NETePay 5

Version: 5.06

PA-DSS 3.1 Implementation Guide

Document Version: 0.00

Date: XX August 2015

Document Owners

Lee Morsillo

Vice President - Technology

Datacap Systems, Inc.

Table of Contents

Notice

THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. Datacap Systems MAKES NO REPRESENTATION OR WARRANTY AS TO THE ACCURACY OR THE COMPLETENESS OF THE INFORMATION CONTAINED HEREIN. YOU ACKNOWLEDGE AND AGREE THAT THIS INFORMATION IS PROVIDED TO YOU ON THE CONDITION THAT NEITHER Datacap Systems NOR ANY OF ITS AFFILIATES OR REPRESENTATIVES WILL HAVE ANY LIABILITY IN RESPECT OF, OR AS A RESULT OF, THE USE OF THIS INFORMATION. IN ADDITION, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR MAKING YOUR OWN DECISIONS BASED ON THE INFORMATION HEREIN.

Nothing herein shall be construed as limiting or reducing your obligations to comply with any applicable laws, regulations or industry standards relating to security or otherwise including, but not limited to PCI PA-DSS and DSS.

The merchant may undertake activities that may affect compliance. For this reason, Datacap Systems is required to be specific to only the standard software provided by it.

About this Document

This document describes the steps that must be followed in order for your NETePay 5 installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application - Data Security Standards program (version 3.1 dated May 2015)[1].

Datacap Systems instructs and advises its customers to deploy Datacap Systems applications in a manner that adheres to the PCI Data Security Standard (v3.0). Subsequent to this, best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various "Benchmarks", should be followed in order to enhance system logging, reduce the chance of intrusion and increase the ability to detect intrusion, as well as other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, the disabling of infrequently-used or frequently vulnerable networking protocols and the implementation of certificate-based protocols for access to servers by users and vendors.

You must follow the steps outlined in this *Implementation Guide* in order for your NETePay 5 installation to support your PCI DSS compliance efforts.

[1] PCI PA-DSS 3.1 can be downloaded from the PCI SSC Document Library.

Revision Information

Name	Title	Date of Update	Summary of Changes
NETePay 5	PA-DSS 3.1 Implementation Guide	XX Aug 2015	Document Creation

Note (PA-DSS 13.1): This PA-DSS Implementation Guide will be reviewed on a yearly basis, whenever the underlying application changes or whenever the PA-DSS requirements change. Updates will be tracked and reasonable accommodations will be made to distribute or make the updated guide available to users. Datacap Systems Inc. will distribute the IG to new customers via web download.

Executive Summary

NETePay 5 Ver. 5.06 has been Payment Application - Data Security Standard (PA-DSS) validated, in accordance with PA-DSS Version 3.1. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Coalfire Systems, Inc. 361 Centennial Parkway Suite 150 Louisville, CO 80027	Coalfire Systems, Inc. 1633 Westlake Ave N #100 Seattle, WA 98109

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document then provides specific installation, configuration, and ongoing management best practices for using Datacap Systems's NETePay 5 Version 5.06 as a PA-DSS validated Application operating in a PCI DSS compliant environment.

PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs (PA-DSS, PCI DSS, etc):

- Payment Card Industry Payment Applications - Data Security Standard (PCI PA-DSS)
  https://www.pcisecuritystandards.org/security_standards/index.php
- Payment Card Industry Data Security Standard (PCI DSS)
  https://www.pcisecuritystandards.org/security_standards/index.php
- Open Web Application Security Project (OWASP)
  http://www.owasp.org
- Center for Internet Security (CIS) Benchmarks (used for OS Hardening)
  https://benchmarks.cisecurity.org/downloads/multiform/

Application Summary

Payment Application Name	NETePay 5	Payment Application Version	5.06

Application Description

NETePay is client-server based payment middleware designed to integrate with POS systems needing payment capabilities for a wide variety of transaction types, markets and processing providers.

NETePay 5 is an application that resides on a server that monitors encrypted transaction requests from client machines using a POS or restaurant application integrated with DSIClientX, dsiPDCX or dsiEMVX Datacap's ActiveX controls.

When NETePay 5 receives an encrypted transaction request from a client machine using DSIClientX, dsiPDCX or dsiEMVX, it sends the request directly to the payment processor host for approval via the Internet using the secure protocol specified by the processor. The approved but unsettled transactions are stored encrypted in a database that resides on the server with NETePay 5. Once transactions are settled, cardholder data is permanently deleted (truncated).

NETePay removes the need for POS software to have any interaction with or visibility to cardholder data. By eliminating the need to handle, transmit or store any type of cardholder information, NETePay may provide POS software systems with a streamlined path to achieve PA-DSS compliance.

Some of the POS systems developers who have incorporated the NETePay dsiPDCX or dsiEMVX interface are: * Ace Retail * Brink Software * Intercard * Logivision * OmniTerm * Osprey Retail * Sky View Logic * Smyth Retail * Squirrel Systems * Ultimate Retailer * dsitrib-u-tec * Cap Retail * Lucas Systems * The EdgePOS * JKSoft * Flo POS * Pipeline Software * Topline Software * Café Cartel * MCR POS * CigarBox Software * Pensmore * POSi-Tab * Tyger POS * Skywire POS * iVend * UnTill * Oceanside Software * POSKioskSoftware * PDQ Signature Systems. In addition, NETePay offers an EMV interface solution option. Some of the POS systems developers who have incorporated the NETePay dsiEMVClientX interface are: * Acme POS * Auphan Software * ECR Software * CenterEdge Software * Digital Dining * Future Point of Sale * Ideal POS * Logivision * Maitre'D * Pixel Point * RDC Positouch * Restaurant Manager * Samco Software * Squirrel Systems * Vivonet * Volante Systems * WIN POS * Windward Software * distrib-u-tec

Typical Role of Application

NETePay 5 is payment middleware typically integrated with POS (or other) software to enable secure payments via the Internet or dial backup for Retail, Restaurant, MOTO industry segments.

Target Market for Payment Application

Target Market for Payment Application (check all that apply):					
X	Retail		Processors		Gas/Oil
	e-Commerce	X	Small/medium merchants		
X	Others (please specify): Restaurant, MOTO				

Stored Cardholder Data

The following is a brief description of files and tables that store cardholder data:	
File or Table Name	Description of Stored Cardholder Data

	MS SQLExpress (custom instance) Versions Supported: 2005 2008 R2 DB: MSSQL$DatacapInstance Files: dbnetepay.mdf dbnetepay.ldf Tables: batch, version	PAN (Primary Acct No.) Expiration Date
	Individual access to cardholder data is logged as follows: NETePay 5 does not log full text PAN's or expiration dates in any context - only truncated data (i.e. last 4 digits, of PAN's) are recorded. Since NETePay 5 only logs truncated cardholder data, it does not track or record log access activity.	
Components of the Payment Application	The following are the application-vendor-developed components which comprise the payment application:	
	NETePay.exe: Wndows desktop application that provides transaction processing services for requests received from DSIClientX, dsiPDCX or dsiEMVX direct to Payment Service Provider using secure protocols over the Internet. **DSIClientX.ocx, dsiPDCX.ocx or dsiEMVX.ocx:** Windows ActiveX controls integrated with third party POS software on primary POS terminals that communicate transactions requests securely to NETePay application. **SQLExpress:** A customized Datacap instance (MSSQL$DatacapInstance) installed with NETePay for secure storage of unsettled transactions.	
Required Third Party Payment Application Software	The following are additional third party payment application components required by the payment application:	
	None	
Database Software Supported	The following are database management systems supported by the payment application:	
	Microsoft SQLExpress	
Other Required Third Party Software	The following are other required third party software components required by the payment application:	
	None	
Operating System(s) Supported	The following are Operating Systems supported or required by the payment application:	
	• Windows 7 • Windows 8 • Windows 10 • Windows Server 2008 • Windows Server 2012	
Application Authentication	During installation, NETePay installs a license file that contains data whereby we know	

<table>
<tr><td></td><td>the product has been successfully activated and therefore it is valid to use it for processing. The same license file contains the merchant settings. There is no other authentication data. The license file is encrypted, proprietary to Protection Plus.</td></tr>
<tr><td>Application Encryption</td><td>See the ePay Crypto Overview section at the end of this document.</td></tr>
<tr><td>Application Functionality Supported</td><td>Payment Application Functionality (check only one):
<table>
<tr><td></td><td>Automated Fuel Dispenser</td><td></td><td>POS Kiosk</td><td></td><td>Payment Gateway/Switch</td></tr>
<tr><td></td><td>Card-Not-Present</td><td></td><td>POS Specialized</td><td>X</td><td>Payment Middleware</td></tr>
<tr><td></td><td>POS Admin</td><td></td><td>POS Suite/General</td><td></td><td>Payment Module</td></tr>
<tr><td></td><td>POS Face-to-Face/POI</td><td></td><td>Payment Back Office</td><td></td><td>Shopping Cart & Store Front</td></tr>
</table></td></tr>
<tr><td>Payment Processing Connections:</td><td>NETePay 5 is a Windows desktop application that resides on a computer running the Windows operating system that monitors encrypted transaction requests via IP from client machines using a POS or restaurant application exclusively integrated with DSIClientX, dsiPDCX or dsiEMVX, Datacap’s ActiveX controls.

When NETePay 5 receives an encrypted transaction request from a client machine using DSIClientX, dsiPDCX, or dsiEMVX, it transforms the request into a format required by the specific payment processor and sends it directly to the processing host for approval using the secure protocol specified by the processor via the Internet or VPN.

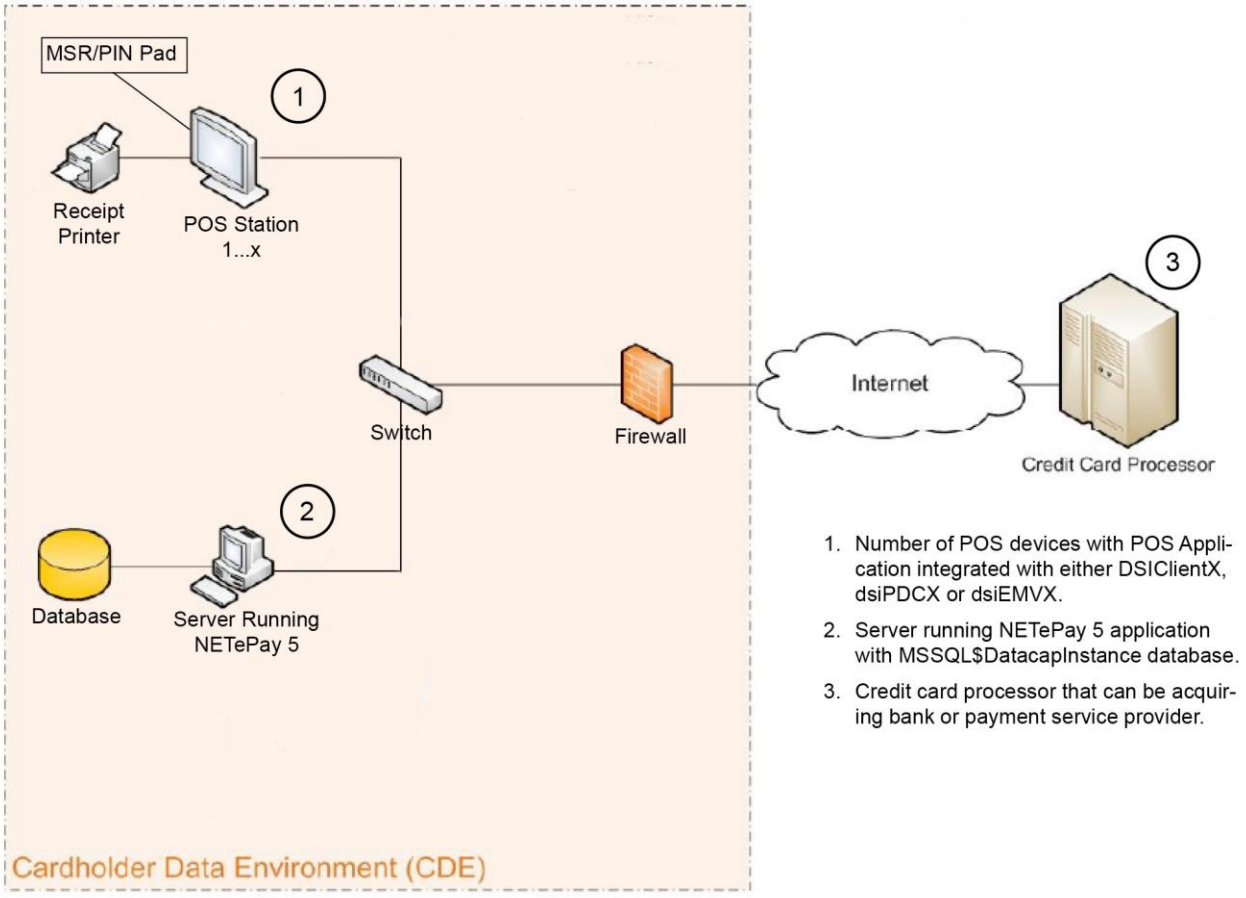
The processing host returns a reply directly to NETePay 5 using the processor’s specified secure protocol via the Internet. NETePay 5 reformats the response and returns the reply to the requesting client control using a secure connection.

For terminal based processing providers, the approved but unsettled transactions are stored encrypted in a database that resides on the server with NETePay 5. Once transactions are settled, cardholder data is permanently deleted (truncated) from the database. Installations of NETePay 5 utilizing host based processing providers does not utilize a database.</td></tr>
<tr><td>Description of Listing Versioning Methodology (PA-DSS 5.4.4)</td><td>NETePay 5 versioning has three levels, Major, Minor, and Build:

• Major changes include significant changes to the application and would have an impact on PA-DSS requirements.
• Minor changes include small changes such as minor enhancements and may or may not have an impact on PA-DSS requirements.
• Build changes include bug fixes or rollups and would have no negative impact on PA-DSS requirements and are indicated by the WILDCARD (X).

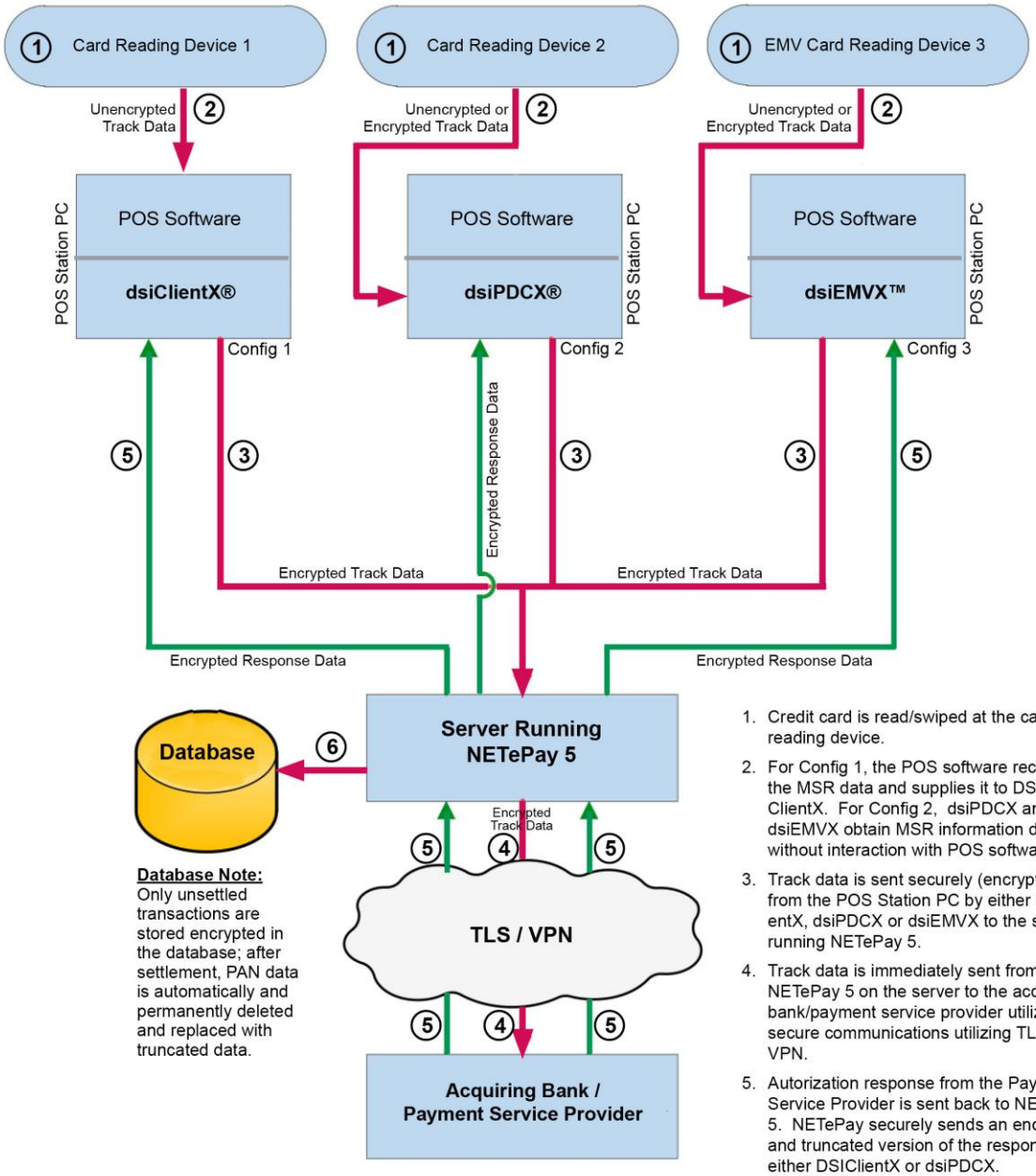
Based on the above versioning methodology the application version being listed with the PCI SSC is: 5.06</td></tr>
</table>

NETePay 5 - Typical Network Implementation



1. Number of POS devices with POS Application integrated with either DSIClientX, dsiPDCX or dsiEMVX.
2. Server running NETePay 5 application with MSSQL$DatacapInstance database.
3. Credit card processor that can be acquiring bank or payment service provider.

NETePay 5 - Credit/Debit Cardholder Dataflow Diagram



Notes:

1. No MSR track, CVV or PIN data is stored at any time.
2. PAN is not stored if transaction request is not approved.
3. Only unsettled transactions are stored encrypted in the database; after settlement, PAN data is permanently deleted and replaced with truncated data.
4. DSIClientX, dsiPDCX and dsiEMVX have no persistent data storage capability and never retain any cardholder data.

Difference between PCI Compliance and PA-DSS Validation

As a software vendor who develops payment applications, our responsibility is to be "PA-DSS Validated." We have performed an assessment and payment application validation review with our independent assessment firm (PAQSA), to ensure that our platform does conform to industry best practices when handling, managing and storing payment related information.

PA-DSS Version 3.1 is the standard against which Payment Application has been tested, assessed, and validated.

PCI Compliance is then later obtained by the merchant, and is an assessment of your actual server (or hosting) environment called the Cardholder Data Environment (CDE).

Obtaining "PCI Compliance" is the responsibility of you the merchant and your hosting provider, working together, using PCI compliant architecture with proper hardware & software configurations and access control procedures.

The PA-DSS Validation is intended to ensure that NETePay 5 will help you facilitate and maintain PCI Compliance with respect to how the payment application handles user accounts, passwords, encryption, and other payment data related information.

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process, or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

The 12 Requirements of the PCI DSS:

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*

Considerations for the Implementation of Payment Application in a PCI-Compliant Environment

The following areas must be considered for proper implementation in a PCI-Compliant environment.

- ✓ Remove Historical Sensitive Authentication Data
- ✓ Handling of Sensitive Authentication Data
- ✓ Secure Deletion of Cardholder Data
- ✓ All PAN is masked by default
- ✓ Cardholder Data Encryption & Key Management
- ✓ Removal of Historical Cryptographic Material

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4)

Previous versions of NETePay 5 did not store sensitive authentication data. Therefore, there is no need for secure deletion of this historical data by the application as required by PA-DSS v3.1.

Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

Datacap Systems does not store Sensitive Authentication Data for any reason. We strongly recommend that you do not store Sensitive Authentication Data for any reason. However, if you should do so, the preceding guidelines must be followed when dealing with Sensitive Authentication Data used for pre-authorization (swipe data, validation values or codes, PIN or PIN block data):

- Collect sensitive authentication data only when needed to solve a specific problem
- Store such data only in specific, known locations with limited access
- Collect only the limited amount of data needed to solve a specific problem
- Encrypt sensitive authentication data while stored
- Securely delete such data immediately after use

Secure Deletion of Cardholder Data (PA-DSS 2.1)

The following guidelines must be followed when dealing with Cardholder Data (Primary Account Number (PAN); Cardholder Name; Expiration Date; or Service Code):

- A customer defined retention period must be defined with a business justification.
- Cardholder data exceeding the customer-defined retention period or when no longer required for legal, regulatory, or business purposes must be securely deleted.
- Here are the locations of the cardholder data you must purge:

  Files: dbnetepay.mdf *and* dbnetepay.ldf
  Tables: MSSQL$DatacapInstance – Tables: batch, version

- To purge the cardholder data you must do the following two things:

  1. The application automatically and permanently purges (truncates) settled transactions. Unsettled transactions are stored in encrypted form. A user may manually purge all transactions by removing the database using the Datacap Systems Inc supplied *NETePay Database Utility* as to delete the previous NETePay database, any backups and all logs:

  1. Shut down **NETePay**
  2. Using Windows Control Panel, select Add/Remove Programs
  3. Select **NETePay** and remove it
  4. Locate the **NETePay** folder in **<bootdrive>:/Program Files/Datacap Systems** and use a secure file deletion utility to remove it. (Such as Eraser {http://eraser.heidi.ie} or Microsoft SDelete {http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx})
  5. Install **NETePay 5.0**
  6. From the **Programs/Software from Datacap** group, run the **NETePay Database Manager**
  7. Select Connect
  8. Select Create New Database
  9. Shut down **NETePay Database Manager**
  10. Start **NETePay 5.0**

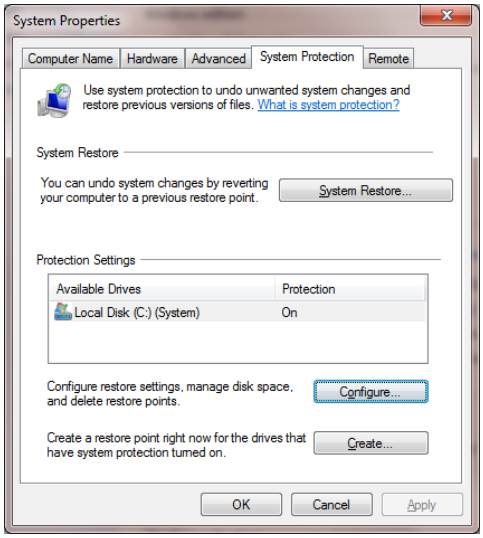
  Important Note: Unsettled transactions should be settled before performing the procedure outlined above. Any unsettled transactions in the database when purged will be permanently lost.

  2. In the operating system you must configure appropriate settings to prevent inadvertent retention of cardholder data.

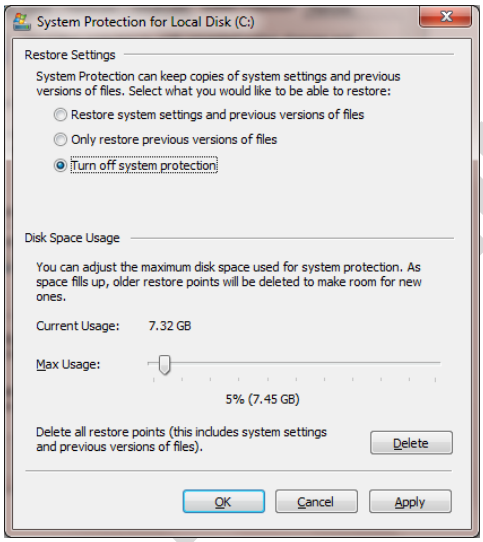
To Address Inadvertent Capture of PAN on Windows 7:

Disabling System Restore – Windows 7

- Right Click on Computer > Select “Properties”
- Select “System Protection” on the top left list, the following screen will appear:



- Select Configure, the following screen will appear:

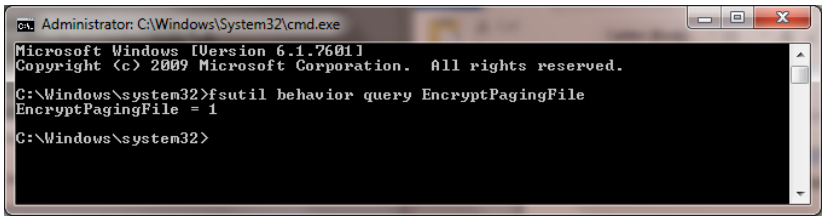


- Select “Turn off system protection”
- Click apply, and OK to shut the System Protection window
- Click OK again to shut the System Properties window
- Reboot the computer

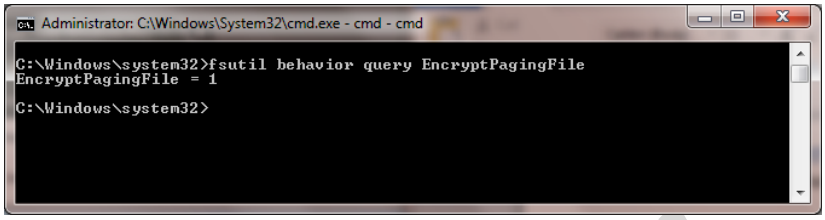
Encrypting the System PageFile.sys – Windows 7

* Please note that in order to perform this operation the hard disk must be formatted using NTFS.

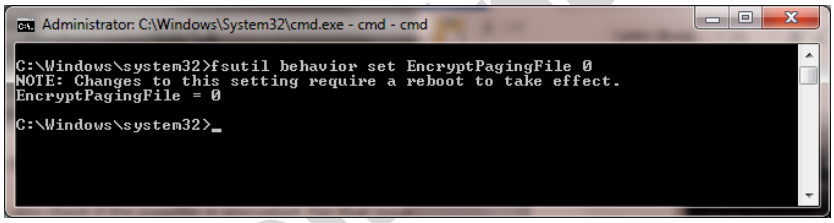
- Click on the Windows “Orb” and in the search box type in “cmd”.
- Right click on cmd.exe and select “Run as Administrator”
- To Encrypt the Pagefile type the following command: fsutil behavior set EncryptPagingFile 1



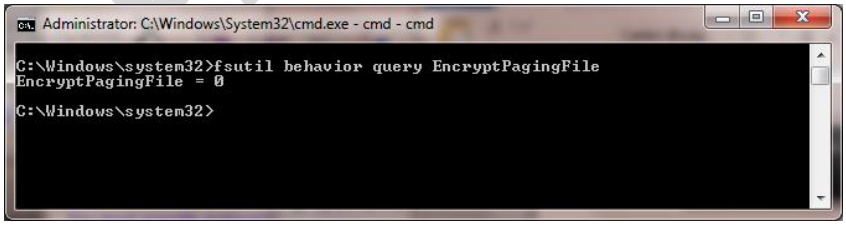
- To verify configuration type the following command: fsutil behavior query EncryptPagingFile



- 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



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



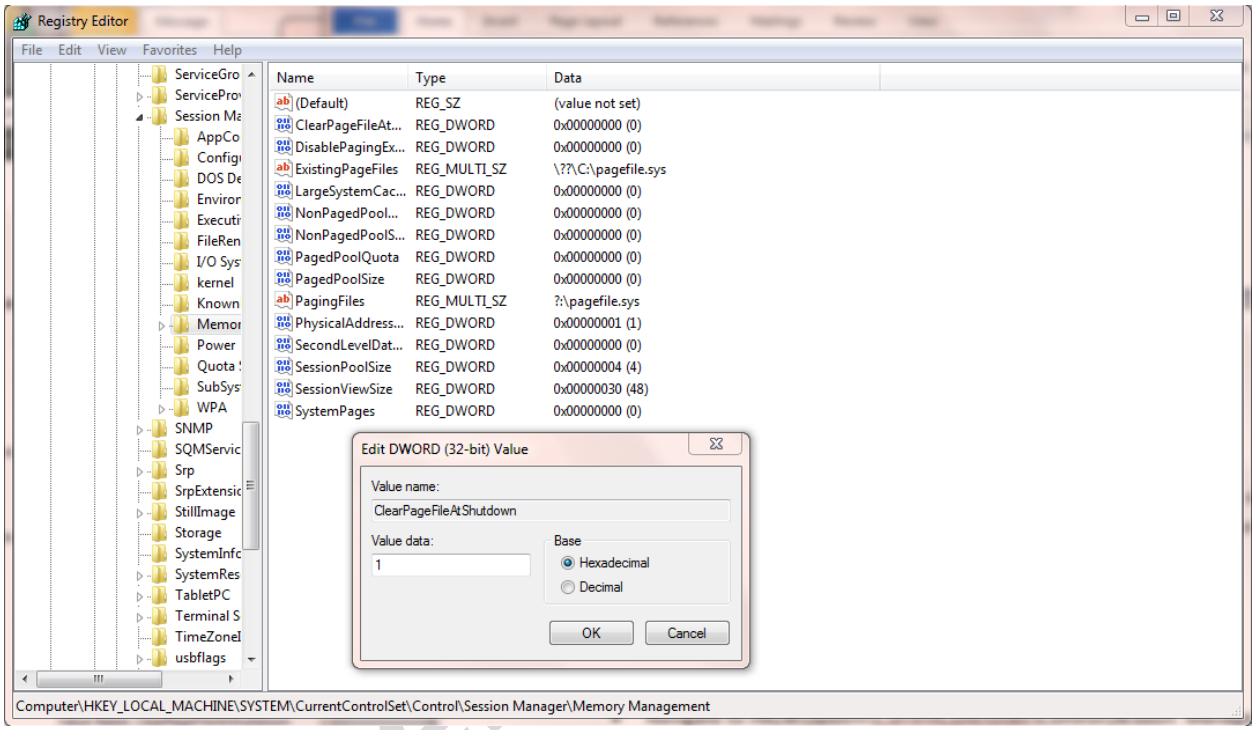
- If encryption is disabled EncryptPagingFile = 0 should appear

Clear the System Pagefile.sys on shutdown – Windows 7

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.

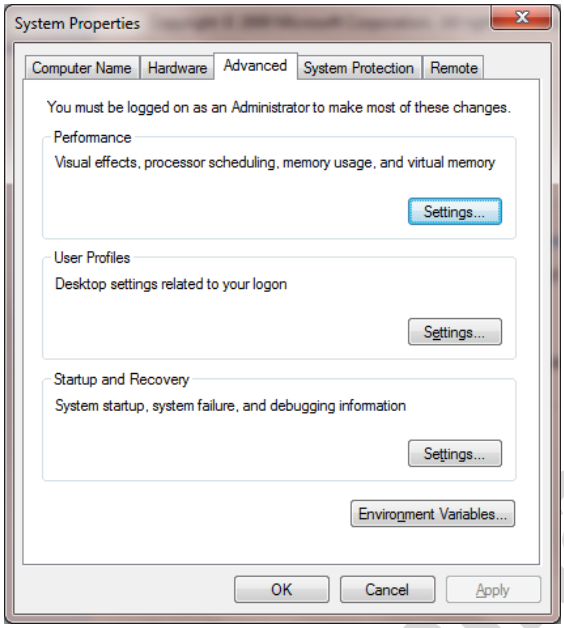
- Click on the Windows “Orb” and in the search box type in “regedit”.
- Right click on regedit.exe and select “Run as Administrator”
- Navigate to HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
- Change the value from 0 to 1
- Click OK and close Regedit



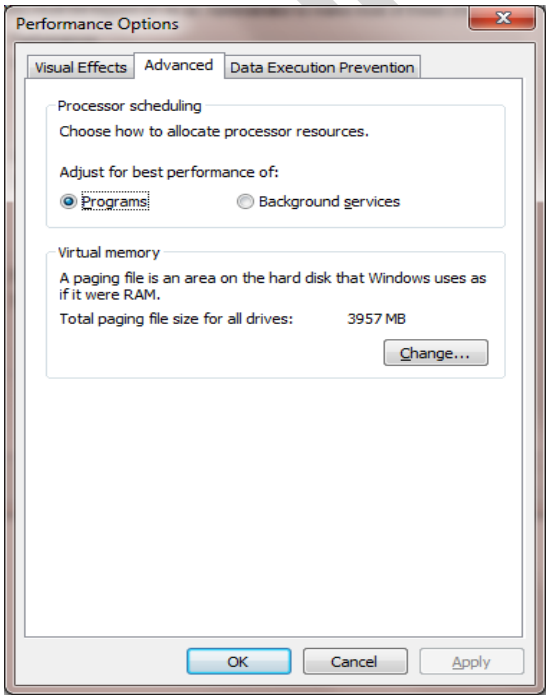
- If the value does not exist, add the following:
  - Value Name: ClearPageFileAtShutdown
  - Value Type: REG_DWORD
  - Value: 1

Disable System Management of PageFile.sys – Windows 7

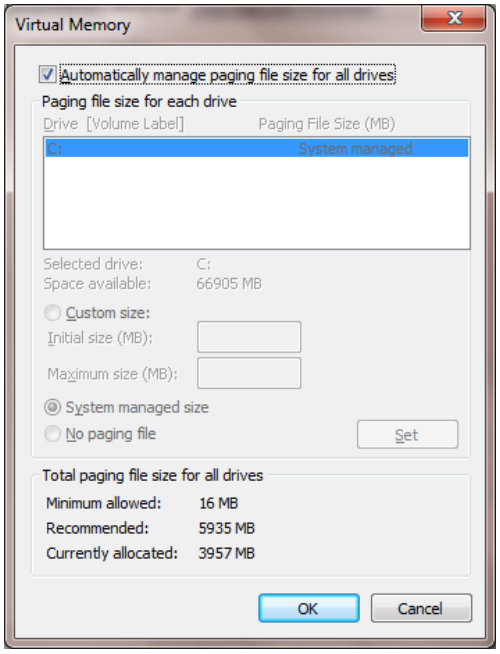
- Right Click on Computer > Select “Properties”
- Select “Advanced System Settings” on the top left list, the following screen will appear:



- Under performance select “Settings” and go to the “Advanced” tab, the following screen will appear:



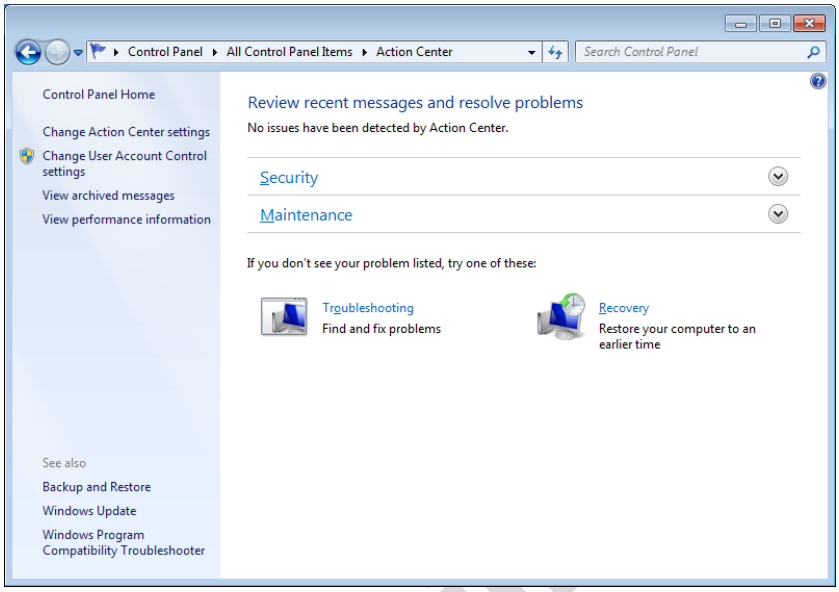
- Select “Change” under Virtual Memory, the following screen will appear:



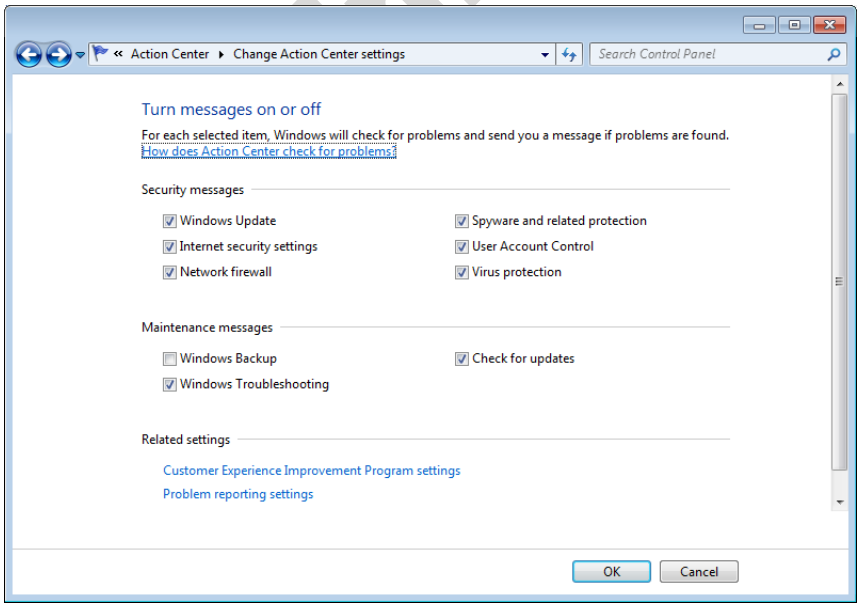
- Uncheck “Automatically manage page file size for all drives”
- Select “Custom Size”
- Enter the following for the size selections:
  - Initial Size – as a good rule of thumb, the size should be equivalent to the amount of memory in the system.
  - Maximum Size – as a good rule of thumb, the size should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

Disable Windows Error Reporting – Windows 7

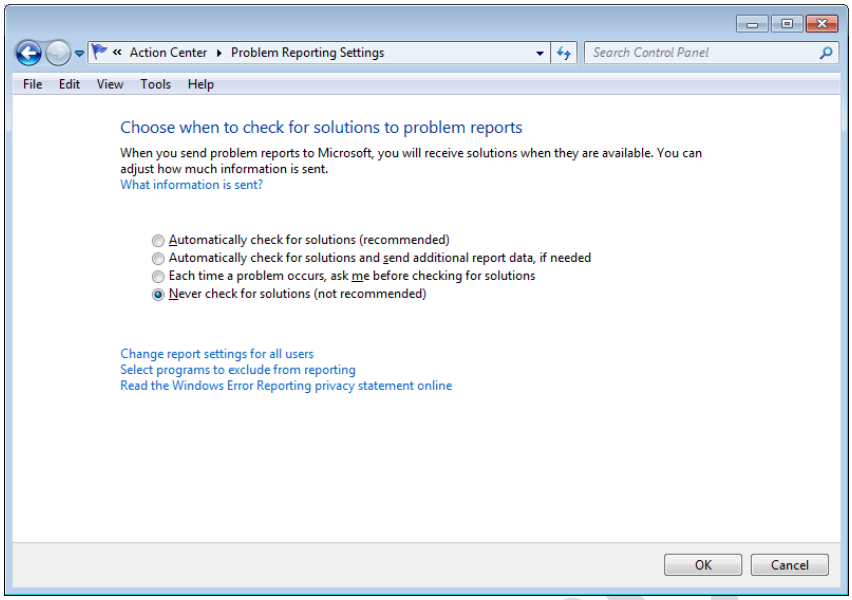
- Open the Control Panel
- Open the Action Center
- Select “Change Action Center Settings”



- Select “Problem Reporting Settings”



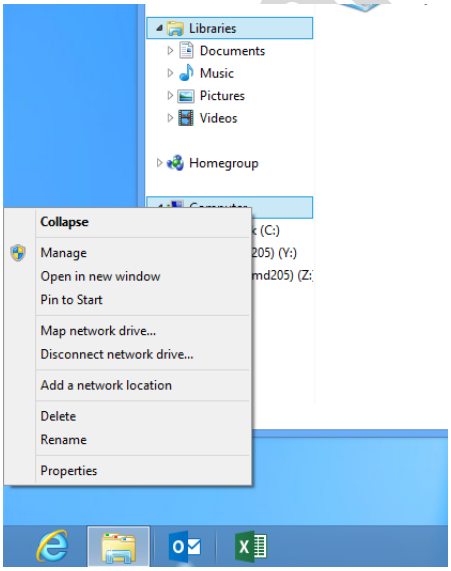
- Select “Never Check for Solutions”



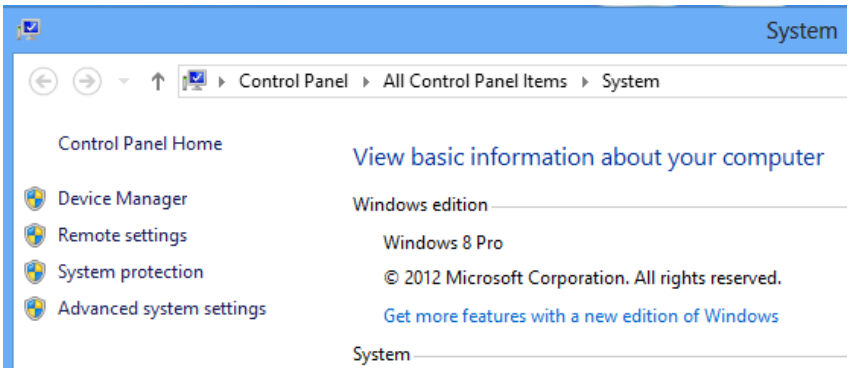
To Address Inadvertent Capture of PAN on Windows 8:

Disable System Restore – Windows 8

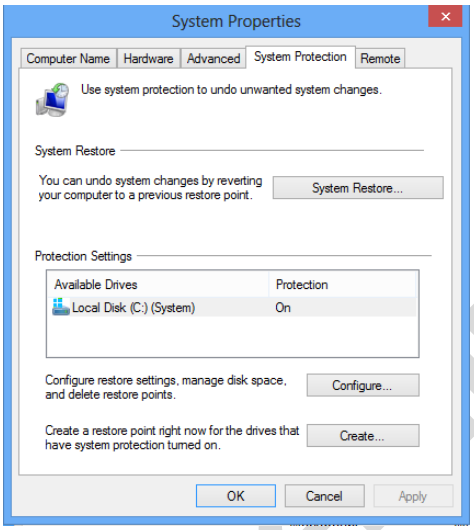
- Right Click on Computer > Select “Properties”:



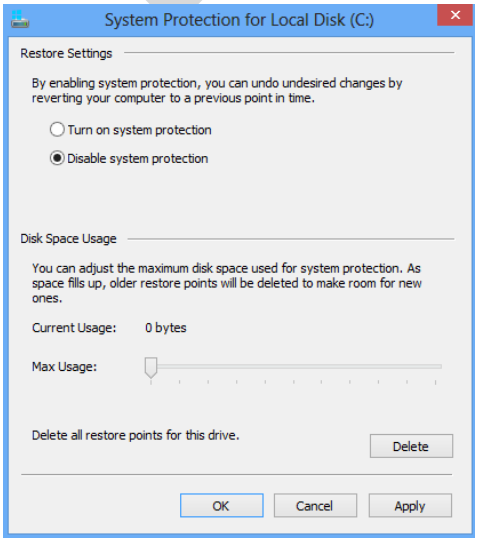
- Select “Advanced System Settings” from the System screen:



- Select “System Protection” on the top left list, the following screen will appear:



- Select Configure, the following screen will appear:



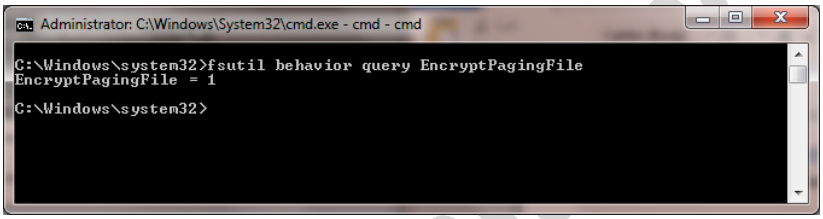
- Select “Disable system protection”

- Click apply, and OK to shut the System Protection window
- Click OK again to shut the System Properties window
- Reboot the computer

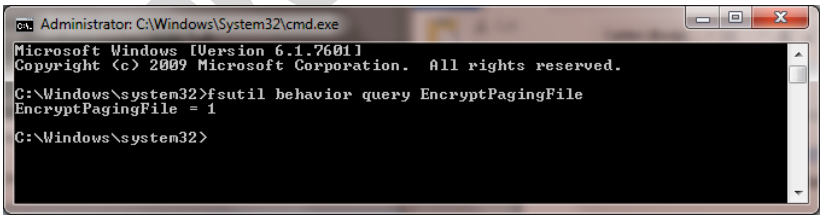
Encrypt PageFile.sys – Windows 8

* Please note that in order to perform this operation the hard disk must be formatted using NTFS.

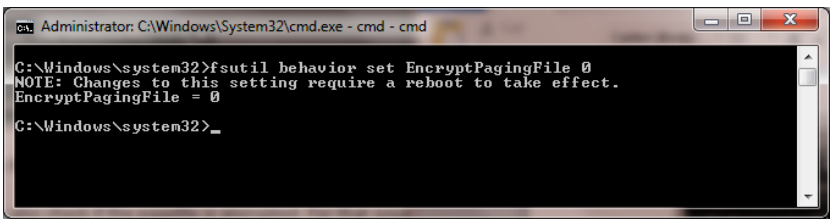
- From the desktop hold down the “Windows” key and type “F” to bring up the “Search” charm, select “Apps” in the “Apps” box type in “cmd”.
- Right click on “Command Prompt” icon located on the left side of your screen, a selection bar will appear at the bottom of the screen, select “Run as Administrator”
- 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
- To Encrypt the Pagefile type the following command: fsutil behavior set EncryptPagingFile 1



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

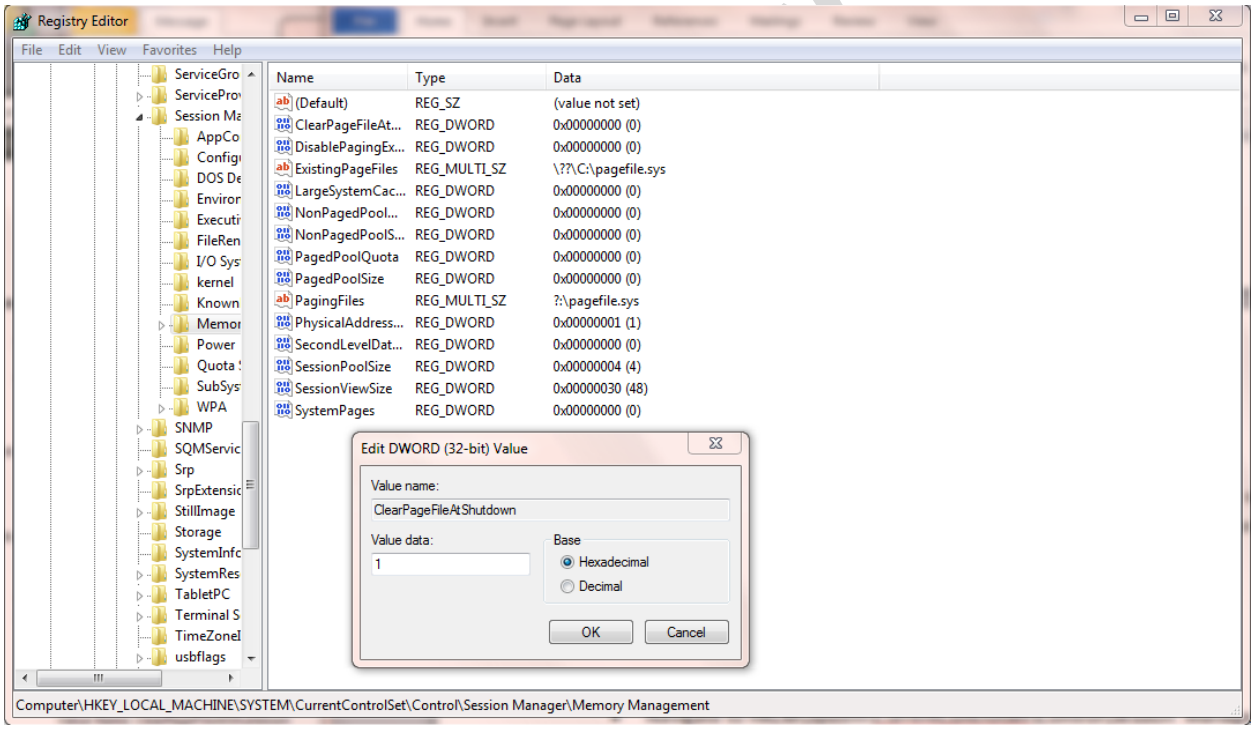


Clear the System Pagefile.sys on shutdown – Windows 8

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.

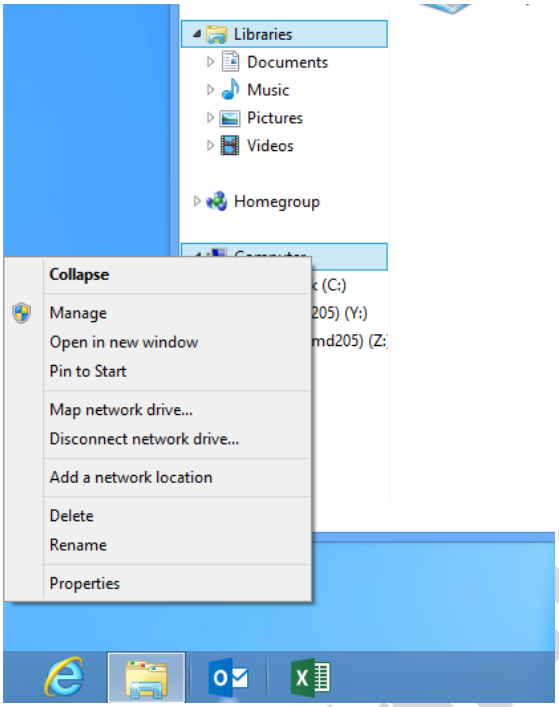
- From the desktop hold down the “Windows” key and type “F” to bring up the “Search” charm, select “Apps” in the “Apps” box type in “regedit”.
- Right click on regedit.exe and select “Run as Administrator”
- Navigate to HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
- Change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



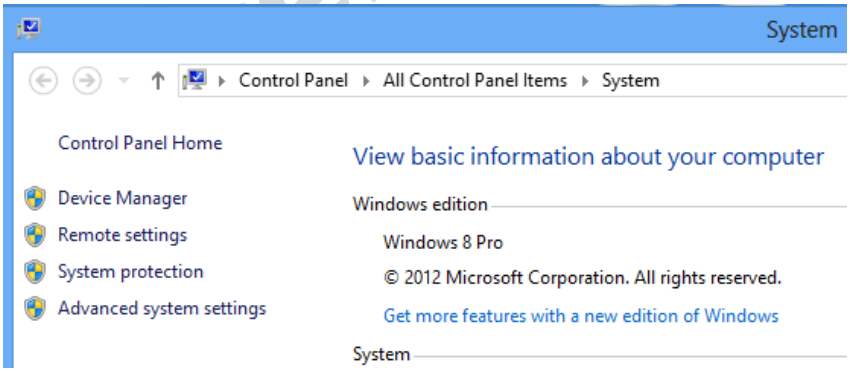
- If the value does not exist, add the following:
  - Value Name: ClearPageFileAtShutdown
  - Value Type: REG_DWORD
  - Value: 1

Disable System Management of PageFile.sys – Windows 8

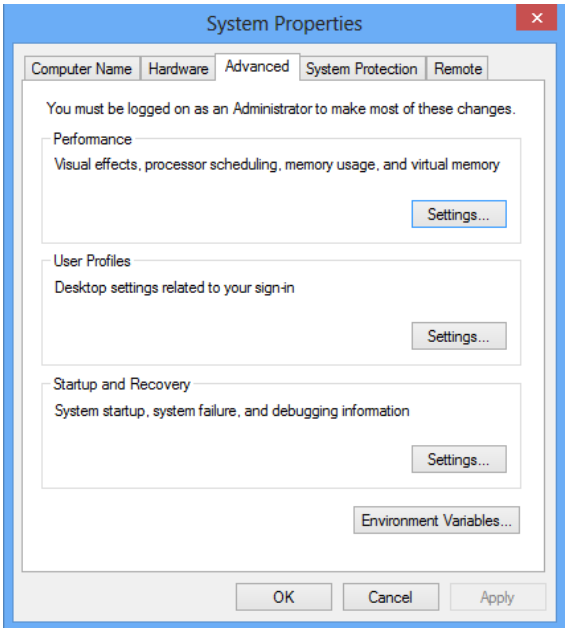
- Right Click on Computer > Select “Properties”:



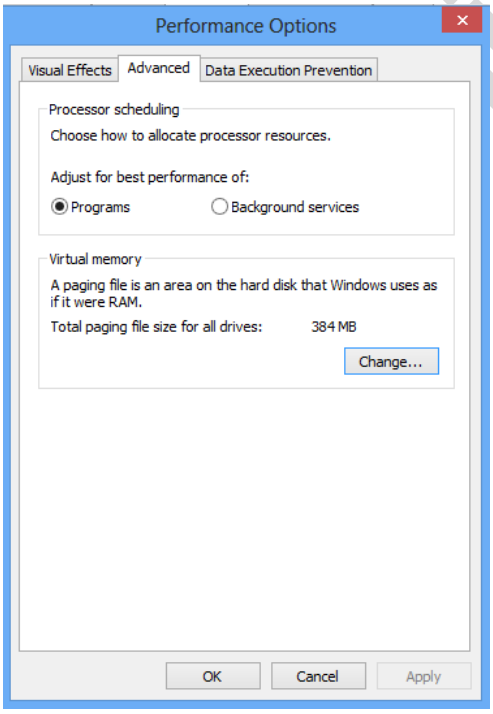
- Select “Advanced System Settings” from the System screen:



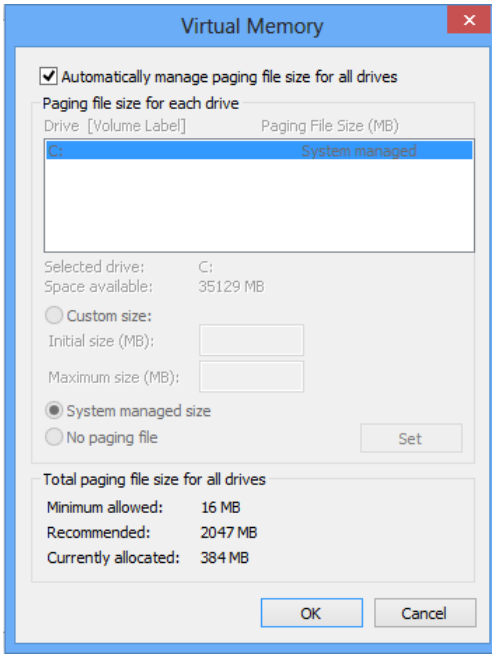
- Select the “Advanced” tab:



- Under performance select “Settings” and go to the “Advanced” tab, the following screen will appear:



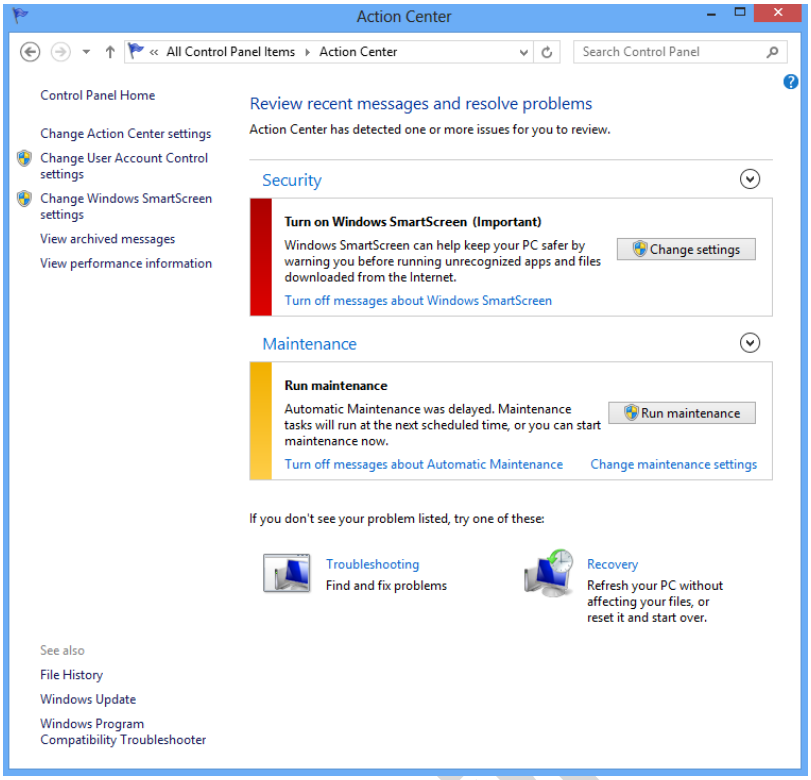
- Select “Change” under Virtual Memory, the following screen will appear:



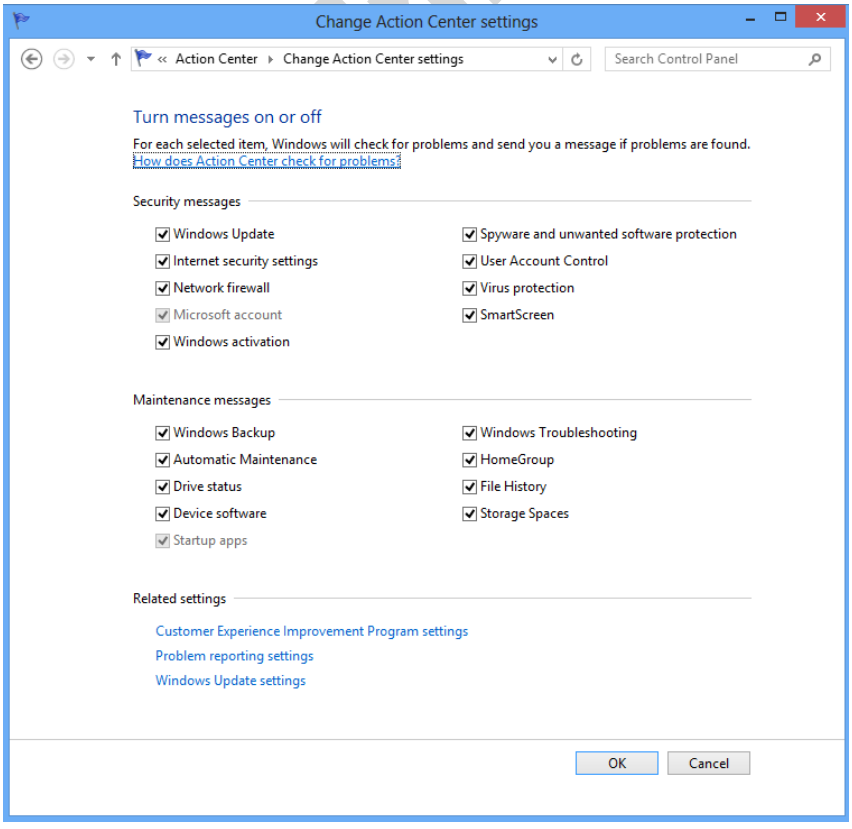
- Uncheck “Automatically manage page file size for all drives”
- Select “Custom Size”
- Enter the following for the size selections:
  - Initial Size – as a good rule of thumb, the size should be equivalent to the amount of memory in the system.
  - Maximum Size – as a good rule of thumb, the size should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

Disable Windows Error Reporting – Windows 8

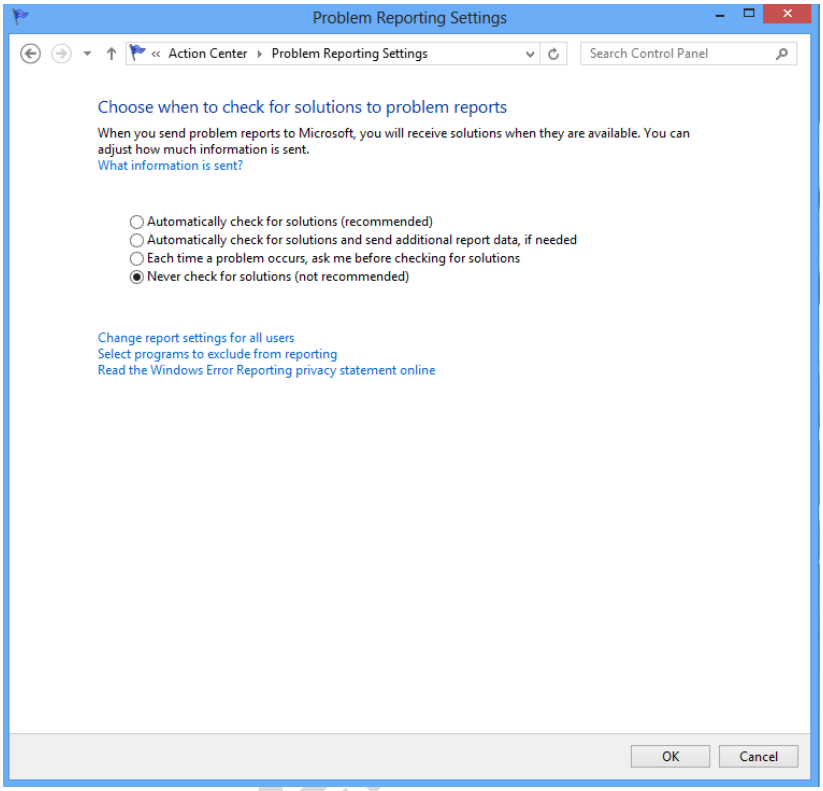
- From the desktop hold down the “Windows” key and type “I” to bring up the “Settings” charm, select “Control Panel”.
- Open the Action Center
- Select “Change Action Center Settings”:



- Select “Problem Reporting Settings”:



- Select “Never Check for Solutions”:



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

Any cardholder data you store outside of the application must be documented and you must define a retention period at which time you will purge (render irretrievable) the stored cardholder data.

All PAN is Masked by Default (PA-DSS 2.2)

NETePay 5 does not have the ability to display full PAN for any reason and therefore there are no configuration details to be provided as required for PA-DSS v3.1.

Cardholder Data Encryption & Key Management (PA-DSS 2.3, 2.4, and 2.5)

NETePay 5 does store cardholder data and does not have the ability to output PAN data for storage outside of the payment application. NETePay 5 uses an encryption methodology with

dynamically generated keys to automatically encrypt all locations/methods where cardholder data is stored.

NETePay 5 does not output PAN for use or storage in a merchants environment for any reason therefore there are no location or configuration details to provide as required by PA-DSS v3.1.

The following key management functions are performed automatically by NETePay 5 using 3DES 192bit dynamic encryption key methodology and there are no key custodians or intervention required by customers or resellers/integrators.

- Generation of strong cryptographic keys.
- Secure cryptographic key distribution.
- Secure cryptographic key storage.
- Cryptographic key changes for keys that have reached the end of their cryptoperiod.
- Retire or replace keys when the integrity of the key has been weakened and/or when known or suspected compromise. If retired or replaced cryptographic keys are retained, the application cannot use these keys for encryption operations.
- Manual clear-text cryptographic key-management procedures require split knowledge and dual control of keys.
- Prevention of unauthorized substitution of cryptographic keys.

Removal of Historical Cryptographic Material (PA-DSS 2.6)

NETePay 5 has the following versions that previously encrypted cardholder data:

- Version 5.00
- Version 5.05
- NETePay 5 uses previously validated encryption algorithms that are PCI Compliant. Therefore there is no need to render historical cryptographic keys or cryptograms irretrievable as they are still in use by the payment application.

Set up Strong Access Controls (3.1 and 3.2)

The PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by more than one user or process.

Authentication credentials are not generated or managed by the payment application. Instead, authentication credentials used by the payment application are provided by the Windows operating system. To maintain PCI DSS compliance the following 11 points must be followed per the PCI DSS:

1. You must not use or require the use of default administrative accounts for other necessary or required software (for example, database default administrative accounts) (PCI DSS 2.1 / PA-DSS 3.1.1)

2. You must assign unique IDs for all user accounts. (PCI DSS 8.1.1 / PA-DSS 3.1.3). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated below.*
3. You must provide at least one of the following three methods to authenticate users: (PCI DSS 8.2 / PA-DSS 3.1.4). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated below.*
    a. Something you know, such as a password or passphrase
    b. Something you have, such as a token device or smart card
    c. Something you are, such as a biometric
4. You must NOT require or use any group, shared, or generic accounts and passwords (PCI DSS 8.5 / PA-DSS 3.1.5). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated below.*
5. You must configure passwords must to be at least 7 characters and includes both numeric and alphabetic characters (PCI DSS 8.2.3 / PA-DSS 3.1.6). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated below.*
6. You must configure passwords to be changed at least every 90 days (PCI DSS 8.2.4 / PA-DSS 3.1.7). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated below.*
7. You must configure passwords so that password history is kept and requires that a new password is different than any of the last four passwords used (PCI DSS 8.2.5 / PA-DSS 3.1.8). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated below.*
8. The payment application limits repeated access attempts by locking out the user account after not more than six logon attempts (PCI DSS 8.1.6 / PA-DSS 3.1.9). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated below.*
9. The payment application sets the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (PCI DSS 8.1.7 / PA-DSS 3.1.10). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated below.*
10. The payment application requires the user to re-authenticate to re-activate the session if the application session has been idle for more than 15 minutes. (PCI DSS 8.1.8 / PA-DSS 3.1.11). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated below.*

You must assign strong passwords to any default accounts (even if they won't be used), and then disable or do not use the accounts.

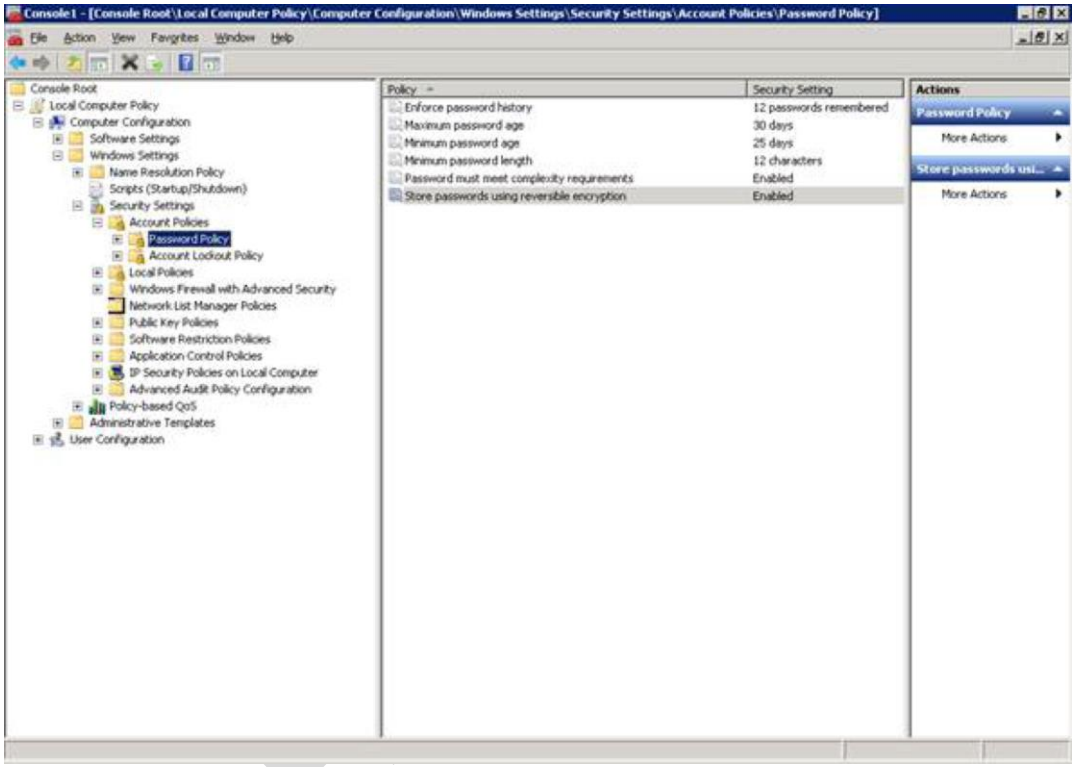
These same account and password criteria from the above 10 or 11 requirements must also be applied to any applications or databases included in payment processing to be PCI compliant. NETePay 5, as tested in our PA-DSS validation, meets, or exceeds these requirements.

PA-DSS 3.2: Control access, via unique username and PCI DSS-compliant complex passwords, to any PCs or servers with payment applications and to databases storing cardholder data.

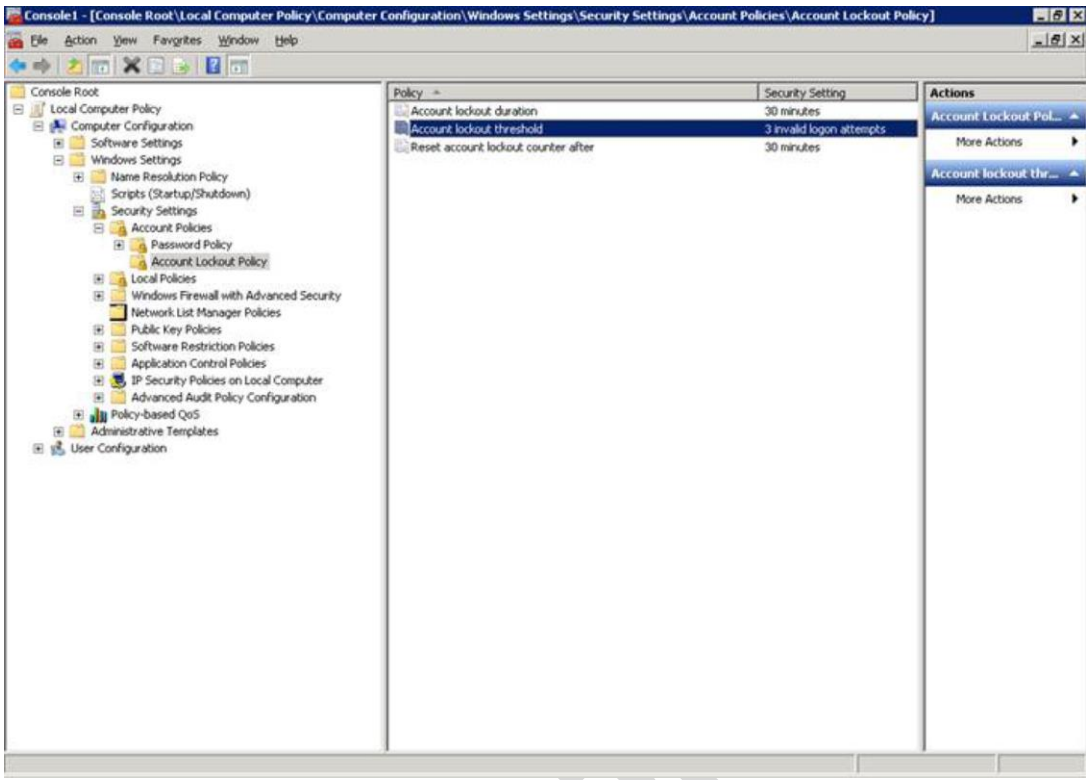
Establishing a Windows Secure Group Access Policy

Users should configure a Windows secure group access policy on the machine on which NETePAY 5 is installed.

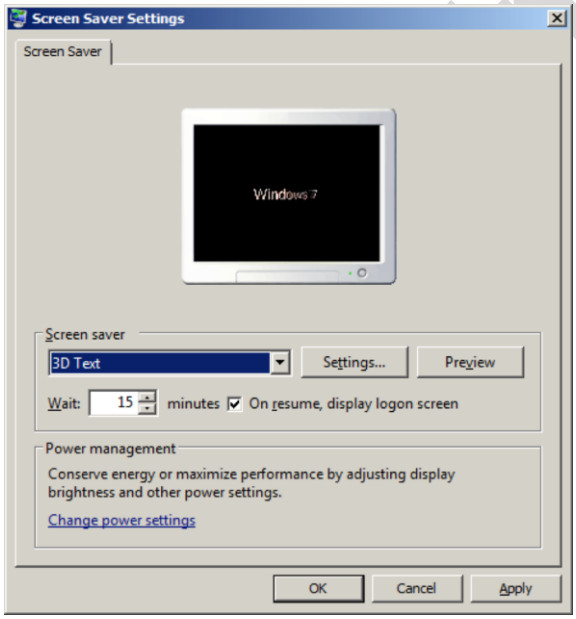
Your Windows operating system environment must be modified to comply with the above requirements. Access these settings by going to Start/Run and type MMC. Add the snap-in for Group Policy Editor and change the security settings as shown below. Under Account Policies select Password Policy and change the settings to the recommended settings shown to enforce password history, password age, password complexity and password encryption:



In addition to setting the password duration and complexity, you should also change the default settings for account lockout policy as shown below. The account should be locked out after three invalid login attempts for a minimum of 30 minutes:



Local client machines or desktops must be configured to have a screen saver that is password protected that will be enabled if the system sits idle for 15 minutes:



Properly Train and Monitor Admin Personnel

It is your responsibility to institute proper personnel management techniques for allowing admin user access to cardholder data, site data, etc. You can control whether each individual admin user can see credit card PAN (or only last 4).

In most systems, a security breach is the result of unethical personnel. So pay special attention to whom you trust into your admin site and who you allow to view full decrypted and unmasked payment information.

Log settings must be compliant (PA-DSS 4.1.b, 4.4.a, 4.4.b)

4.1.b: NETePay 5 has PA-DSS compliant logging enabled by default. This logging is not configurable and may not be disabled. Disabling or subverting the logging function of NETePay 5 in any way will result in non-compliance with PCI DSS.

4.4.b: NETePay 5 facilitates centralized logging.

NETePay 5 records logs of all activity initiated by a DSIClientX, dsiPDCX or dsiEMVX clients. The logs do not record any sensitive cardholder information. Only truncated PAN's and truncated expiration dates are included in the logs. The log files are in the following location on the install volume:

/Program Files/Datacap Systems/NETePay/DATACAP_LOGS

Log files are recorded by date in individual ASCII files named as follows:

DSIMMDDYYYY.log

Where MM = Month, DD = Day and YYYY = Year.

The format of the log files is plain text which may be imported into appropriate logging utilities.

Services and Protocols (PA-DSS 8.2.c)

NETePay 5 does not require the use of any insecure services or protocols. Here are the services and protocols that NETePay 5 does require:

NETePay requires and supports TLS 1.0, 1.1 or 1.2 and will automatically use the most secure version supported by the payment processing service.

NETePay 5 must be installed on a system that supports TLS 1.0, 1.1 or 1.2. These secure protocols must be enabled in order for use by the Windows Crypto library. If necessary, users should enable these protocols in IE (which will apply the appropriate registry settings).

PCI-Compliant Wireless settings (PA-DSS 6.1 6.2.c and 6.3)

NETePay 5 does not support wireless technologies. However, should the merchant implement wireless access within the cardholder data environment, the following guidelines for secure wireless settings must be followed per PCI Data Security Standard 1.2.3, 2.1.1 and 4.1.1:

2.1.1: Change wireless vendor defaults per the following 5 points:

1. Encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions
2. Default SNMP community strings on wireless devices must be changed <
3. Default passwords/passphrases on access points must be changed
4. Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks
5. Other security-related wireless vendor defaults, if applicable, must be changed

1.2.3: Perimeter firewalls must be installed between any wireless networks and systems that store cardholder data, and these firewalls must deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

4.1.1: Industry best practices (for example, IEEE 802.11.i) must be used to implement strong encryption for authentication and transmission of cardholder data.
Note: The use of WEP as a security control was prohibited as of June 30, 2010.

Never store cardholder data on internet-accessible systems (PA-DSS 9.1.c)

Never store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server.)

PCI-Compliant Remote Access (PA-DSS 10.1 and 10.2)

NETePay 5 does not natively support any remote access functionality.

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism. The means two of the following three authentication methods must be used:

1. Something you know, such as a password or passphrase
2. Something you have, such as a token device or smart card
3. Something you are, such as a biometric

PCI-Compliant Delivery of Updates (PA-DSS 10.2.1.a)

Datacap Systems Inc. does not deliver separate patches and updates for NETePay 5. Any NETePay 5 application updates needed to address security issues are released as a new full installation package in the form of a self-extracting installer which is code signed with a VeriSign certificate. Datacap will notify users of the availability and advisability of installing updated applications via email and will supply a download link to obtain the updated application installer. The user must use the Windows Remove Application function from the Control Panel to remove the previous version of NETePay 5 then execute the new self-extracting installer to re-install the NETePay 5 application.

As a development company, we keep abreast of the relevant security concerns and vulnerabilities in our area of development and expertise.

Our continuing security education activities are comprised of the following:

- **Attendance at Coalfire (and other) Security Seminars**

  Datacap underwrites attendance of development personnel at appropriate security seminars. Emphasis is on Coalfire content and presentation because of the their emphasis on PCI-DSS and PA-DSS security issues. However, relevant presentations by other businesses or organizations, such as Microsoft, with expertise in application security are regularly considered.

- **Encourage recommendations for technical library purchases on security subjects**

  Datacap encourages all members of the technical staff to select, review and recommend purchase by the company of relevant books (and other printed or electronic materials) for inclusion in the company's permanent reference collection. Recommended purchases are discussed among staff members at regular and informal meetings for their relevance and usefulness.

- **Regular review of OWASP (Open Web Application Security Project) website**

  Datacap encourages all members of the technical staff to regularly visit the website of the Open Web Application Security Project at www.owasp.org. Particular attention to the Columns and Papers sections is encouraged to provide current perspectives on trends and issues in application security.

- **Regular review of US-CERT Current Activity**

  Datacap encourages all members of the technical staff to regularly visit the website of US-CERT (United States Computer Emergency Readiness Team) at (http://www.us-cert.gov/current/) to monitor potential threats to security. Review of this website is encouraged for all members of the technical staff weekly for relevance to NETePay security.

- **Regular review of SecurityTracker Weekly Vulnerability Summary Newsletter**

  Datacap subscibes to SecurityTracker's Weekly Vulnerability Summary Newsletter (www.securitytracker.com) and encourages all members of the technical staff to review updates weekly for relevance to NETePay security.

Once we identify a relevant vulnerability, we work to develop and test an updated NETePay 5 application that helps protect NETePay 5 against the specific, new vulnerability. We attempt to publish an updated application within 10 days of the identification of the vulnerability. We will then contact vendors and dealers to encourage them to install the updated application. Typically, merchants are expected to respond quickly to and install available updated applications within 30 days.

We do not deliver software and/or updates via remote access to customer networks. Instead, software and updated NETePay 5 applications are available via download from a Datacap supplied URL in an email notification. Downloads are code signed with a VeriSign certificate to assure integrity.

We recommend the use of a personal firewall product if computer is connected via VPN or other high-speed connection, to secure these "always-on" connections, per PCI Data Security Standard 1.3.10.

PCI-Compliant Remote Access (PA-DSS 10.1.1.a and 10.2.3.a)

NETePay 5 does not natively support any remote access functionality.

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate).

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited.

If users and hosts within the payment application environment may need to use third-party remote access software such as Remote Desktop (RDP)/Terminal Server, PCAnywhere, etc. to access other hosts within the payment processing environment, special care must be taken.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). For RDP/Terminal Services, this means using the high encryption setting on the server, and for PCAnywhere, it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements will apply to these access methods as well.

When requesting support from a vendor, reseller, or integrator, customers are advised to take the following precautions:

- Change default settings (such as usernames and passwords) on remote access software (e.g. VNC)
- Allow connections only from specific IP and/or MAC addresses

- Use strong authentication and complex passwords for logins according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS 8.1, 8.3, and 8.5.8-8.5.15
- Enable encrypted data transmission according to PA-DSS 12.1 and PCI DSS 4.1
- Enable account lockouts after a certain number of failed login attempts according to PA-DSS 3.1.8 and PCI DSS 8.5.13
- Require that remote access take place over a VPN via a firewall as opposed to allowing connections directly from the internet
- Enable logging for auditing purposes
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

Data Transport Encryption (PA-DSS 11.1.b)

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with TLS 1.2 or higher (configured to prevent fallback to SSLv3) or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments).

PCI DSS requirement 4.1: Use strong cryptography and security protocols such as transport layer security (TLS 1.2 or higher - configured to prevent fallback to SSLv3) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in scope of the PCI DSS are:

- The Internet
- Wireless technologies
- Global System for Mobile Communications (GSM)
- General Packet Radio Service (GPRS)

Refer to the Dataflow diagram for an understanding of the flow of encrypted data associated with NETePay 5.

PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2.b)

NETePay 5 does not allow or facilitate the sending of PANs via any end user messaging technology (for example, e-mail, instant messaging, and chat).

Non-console administration (PA-DSS 12.1)

Although NETePay 5 does not support non-console administration and we do not recommend using non-console administration, should you ever choose to do this, must use SSH, VPN, or TLS 1.2 or higher (configured to prevent fallback to SSLv3) for encryption of this non-console administrative access.

Network Segmentation

The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

- Refer to the standardized Network diagram for an understanding of the flow of encrypted data associated with NETePay 5.

Maintain an Information Security Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self Assessment Questionnaire.
- Call in outside experts as needed.

Application System Configuration

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

- Microsoft Windows Windows Server 2008 or 2012, Windows 7 SP1 or Windows 8. All latest updates and hotfixes should be applied.
- 2 GB of RAM minimum, 4 GB or higher recommended
- 50 GB of available hard-disk space
- Microsoft Internet Explorer with 128-bit encryption, Microsoft Internet Explorer 6.0 or higher recommended
- TCP/IP network connectivity. (Persistent Internet connection recommended)
- SQLExpress2008 R2 - All latest updates and hotfixes should be applied.

Payment Application Initial Setup & Configuration

- Installation of NETePay 5 and associated database and utilities requires Administrator access in Windows. Datacap advises users to change default password and manage Windows passwords according to PCI DSS 3.1

ePay Crypto Overview

Assumption

In this document '**Client**' refers to any one of DSIClientX.ocx, dsiPDCX.ocx or dsiEMVX.ocx and '**Serve**r' refers to a NETePay5 V5.06 application.

Client / Server Communication

1. Client is requested by POS to perform a transaction.
2. Client acquires a Crypto Context (128-bit).
3. Client takes predefined embedded obfuscated key and hashes it using MD5 Hashing algorithm.
4. It uses this hash to generate a 128-bit key and destroys the hash in memory.
5. Client generates a chunk of random data (using MS Crypto API) and uses the newly generated key to encrypt the random data using an RC4 Cipher.
6. Client Connects to Server TCP/IP Stream Socket
7. Server Accepts Connection
8. Server acquires a Crypto Context (128-bit).
9. Server takes predefined embedded obfuscated key and hashes it using MD5 Hashing algorithm.
10. It uses this hash to generate a 128 bit key and destroys the hash in memory.
11. Server generates a chunk of random data (using MS Crypto API) and uses the newly generated key to encrypt the random data using an RC4 Cipher.
12. Server transmits the clear text random data as a 'challenge' to the client.
13. Client encrypts this random data sent by the server
14. Client sends the encrypted data back as a 'response' to the challenge. It also sends its random data as a 'challenge' to the server.
15. The server compares the encrypted data to what the client sent back. If it does not match the client socket is gracefully disconnected. If it does, processing continues.
16. Server Sends back its response to the Servers Challenge and tells the client it liked the response.
17. The Client performs a similar check. The Client compares its encrypted random data to what the Server sends back. If it does not match, the socket is gracefully disconnected; if it does, processing continues.
18. At this point The Server knows it is speaking to one of its clients and the client knows it is speaking to one of its servers. There is a password option available to make this check even more granular. The previous has no bearing on the encryption of the actual financial transaction just client server authentication. Even though the software is designed to run at the local level, this extra authentication helps defend against a man-in-the-middle attack, and adds a layer of security not found in other models.
19. The Client and Server are connected at this point. When the server starts for the first time, it creates a Keyset. This Keyset is created using RSA Full strength 1024 bit keys. This Keyset is a public / private key pair.
20. As part of the initial dialogue, the server transmits its public key the client.

21. The client takes this public key, imports it into its Crypto API context, and generates a session key.
22. The Client uses the generated session key to encrypt the data it is going to send to the server.
23. It then exports the session key blob from the Crypto API.
24. This key blob is then transmitted to the server along with the encrypted data.
25. The Server takes the key blob and imports it into the Crypto API. It then uses this and its private key to decrypt the request.
26. It processes the request and uses the session key to encrypt the response.
27. Even though there is no sensitive data in the response, the response is encrypted using the session key generated by the client uniquely on each request. Some error responses are not encrypted. For instance, a failure to encrypt due to insufficient crypto libraries installed.

Data Store

1. When the Server starts for the very first time, it generates a unique session code. This code is stored in the encrypted license file that is used for software activation. Each Server uses this value along with several other pieces of fixed data (different for each product) to encrypt sensitive data in the database.
2. Starting with PCI 2.0 the server now also uses the EPOCH of the machine on each transaction – this makes each record uniquely encrypted. Before submitting this fixed and variable data this unique string is put through a prime number modification algorithm.
3. The encryption starts by taking this value and hashing it using SHA Hashing Algorithm.
4. It uses this hash to generate a 128-bit key and destroys the hash in memory.
5. Server uses the generated key to encrypt the random data using an 3DES Cipher.
6. The Server encrypts any column that needs to store an account number or expiration date. Some Servers never need to encrypt because they never store the account number or expiration date.
7. The Servers that need to encrypt account numbers do so because this information is required to transmit the batch at the end of the day.
8. After successful settlement, the Server updates all of the rows with any encrypted columns to make the data invalid. Usually this is done by writing an 'X' over any encrypted data.
9. On Servers that are forced to require encryption, batch sizes are limited. If a merchant forgets to settle his/her batch and exceeds the batch size limit, processing new transactions is halted until the current batch is settled.