PixelPoint® v17.x.x

PCI PA-DSS Implementation Guide

Initial Release 10/10/2017

Powering Better Guest Experiences

Publication Details

Trademarks
PixelPoint, ParTech, and their respective logos are all trademarks of PAR Technology Corporation.

PAR may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document.

Except as expressly provided in any written license agreement from PAR, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and/ or other countries. Other product names may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Disclaimer
PAR has thoroughly reviewed this document and believes it to be reliable. However, this document is provided for informational purposes only and PAR makes no warranties, either expressed or implied, in this document. Information in this document is subject to change without notice. Risk of use and responsibility for the results of use of this document lie with the user.

Patents
The following patents apply to some areas of functionality within the PixelPoint software suite: Pat. 6,384,850; 6,871,325; 6,982,733; 8,146,077; 8,287,340

Technical Support
Technical Support is available to the end user with a valid support contract or by a per-call billing basis provided by the ParTech, Inc. Customer Support Center.

Contact
ParTech, Inc. New Hardford, NY.
Direct 1-800-448-6505
www.partech.com

Revision History

Initial Release – 10/10/2017	

Table of Contents

Introduction

PixelPoint POS is a commercial hospitality Point of Sale software product. PixelPoint POS is sold globally through a Value Add Reseller channel that provides system integration and ongoing services to our shared customers. PixelPoint POS software is designed to be installed and configured by official PAR Solution Partners. These Solution Partners are required to employ PixelPoint Certified Professionals who have been certified by ParTech Inc. PixelPoint POS should never be installed, integrated, or serviced by anyone other than a PixelPoint Certified Professional.

PixelPoint POS software supports a wide range of payment options for credit card processing through a variety of optional integrations with 3rd party payment middleware solutions. This guide is relevant for all PixelPoint POS software installations where optional integrated credit card payment functionality will be utilized. This guide is not required when using non-integrated credit card processing, though all security recommendations should still be applied.

PixelPoint Certified Professionals act as the POS system architects and integration experts on behalf of the end user license agreement holder who will be using this software product. Responsibility for all configuration and security of the POS system is shared by the end user license agreement holder and the PAR Solution Partner servicing them. PAR recommends that our Solution Partners review all recommendations within this guide with the end user before beginning the installation of a PixelPoint POS based solution.

Before deploying a PixelPoint POS software-based POS solution, the system integrator must determine if the credit card payment solution and PixelPoint POS software solution will fall within scope of PCI Compliance and use this guide accordingly. The vendor providing the credit card payment middleware solution may have a similar guide and should be able to provide information about the scope.

This guide is written with the assumption that the credit card payment option to be utilized will be fully integrated and result in the PixelPoint POS software falling within the scope of PCI.

Customer Responsibilities

PCI Compliance

PCI Compliance is required of all organizations that store, process and transmit cardholder data.

The Payment Card Industry Data Security Standard (PCI-DSS) and the Payment Applications Data Security Standard (PA-DSS) define specific requirements for all organizations that store, process and transmit cardholder data.

Further information regarding either is available at the PCI Security Council website:

http://www.pcisecuritystandards.org/

PCI Data Security Standard

The PCI Data Security Standard 1consists of twelve basic requirements:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Obtaining PCI Compliance using PixelPoint POS

With the release of PixelPoint v17, you have the ability to configure PixelPoint to utilize security functionality to protect all sensitive credit data, as outlined in the Payment Applications Data Security Standard Guidelines. If you utilize the security functionality, all sensitive credit data within the system will be secured. In addition to utilizing the security features within PixelPoint, there are several key actions that can be taken to further secure the data within each location. All statements are made to help you achieve PCI DSS compliance. If any statement is made which would affect your PCI compliance the PCI DSS 3.x guidelines should be referenced as the ultimate authority on the topic.

NOTE: Failure to follow the actions, guidance, and processes documented in this Implementation Guide may jeopardize the merchant's PCI Compliance.

1 Payment Card Industry (PCI) Data Security Standard, v3.1

PixelPoint v17.x.x and the PCI Data Security Standard

This section contains a description of the twelve basic requirements of the PCI Data Security Standard and how PixelPoint can be implemented and configured to help you achieve compliance with the PCI DSS Standard.

PixelPoint POS v17.v.v includes an option to implement and configure Datacap NETePay dsiPDCX which is a validated out-of-scope interface maintaining complete separation between cardholder data and PixelPoint POS. PixelPoint POS is "payment unaware" and not subject to PA- DSS validation when interfaced to Datacap's NETePay dsiPDCX.

It is important to note that even though PixelPoint POS integrated to NETePay dsiPDCX may be 'Out of Scope' for PA-DSS validation the merchant maintains responsibility to comply with all applicable PCI DSS requirements.

If merchant chooses not to implement Datacap NETePay dsiPDCX, PixelPoint v17.x.x will remain in scope for both PA-DSS and PCI DSS.

Section 1: Build and Maintain a Secure Network and Systems

PCI-DSS Requirement 1: Install and maintain a firewall configuration to protect cardholder data:

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria. All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network. Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 12.

PA-DSS References: 6.1, 6.3, 9.1, 11.1.

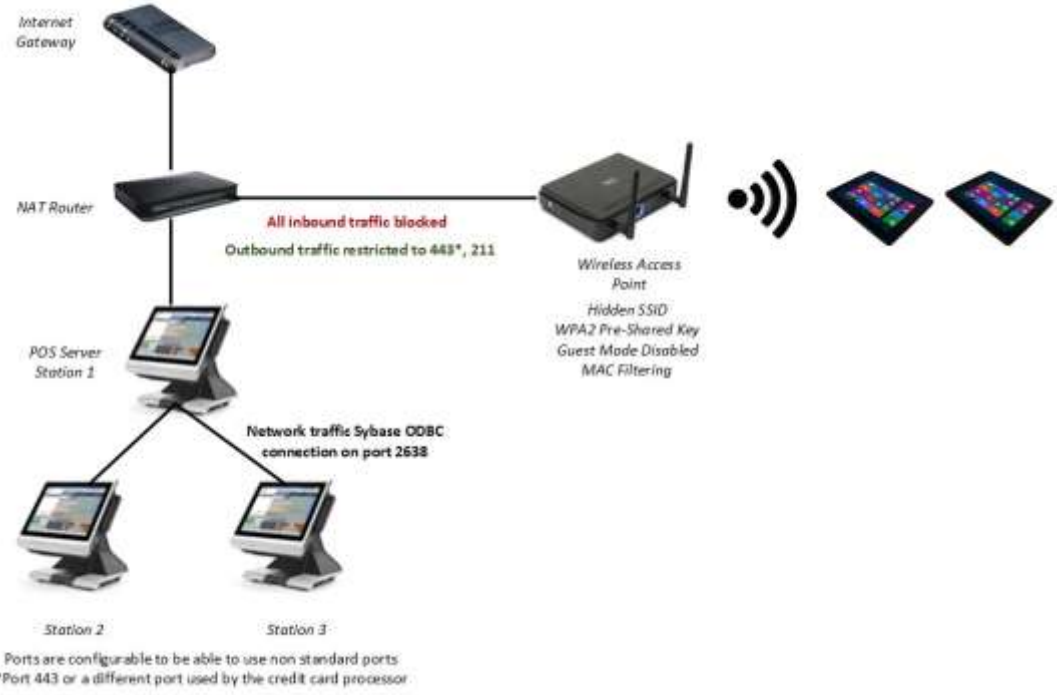
2 Payment Card Industry (PCI) Data Security Standard, v3.10,

PAR does not provide system integrators or end user customers with specific instructions for network configuration but in accordance with the PCI-DSS, PAR mandates that every PixelPoint installation maintain a firewall on the POS network to protect data. Configure your network such that POS Terminals always reside behind a firewall and have no direct access to the internet. The firewall configuration must restrict connections between internet-facing servers and wireless networks, and the POS system.

The firewall configuration must place the POS system, which houses cardholder data, in an internal network zone, segregated from the internet where no inbound connections are allowed. No software application or software client requiring inbound connectivity from the Internet can be used within this required network configuration.

Typical Network Component Diagram

PA-DSS Reference: 8.2



Wireless Implementation

PA-DFF Reference: 8.2

A wireless network should never be granted access to the cardholder data environment. There should be appropriate firewalls separating the wireless network from any other network. The firewalls must be configured to deny or control any traffic from the wireless environment into the cardholder data environment (PCI DSS requirement 1.2.3). It is recommended that the wireless network be configured using industry standard WPA2 security. If there are any questions regarding Visa standards for wireless security, refer to the PCI Security Standards Council's Requirements documentation (PCI-DSS 3.x Guidelines).

The following wireless network security practices must be employed:

- Do not broadcast the wireless SSID (Secure Socket ID)
- Connect wireless access points to a switch port, not a shared device (such as a hub).
- Change wireless encryption keys from the default settings
- Use WPA2 encryption. Other methods such as TLS 1.2, and 128bit WEP can be used provided an additional methodology is in use to protect the data (such as RADIUS).
- For automated key rotation processes (LEAP), force key change every 10-30 minutes.
- All management of wireless environments should be from the console only.
- Ensure that wireless virus signatures are included in the virus protection mechanisms.
- Restrict access to the wireless access points using MAC address filtering.
- Use static IP addresses on wireless access points
- The default Simple Network Management Protocol (SNMP) community strings and passwords on access points must be changed.
- Disable file-sharing on all client stations
- Logging and auditing must be enabled.
- Physical access to gateways, access points, and handheld devices must be appropriately restricted.
- Change wireless encryption keys, passwords and SNMP strings anytime anyone with knowledge of the keys/passwords leaves the company or changes positions.

Internet Connectivity and Security

PA-DSS References: 9.1, 11.2

The following security recommendations are to be applied:

- Internet firewall protection is mandatory.
- Anti-virus software is mandatory with routine updates to the virus definitions.
- Staff must be restricted from having any Internet access.
    - The use of instant messaging, email or other similar technologies are highly discouraged. If these technologies are enabled by the customer they must enable strong cryptography to prevent unencrypted PANs from being sent over the public internet.
- A Web server and database server must never co-exist on the same device.
- All unnecessary services should be disabled on the back office server and terminals.
    - The firewall that protects the back office server should have a very restrictive set of rules.
- Instructions not to store cardholder data on public-facing systems.

For more information and recommendations, refer to the PCI Security Standards Council's Requirements documentation.

Located at http://technet.microsoft.com/en-us/dd229319.aspx are three guides for Microsoft Windows Desktop and Server Operating Systems (O/S). You will need to follow all of them for your O/S in order to achieve Evaluation Assurance Level (EAL) 4 [CC certification is an international standard for ensuring that IT products conform to stringent security requirements.]. The guides are: Administrator's Guide, Configuration Guide and User's Guide.

Network Security

PA-DSS References: 9.1, 11.1

Instructions for verifying that only trusted keys and/or certificates are accepted:

PixelPoint only uses strong cryptography for payment data transfer over networks. TLS 1.2 is invoked by the application by default, no PixelPoint configuration is necessary.

In addition:

- For any configuration that may require data transmission over the internet, TLS 1.2 protection is required.
- For remote access, it is required that the location has firewall protection and implemented security procedures that utilize individual user IDs and passwords. It should also have a very restrictive set of ACLs or rules for access.
- All unnecessary and insecure services and protocols (such as unencrypted FTP) should be disabled. If such services are required, you should ensure that such services are encrypted.

Required Protocols/Services/Dependant Hardware & Software

PA-DSS Reference: 8.2

PixelPoint POS requires certain protocols, services, hardware and software in which to operate. A list of these items follows:

Protocols/Services/Ports

- TCPIP
- ODBC
- TLS
- Ports required: 211, 443, 2638, 9000

Hardware / Software

- OPOS
- PAR Proprietary Hardware Drivers
- Datacap NETePay disClient

Section 2: User Accounts and Passwords

PCI-DSS Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters:

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.3

User Account and Password Considerations

PA-DSS References: 3.1, 3.2

PixelPoint demands the use of PA-DSS compliant complex passwords. This requirement is a configurable element of the PixelPoint POS software and Windows. Within PixelPoint POS all passwords are stored using encryption to render them unreadable at all times, including during transmission.

The following configuration must be applied through the Security tab found in PixelPoint BackOffice System Setup:

- **Enable Strong Employee Passwords**: Checks passwords at login to ensure that they match the criteria set forth by the Security Tab options described in the points that follow.
- **Number of days password expires**: Determines how many days the same password can be used for before a change is required. Passwords must be changed at least once every 90 days.
- **Minimum password character length**: Determines the minimum number of characters required within the password. Passwords must be at least 7 characters in length.
- **Number of password entry retries**: The number of failed login attempts allowed before the employee is locked out and their password must be reset. The required configuration is that no more than 6 attempts may be allowed.
- **Number of history passwords use**: Must be set to enforce the use of newly-created unique passwords that have not been used the last 4 times.
- **Allow Alphanumeric passwords**: Switches to an alphanumeric keyboard at login instead of numeric keypad. Must be enabled to enforce use of strong employee passwords containing upper/lower case letters and numbers.

Also under the Advanced tab in BackOffice Employee Setup:

- **Must change password on next login**: Forces employees to change their password on next login. Required to enforce unique passwords.

The following PixelPoint and Windows access controls and recommendations must be applied.

PixelPoint POS:

- The default Supervisor's manual entry number must be changed from its initial setting, replacing it with a magnetic swipe card or complex manual entry number.
- The default manual entry number for all PixelPoint utilities must be changed.
- Ensure that manual entry numbers are not communicated verbally and provide protection of the manual entry number when used by a support technician, either in person or during remote dial-in sessions.
- Magnetic swipe, biometric, and manual login are the only methods of PixelPoint access provided to staff capable of closing or authorizing transaction functions on a guest check.
- Do not re-use employee swipe cards. The employee swipe card should be returned.
- The former employee's record must be set as 'Inactive' and delete the card number field in the PixelPoint employee record.
- It is the VAR's responsibility to create support accounts in the PixelPoint application if they intend for PAR support personnel to have access to their system.

Windows Operation System:

- Do not use group, shared or generic accounts and passwords.
- PA-DSS compliant complex passwords require the following criteria:
    - They are at least 7 characters in length.
    - They contain both upper case and lower-case letters.
    - They contain numbers and (if possible) special characters.
    - Change user passwords at least every 90 days.
    - Do not allow an individual to submit a new password that is the same as any of the last four passwords they have used.
- PixelPoint will log a failed attempt to gain access to any action after three (3) failed attempts.
- Limit repeated access attempts by locking out the user ID after not more than six attempts.
- Set the lockout duration to thirty minutes or under.
    - If a session has been idle for more than 15 minutes, require the user to re-enter the password or re-activate the terminal. This can be accomplished using the Window's Screen Saver utility if the back office does not support a computer lock out feature.
    - Disable guest accounts to any server. Only accounts with authorized usernames and passwords should be granted access to any application.
- It is the VAR's responsibility to create support accounts in the Windows Operating System if they intend for PAR support personnel to have access to their system.

Changing compliant settings will result in non-compliance with the PCI DSS.

For further information and recommendations, refer to the PCI Security Standards Council's Requirements documentation.

3 Payment Card Industry (PCI) Data Security Standard, v3.1,

Section 3: Protect Cardholders Data

PCI-DSS Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.4

PA-DSS Reference: 2.2

PixelPoint POS uses PAN masking and Triple DES 160 via Windows Encryption API to ensure cardholder data is stored in a manner that is PCI-DSS compliant.

PixelPoint does not allow unmasked cardholder data to be printed on receipts, displayed on the POS or contained in log files.

If PixelPoint POS is deployed in conjunction with Datacap's NETePay dsiPDCX integration, no card data is ever shared or present within the PixelPoint POS software.

During manual entry of customer PANs via a payment device, such devices may or may not mask the PAN during entry. PixelPoint does not support entry of PANs into the POS directly.

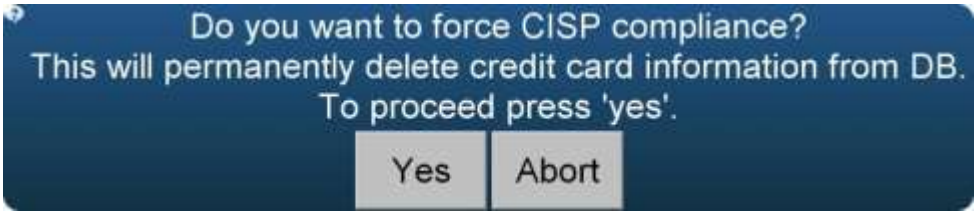
Historical Clean Up

PA-DSS Reference 1.1.4

Historical data must be removed (track data, card verification codes, PINs, or PIN blocks stored by previous versions of the payment application). Such removal is absolutely necessary for PCI DSS compliance.

PixelPoint POS v9.0 and older did not fall within PA-DSS guidelines. If you are upgrading an existing PixelPoint site from v9.0 or earlier to v17, you will need to upgrade to v10.0 first.

1. Back up your current database.
2. Upgrade PixelPoint to v10.0 using the relevant upgrade guides.
3. Run PixelPoint POS and BackOffice to perform necessary updates to the database.
4. Back up your upgraded database.
5. Run "EnforceCISPRules.exe" to clear historical credit data. The EXE is in the "\PixelPOS" folder.



Sensitive Data Collection and Retention

PA-DSS References: 1.1.5, 2.2, 2.3, 3.1

Do not store sensitive authentication data on vendor systems. If any sensitive authentication data (pre-authorization data) must be used for debugging or troubleshooting purposes, ensure the following:5

- *Sensitive authentication data is collected only when needed to solve a specific problem.*
- *Such data is stored in a specific, known location with limited access.*
- *The minimum amount of data is collected as needed to solve a specific problem.*
- *Sensitive authentication data is encrypted with strong cryptography while stored.*
- *Data is securely deleted immediately after use, including from:*
    - *Log files*
    - *Debugging files*
    - *Other data sources received from customers.*

Cardholder data exceeding the customer-defined retention period must be securely deleted

4 Payment Card Industry (PCI) Data Security Standard, v3.1,

5 Payment Card Industry (PCI) Payment Application Data Security Standard, v3.1,

PixelPoint will only retain essential information long enough to reasonably support credit card transactions. The storage path and file types containing encrypted cardholder information for PixelPoint is c:\PixelPOS\Auths\9999.txt, but this file is automatically deleted during authorization. If for some reason this file is not deleted, the completion of a batch settlement will securely delete this file.

The automated removal of encrypted cardholder information can't be considered 100% fail-safe. Each customer should still establish a defined retention period and double check the PixelPoint POS server to ensure that all data was in fact securely deleted within their defined period.

Payment Receipts display a truncated PAN by default, but this information is not stored. As a one-time event, PixelPoint prints a masked PAN on the initial Auth Slip Receipt printout.

If PixelPoint POS is deployed in conjunction with Datacap's NETePay dsiPDCX integration, no card data is ever shared or present within the PixelPoint POS software.

Securely Deleting Files

To securely delete files and/or old data files which may contain sensitive cardholder data, a tool such as Eraser should be used. Eraser is an advanced security tool (for Windows), which allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected pattern. This tool is available from http://eraser.heidi.ie/.

Removal of Historical data must be removed (track data, card verification codes, PINs, or PIN blocks stored by previous versions of the payment application) is absolutely necessary for PCI DSS compliance.

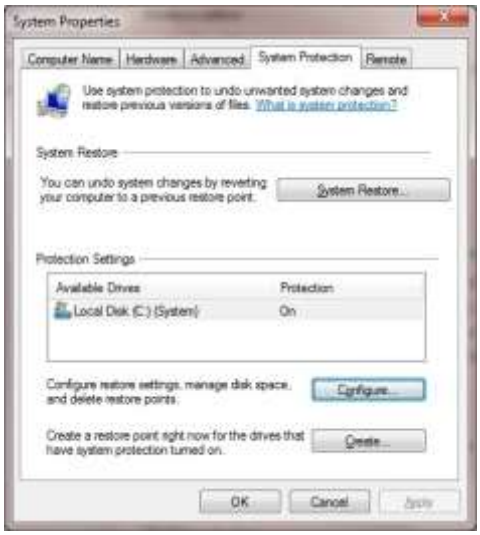
Addressing Inadvertent Capture of PAN

Instructions for Windows 7 and 8 can be found below.

Windows 7

Disabling System Restore

1. Right click on Computer > Select "Properties".
2. Select the "System Protection" tab.



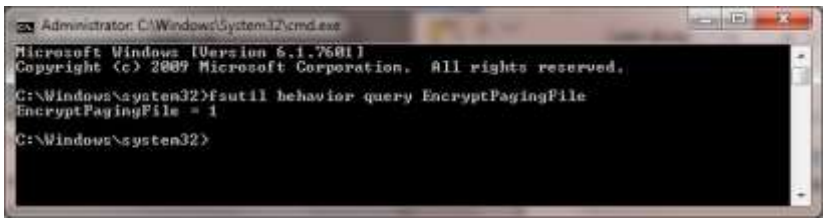
3. Select Configure.

4. Select "Turn off system protection".
5. Click Apply, and OK to close the System Protection and System Properties windows.
6. Reboot the computer.

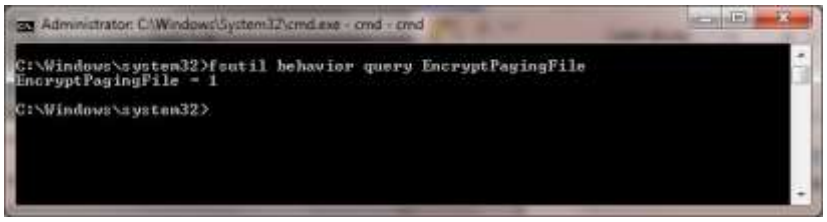
Encrypting PageFile.sys

Note: In order to perform this operation, the hard disk must be formatted using NTFS

1. Search "cmd" to locate the Windows Command Prompt. Right click on cmd.exe and select "Run as Administrator"
2. To Encrypt the Pagefile type the following command: fsutil behavior set EncryptPagingFile 1

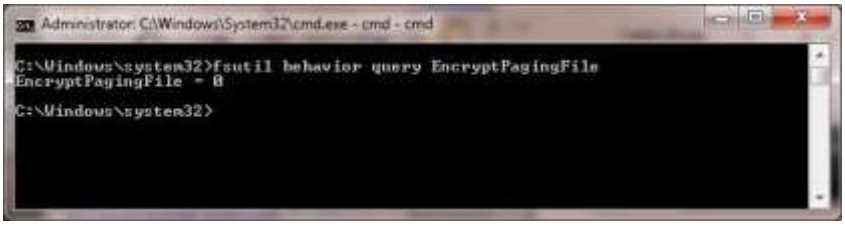


3. To verify configuration type the following command: fsutil behavior query EncryptPagingFile



4. If encryption is enabled EncryptPagingFile = 1 should appear
    - In the event you need to disable PageFile encryption type the following command: fsutil behavior set EncryptPagingFile 0

5. To verify configuration type the following command: fsutil behavior query EncryptPagingFile

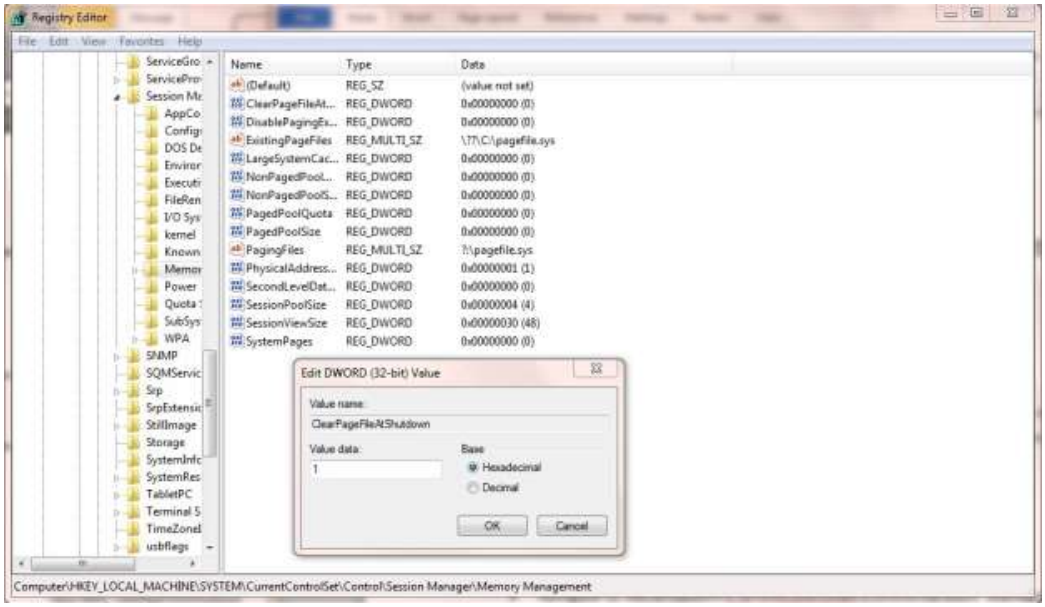


6. If encryption is disabled EncryptPagingFile = 0 should appear

Clear the system Pagefile.sys on shutdown

Windows has the ability to clear the Pagefile.sys upon system shutdown. This will purge all temporary data from the pagefile.sys (temporary data may include system and application passwords, cardholder data (PAN/Track), etc.). **Note:** Enabling this feature may increase windows shutdown time.

1. Open the Windows system search and type in "regedit".
2. Right click on regedit.exe and select "Run as Administrator"
3. Navigate to HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
4. Change the value from 0 to 1
5. Click OK and close Regedit

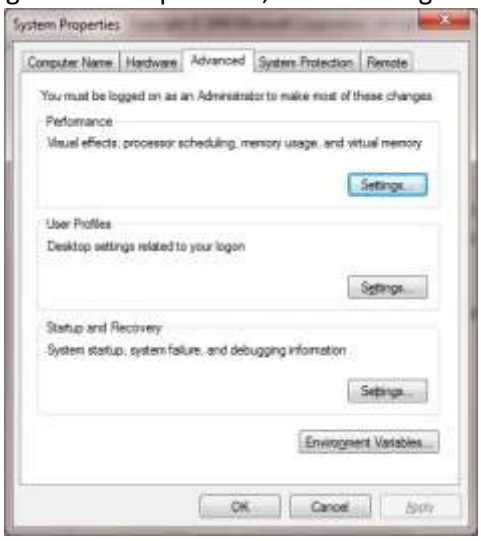


If the value does not exist, add the following:

- Value Name: ClearPageFileAtShutdown
- Value Type: REG_DWORD
- Value: 1

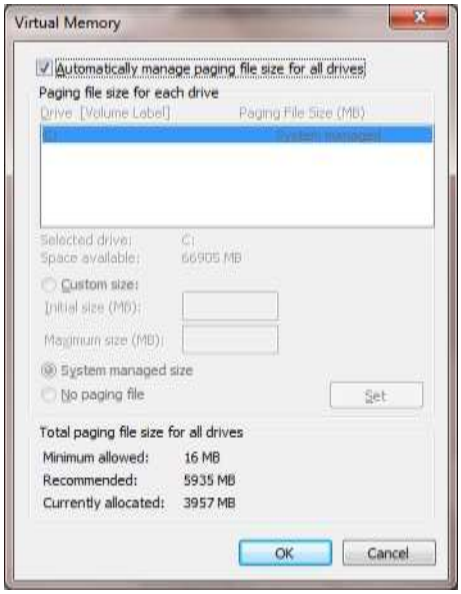
Disabling System Management of PageFile.sys

1. Right click on Computer > Select "Properties".
2. Select "Advanced System Settings" on the top left list, the following screen will appear:



3. Select the Settings button in the Performance section.

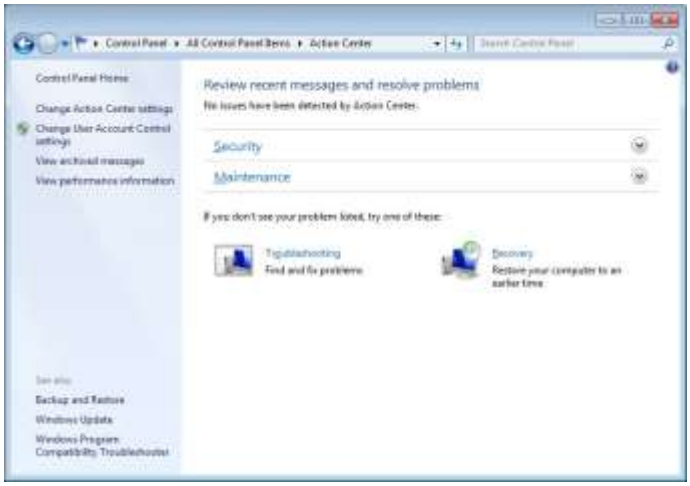
4. Select "Change" in the Virtual Memory section.



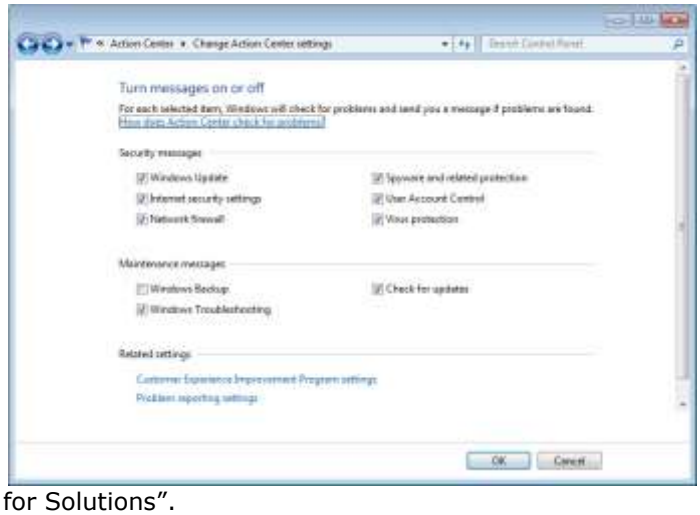
5. Uncheck "Automatically manage page file size for all drivers",
6. Select Custom Size. Enter the following selections:
    - Initial Size – as a good rule of thumb, the size should be equivalent to the amount of memory in the system.
    - Maximum Size – as a good rule of thumb, the size should be equivalent to 2x the amount of memory in the system.
7. Save all changes and exit the setup windows.
8. Restart the computer.

Disabling Windows Error Reporting

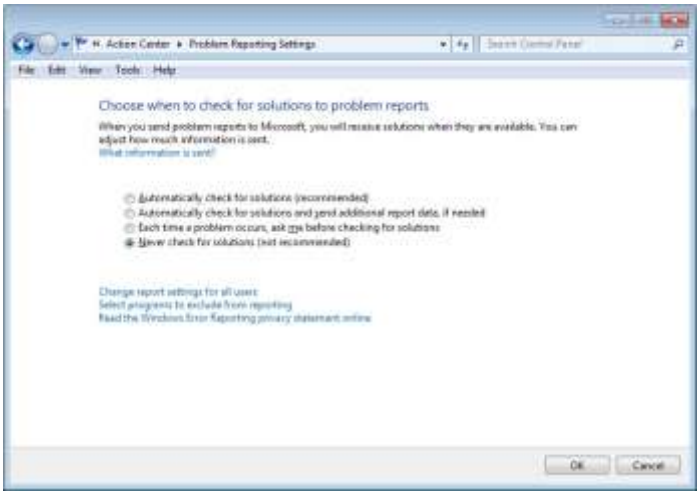
1. Open the Control Panel.
2. Open the Action Center.
3. Select "Change Action Center Settings".



4. Select "Problem Reporting Settings".



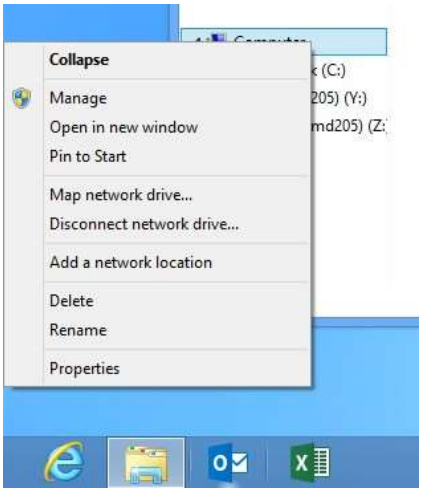
5. Select "Never Check for Solutions".



Windows 8

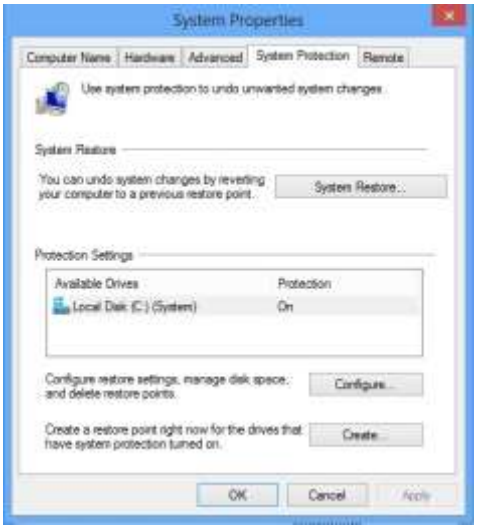
Disabling System Restore

1. Right Click on Computer > Select "Properties":

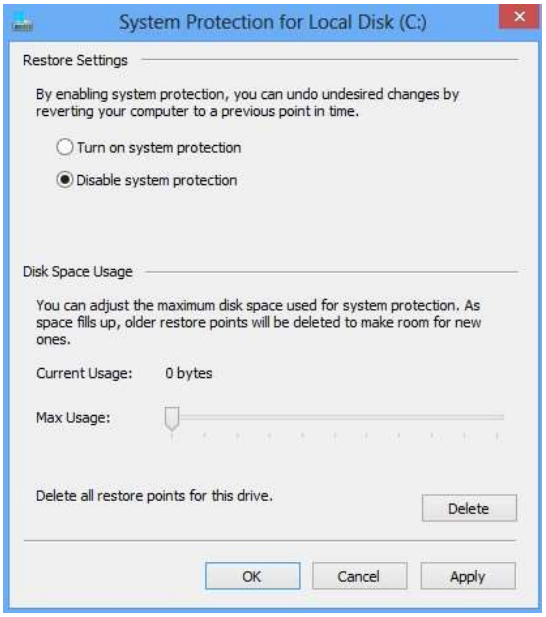


2. Select "Advanced System Settings" from the System screen:

3. Select "System Protection" on the top left list, the following screen will appear:



4. Select Configure, the following screen will appear:

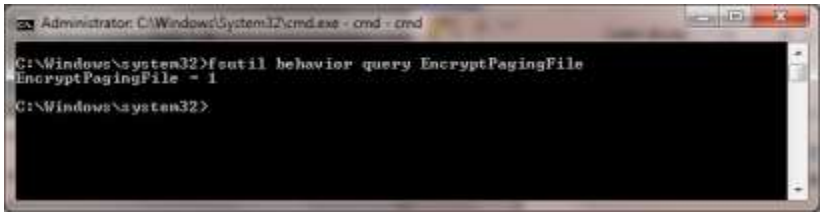


5. Select "Disable system protection".
6. Click apply, and OK to shut the System Protection window.
7. Click OK again to shut the System Properties window.
8. Reboot the computer.

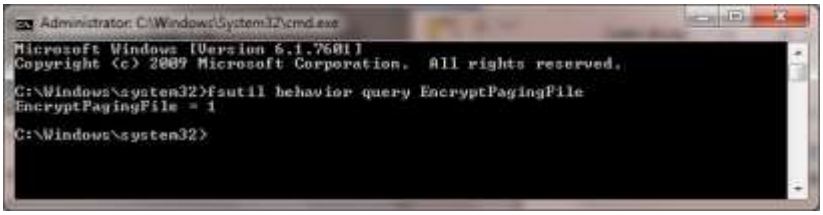
Encrypting PageFile.sys

Note: In order to perform this operation the hard disk must be formatted using NTFS.

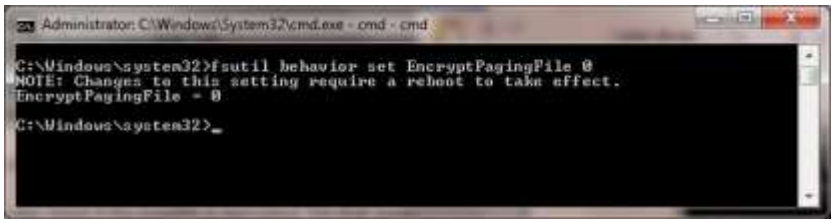
1. From the desktop hold down the "Windows" key and type "F" to bring up the "Search" window, select "Apps" in the "Apps" box type in "cmd".
2. Right click on "Command Prompt" icon located on the left side of your screen, a selection bar will appear at the bottom of the screen, select "Run as Administrator".
3. To verify configuration type the following command: fsutil behavior query EncryptPagingFile".
   - If encryption is enabled EncryptPagingFile = 1 should appear
   - If encryption is disabled EncryptPagingFile = 0 should appear



4. To Encrypt the Pagefile type the following command: fsutil behavior set EncryptPagingFile 1



5. In the event you need to disable PageFile encryption type the following command: fsutil behavior set EncryptPagingFile 0

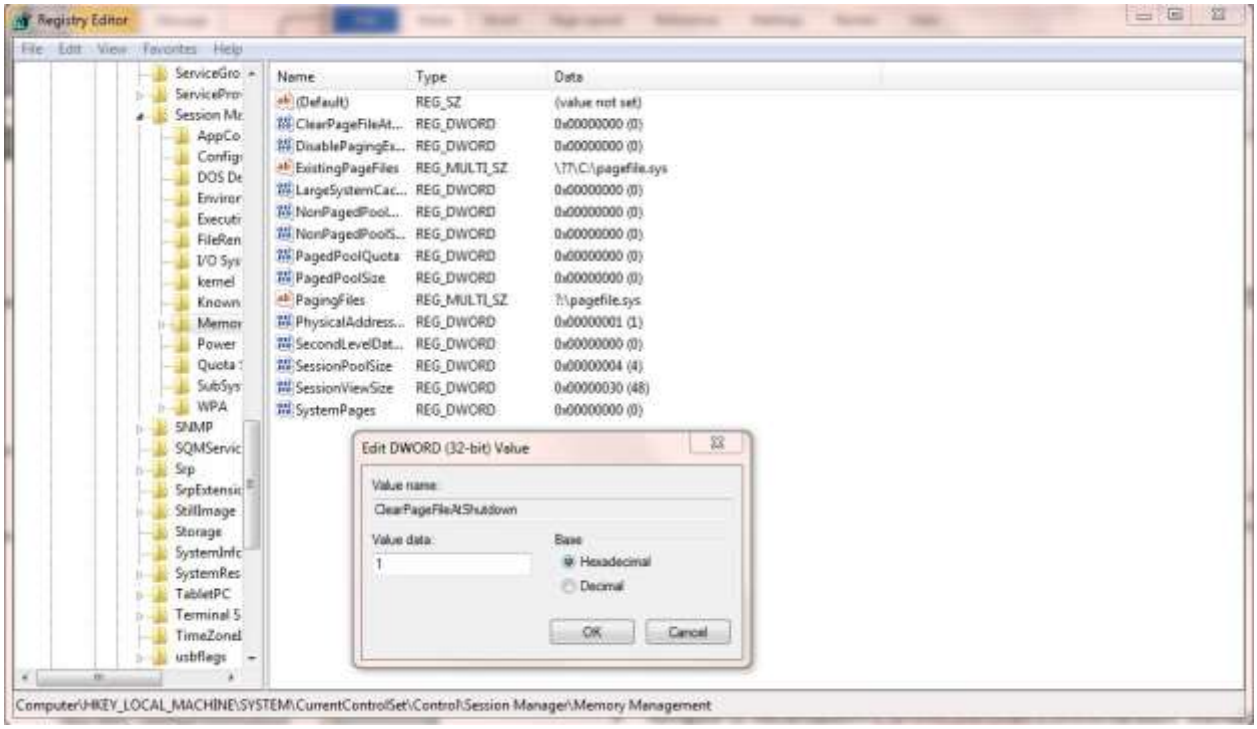


Clear the System Pagefile.sys on Shutdown

Windows has the ability to clear the Pagefile.sys upon system shutdown. This will purge all temporary data from the pagefile.sys (temporary data may include system and application passwords, cardholder data (PAN/Track), etc.).

Note: Enabling this feature may increase Windows shutdown time.

1. From the desktop hold down the "Windows" key and type "F" to bring up the "Search" window, select "Apps" in the "Apps" box type in "regedit".
2. Right click on regedit.exe and select "Run as Administrator"
3. Navigate to HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
4. Change the value from 0 to 1 on the "ClearPageFileAtShutdown" DWORD.
5. Click OK and close Regedit.



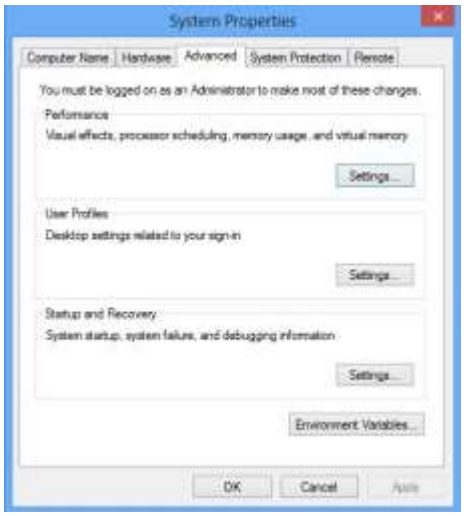
If the value does not exist, add the following:

- Value Name: ClearPageFileAtShutdown
- Value Type: REG_DWORD
- Value: 1

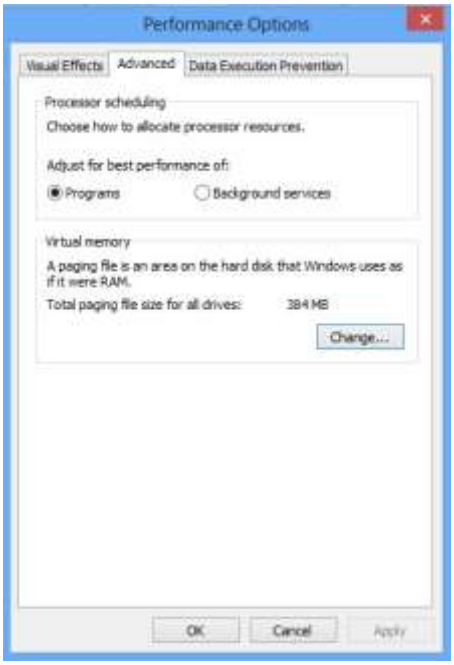
Disabling System Management of PageFile.sys

1. Right Click on Computer > Select "Properties".
2. Select "Advanced System Settings" from the System screen.

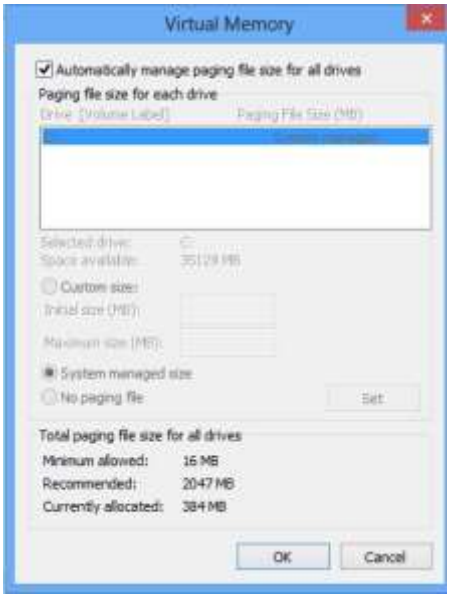
3. Select the "Advanced" tab.



4. Under performance select "Settings" and go to the "Advanced" tab, the following screen will appear.



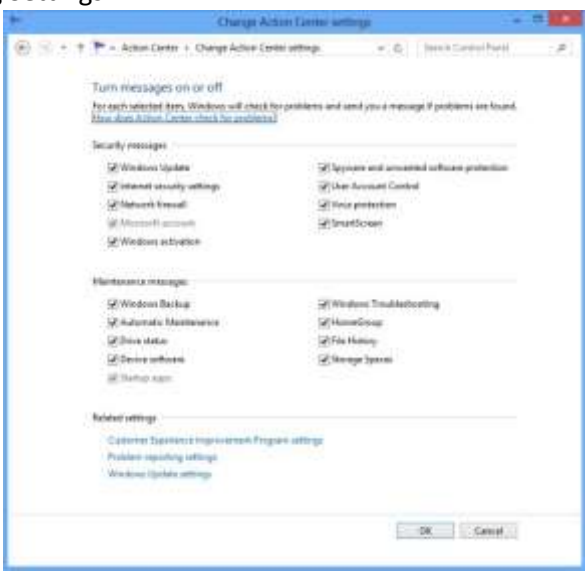
5. Select "Change" under Virtual Memory, the following screen will appear.



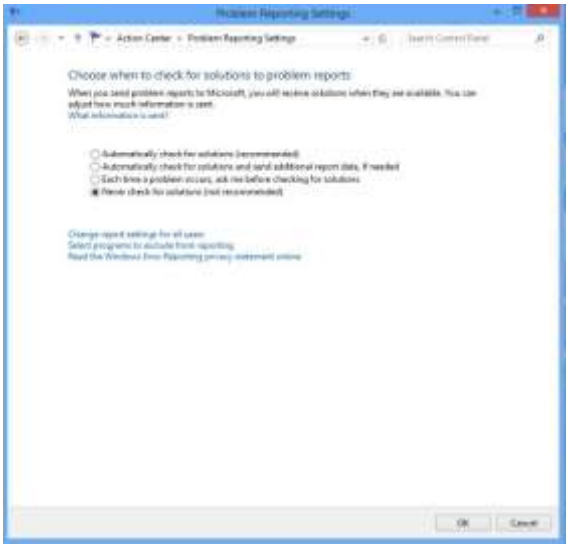
6. Uncheck "Automatically manage page file size for all drives"
7. Select "Custom Size"
8. Enter the following for the size selections:
    - Initial Size – as a good rule of thumb, the size should be equivalent to the amount of memory in the system.
    - Maximum Size – as a good rule of thumb, the size should be equivalent to 2x the amount of memory in the system.
9. Click "Ok", "OK", and "OK"
10. You will be prompted to reboot your computer.

<u>Disabling Windows Error Reporting</u>

1. From the desktop hold down the "Windows" key and type "I" to bring up the "Settings" window. Select "Control Panel".
2. Open the Action Center.
3. Select "Change Action Center Settings".
4. Select "Problem Reporting Settings".



5. Select “Never Check for Solutions”.



6. Select “OK” twice and then close Action Center.

Section 4: Cardholder Data Encryption

PCI-DSS Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.6

PixelPoint POS uses Triple DES 160 via Windows Encryption API to ensure cardholder data is always secure when transmitted within the secure internal POS network.

If PixelPoint POS is deployed in conjunction with Datacap's NETePay dsiPDCX integration, no card data is ever shared or present within the PixelPoint POS software.

Section 5: Maintain a Vulnerability Management Program

PCI-DSS Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans— enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place. 7

In accordance with the PCI Data Security Standard, PAR mandates regular use and regular updates of anti-virus software for all PixelPoint POS installations. It is the shared responsibility of the VAR and restaurant merchant customer to ensure this is in place. Anti-virus software must be deployed on all systems commonly affected by viruses, particularly personal computers and servers.

Section 6: Develop and Maintain Secure Systems and Applications

PCI-DSS Requirement 6: Develop and maintain secure systems and applications

PAS-DSS Reference 10.2.1

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.8

PAR uses standard system development processes to ensure software integrity and security. Updated patches and security updates are made available by PAR. While PAR makes every possible effort to conform to Requirement 6 of the PCI-DSS, certain parameters, including following change control procedures for system and software configuration changes, and the installation of available security patches, depend on VAR and customer specific protocol and practices.

As a PAR PPCP implementations expert it is your responsibility to ensure all PixelPoint software patches and new version releases have been made available and offered to your customers.

Section 7: Implement Strong Access Control Measures

PCI-DSS Requirement 7: Restrict access to cardholder data by business "need to know"

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.9

PixelPoint POS provides user access based upon roles and security levels. These mechanisms ensure access to sensitive information is restricted, password protected, and based on a need-to- know basis. If PixelPoint POS is deployed in conjunction with Datacap's NETePay dsiPDCX integration, no card data is ever shared or present within the PixelPoint POS software.

PCI-DSS Requirement 8: Identify and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and process.

The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.10

PCI-DSS Requirement 8.1 and 8.2:

- Control Access to any PC's, servers, and databases with payment applications via unique user ID and PCI DSS-compliant secure authentication.
- Control Access to any PC's, servers, and databases with cardholder data via unique user ID and PCI DSS-compliant secure authentication.

Unique User ID Requirements

PA-DSS References 3.1, 3.2

PixelPoint requires each user to have a unique user ID and password in order to access the POS system. The default, "out of the box," installation of PixelPoint facilitates the use of unique user IDs and secure authentication for all administrative access and for all access to cardholder data.

- Do not use the default administrative accounts for payment application logins
    - Assign secure authentication to these default accounts and then disable or do not use the accounts.
- Assign secure authentication for the PixelPoint application and systems whenever possible.
- Changing the default setting for unique user IDs and secure authentication will result in non-compliance with PCI DSS.

Establishing Administrative Account Access

To align with PCI DSS Requirements, no generic or shared administrative accounts should exist. To establish administrative account access, follow these steps:

<u>Windows</u>
To align with PCI DSS Requirement 8.5.8, no generic, group, or shared administrative accounts may exist. No generic, group, or shared passwords may be used either. Ensure that any guest accounts have been disabled. To establish Windows administrative account access, follow these steps:

1. Login as the default Windows user.
2. Create a new administrative account user. Log in to the new account.
3. Assign secure authentication to both the default and the new user account, and then disable the default user.

4. Repeated access attempts to log in to Windows must be limited by locking out the user ID at three attempts. The lockout duration should be set to 30 minutes or until the administrator re-enables the user ID.
5. The PCI DSS and PA-DSS standards require complex passwords that meet with the following criteria:
    - They are at least 7 characters in length.
    - They contain upper and lower case letters, numbers, and special characters.
    - They are changed at least once every 90 days.
    - New passwords must not be the same as any of the last four passwords.

PixelPoint
In BackOffice under System Setup, go to the Security tab and enable Strong Employee Passwords. Then, open Employee Setup:

1. Press [+] button in the navigation section, at the bottom of the window
2. Fill out Employee Name, Last name, P.O.S Name
3. Make visible
4. Assign Card swipe #
5. In Job Position Setup section press [+ Add] to add a Job Position.
6. Select System Administrator and set pay rate.
7. Press [P] button to save.

10 Payment Card Industry (PCI) Data Security Standard, v3.1,

Remote Access Security Guidelines

PA-DSS References 10.2.3, 12.1, 12.2

Customers must enable Remote Access only when needed and disable immediately when Remote Access session has completed.

To align with PCI DSS Requirements, Remote Access products should be implemented in a secure fashion.

The following examples of remote access security features should be considered:

- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each user).
- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication and complex passwords for logins
- While the application does not support non-console access, enable encrypted data for all non-console administrative access with strong cryptography, using technologies such as SSH or VPN or TLS 1.2+.
- Enable account lockout after a certain number of failed login attempts.
- Enable the logging function.
- Restrict access to passwords to authorized reseller/integrator personnel.
- Establish passwords according to PA-DSS Requirements 3.1.1 through 3.1.11. See the section titled "User Account and Password Considerations" above.

Section 8: Restrict Physical Access to Cardholder Data

PCI-DSS Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.11

In accordance with the PCI-DSS, PAR mandates the restriction of physical access to cardholder data when implementing any PAR POS. Inbound and outbound traffic to the cardholder data environment must be restricted.

Internet access must not be available for any device used to store cardholder data. The POSServer must never be used as a restaurant Back Office and never provide access to any applications such as a web browser or email client which can access the internet.

If PixelPoint POS is deployed in conjunction with Datacap's NETePay dsiPDCX integration, no card data is ever shared or present within the PixelPoint POS software.

Section 9: Regularly Monitor and Test Networks

PCI-DSS Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.12

Section 10: System Logging

System Logging Options

PixelPoint POS employs PCI-DSS compliant logging by default. Disabling any of these logs will result in a non-compliant application.

It is required that the customer establish and maintain PCI DSS-compliant logs to include:

- Individual accesses to cardholder data
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanism
- Initialization of the audit logs
- Creation and deletion of system-level objects
- User identification
- Type of event
- Data and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource

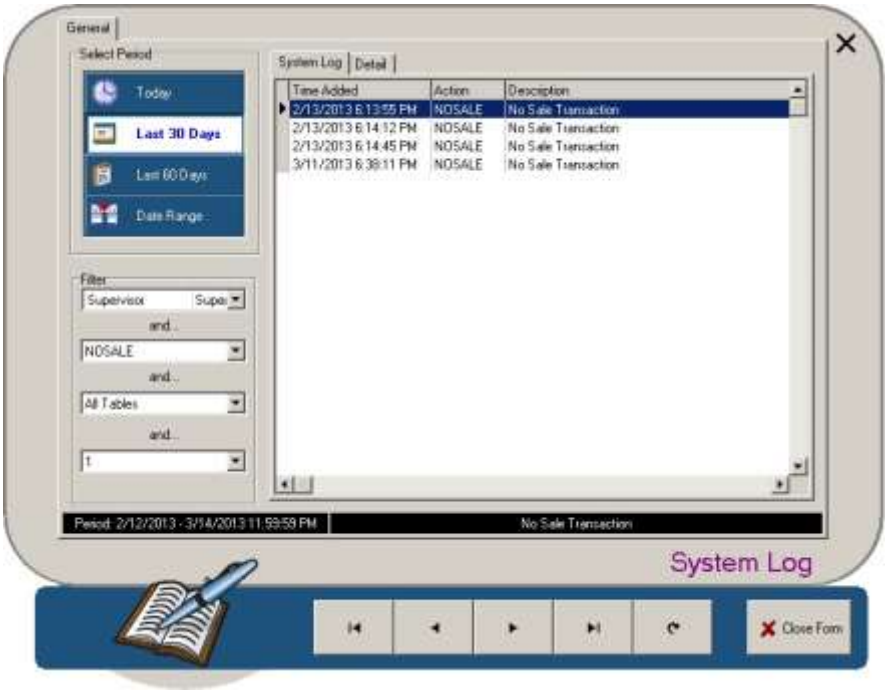
Not establishing these logs will result in a non-compliant system.

11 Payment Card Industry (PCI) Data Security Standard, v3.1,

12 Payment Card Industry (PCI) Data Security Standard, v3.1,

PixelPoint POS Audit and Log

The PixelPoint System Log must be configured by setting the SecEventLog policy to Yes to view all POS event logs within the PixelPoint BackOffice. The form shown below from the PixelPoint BackOffice allows for audit review of all POS events. These logs are stored within the PixelPoint POS database.



Control what activity is displayed on the right side of the screen by using the controls on the left.

You can filter the data by employee, database table, specific actions, and station number by using one or more of the drop-down boxes on the bottom-left of the screen. You can also choose to review actions from the current day, the last 30 days, last 60 days, or a different specified date- range, by selecting the respective blue button on the upper-left. Only actions that have occurred at least once will appear in the Actions filter list.

Centralized Logging is provided through the PixelPoint System and Security Log and by the Windows Operating System.

Beyond the built-in audit trails listed above, centralized logging may be facilitated by exporting the 'PixelPoint' Windows Event Log that is present for all PixelPoint POS stations and POS Server. Any standard log export tools that support Windows Event logging may be used. See below for more information about Windows Audit capability including the Windows Event Log.

Windows OS Audit

Audit functionality is available within Microsoft Windows Operating Systems to log and track all system events. The Windows Help and Support utility can provide detailed configuration information to assist with the following tasks:

- Turning on Windows security logging.
- Archiving event logs.
- Opening archived event logs.

You must use Windows security policies to configure audit within the following directories:

- \PixelPOS (and sub-folders)
- \PixelSQL
- Folders storing 3rd party credit card software (such as DataCap, Monetra, etc).

The Microsoft Windows Help and Support system has detailed information which will assist in enabling:

- Enabling Windows Firewall Logging (search: windows firewall)
- Setting the path and file name for the Windows Firewall log file
- Turn on Windows security logging (search: security logging)
- Archive an event log (search: event log)
- Open an archived event log

There are registry settings which will allow auto-archiving of event logs. More information can be found on the Event Log Key http://msdn.microsoft.com/en-us/library/aa363648(VS.85).aspx

Auditing and Log File Data Retention

- PCI-DSS requirements state that you should employ a backup procedure that archives and stores all security logs for at least one year.
- PA-DSS requirements state that merchants must employ a backup procedure to archive security logs for at least one year.
- It is possible to auto-archive event logs by modifying the EventLog Registry Key. Information on this can be found here: http://msdn.microsoft.com/en-us/library/aa363648(VS.85).aspx
- For more information on Windows Auditing, see here: http://support.microsoft.com/kb/310399
- For instructions on how to configure Windows auditing, refer to the following website: http://technet2.microsoft.com/windowsserver/en/technologies/featured/audit/default.mspx

Section 11: Regularly Test Security Systems and Processes

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.13

In accordance with the PCI-DSS, PAR mandates regular testing of security systems and processes.

Section 12: Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.14

In accordance with the PCI-DSS, PAR mandates a maintained policy that addresses information security. A site's maintained information security policy should include information on physical security, data storage, data transmission and system administration.

Additional Security Information

Granting Temporary System Support Access

To grant temporary support administrative account access, follow these steps:

1. Login as the Administrative Account user.
2. Create a new Administrative Account user utilizing the Support Representative's name with a unique strong password.
3. Grant the Support Representative system access.
4. When the support session ends, disable the Support Representative's user.

Key Management

PA-DSS References 2.4, 2.5, 2.6

PAR has implemented a programmatic, dynamic key management system that requires no human intervention. Keys are generated programmatically and not stored on the system. The dynamic key management system controls the generation and management of cryptographic keys by unique record. There is no customer action required on upgrade.

Example: Keys are stored only in volatile RAM. Pass Phrase is generated using a salt value, never stored, and always generated. Need to provide enough information to be able to defend it. There is no customer configuration or action required.

Web-Based Applications

PixelPoint has no web-based applications as part of the product offering.

Remote Desktop Support & Management

PA-DSS Reference 10.1

PAR's approved remote access tool is GoToAssist, Version 10.x.

To enable a GoToAssist support session, the following steps should be followed:

1. The PAR Remote Support Technician establishes a GoToAssist session.
2. The Store Manager is contacted via telephone and instructed to connect to the Remote
3. Support Session established in step 1.
4. The Store Manager grants temporary access to the store system for the duration of the
5. Remote Support Session. It is this activity that is considered the second authentication factor.

If employees, administrators or vendors can access the application remotely, access should be authenticated using a 2-factor authentication mechanism. Establish and utilize a secure, encrypted methodology for remote desktop support and management utilizing the following recommendations:

- Implement two-factor authentication for remote access to the network and/or POS system by employees, administrators, and third parties.
- If the customer chooses to use Remote Desktop Protocol (RDP) or pcAnywhere over a public network and/or a RAS connection the session needs to be encrypted using 128-bit encryption and the RC4 encryption algorithm.
    - pcAnywhere version 10+ needs to use the serial ID in addition to the username and complex password.
- All remote-access technologies must only be activated when needed by vendors and/or third-party support with immediate deactivation after use.
- PixelPoint will work with RADIUS and VPN data protection.

Software Version Tracking

PixelPoint POS Software is using an YY.MM.DD.x versioning sequence. Builds are made nightly and released once a month. The 'x' represents the sequential non-resettable build number

Examples of this scheme is use are:

17.9.10.154

Release number wildcard updates are delivered when:

- Critical and medium bug fixes are required which have no impact on integrated payment processing logic.
- Usability improvements are required to existing feature sets that have no impact on core functionality and no impact on integrated payment processing functionality or logic.
- Adjustments are required to existing fiscal and labour compliance functionality that has no impact on integrated payment processing functionality or logic

Wildcards are never used for any change that has an impact on security or any PA-DSS requirements.

Any element of the version number used to represent a non-security-impacting change (including wildcard element) must never be used to represent a security impacting change.Any elements to the right of a wildcard cannot be used for a security-impacting change. Version elements reflecting a security-impacting change must appear "to the left" of the first wildcard element.

Security Patches

Ensure that all system components and software have the latest vendor-supplied security patches installed. All critical security patches must be installed in accordance to the PCI DSS guidelines.

Remote Payment Application Updates

PA-DSS Reference 10.2.1

To align with PCI DSS Requirements, all Remote Payment Application Updates are to be delivered using secure methods, such as the Remote Desktop Support & Management section above.

Below are two main points for consideration:

- Activate remote-access technologies for payment application updates only when needed for downloads, and turn off immediately after the download completes.
- If the system is connected via VPN or other high-speed connection, receive remote payment application updates via a securely configured firewall.

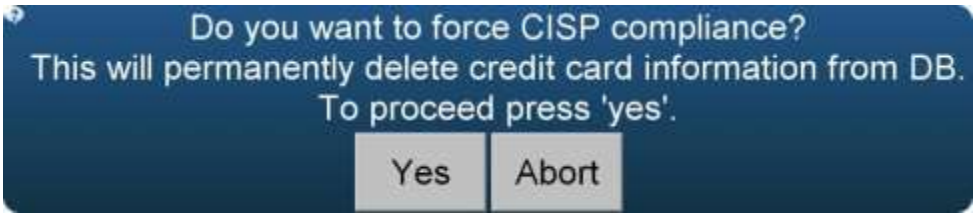
Utilities

Included utility applications which may be used to assist in meeting the PCI DSS include:

Upgrading Older Systems

PixelPoint POS v9 and older did not fall within PA-DSS guidelines. If you are upgrading an existing PixelPoint site from v9.0 or earlier to v17, you will need to upgrade to v10 first.

1. Back up your current database.
2. Upgrade PixelPoint to v9.1 using the relevant upgrade guides.
3. Run PixelPoint POS and BackOffice to perform necessary updates to the database.
4. Back up your upgraded database.
5. Run "EnforceCISPRules.exe" to clear historical credit data. The EXE is in the "\PixelPOS" folder.



If the PixelPoint system is integrated with 3rd party software, it may be necessary to identify whether an upgrade of those files is required. It is also possible that the current version of that software may have log files which are retaining sensitive data (such as the log files from a credit card verification system). Research which (if any) files need to be cleared and whether an upgrade to that software is required for PA-DSS compliance.

Glossary

Backup	A duplicate copy of data made for archiving purposes or for protecting against damage or loss.
BOC / BOH	Back of House Computer
Cardholder	The customer to whom a card has been issued or the individual authorized to use the card.
Complex Password	A password of at least 7 characters with both numeric and alphabetic characters. Preferably (where applicable) with special characters as well. Complex passwords should be changed every 90 days.
DMZ	Demilitarized Zone is a part of the network that is neither part of the internal network nor directly part of the Internet. It basically sits between the two.
Encryption	The process of converting information into a form unintelligible to anyone except holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (inverse to encryption) against unauthorized disclosure.
Firewall	Hardware and/or software that protects the resources of one network from users from other networks. It prevents outsiders from accessing the system's private data resources.
FOH	Front-Of-House POS Terminal
HTTPS	Hypertext Transfer Protocol Secure. This enables the secured transmission of web pages.
IP Address	A numeric code (Internet Protocol address) that uniquely identifies a particular computer on the Internet. A "Static" IP address is one that is assigned to a specific PC and never changes.
Key	In reference to encryption, a key is a value applied using an algorithm to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message.
Magnetic Swipe	A card encoded with a magnetic stripe which contains data identifying the cardholder and other pertinent data. Employee access cards are one example of magnetic swipe cards in which the cardholder logs into the POS. Credit cards are another example of magnetic swipe cards which identify the cardholder's account number and other private information.
Manual Entry Number	Access to PixelPoint POS is possible by applying a numeric access code. It is not as secure as the Magnetic Swipe or Bio-Metric scan methods.
Password	A string of characters that serve as an authenticator of the user.
TLS 1.2	Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet.
Virus	A program or string of code that can replicate itself causing the modification or destruction of software or data.
WPA/WPA2	Wi-Fi Protected Access is a new standard for wireless networks. A certification program developed by the Wi-Fi Alliance to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined the protocol in response to several serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy).

