you start accepting payment cards you are also agreeing to take the steps necessary to protect your customer's card data. If you use the QuickBooks POS Merchant Service to authorize and settle credit and/or debit card transactions in Point of Sale, this standard and this implementation guide apply to you.

Compliance to the standard not only is good for business, as it assures your customers that their card information is being handled in a secure manner, but also is fiscally important–a security breach could result in significant fines.[1]

When determining the measures that need to be taken for compliance, you need to review your entire system configuration:

- Your operating system (Windows) configuration and account controls
- Your network architecture and, if applicable, remote and wireless access to it
- Implementation of security software, such as antivirus and firewall applications
- Implementation of and access controls to card payment applications (Point of Sale, used in conjunction with the QuickBooks POS Merchant Service, is a card payment application)
- Written policies and procedures for implementing and monitoring all of the above

This guide serves to help you implement Point of Sale and your overall system in such a manner as to be in compliance with the PCI DSS.

Table 1 summarizes the major PCI DSS requirements, what Point of Sale provides to help you meet the requirements, what you are responsible for, and where to get more information on that particular requirement. The remainder of this guide provides recommendations and instructions for your use of Point of Sale in a compliant manner.

Throughout this guide we provide links to Internet sites of providers of security related products and information, and to industry organizations that can provide additional assistance with understanding the PCI DSS requirements. These links are provided for your convenience. Unless specifically stated otherwise, Intuit does not own, endorse, or specifically recommend any of the products or vendors listed. Security recommendations should take into account relevant factors that may be unique to your business.

You can learn more about and get a copy of the PCI DSS standard at the PCI Security Standards Council™ site:

https://www.pcisecuritystandards.org.

[1] For details, please consult: http://www.visa.com/cisp

Note: *This guide applies specifically to QuickBooks Point of Sale versions 8.0 and 9.0. If you also use QuickBooks financial software, visit the QuickBooks Payment Card Protection Resource Center at http://security.intuit.com/pci-dss.html for details about the PCI DSS features available in the version you have.*

Terminology Used in this Guide

PCI DSS: Acronym for Payment Card Industry Data Security Standard, the subject of this guide. Retailers that use applications, like Point of Sale, to process, store, or transmit payment card data to authorize or settle transactions are subject to this standard.

PABP: Acronym for Payment Application Best Practices; a Visa U.S.A standard for validation of payment processing applications, such as Point of Sale. PABP-compliant applications have built-in card protection features, and provide tools and information to help retailers comply with the PCI DSS.

Cardholder data: Cardholder's name, card type, account number, and expiration date that may be stored on authorized card transactions.

Sensitive authentication data (also called **Card swipe data**): Card or account verification and PIN information stored in the magnetic stripe on a payment card.

Encryption: Process of encoding data so that it is unreadable to those without the proper permissions or "key" to decode it.

PAN: Acronym for **Primary Account Number**. Storage of customers' payment card PANs is the deciding factor if the PCI DSS and PABP standards apply to retailers and application vendors respectively. Point of Sale stores PANs in an encrypted format.

SSL: Secure sockets layer; a common encryption technology used to secure transmissions of data across public networks.

Installation/Upgrading to Point of Sale

Instructions for installing or upgrading to Point of Sale can be found in the printed QuickStart Guide that accompanied your software. Information about signing up for an account with the QuickBooks POS Merchant Service is included in that guide and within the Point of Sale program.

The QuickStart Guide, this guide, and a complete User's Guide are available in electronic format from the Help menu within Point of Sale(viewing requires Adobe Acrobat Reader).

After successfully upgrading from a previous version, PCI standards require that you securely delete the data file and any backup files in your previous version that might contain cardholder or card swipe data. For additional information about the secure deletion of this data, see Deleting Card Data in Previous Point of Sale Versions later in this guide.

Table 1: Summary of PCI DSS Requirements

Build and Maintain a Secure Network			
PCI DSS Requirement	**What Point of Sale provides…**	**What you need to do…**	**For more information…**
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	Is designed to operate securely in a network with firewalls and security devices. Works with several major antivirus and firewall vendors for out-of-the-box compatibility.	Configure the network to block unauthorized traffic. Review and update your firewall configuration and software regularly.	Consult your firewall documentation and vendor web site for best practices consistent with your business needs. Refer to Figure 1 in this guide and read Appendix C in the Point of Sale User's Guide.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	Features to require password logins, encrypt files with passwords, and set individual or group security access to sensitive program data or features.	Set your own unique user names and passwords on all wired or wireless network devices and at the operating system level. It is strongly recommended that you use complex passwords, especially for system administrators.	See www.staysafeonline.org for more information about general security practices. For more detailed guidance, IT professionals may refer to www.cisecurity.org. This includes specific guidance on Windows and networking configuration best practices.
Protect Cardholder Data			
Requirement 3: Protect stored cardholder data	Stores cardholder information in an encrypted format and automatically changes the encryption keys at least once per year. Provides a process for you to manually change the encryption keys and re-encrypt stored data. Does not store card swipe verification data.	Be alert to possible fraudulent attempts to access stored data. Manually generate new encryption keys if a breach is suspected or confirmed. Delete stored card data from previous version of Point of Sale after successfully upgrading to this version.	Refer to Protecting Cardholder Data in this guide.
Requirement 4: Encrypt transmission of cardholder data across open, public networks	Applies SSL encryption to all transmitted data.	If deploying a wireless network, protect it with equipment and a configuration that employs WPA encryption methods (rather than WEP methods).	Consult your vendor documentation for wireless security information. IT professionals may refer to www.cisecurity.org for detailed guidance on configuring wireless networking security.

Maintain a Vulnerability Management Program			
PCI DSS Requirement	**What Point of Sale provides…**	**What you need to do…**	**For more information…**
Requirement 5: Use and regularly update anti-virus software	Is designed to operate securely in a network protected with anti-virus, anti-spyware, and personal firewall products.	Use well-known and supported security products on all your business computers. Regularly install software updates to Windows, anti-virus software, and other security products.	For recommendations for anti-virus and system security tools, refer to www.ConsumerReports.org, or consult an IT Professional.
Requirement 6: Develop and maintain secure systems and applications	Is stringently tested for security issues before release. Program updates, to address evolving standards, are made available for automatic and manual download. Logs application and data access activities.	Keep your systems current with the latest software updates—operating system, antivirus and firewall applications, and Point of Sale. If possible, test updates on systems other than your production business systems first to be sure they will not affect your ongoing operation.	Microsoft® Windows® Update is available at: windowsupdate.microsoft.com Consult other software vendors' support sites for more information regarding updates and security alerts. IT Professionals should refer to www.cert.org for regular updates on security patches and alerts. Refer to Point of Sale Updates in this guide.
Implement Strong Access Control Measures			
Requirement 7: Restrict access to cardholder data by business need-to-know	Blocks all user access to stored cardholder data. Provides access control features to restrict access to financially sensitive information.	Use Windows and Point of Sale administrator accounts only for system configuration tasks. Use a regular user account at all other times. Use Point of Sale security right controls to ensure that your employees have access to data on an as-needed basis.	For information about Windows user accounts, consult your Windows help system. IT Professionals can visit http://support.microsoft.com/kb/307882 for information on the Group Policy Editor. Refer to Implementing Strong Access Control Measures in this guide.
Requirement 8: Assign a unique ID to each person with computer access	If logins are required, program enforces unique user names and passwords for access.	Set up each user with a user name and password and then require logins, along with assigned security rights, to restrict access to sensitive data.	Refer to Protecting Your Data with Unique IDs and Passwords in this guide. Refer to the PCI Security Standards for more information, at *www.pcisecuritystandards.org*
Requirement 9: Restrict physical access to cardholder data	Displayed and printed card numbers are masked. Data is stored only on one workstation, facilitating ability to physically secure it.	Physically secure the Point of Sale Server Workstation to keep your data, backups, and reports in a secure location (a locked office is recommended). Use a shredder to dispose of printouts that might contain payment information when no longer needed.	Refer to Limiting Physical Access to Your Data Files in this guide. Refer to http://www.us-cert.gov/reading_room/CSG-small-business.pdf for more information about physical security and other information security topics.
Regularly Monitor and Test Networks			
Requirement 10: Track and monitor all access to network resources and cardholder data	Logs access and other data security activities to the Audit Log and/or to the Windows Event log.	Review the audit log within Point of Sale and the Windows Event log regularly to detect possible instances of unauthorized access to your network or cardholder data. Keep audit logs and backups for at least one year.	Refer to Review Security Logs Regularly in this Guide.
Requirement 11: Regularly test security systems and processes	Provides activity logs to assist in your reviews.	Follow the guidance in the PCI Security standards as appropriate for your Merchant Level.	Refer to the PCI Security standards for detailed guidance on security assessments: Defining Your Merchant Level Validation Requirements & Procedures

Maintain an Information Security Policy			
PCI DSS Requirement	**What Point of Sale provides…**	**What you need to do…**	**For more information…**
Requirement 12: Maintain a policy that addresses information security	Provides this guide. Facilitates security policies with access controls and audit logging.	Maintain a written policy and training manual for the implementation of security program. Review your security program and network configuration at least once each year.	Refer to http://www.us-cert.gov/reading_room/CSG-small-business.pdf for more information about issues that should be addressed in your security practices. IT Professionals may refer to http://www.sans.org/resources/policies/ for more information about establishing and maintaining security policies.

Building and Maintaining a Secure Network

Conceptually, your company network should be constructed like the model shown in Figure 1.

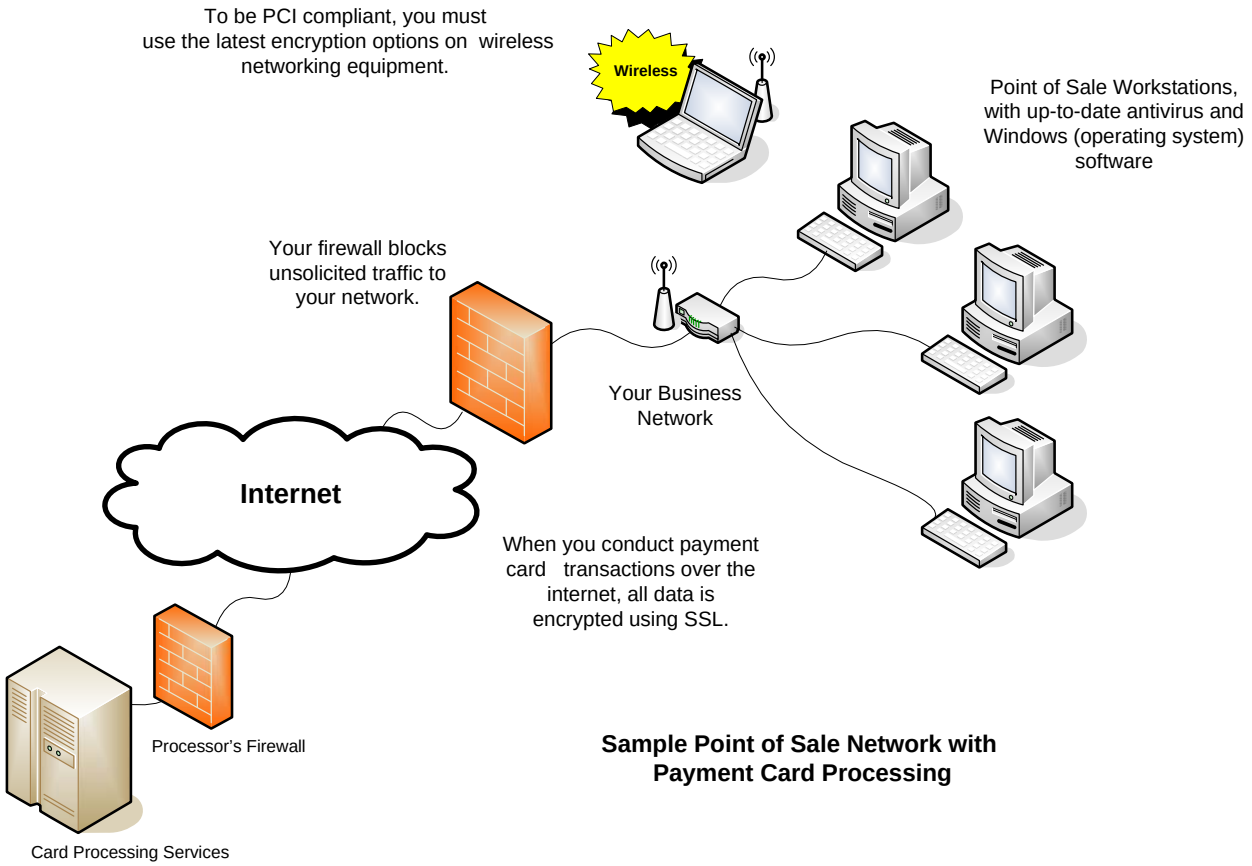


Figure 1 - PCI-Compliant Network Configuration

Consistent with careful business practices, the PCI standard require that your network:

- Be protected from unauthorized traffic using a firewall
- Have anti-virus software installed (and updated regularly)
- Is regularly updated with the latest operating system (Windows) and network software patches to keep your system current

The following guidelines are general in nature. It is recommended that you consult a qualified network administrator to review your particular network setup for purposes of implementing the best protective measures for your situation.

Build and maintain your network carefully. Your data file on the Point of Sale Server Workstation should be well protected within your network, behind a firewall and should not be stored on systems such as Internet-facing web servers or remote-access servers.

Remote Network Access

If you build out or allow remote access to your network, use applications that provide strong encryption, authentication, and access controls into your network. Products should be based on well-known and Internet-standard protocols such as SSL/TLS and SSH.

When Point of Sale connects with online services to conduct payment transactions, they do so using SSL-protected connections. Point of Sale has been constructed to facilitate compliance with PCI requirements in this regard.

Point of Sale does not provide tools or means to remotely access the data stored in your company file. If you use a third-party remote access application to allow customers, accountants, or technical advisors to access your data, you must make certain that your use of that application ensures that access to cardholder data is performed by, and can be traced to, known and authorized users. Specifically, you should:

- Not use default settings in the remote access application
- Identify all users with a unique user name
- In addition to a unique user name, require at least one of the following methods to authenticate users:
  - Passwords. We strongly recommend the use of complex passwords for logins (see Protecting Your Data with Unique IDs and Passwords for more information about establishing complex passwords)
  - Token devices (such as SecureID, certificates, or public key)
- Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.
- Authenticate all access to your data; including access by other applications, administrators, and all other users

- Allow connections only from specific, known IP/MAC addresses
- Require a Virtual Private Connection (VPN) via a firewall before allowing access
- Enable encryption of transmitted data
- Enable account lockout (30 minutes or until administrator resets user ID) after a specified number (maximum 6) of failed login attempts
- Enable logging of access activities
- Restrict access to customer passwords to authorized personnel
- Encrypt all passwords during transmission and for storage on your system
- Follow good user authentication and password management practices for employees, administrators, advisors, or technical support users. Refer to Protecting Your Data with Unique IDs and Passwords for more information.

Wireless Networks

When you build out a wireless network, consult your networking vendor's documentation and online resources carefully for optimal security configurations.

When using wireless networks:

- Install perimeter firewalls between any wireless network and computers running QuickBooks Point of Sale workstations. You need to configure these firewalls to deny or control (if such traffic is necessary for your other business purposes) any traffic from the wireless environment into the cardholder data environment.
- Install firewall software on any wireless computers which are used to access your network (see Using Firewalls).
- Change wireless vendor default settings, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.
- Encrypt wireless transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:
  - Use with a minimum 104-bit encryption key and 24 bit-initialization value
  - Use only in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS
  - Rotate shared WEP keys quarterly (or automatically if the technology permits)
  - Rotate shared WEP keys whenever there are changes in personnel with access to keys

- Restrict access based on media access code (MAC) address.

Refer to the sources in Table 3 for more information.

Using Firewalls

Firewalls monitor communication traveling through your computer's ports and block any communication that they do not know is safe. This provides you with an essential component of the protection you need to minimize your exposure to dangers from malicious users.

There are many different firewalls available to you, and they can be either software or hardware-based (for example, many routers have built-in firewalls). On a typical network, there is a single point of connection to the Internet (such as the network server) and this is the critical point requiring a firewall.

In addition to your store's computer network being protected by a firewall, you also must install firewall software on any wireless, mobile, and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are also used to access your network.

Firewalls and Point of Sale

In order to ensure that desired communication is not blocked, your firewall program has to be instructed to allow that communication.

Your Point of Sale software is "white-listed" with several major firewall software vendors, such as McAfee, Symantec, Trend Micro, and Check Point. What this means is that if you use firewall software from one of these vendors, and you keep the firewall software updated, it is pre-configured to recognize Point of Sale and the communications necessary within Point of Sale are automatically allowed.

If not using one of the white-list vendors, you may need to specify the particular ports and files that will be used by Point of Sale so that your firewall allows the communication. How this is done will vary depending upon the particular firewall you are using.

See the Appendix titled "Configuring Firewalls in your Point of Sale User's Guide for specific information about the activities and ports used, and some sample firewall configurations.

You can find out more about industry-certified products from the list of sites listed in Table 3. Many of the sites listed contain references for further information.

Protecting Cardholder Data

Encrypting Card Information

Point of Sale encrypts the cardholder data stored in your company data with encryption keys using an industry-standard, strong encryption process that meets current PCI DSS requirements. Point of Sale automatically generates new encryption keys at least once per year. No action is required on your part to enable this security feature.

Note: The encrypted cardholder data stored in your company file is not accessible to any Point of Sale user; even the Point of Sale system administrator is blocked from viewing this information. Cardholder data is also not available on Point of Sale reports or in data exports from Point of Sale.

Note: This version of Point of Sale does not store the card swipe data used to verify payment cards or PIN information. You are not required to manually delete this information as described in the PCI requirements, or take extra steps to remove this information, since Point of Sale does not store it.

Additional security measures to protect cardholder data and comply with PCI DSS standards include the following.

- The ability for you to manually generate new encryption keys if you suspect your data has been compromised or an unauthorized attempt to access the data was made. See If You Suspect a Security Breach.
- Old encryption keys are automatically deleted anytime new keys are generated.
- Card information is automatically stripped from stored transactions at sixty days of age; so that cardholder data is not retained any longer than necessary.
- In this version of Point of Sale, card swipe data is not stored. However, previous versions may contain stored cardholder or swipe data. If you upgraded from a previous version, this data must be securely deleted to be in compliance with PCI DSS requirements. See Deleting Card Data in Previous Point of Sale Versions.
- An Audit Log records all activities related to data access, payment card transactions, and changes to card encryption keys. In addition, failed attempts to log in to Point of Sale are logged in the Windows Event Log.

If You Suspect a Security Breach

If an unauthorized attempt to access your data has been made or you are aware of an actual breach of your security system that has compromised your or your customers' data, you should immediately:

1. Backup your data file and store the backup in a secure location.
2. If you suspect involvement by a specific user or users, delete or disable the user account(s). This will block further access to your data by the user(s) while you have an opportunity to investigate.
3. Review the Audit Log and Windows Event Log to examine entries related to the suspicious activity and users.
4. Change your Windows and Point of Sale administrator passwords. It is recommended you also change, or require to be changed, all other user passwords.
5. Manually generate new encryption keys:
    a. Log in to Point of Sale as the Sysadmin user.
    b. From the Point of Sale File menu, select **Utilities**.
    c. Select **Generate New Credit Card Keys**.

       The new keys are used to encrypt all new transactions. In addition, stored transactions are re-encrypted with the new keys. The previous keys are destroyed and are unrecoverable. A confirmation message is displayed upon successful update of the stored card transactions.
    d. Log off the Sysadmin user.

See Appendix B: Encryption Key Management for additional Key Management information.

Deleting Card Data in Previous Point of Sale Versions

When you upgrade from a previous version of Point of Sale, the program makes a copy of the data file from your previous version and converts it for use with the current version. All card swipe data is stripped from the converted data and cardholder data on authorized transactions less than 60 days old is re-encrypted with a new set of keys.

However, your previous version data file(s) and any backups of those files may still contain stored card swipe or cardholder data. After you have successfully upgraded to the current version of Point of Sale, secure deletion of the card data in your previous version(s) is absolutely necessary for PCI DSS compliance.

What is secure deletion?

Secure deletion of data can be compared to the shredding of confidential papers. If you simply throw such papers into the trash, they are vulnerable to recovery and use by ill-intentioned persons. But a good shredder will make it near impossible to ever read the papers again. Likewise, in electronic files, secure deletion overwrites the data with a series of random characters multiple times, until the original data can no longer be recovered.

Secure Deletion Tools

Standard file deletion tools typically do not meet the secure deletion standard—they are equivalent to throwing your data into a trash can.

You must obtain and use a secure deletion application for this purpose or utilize a qualified third-party that offers this service. You can find secure deletion utilities on the Internet. Some of these utilities are available free or at minimal cost. One such utility is MS SDelete. For more information or to download this utility visit http://www.microsoft.com/technet/sysinternals/FileAndDisk/SDelete.mspx.

Alternatively, use your Internet browser to search for "secure file deletion" to locate other secure delete applications. When selecting a program, look for one that:

- Supports your version of Windows
- Meets the latest Department of Defense (DOD) standards for secure deletion

What files do I need to delete?

Table 2 lists the previous version data and backup file locations that should be securely deleted.

If you installed or made backups to other than the default locations, you must locate and securely delete the files in those alternate locations as well.

Point of Sale data and backup files can be identified by the .qpb file extension. Actual backup file name is not fixed and if you specified something different when backups were made, adjust this process to delete those files.

Table 2: Files to Securely Delete in Previous Versions

Version	Type	Default Location	Instructions
1.0 –3.0	Data	C:\Program Files\Intuit\qbpos\ RPRO\EFT\Data	Delete entire folder.
1.0 –3.0	Backup	C:\Program Files\Intuit\qbpos \RPRO\Backup\qbpos.qpb	Optional deletion. These backups do not contain credit card data.
4.0	Data	C:\Program Files\Intuit\ QuickBooks Point of Sale 4.0\Data\<Company name>	Delete entire data folder or the data sub-folders for specific company files that contain cardholder data.
4.0	Backup	C:\Program Files\Intuit\ QuickBooks Point of Sale 4.0\Data\<Company name>\Backup*.qpb	Delete entire data folder or just the backup sub-folders for specific company files that contain cardholder data.
5.0	Data	C:\Program Files\Intuit\ QuickBooks Point of Sale 5.0\Data\<Company name>	Delete entire data folder or just the data sub-folders for specific company files that contain cardholder data.
5.0	Backup	C:\Program Files\Intuit\ QuickBooks Point of Sale 5.0\Data\<Company name>\Backup*.qpb	Delete entire data folder or just the backup sub-folders for specific company files that contain cardholder data.
6.0	Data	C:\Documents and Settings\All Users\Shared Documents\Intuit\QuickBooks Point of Sale 6.0\Data\<Company name>	Delete entire data folder or just the data sub-folders for specific company files that contain cardholder data.
6.0	Backup	C:\Documents and Settings\All Users\Shared Documents \Intuit\QuickBooks Point of Sale 6.0\Data\<Company name>\Backup*.qpb	Delete entire data folder or just the backup sub-folders for specific company files that contain cardholder data.
7.0	Data	C:\Documents and Settings\All Users\Shared Documents\Intuit\QuickBooks Point of Sale 7.0\Data\<Company name>	Delete entire data folder or just the data sub-folders for specific company files that contain cardholder data.
7.0	Backup	C:\Documents and Settings\All Users\Shared Documents \Intuit\QuickBooks Point of Sale 7.0\Data\<Company name>\Backup*.qpb	Delete entire data folder or just the backup sub-folders for specific company files that contain cardholder data.
8.0	Data	C:\Documents and Settings\All Users\Shared Documents\Intuit\QuickBooks Point of Sale 8.0\Data\<Company name>	Delete entire data folder or just the data sub-folders for specific company files that contain cardholder data.
8.0	Backup	C:\Documents and Settings\All Users\Shared Documents \Intuit\QuickBooks Point of Sale 8.0\Data\<Company name>\Backup*.qpb	Delete entire data folder or just the backup sub-folders for specific company files that contain cardholder data.
9.0	Data	C:\Documents and Settings\All	Delete entire data folder or just the data sub-

Version	Type	Default Location	Instructions
		Users\Shared Documents\Intuit\QuickBooks Point of Sale 9.0\Data\<Company name>	folders for specific company files that contain cardholder data.
9.0	Backup	C:\Documents and Settings\All Users\Shared Documents \Intuit\QuickBooks Point of Sale 9.0\Data\<Company name>\Backup*.qpb	Delete entire data folder or just the backup sub-folders for specific company files that contain cardholder data.

Transmitting and Sharing of Cardholder Data

Point of Sale encrypts all cardholder data stored in your company file. When connecting with online services to conduct payment transactions, Point of Sale does so using SSL-protected connections.

If you transmit data using the options available within Point of Sale, this encryption ensures a secure transmission.

Also, when using the transmission options included within Point of Sale:

- Card swipe data is never transmitted
- No card data is sent between stores in a multi-store configuration

If Your Data is Requested by Intuit

Occasionally, it may become necessary for a user to submit data files to Intuit Technical Support for troubleshooting or data recovery. Intuit maintains a written policy governing how your data is collected, transmitted, stored, and used for support purposes in a secure manner. Highlights of this policy include:

- Intuit does not request magnetic strip data, card validation codes or values, PINs, or PIN block numbers for any support purposes
- Cardholder or authentication data is collected only with your express permission and only when needed to solve a specific issue
- Collection is limited to the data needed to solve the specific problem
- Data is encrypted and stored in a limited-access location while in use
- Data is securely deleted immediately after use
- Intuit's use of the data is further governed by the Point of Sale Privacy Policy, which you can review from the Help menu within Point of Sale

If You Share Your Data with Other Parties (such as System Integrators)

If you transmit or share your data file outside of Point of Sale, such as with an accountant or technical advisor, it is your responsibility to understand and follow the PCI DSS requirements for the security of such transmissions.

You should never e-mail or transmit unencrypted cardholder data; this data should be transmitted only in an SSL-encrypted format.

We strongly recommend you familiarize yourself with the requirements outlined at http://www.visa.com/cisp and the additional security resources included in Table 3.

Maintaining a Vulnerability Management Program

Windows Update

Microsoft routinely releases Windows and other application software updates to address security issues. These security patches should be installed to maintain a high level of system protection.

Find out more about Windows security and Windows Update services from Microsoft at http://www.microsoft.com/security/.

Point of Sale Updates

Updates to this version of Point of Sale are released periodically to add or enhance functionality and to fix identified defects. If there are changes in PCI DSS requirement or in related Point of Sale features, the updates will include updated electronic documentation, including this guide, to help you stay in compliance. Check the "What's New" release notes and electronic version of this guide periodically for updated information (select **What's New** and **User Guides** from the Help menu in Point of Sale).

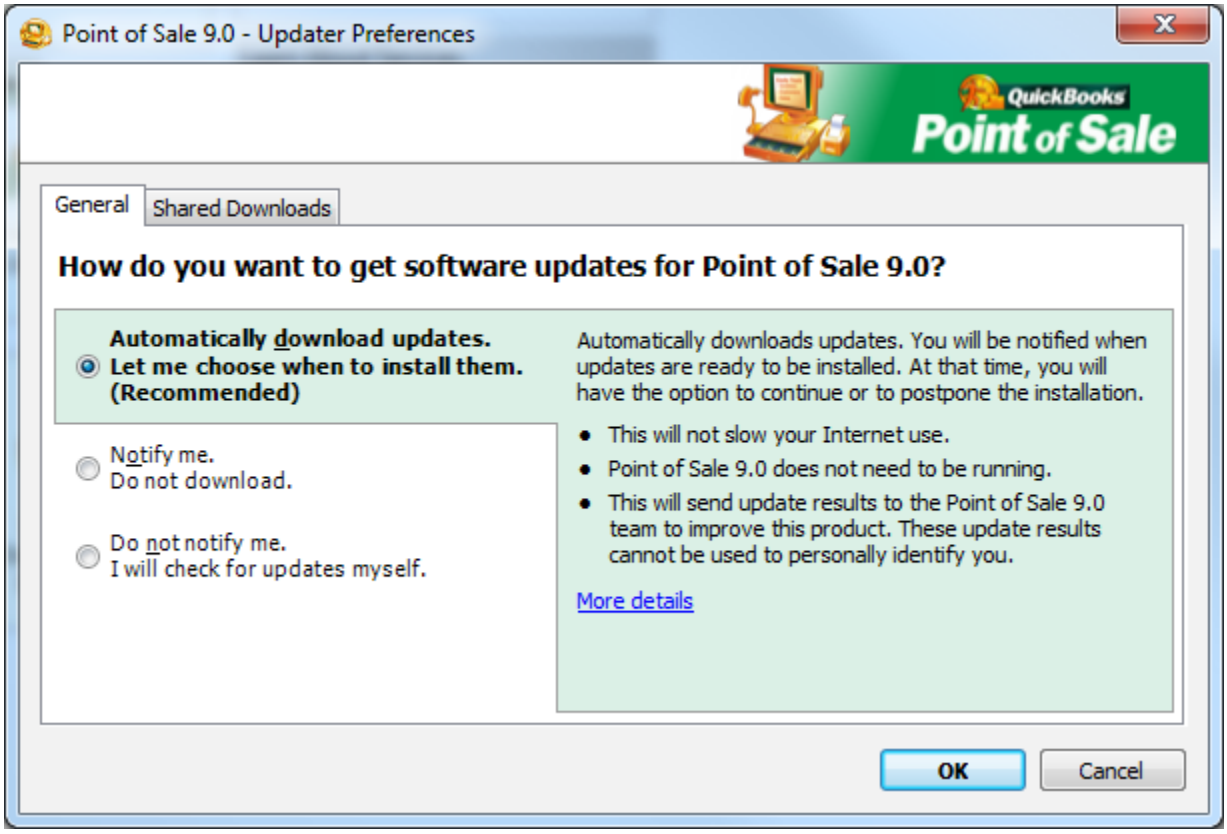
It is strongly recommended that you enable the automatic update preference in Point of Sale and consider upgrading to new versions as they are made available to stay current and in compliance with PCI DSS standards.

Intuit does not remotely connect to your network, without your permission, to "push" program updates to you. You have complete control over when and how Point of Sale updates are downloaded and installed to your system.

To review or change your Point of Sale update preferences:

1. From the Help menu, select **Software Updates > Updater Preferences**.

   The Updater Preferences dialog is opened.



2. Select an update notification level.

We recommend you select **Download only. Let me choose when to install.** With this choice, updates are downloaded anytime you are connected to the Internet, but you can install them at your convenience.

3. If you have multiple workstations, we recommend you select the **Shared Downloads** tab and choose the option to update all workstations from a single download location.
4. Select **OK**.

   ***Note**: All workstations must install the updates to maintain access to the data file and remain current with any included PCI compliance changes. The shared download option can be useful for this purpose if you have workstation without direct Internet access*

Manually Downloading Updates

If you choose not to enable automatic notification of Point of Sale updates, you are encouraged to manually check for and download updates from http://support.quickbooks.intuit.com/support/productupdates.aspx. Click on the **Product Updates** tab and review the available Point of Sale updates.

Antivirus Software

Install anti-virus and spyware detection software and keep it up to date.

These software products are designed to detect and remove malicious software code that typically is installed on your computer without your knowledge or permission for the purpose of damaging files or data, intercepting sensitive information, or tracking your computer and Internet activities.

You can find out more this class of software and related information from the sites listed in Table 3.

Implementing Strong Access Control Measures

About System Administrators

Operating System (Windows): Your Windows Administrator account must be protected with a complex password and should be used only when required to complete tasks that are limited to the administrator. At all other times, you should log in as a limited-right user to help prevent unauthorized access to the administrative areas of your operating system.

In addition, you must implement Windows user account controls, including password, account lockout, and automatic logout policies following the requirements outlined in Appendix A.

Following the requirements in Appendix A is an absolute must to control access to the Point of Sale Server Workstation, which holds your company data and the database server applications used to access the data.

Point of Sale: In Point of Sale, only the "Sysadmin" user can turn on/off the requirement of password logins to use the program, add employees and define their initial password, access all data and features (except encrypted card information), or perform certain data-sensitive tasks. It is strongly recommended that you use complex passwords for this user.

As with Windows, you should not use the Point of Sale "Sysadmin" user account for routine tasks. This user accounts should be used for application administration purposes only.

Never leave your computer unattended with an administrator user logged in!

Protecting Your Data with Unique IDs and Passwords

Your security system will be most effective when all activities by each user on the system can be accounted for and tracked. Requiring user names and password logins is one of the easiest steps you can take to protect your data.

Point of Sale, like any Windows application, relies on security features within Windows to help protect your data. For the best protection, you must set up unique user accounts/names and passwords for logins to both Windows and Point of Sale.

> *Note: See Appendix A for information on configuring your Windows user accounts, lockout policies, and automatic logouts.*

In Point of Sale, we strongly recommend "complex" passwords for all users and all processes. This is especially important for:

- The Point of Sale system administrator (Sysadmin) user who has access to virtually all Point of Sale data and features
- Processes, such as sending Store Exchange files between stores
- Any data shared with advisors or accountants via e-mail or public networks

  Note: While Point of Sale does not enforce complex passwords for the Sysadmin user, it is a requirement for PCI compliance if you are processing card payments.

What is a complex password?

For purposes of Point of Sale, a complex password meets the following rules (this may vary with other programs):

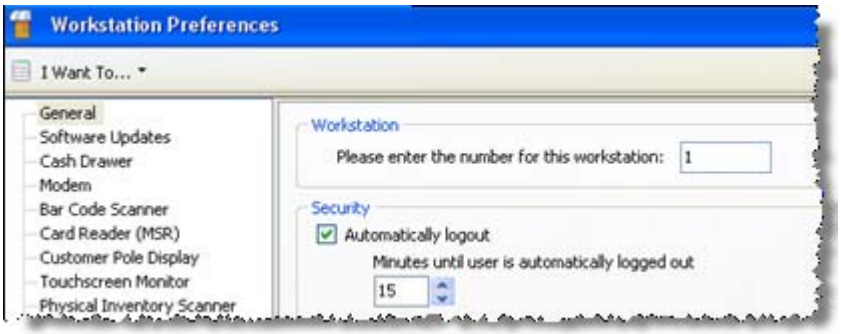
- Is at least seven characters long
- Includes at least one each of:
  - Numerals (0-9)
  - Upper-case letters (A, B, C)
  - Lower-case letters (… a, b, c)
  - Special symbols (characters other than letter or numbers)
- Is changed at least every 90 days

- Does not reuse any of your last four passwords

In addition, you should follow good practices for authentication and password management, as follows:

- Restrict addition, deletion, and modification of user IDs, passwords, and other identifiers to actual users or administrators
- Verify user identity before allowing password resets
- The Sysadmin should initially set user passwords to a unique value and require users to change it immediately after first use
- Immediately revoke access of terminated users and remove inactive user accounts every 90 days
- If you allow vendors or advisors to access your systems remotely, provide them with active accounts only for the duration of time required for them to perform their services
- Communicate your password procedures and policies to all users that have access to cardholder information
- Do not use group, shared, or generic accounts or passwords
- Enable automatic logouts after 15 minutes of no activity on your Point of Sale workstations; requiring users to re-login to continue.

  From the Edit menu, select **Preferences > Workstation**, and then select **General** from the left-side menu to access this setting. This preference must be set on each workstation independently.



Other Password Recommendations

From a practical standpoint, the most important thing about a password is that others cannot easily guess it or figure it out.

Today's techno-thieves have powerful password-guessing software at their disposal. While password protection may be the easiest step you can take to protect your data, it is also one of the easiest links for them to crack if you do not invest the effort to make your passwords complex and strong.

Other considerations when coming up with passwords include the following. We recommend you make these suggestions part of your password policy that you share with employees and others that have access to your data:

- Use a password that you can remember, but don't use your name, user name, business name, your birth date, your address, or anything else that could be easily guessed.
- Avoid other common words and names.
- Do not write your password down and leave it near your computer. If you do write down your password, lock it away in a safe or store it off-site.
- Be creative and unpredictable.

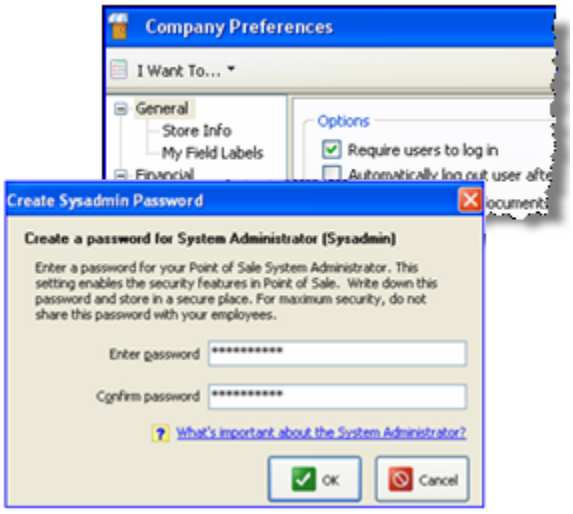
  Example: "mypassword" is a very weak password

  "mio+dRow88ap" is much stronger, though similar.

  Explanation: "mio" = "my" in Italian, the + is a symbol with no meaning, "password" is still there but spelled backward with the letter "s" replaced with 8's and the R made upper-case.

  Such a password would foil the average hacker and slow down all but the most sophisticated password-cracking tools.

Creating Your Passwords in Point of Sale



You are prompted to create a Sysadmin password when you turn on the company preference requiring users to log in to use the program and again anytime you toggle this option off/on. Enter a complex password of at least seven characters.

Once turned on, only Sysadmin can change this setting, add new employees, and perform certain other data-critical tasks.

Creating Passwords for Employees

Only Sysadmin can add a new employee, assign login names, and create initial passwords.

1. From the Employees menu, select **Employee List.**
2. Select **New Employee**.
3. Enter a **Login Name** and other employee information and then select **Create Password**. Enter a unique initial password for the employee.
4. Select **Save**.

New employees should be required to change the Sysadmin-assigned password the first time they log in using the option below.

Employees Changing Their Own Password

Once defined, any user can change his/her own password at anytime. To do so, log in with your current password and then from the Employee menu, select **Change Employee Password**. You must enter your old password before you are allowed to create a new one.

The Sysadmin can change any employee's password by editing the employee record.

Restrict Access with Security Rights

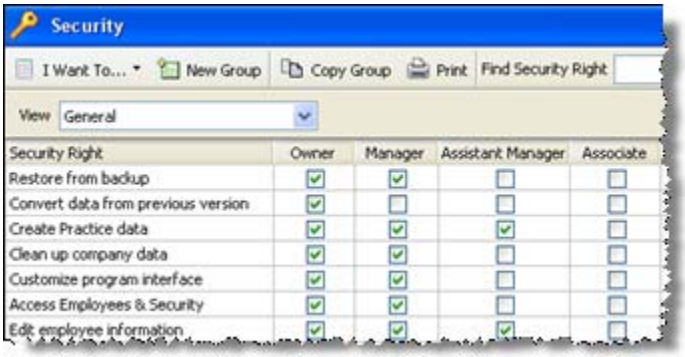
Point of Sale provides security controls that allow you to restrict access of your employees to hundreds of program areas, sensitive data, and reports. We strongly recommend you take advantage of these security controls to protect your data.

Note: Encrypted card information stored in Point of Sale is never accessible by any employee, including the Sysadmin user, or available on reports, logs, or documents whether you choose to use the other security features or not.

Configure Point of Sale security rights for your employees as appropriate for your business.

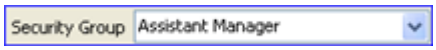
To assign security rights in Point of Sale:

1. From the Employees menu, select **Security**. The Security window displays the list of rights you can assign.



2. Grant or remove rights to perform a task or view data by selecting or clearing the check-boxes, respectively, in the security group columns.
    - There are four predefined groups, **Owner**, **Manager**, **Assistant Manager**, and **Associate**, with default rights being highest for the Owner and then progressively lower for the other three groups. You can change the rights for these default groups or create new groups and assign the rights you deem necessary.
    - Change the selection in the **View** drop-down list to show the available rights by program area.
    - Take special care when assigning employee rights for access to data-related tasks or to edit these security controls. For security purposes, it is important that only people you select and trust have access to these functions.

3. From your employee list, add employees with unique login names and passwords as described earlier and them assign them to a security group as appropriate.



4. If not already enabled, turn on the company preference requiring users to log in.

When an employee logs in, only the program areas, tasks, and data you have given them rights to will be available.

When an Employee Leaves

When an employee leaves your company, disable their account by deleting the employee record so that no further access to your data through that user name and password is possible (if you wish to keep the employee record, change their password and reassign them to a security group with no rights).

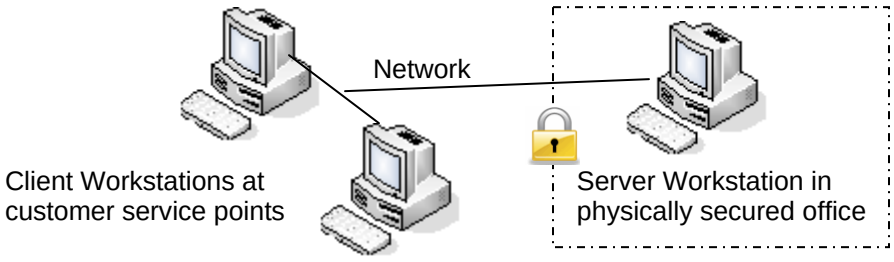
Limiting Physical Access to Your Data Files

Anyone with access to the computer with your data file may be able to retrieve data from that file be it by theft or unauthorized access.

For this reason, we recommend you limit physical access to the computer with your data file to employees on a need-to-know basis.

This is best accomplished with a network configuration that places your Point of Sale Server Workstation in a secured location. If this computer has an Internet connection, ensure it is protected by firewall and anti-virus software as outlined in this guide.

Employees will still be able to perform tasks for which they have security rights across the network, but the computer and hard drive that actually holds your data is more physically secure.



Scheduling Tasks in Point of Sale

Certain Point of Sale tasks, such as data backups and Store Exchange of information, can be scheduled to occur when your computer is unattended. This allows you to perform these tasks during off-hours, when network or Internet traffic and overhead costs are lower. However, you should be aware that this practice carries additional security risks because the Point of Sale Server Workstation must be running with a user logged in for the scheduled tasks to be completed.

If you are scheduling tasks to occur when your computer is unattended, special precautions should be taken:

- Set up a user with security rights to only the scheduled tasks, and log in as this user before leaving your computer.
- Use the Windows "lock" feature to effectively "lock the door" on your computer during the time it will unattended. For most versions of Windows, assuming you have set up user accounts and passwords, you can lock your computer by simultaneously pressing the Windows logo key + L on your keyboard.

***Note**: Depending on your Windows version and configuration, and your keyboard layout, this procedure may vary. Consult your Windows help system if this key combination doesn't work for your setup.*

Monitoring and Testing Your Network

Review Security Logs Regularly

Point of Sale automatically logs all data access, data security, card transactions, and encryption key changes to its own Audit Log or to the Windows Event Log; you do not need to turn this feature on manually.

We recommend you review these logs daily (or as often as possible) to comply with the PCI security standards.

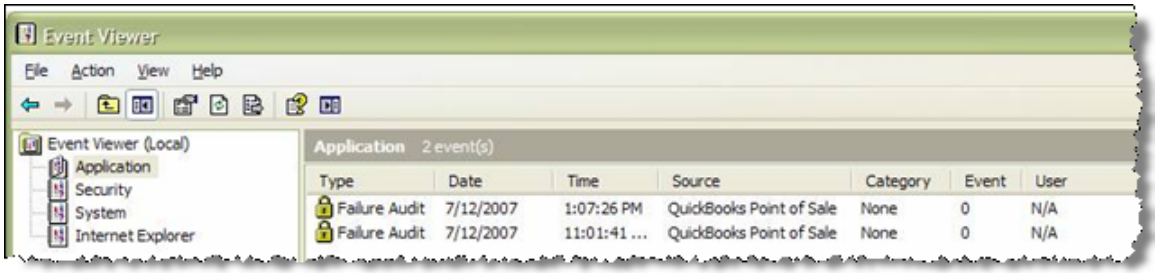
Windows Event Log

Because the Point of Sale database, and thus the Audit Log, is not accessible until a user successfully logs in to Point of Sale, unsuccessful attempts to start and log in are recorded in the Windows Event Log.

If you have your Windows user controls set appropriately, only an administrator-level user should have access to this log.

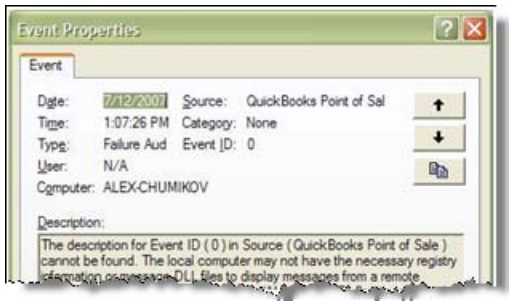
To check the Windows Event log:

1. From the Windows Control Panel, select **Administrative Tools** and then **Event Viewer**.



2. Select **Application** from the options on the left of the window.

   To see only Point of Sale log entries: From the **View** menu select **Find**, select the check-box for **Failure Audit** only, choose "QuickBooks Point of Sale" as the **Event Source** and then select **Find Next** to display matching entries.



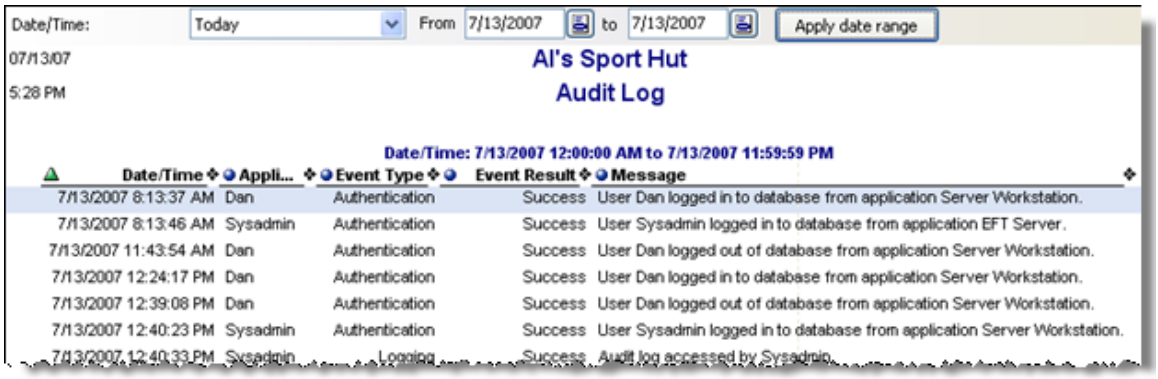
3. To view more detail, including the computer from which the attempt was made, right-click an entry and select Properties.

Point of Sale Audit Log

After logging in to Point of Sale, all security activities are recorded in the internal Audit Log. Only the Sysadmin can view this log.

To view the Audit Log:

1. Log in as the Sysadmin user.
2. From the Point of Sale **File** menu, select **Utilities** > **View Audit Log**.



3. Use normal Point of Sale report options to change the appearance or filter the Audit Log report by date, user, or other included data. Refer to the Point of Sale help system for instructions to modify reports.
4. When done, close the report and log off as Sysadmin.

Maintaining an Information Security Policy

Keep Up with Emerging Security Standards

Merchants accepting credit and debit cards for payment are now required to comply with the Payment Card Industry (PCI) security standards.

Find out more about these standards at http://www.visa.com/cisp and https://www.pcisecuritystandards.org.

Emergency Preparedness

Back Up Your Data File Frequently

Back up your data daily and before running tasks that change your data in a significant way. Keep the backup files in a safe location, preferably off-site in a fireproof safe, or at a business records management facility.

Install Uninterruptible Power Supplies (UPS)

A UPS helps ensure data integrity in the event of a sudden power loss by providing a few critical minutes of backup power in which you can complete and save in-progress transactions. Without a UPS, these transactions are usually lost and, as with any software, the data file can become corrupt if disk-write operations were in progress when the power was lost. We recommend a UPS on each Point of Sale workstation, but most importantly on the Server Workstation, which stores your data.

Keep your Business Running when Disaster Strikes

Only trusted people in your company should perform administration of your Point of Sale data file and system configuration. If you allow a temporary or limited-skill employee to install and set up Point of Sale, they may not be capable of supporting you in a critical data security situation.

Plan for situations where your trusted technical advisor or accountant is unavailable. Remember that the Point of Sale system administrator (Sysadmin) account and password are critical to the operation and protection of your business, and you should handle this account with care.

If your data file is damaged, or the Sysadmin password is compromised or lost, and you purchase data recovery services from Intuit, Intuit may need to contact the owner of the business to recover your company data file, for security reasons. You can review the Point of Sale Security Policy that governs our access to your data file from the Help menu in Point of Sale.

Further Information

Table 3: Security Web Sites

Intuit does not endorse or specifically recommend any of the products listed in the table below. Security recommendations should take into account relevant factors that may be unique to your business. No single product or security technique by itself will assure complete protection of your data. Combinations of the products and practices listed here will help to protect your Point of Sale data.

Additional information may be obtained by using your favorite search engine to search for anti-virus, firewall, and other security products.

Web Site	Description
www.staysafeonline.info	A government-industry sponsored site to educate the public on computer security. Look for advice for small businesses under the "Beginners Guides."
www.consumerreports.org	Consumer Reports has issued ratings on personal firewalls and anti-virus software; search for "firewalls," and "anti-virus" for more details.
www.cisecurity.org	This site is for IT professionals looking for best practices documents for system configuration.
www.cert.org/homeusers	This site offers an excellent set of guidelines issued by the Computer Emergency Response Team ant Carnegie Mellon University for home (and small business) users.
http://www.us-cert.gov/reading_room/CSG-small-business.pdf	Guidance from a cross section of industry, government and academic sources on security matters as they relate to small businesses.
www.getnetwise.org	Refer to the sections on wireless networking and remote access for security advice.
www.visa.com/cisp	Visa's information site for Payment Card Industry standards and related information
www.pcisecuritystandards.org	The official site for the Payment Card Industry Data Security Standards.

How to Contact Us

If you need technical assistance, with your Point of Sale software please select **Help & Support** from the Help menu within Point of Sale to learn about the various free and assisted support resources available to you.

You may also use the following QuickBooks POS Merchant Account resources:

- To learn more about a Merchant Service Account, visit us at http://payments.intuit.com
- To get help with an existing account, call 800-558-9558, 24 hours a day, 7 days a week. Free support for account holders.

Appendix A: Windows Account Security

In all recent versions of Windows, from Windows 2000 to Windows 7, account policy settings have been available to mitigate risks associated with attacks on Windows authentication. In order to comply with PCI Data Security Standards, you should configure your systems as described below.

In addition to the following, when you assign passwords to new users:

- Select the option to require the user to change their password at next login. Accounts for employees that leave your company must be disabled immediately, and inactive accounts should be removed at least every 90 days.
- If you allow vendors or contractors to access your systems remotely, provide them with accounts (in compliance with these settings) only for the duration of time required for them to perform their services.
- You should communicate password and authentication security policies to all employees of your company that have access to cardholder information. When they select passwords for their accounts, they will need to choose their password carefully to meet the PCI security standards.

Before you make these settings, be aware of the following considerations and situations where account policies may affect how you operate your business. Some points apply only to domain accounts; if your computers operate in a workgroup or stand-alone configuration, some points may not apply. Please read these points carefully and review your practices to head off problems.

1. **Don't share accounts**. If the same domain account is logged in on more than one machine, and another user attempts to login to another machine after the password has been changed by one user, other users may lockout the account.
2. **Avoid resetting of passwords by the Windows administrator**. While this is sometimes unavoidable, when user passwords are reset by the Windows administrator, you may find that data protected using some Windows encryption facilities will not be recoverable. For example, under Windows EFS (Encrypting File System), any data encrypted for an account provisioned with the old password will be unrecoverable under the new password. Similarly, data encrypted with the Windows Data Protection APIs will also be unrecoverable after the administrator resets the user's password.
3. **Be careful when configuring lockout on publicly accessible machines**. For any system that's accessible by a large population of people in your company, where the accounts on that machine are used elsewhere, be aware that someone can place that account in a lockout state on that machine that affects all other machines in your domain.
4. **Periodically examine all user accounts on your system to determine their password age and their lockout status**. Microsoft has a number of tools available to assist you in securing your Windows systems. Among the tools you may find useful are:

a. **LockoutStatus.exe**: This tool displays a list of locked out users and the last time they attempted to login, the number of times they failed to login and the domain controllers that were referenced in authentication.

b. **ALockout.dll**: This is a logging component that will assist you in determining which application or service is using an incorrect password and causing an account to enter a lockout state. For example, this tool may be useful in identifying background processes that are being locked out because of outdated credentials.

These and other tools are available in the ***ALTools.exe*** collection of tools to manage authentication in your Windows domain. This is available from Microsoft: http://www.microsoft.com/downloads/details.aspx?FamilyID=7af2e69c-91f3-4e63-8629-b999adde0b9e&DisplayLang=en

Microsoft provides extensive information about password policies and account lockout in their **Account Lockout Best Practices** document. This is available at: http://www.microsoft.com/downloads/details.aspx?FamilyID=8c8e0d90-a13b-4977-a4fc-3e2b67e3748e&DisplayLang=en

Microsoft recommends that you do not exempt the privileged accounts from password policies. Your privileged accounts should have complex passwords, an expiration period, and the passwords should be a minimum of fifteen characters in length. Microsoft also recommends that you also protect the local accounts (non-domain clients) by using a local password policy for all users. For all workstations in a domain, set a domain-level Group Policy and filter it to apply to the domain member computer.

Configuring Local User Accounts to be PCI Compliant

For a stand-alone workstation, set the appropriate registry values by configuring the local policy:

1. Select **Start** and then **Run**, type **gpedit.msc**, and then press Enter.
2. In the Group Policy editor window, select **Computer Configuration > Windows Settings > Security Settings > Account Policies** and then either **Account Lockout Policy** or **Password Policy**.
3. On the right, right-click the setting that you want to change, and then select **Properties**.
4. If you are defining this policy setting for the first time, select **Define this policy setting**.
5. Select the options that you want, and then click **OK**.

   See recommended setting for PCI compliance below.

Setting Password Policies

Figure 2 - Password Policy Setting

Figure 2 shows default Password Policy values you are likely to see when first opening the Group Policy editor. PCI Standards recommend the following settings:

- Enforce password history: 4 passwords remembered.
- Maximum password age: 90 days
- Minimum password age: 0 days
- Minimum password length: 7 characters
- Password must meet complexity requirements: Enabled
- Store password using reversible encryption: Disabled

These settings will require that each employee of your company select a Windows password that's 7 or more characters in length, and comply with the following complexity rules:

- Do not contain all or part of the user's account name.
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z).
  - English lowercase characters (a through z).
  - Base-10 digits (0 through 9).
  - Non-alphanumeric (for example, !, $, #, %). extended ASCII, symbolic, or linguistic characters.

Setting Account Lockout Policies

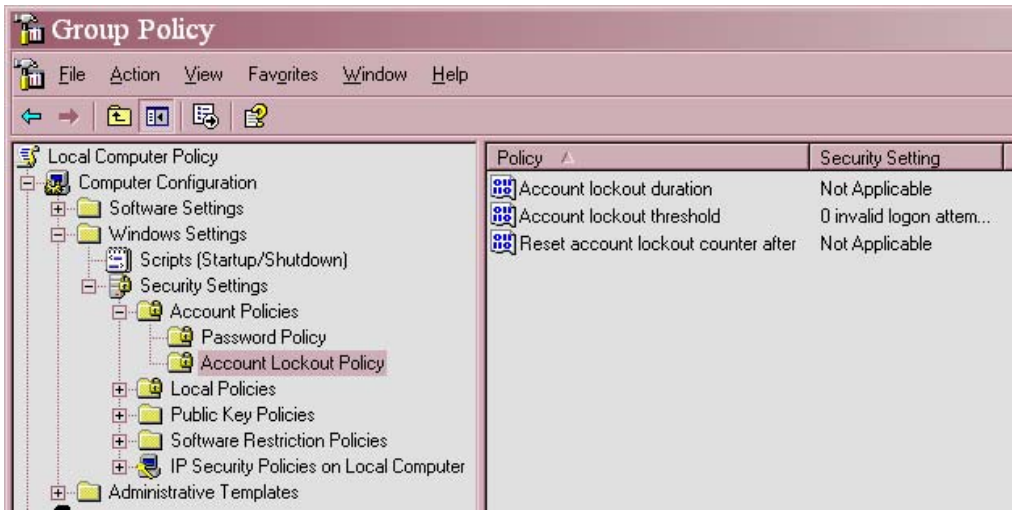


Figure 3 - Account Lockout Policy Settings

Figure 3 shows default Account Lockout values you are likely to see when first opening the Group Policy editor. PCI Security Standards recommend the following settings:

- Account Lockout Duration: 30 (minutes)
- Account Lockout Threshold: 6 invalid login attempts
- Reset account lockout counter after…: 30 (minutes)

Setting Session Idle Time and Screensaver Options

To set session idle timeout behavior to be compliant with PCI Security Standards, configure your screen saver to engage after no more than 15 minutes of idle time. You should also set the option to prompt for a password to resume the session.

Figure 4 - Setting Screen Saver Security Options

Appendix B: Encryption Key Management

1. **Point of Sale complies with PCI security standards that require cardholder information be encrypted using standard algorithms and encryption key lengths**.

   When you initially create your Point of Sale company data, an encryption key is automatically created by Point of Sale. This encryption key is used to encrypt payment card numbers using 1024-bit RSA encryption.

   This key is automatically re-generated once per year by Point of Sale and can also be manually generated by you at anytime if a data security breach is suspected (See If You Suspect a Security Breach).

2. **Permissions to use encryption keys should be properly controlled, according to the PCI standards. Point of Sale internally controls access to the encryption key, which supports the PCI standards.**

   The Point of Sale encryption key is actually made up of a pair of keys: a public key and a private key. When a card transaction is authorized in Point of Sale, the program internally uses the public key to process the authorization. When settling card transactions, Point of Sale internally uses the private key and the System Administrator (SysAdmin) credentials to complete the settlement process.

   Neither of the pair of the keys ever leaves the company file and the private key is never stored unencrypted. Access and use of the private key is limited to the SysAdmin account.

   This is yet another reason why its important to restrict access to your SysAdmin account, protecting it with a complex password that is changed frequently, never leaving your computer unattended with this user logged in, and used for administration purposes only.

3. **Data encryption keys must be stored in a secure manner, to meet the PCI requirements and to properly protect your customers' credit card information.**

   Point of Sale manages the storage of encryption keys in the company file automatically. In doing this, the private key is always stored in an encrypted fashion. The key management hierarchy previously described is applied to protect the stored credit card numbers for each customer.

4. **Key rotation is required in order to be compliant with the PCI Security standards.**

   Key rotation is a term used to refer to the practice of periodically replacing older keys with newer keys. In the event that an encryption key is disclosed, a new key is used to replace it. Rotating keys periodically reduces the risk that the value of the key will be discovered, allowing the decryption of the data protected by that key.

Point of Sale automatically re-generates the encryption keys once per year and you can also manually generate new keys at anytime if a data security breach is suspected (See If You Suspect a Security Breach).

Note: The PCI security standards require that the Point of Sale administrator change their password every 90 days. Point of Sale has been designed in a manner to minimize the set of actions that the Point of Sale administrator needs to follow in order to be PCI-compliant.

5. **When old keys are no longer used to protect data, the PCI standards dictate that these keys be destroyed.**

   Destruction of old keys helps avoid cases where a key might be recoverable and applied to an old copy of the company file (encrypted with the old key).

   When new data encryption keys are generated in Point of Sale, automatically or manually, the new keys overwrite, and therefore delete, the old keys and render them unrecoverable.

6. **Within very large businesses with extensive business systems, a common implementation pattern is to apply dual-control of keys.**

   Under dual-controls, two (or more) people need to be present in order to unlock a key for use.

   Since the target market for Point of Sale is small businesses that may not have dedicated IT staff, no dual control of keys has been implemented.

7. **Point of Sale prevents substitution of an unauthorized key for another (authorized) version of the key. Point of Sale also prevents swapping of rogue data in the company file with another piece of information.**

   When keys and credit card data are encrypted and stored in the company file, information describing that data is also encrypted and stored. The data, and the data describing the data, are encrypted and stored as a single unit. When the data is decrypted, Point of Sale performs checking on the decrypted data to be sure that only valid data is retrieved from the database.

8. **What to do when you suspect your data has been compromised, or if you wish to refresh all encryption keys within Point of Sale.**

   If you suspect that your customers' data has been compromised, you need to take immediate action to disable the account of any suspected user(s) as well as generating new encryption keys. Consult the Point of Sale audit log to examine the activity related to the compromised data. See If You Suspect a Security Breach for additional information.

Appendix C: Disabling System Restore Points in Windows XP

To prevent storing clear text cardholder data, or sensitive authentication data, any systems that are running Windows XP along with payment applications should have Windows System Restore Points disabled. This will prevent violation of PCI DSS requirement 3.2. Instructions for disabling System Restore points are documented in Microsoft Knowledge Base article 310405 accessible here:
http://support.microsoft.com/kb/310405

You will follow these steps:

1. Click **Start**, right-click **My Computer**, and then click **Properties**.
2. In the System Properties dialog box, navigate to the **System Restore** tab.
3. Select the **Turn Off System Restore** checkbox.