
NETePay 5
Reseller Training Guide

Paymentech Terminal
With Dial Backup

Part Number: 8660.92

NETePay 5 Reseller Training & Configuration Guide

Copyright © 2015 Datacap Systems Inc. All rights reserved.

This manual and the hardware/software described in it are copyrighted materials with all rights reserved. Under copyright laws, the manual and the information contained in it may not be copied, in whole or in part, without written consent from Datacap Systems, Inc except as may be required in normal use to make a backup copy of the software. Our policy of continuous development may cause the information and specifications contained herein to change without notice.

Notice:

This document contains information proprietary to Datacap Systems Inc. The only acceptable use for the information contained herein is to configure, interface and maintain third party systems exclusively to Datacap's ePay™ server products. Any other use is strictly prohibited.

Datacap, Datacap Systems, NETePay™, GIFTePay™, DIALePay™, DSIClient™, DSIClientX®, dsiPDCX®, ePay Administrator™, IPTran™, IPTran LT™, TwinTran™, DialTran™, DataTran™ are trademarks or registered trademarks of Datacap Systems Inc.

Microsoft, Windows NT 4.0, Windows 2000 Professional, Windows XP, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Vista, Windows 7, Windows 8, and Windows 98 are registered trademarks of the Microsoft Corporation.

Other products or company names mentioned herein may be the trademarks or registered trademarks of their respective companies.

Revised: 15 Aug 2015

Version Support

This document supports the following application versions:

NETePay 5 (Paymentech Term) - Version 5.06

DSIClientX, Version 3.86

dsiPDCX, Version 1.42

DSIClient Transaction Utility, Version 2.50

ePay Administrator for NETePay, Version 4.00

Payment Processor Support

This document supports the following payment processor:

Paymentech Terminal

CONTENTS

OVERVIEW	5
INTRODUCTION.....	5
<i>About NETePay 5 with Dial Backup</i>	<i>5</i>
WHAT'S INCLUDED ON YOUR CD.....	5
HOW IT WORKS.....	6
PA DSS 3.1 - IMPLEMENTATION GUIDE	7
ABOUT THIS GUIDE	7
NOTICE.....	7
REVISION INFORMATION	8
EXECUTIVE SUMMARY	8
<i>Application Summary</i>	<i>9</i>
<i>Typical Network Implementation.....</i>	<i>13</i>
<i>NETePay 5 – Network Diagram.....</i>	<i>13</i>
<i>The 12 Requirements of the PCI DSS:.....</i>	<i>15</i>
<i>Considerations for the Implementation of Payment Application in a PCI-Compliant Environment.....</i>	<i>16</i>
<i>Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4.)</i>	<i>16</i>
<i>Sensitive Authentication Data requires special handling (PA-DSS 1.1.5)</i>	<i>16</i>
<i>Secure Deletion of Cardholder Data (PA-DSS 2.1)</i>	<i>16</i>
TO ADDRESS INADVERTENT CAPTURE OF PAN ON WINDOWS 7:.....	17
<i>Disabling System Restore – Windows 7.....</i>	<i>17</i>
<i>Encrypting the System PageFile.sys – Windows 7.....</i>	<i>18</i>
<i>Clear the System Pagefile.sys on shutdown – Windows 7</i>	<i>19</i>
<i>Disable System Management of PageFile.sys – Windows 7.....</i>	<i>21</i>
<i>Disable Windows Error Reporting – Windows 7.....</i>	<i>23</i>
TO ADDRESS INADVERTENT CAPTURE OF PAN ON WINDOWS 8, 10, SERVER 2008 OR 2012:	24
<i>Disable System Restore – Windows 8, 10, Server 2008 or 2012</i>	<i>24</i>
<i>Encrypt PageFile.sys – Windows 8, 10, Server 2008 or 2012.....</i>	<i>26</i>
<i>Clear the System Pagefile.sys on shutdown – Windows 8, 10, Server 2008 or 2012.....</i>	<i>26</i>
<i>Disable System Management of PageFile.sys – Windows 8, 10, Server 2008 or 2012</i>	<i>27</i>
<i>Disable Windows Error Reporting – Windows 8, 10, Server 2008 or 2012.....</i>	<i>30</i>
ALL PAN IS MASKED BY DEFAULT (PA-DSS 2.2).....	32
CARDHOLDER DATA ENCRYPTION & KEY MANAGEMENT (PA-DSS 2.3, 2.4, AND 2.5).....	32
REMOVAL OF HISTORICAL CRYPTOGRAPHIC MATERIAL (PA-DSS 2.6).....	32
SET UP STRONG ACCESS CONTROLS (3.1 AND 3.2).....	33
PROPERLY TRAIN AND MONITOR ADMIN PERSONNEL.....	35
LOG SETTINGS MUST BE COMPLIANT (PA-DSS 4.1.B, 4.4.A, 4.4.B)	35
PCI-COMPLIANT WIRELESS SETTINGS (PA-DSS 6.1.A AND 6.2.B).....	36
SERVICES AND PROTOCOLS (PA-DSS 8.2.C).....	36
NEVER STORE CARDHOLDER DATA ON INTERNET-ACCESSIBLE SYSTEMS (PA-DSS 9.1.C).....	36
PCI-COMPLIANT REMOTE ACCESS (PA-DSS 10.1).....	36
PCI-COMPLIANT DELIVERY OF UPDATES (PA-DSS 10.2.1).....	37
PCI-COMPLIANT REMOTE ACCESS (PA-DSS 10.2.3).....	38
DATA TRANSPORT ENCRYPTION (PA-DSS 11.1)	39
PCI-COMPLIANT USE OF END USER MESSAGING TECHNOLOGIES (PA-DSS 11.2.B)	39

NETWORK SEGMENTATION	39
MAINTAIN AN INFORMATION SECURITY PROGRAM.....	40
APPLICATION SYSTEM CONFIGURATION	40
PAYMENT APPLICATION INITIAL SETUP & CONFIGURATION	40
INSTALLATION	41
INTRODUCTION.....	41
REQUIREMENTS	41
<i>Baseline System Configuration</i>	41
<i>Network Requirements</i>	42
INSTALLATION PROCEDURES.....	42
<i>Accessing the NETePay CD-ROM</i>	42
<i>Installing/Upgrading Microsoft Internet Explorer</i>	44
<i>Installing SQL Express 2005 (Required for Windows Server 2008)</i>	44
<i>Installing SQL Express 2008 (Required for Windows Server 2012, Windows 7 & 8)</i>	44
<i>Installing NETePay 5 (Required)</i>	45
<i>Installing DSIClient Application (Conditional)</i>	45
<i>Installing ePay Administrator for NETePay 5 (Required)</i>	46
<i>Installing Datacap DialLink modem (Required for Dial Backup Operation)</i>	46
NETEPAY 5 CONFIGURATION	47
INTRODUCTION.....	47
ACTIVATION AND PARAMETER DOWNLOAD.....	47
VERIFYING YOUR SERIAL NUMBER AND ACTIVATION.....	56
TESTING	56
<i>Important! - Before You Start</i>	56
OPERATIONAL CONSIDERATIONS	56
<i>Important!</i>	56
USING THE NETEPAY - DATABASE MANAGER	58
INTRODUCTION.....	58
<i>Maintenance Functions</i>	58
USING THE NETePAY DATABASE MANAGER.....	59
INDEX	66

OVERVIEW

Introduction

About NETePay 5 with Dial Backup

Developed by Datacap Systems, *NETePay 5* enables retail, restaurant and other businesses to perform fast electronic payment authorizations via the Internet. *NETePay 5* also incorporates automatic dialup backup direct to the processing host in the event of an Internet outage. The dial backup operation is completely automatic and switches back to Internet operation without operator intervention.

NETePay 5 is multi-threaded to accept simultaneous requests from multiple clients, and scalable so that customers can configure their store systems to fit their requirements and get the most favorable rates from their payment service.

What's Included on your CD

The *NETePay 5* CD-ROM includes client and server applications for Windows 2000, XP and Vista Business Edition operating systems for both single and multi-pay point users.

- ***NETePay 5 with Dial Backup*** – server-side software that enables you to process payment authorization requests via the Internet or other TCP/IP Virtual Private Network (VPN) services.
- ***DSIClientX*** – an ActiveX control that integrates with a Point of Sale application and sends encrypted payment authorization requests from client machines on a LAN to *NETePay 5* for processing. *DSIClientX* also includes a utility program to enter test payment transactions called ***DSIClient***.
- ***ePay Administrator for NETePay*** – a software application that provides payment transaction batch management. You can also use *ePay Administrator* to enter and process payment transactions.

For more information about using *ePay Administrator for NETePay*, see the *ePay User Guide*

- ***SQL Express 2005*** - this software provides database services to *NETePay 5* and *ePay Administrator* using Microsoft SQL Express for Windows Server 2008 users.
- ***SQL Express 2008 R2*** - this software provides database services to *NETePay 5* and *ePay Administrator* using Microsoft SQL Express for Windows Server 2012 and Windows 7 & 8 users.
- ***Microsoft Internet Explorer 6.0*** – this version (or later) of Microsoft Internet Explorer will ensure that you can install the necessary encryption capability required for *NETePay 5*.

How it works

NETePay 5 is an application that resides on a server (either at the store level or remotely, at the enterprise level) monitors encrypted transaction requests from client machines using a POS or restaurant application integrated with *DSIClientX*, Datacap's XML ActiveX control.

When *NETePay 5* receives an encrypted transaction request from a client machine, it sends the request to the bankcard processor for approval via the Internet or PSTN dialup direct to the processing host. The transactions are then stored in a database that resides on the server. *NETePay 5* makes use of 128-bit encryption to provide secure transactions over the Internet.

By using *ePay Administrator*, you can view the transactions, settle and close batches, generate reports and process payment transactions. For more information about using *ePay Administrator*, see the *ePay Administrator User Guide*.

Preliminary

PA DSS 3.1 - IMPLEMENTATION GUIDE

About this Guide

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).

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.

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.

Revision Information

Name	Title	Date of Update	Summary of Changes
NETePay 5	PA-DSS 3.1 Implementation Guide	XX Sept 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 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/pci_dss.shtmlhttps://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	<p>NETePay 5 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.</p> <p>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.</p> <p>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).</p> <p>NETePay 5 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 5 may provide POS software systems with a streamlined path to achieve PA-DSS compliance.</p> <p>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 5 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</p>																								
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	<table border="1"> <thead> <tr> <th colspan="4">Target Market for Payment Application (check all that apply):</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>Retail</td> <td><input type="checkbox"/></td> <td>Processors</td> <td><input type="checkbox"/></td> <td>Gas/Oil</td> </tr> <tr> <td><input type="checkbox"/></td> <td>e-Commerce</td> <td><input checked="" type="checkbox"/></td> <td>Small/medium merchants</td> <td><input type="checkbox"/></td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td colspan="5">Others (please specify): Restaurant, MOTO</td> </tr> </tbody> </table>			Target Market for Payment Application (check all that apply):				<input checked="" type="checkbox"/>	Retail	<input type="checkbox"/>	Processors	<input type="checkbox"/>	Gas/Oil	<input type="checkbox"/>	e-Commerce	<input checked="" type="checkbox"/>	Small/medium merchants	<input type="checkbox"/>		<input checked="" type="checkbox"/>	Others (please specify): Restaurant, MOTO				
Target Market for Payment Application (check all that apply):																									
<input checked="" type="checkbox"/>	Retail	<input type="checkbox"/>	Processors	<input type="checkbox"/>	Gas/Oil																				
<input type="checkbox"/>	e-Commerce	<input checked="" type="checkbox"/>	Small/medium merchants	<input type="checkbox"/>																					
<input checked="" type="checkbox"/>	Others (please specify): Restaurant, MOTO																								
Stored Cardholder	The following is a brief description of files and tables that store cardholder data:																								

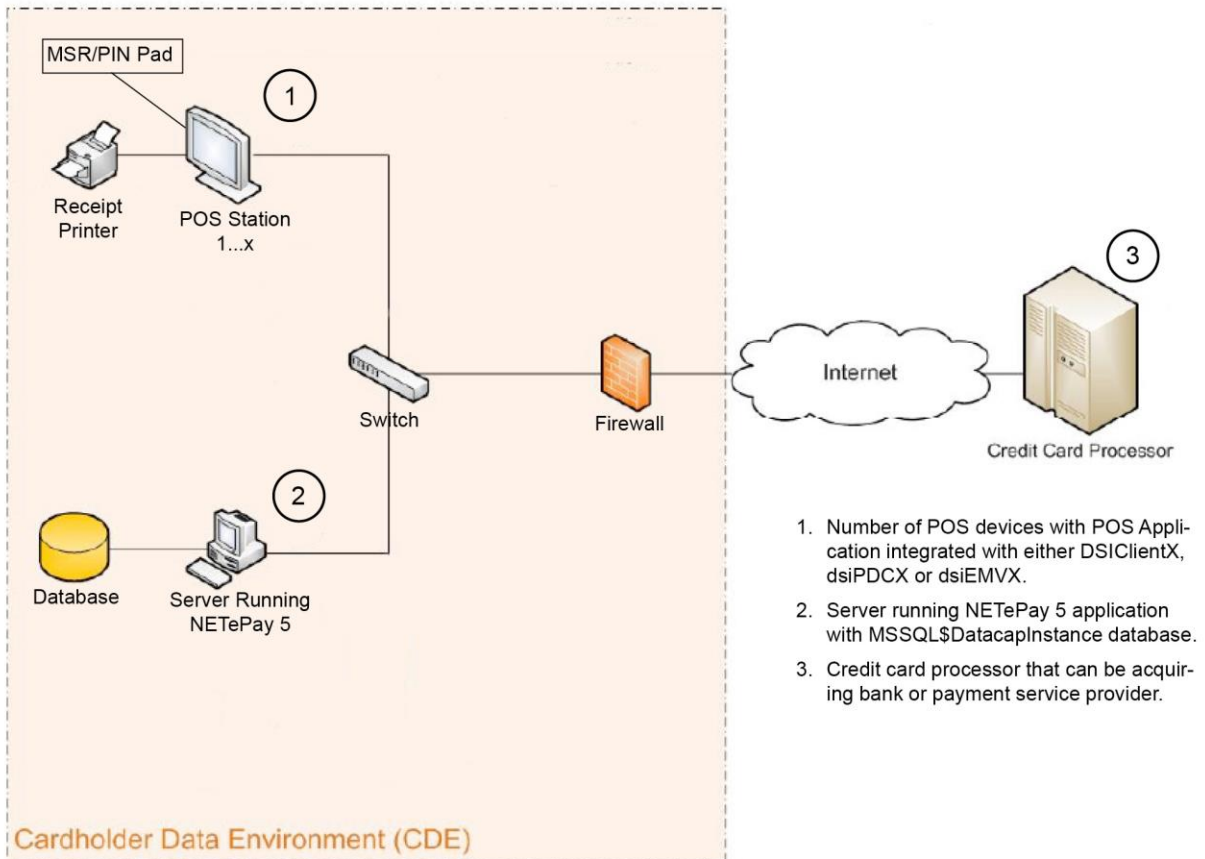
<p>Application Authentication</p>	<p>During installation, NETePay 5 installs a license file that contains data whereby we know the product has been successfully activated and therefore it is valid to use it for processing. The same license file contains the merchant settings. There is no other authentication data. The license file is encrypted, proprietary to Protection Plus.</p>																
<p>Application Encryption</p>	<p>See the <i>ePay Crypto Overview</i> section at the end of this document.</p>																
<p>Application Functionality Supported</p>	<p>Payment Application Functionality (check only one):</p> <table border="1" data-bbox="464 552 1456 747"> <tr> <td>Automated Fuel Dispenser</td> <td>POS Kiosk</td> <td></td> <td>Payment Gateway/Switch</td> </tr> <tr> <td>Card-Not-Present</td> <td>POS Specialized</td> <td>X</td> <td>Payment Middleware</td> </tr> <tr> <td>POS Admin</td> <td>POS Suite/General</td> <td></td> <td>Payment Module</td> </tr> <tr> <td>POS Face-to-Face/POI</td> <td>Payment Back Office</td> <td></td> <td>Shopping Cart & Store Front</td> </tr> </table>	Automated Fuel Dispenser	POS Kiosk		Payment Gateway/Switch	Card-Not-Present	POS Specialized	X	Payment Middleware	POS Admin	POS Suite/General		Payment Module	POS Face-to-Face/POI	Payment Back Office		Shopping Cart & Store Front
Automated Fuel Dispenser	POS Kiosk		Payment Gateway/Switch														
Card-Not-Present	POS Specialized	X	Payment Middleware														
POS Admin	POS Suite/General		Payment Module														
POS Face-to-Face/POI	Payment Back Office		Shopping Cart & Store Front														
<p>Payment Processing Connections:</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>																
<p>Description of Listing Versioning Methodology (PA-DSS 5.4.4)</p>	<p>NETePay 5 versioning has three levels, Major, Minor, and Build: <Major>.<Minor>.<Build></p> <ul style="list-style-type: none"> • 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). <p>Based on the above versioning methodology the application version being listed with the PCI</p>																

	SSC is: 5.06.X.
--	-----------------

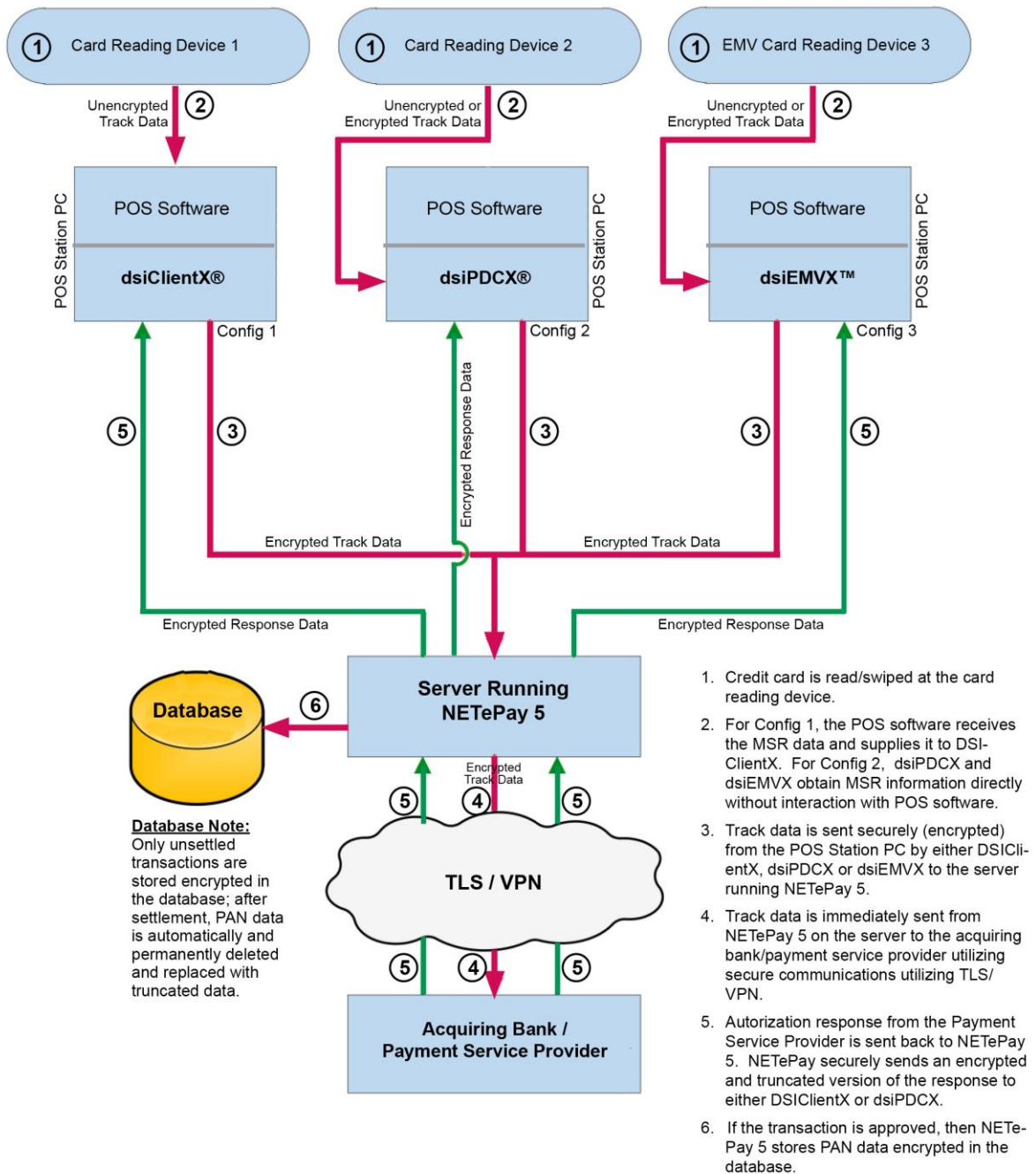
Preliminary

Typical Network Implementation

NETePay 5 – Network Diagram



NETePay 5 – Credit/Debit Cardholder Data Flow Diagram



1. Credit card is read/swiped at the card reading device.
2. For Config 1, the POS software receives the MSR data and supplies it to DSI-ClientX. For Config 2, dsiPDCX and dsiEMVX obtain MSR information directly without interaction with POS software.
3. Track data is sent securely (encrypted) from the POS Station PC by either DSI-ClientX, dsiPDCX or dsiEMVX to the server running NETePay 5.
4. Track data is immediately sent from NETePay 5 on the server to the acquiring bank/payment service provider utilizing secure communications utilizing TLS/VPN.
5. Authorization response from the Payment Service Provider is sent back to NETePay 5. NETePay securely sends an encrypted and truncated version of the response to either DSI-ClientX or dsiPDCX.
6. If the transaction is approved, then NETePay 5 stores PAN data encrypted in the database.

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. DSI-ClientX, 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 removal of this historical data by the application as required by PA-DSS v3.1.

Sensitive Authentication Data requires special handling (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.

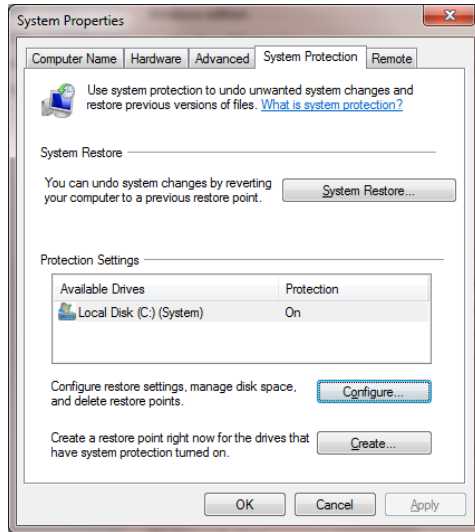
- Here are the locations of the cardholder data you must purge:
 - Files: dbnetepay.mdf *and* dbnetepay.ldf
 - Tables: MSSQL\$DatacapInstance – Tables: batch, version
- To purge the cardholder data you must do the following two things:
 1. The application automatically and permanently purges (truncates) 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.

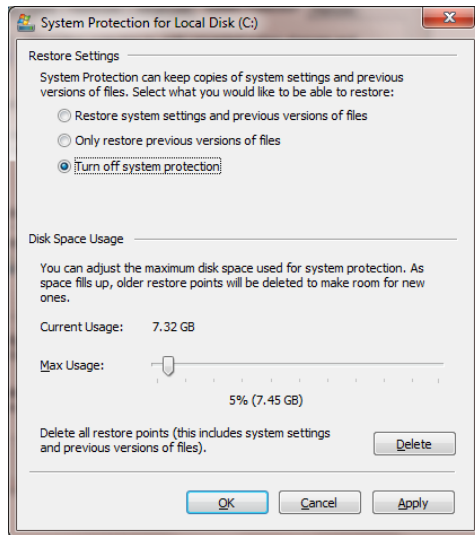
2. In the operating system you must configure appropriate settings to prevent inadvertent retention of cardholder data

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:

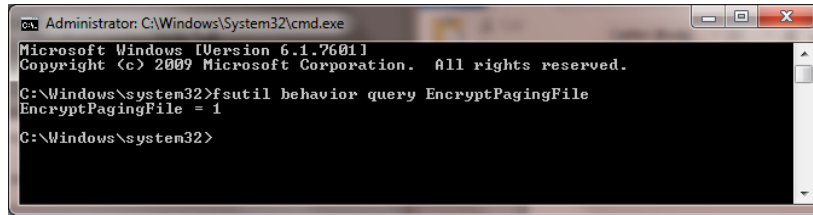


- Select “Turn off system protection”
- Click apply, and OK to shut the System Protection window
- Click OK again to shut the System Properties window
- Reboot the computer

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

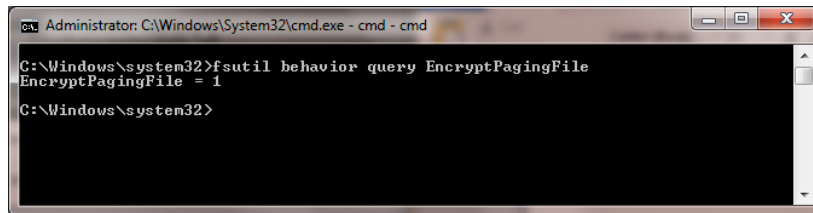


```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 1

C:\Windows\system32>
```

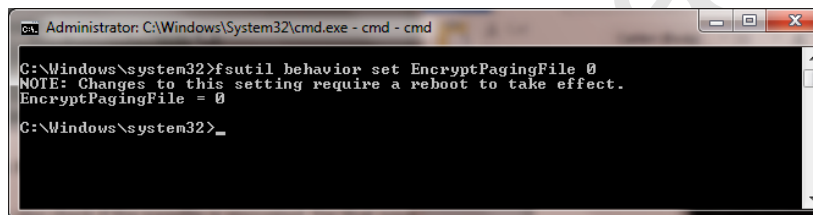
- To verify configuration type the following command: fsutil behavior query EncryptPagingFile



```
Administrator: C:\Windows\System32\cmd.exe - cmd - cmd
C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 1

C:\Windows\system32>
```

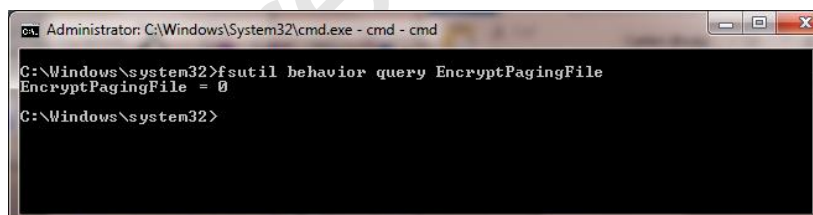
- If encryption is enabled EncryptPagingFile = 1 should appear
- In the event you need to disable PageFile encryption type the following command: fsutil behavior set EncryptPagingFile 0



```
Administrator: C:\Windows\System32\cmd.exe - cmd - cmd
C:\Windows\system32>fsutil behavior set EncryptPagingFile 0
NOTE: Changes to this setting require a reboot to take effect.
EncryptPagingFile = 0

C:\Windows\system32>_
```

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



```
Administrator: C:\Windows\System32\cmd.exe - cmd - cmd
C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 0

C:\Windows\system32>
```

- If encryption is disabled EncryptPagingFile = 0 should appear

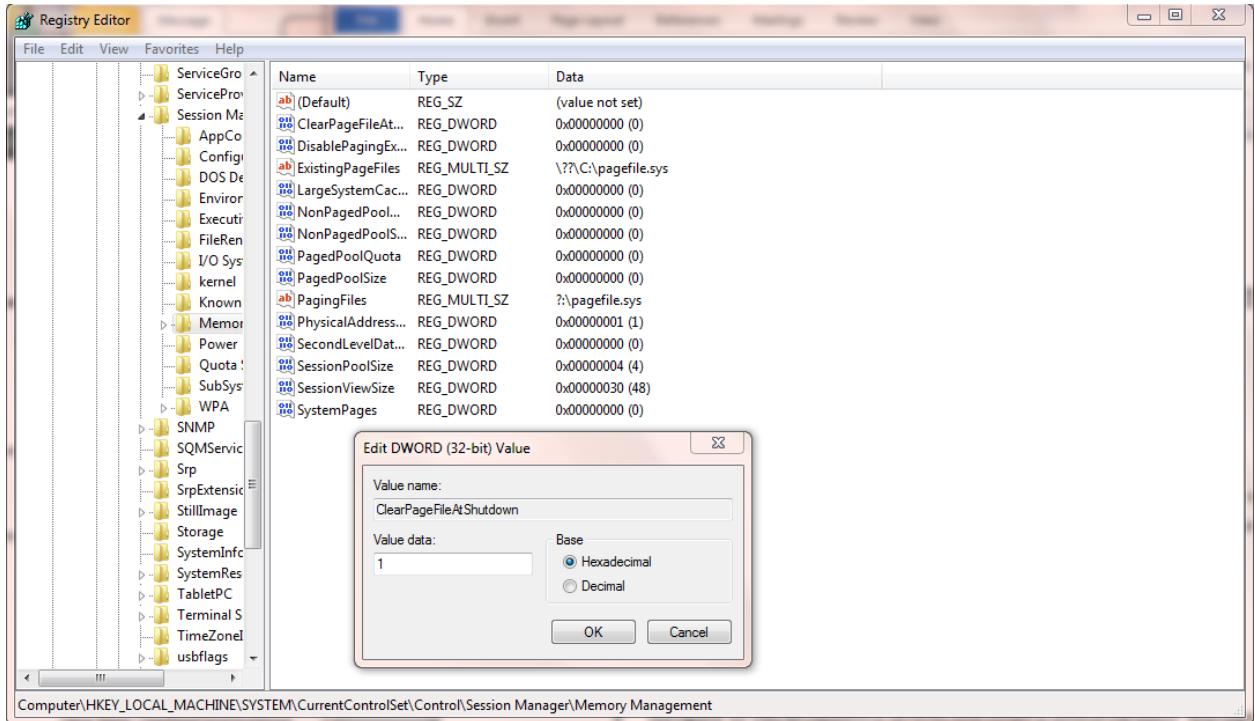
Clear the System Pagefile.sys on shutdown – Windows 7

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

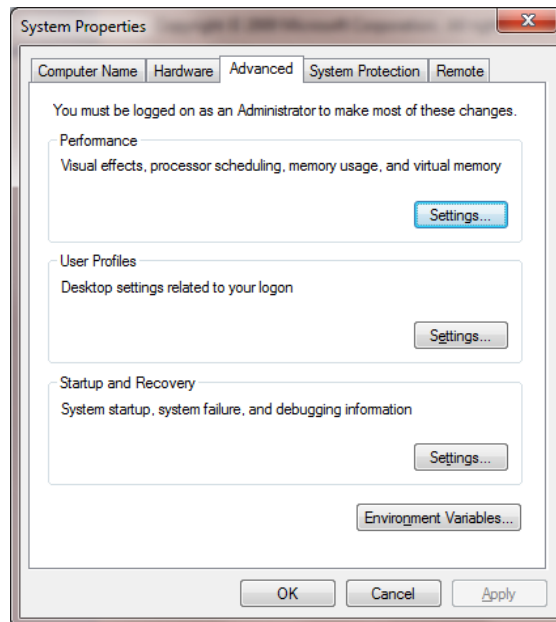
- Change the value from 0 to 1
- Click OK and close Regedit



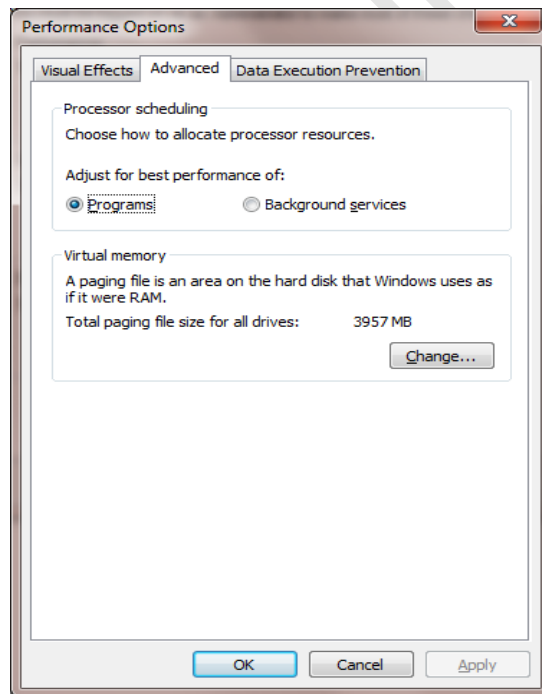
- If the value does not exist, add the following:
 - Value Name: ClearPageFileAtShutdown
 - Value Type: REG_DWORD
 - Value: 1

Disable System Management of PageFile.sys – Windows 7

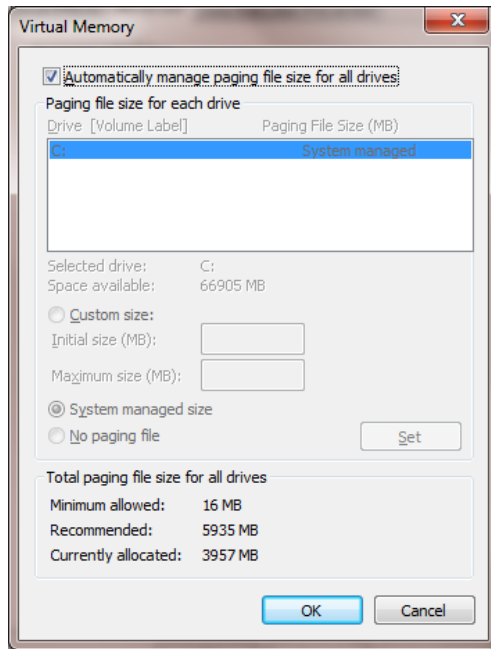
- Right Click on Computer > Select “Properties”
- Select “Advanced System Settings” on the top left list, the following screen will appear:



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



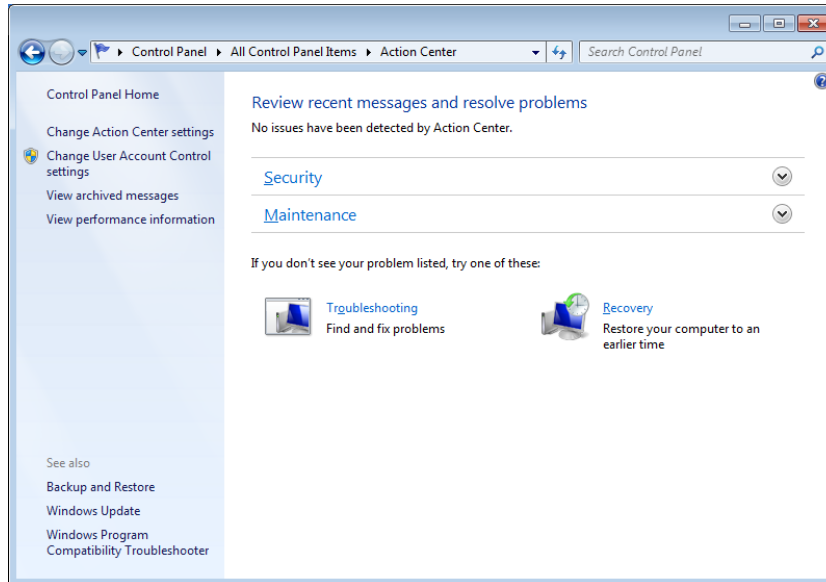
- Select “Change” under Virtual Memory, the following screen will appear:



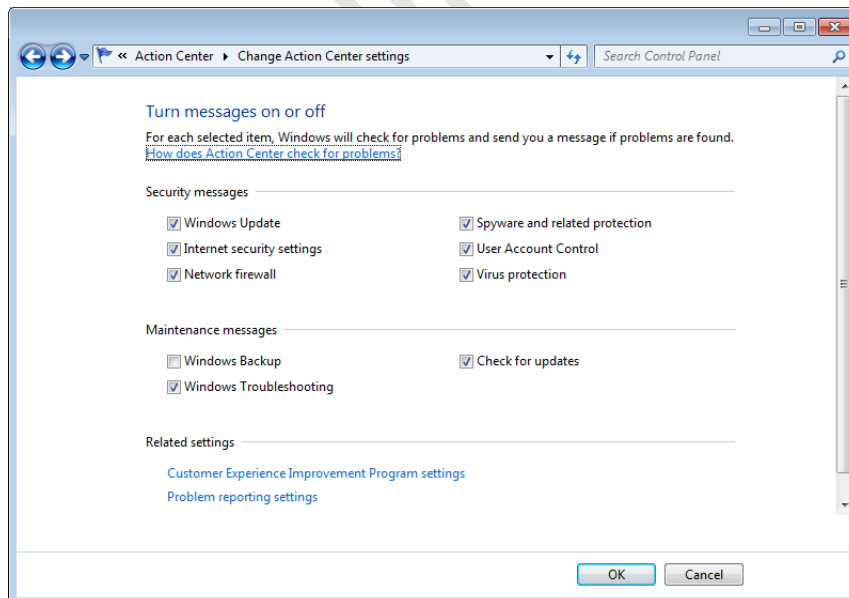
- Uncheck “Automatically manage page file size for all drives”
- Select “Custom Size”
- Enter the following for the size selections:
 - Initial Size – as a good rule of thumb, the size should be equivalent to the amount of memory in the system.
 - Maximum Size – as a good rule of thumb, the size should 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

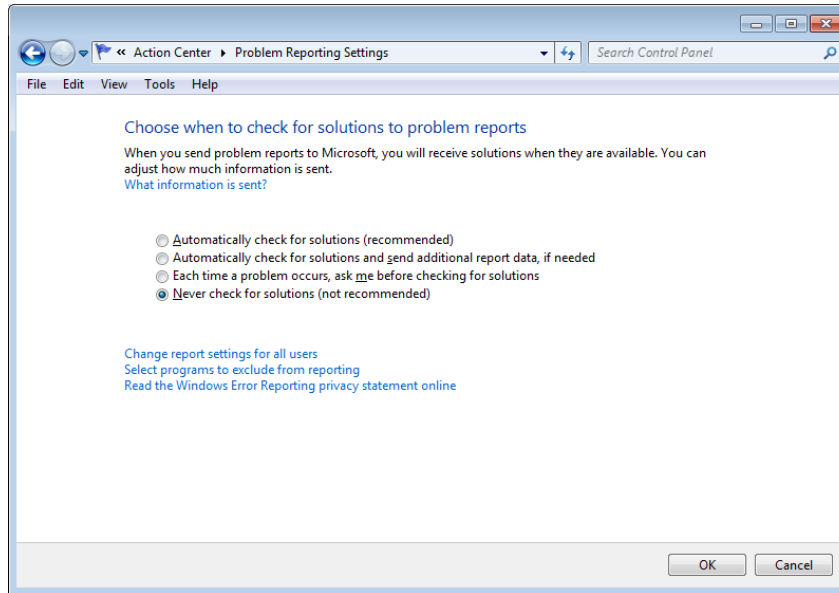
- Open the Control Panel
- Open the Action Center
- Select “Change Action Center Settings”



- Select “Problem Reporting Settings”



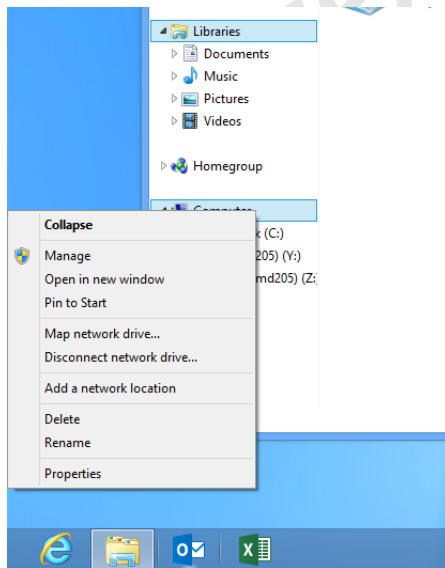
- Select “Never Check for Solutions”



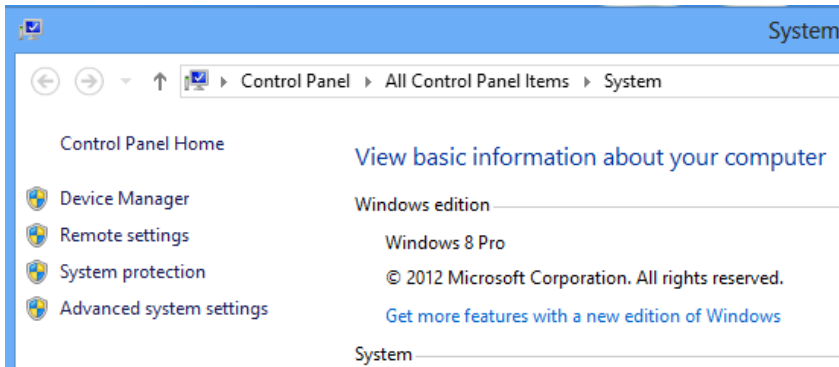
To Address Inadvertent Capture of PAN on Windows 8, 10, Server 2008 or 2012:

Disable System Restore – Windows 8, 10, Server 2008 or 2012

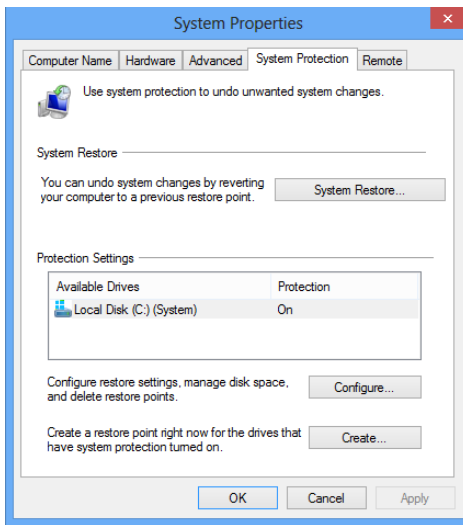
- Right Click on Computer > Select “Properties”:



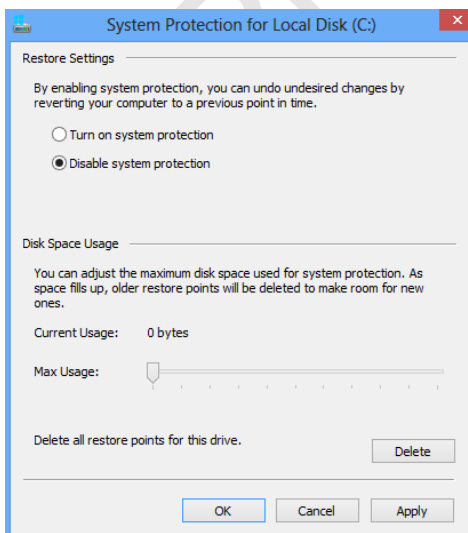
- Select “Advanced System Settings” from the System screen:



- 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, 10, Server 2008 or 2012

* 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”

```
Administrator: C:\Windows\System32\cmd.exe - cmd - cmd
C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 1
C:\Windows\system32>
```

- 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

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 1
C:\Windows\system32>
```

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

```
Administrator: C:\Windows\System32\cmd.exe - cmd - cmd
C:\Windows\system32>fsutil behavior set EncryptPagingFile 0
NOTE: Changes to this setting require a reboot to take effect.
EncryptPagingFile = 0
C:\Windows\system32>
```

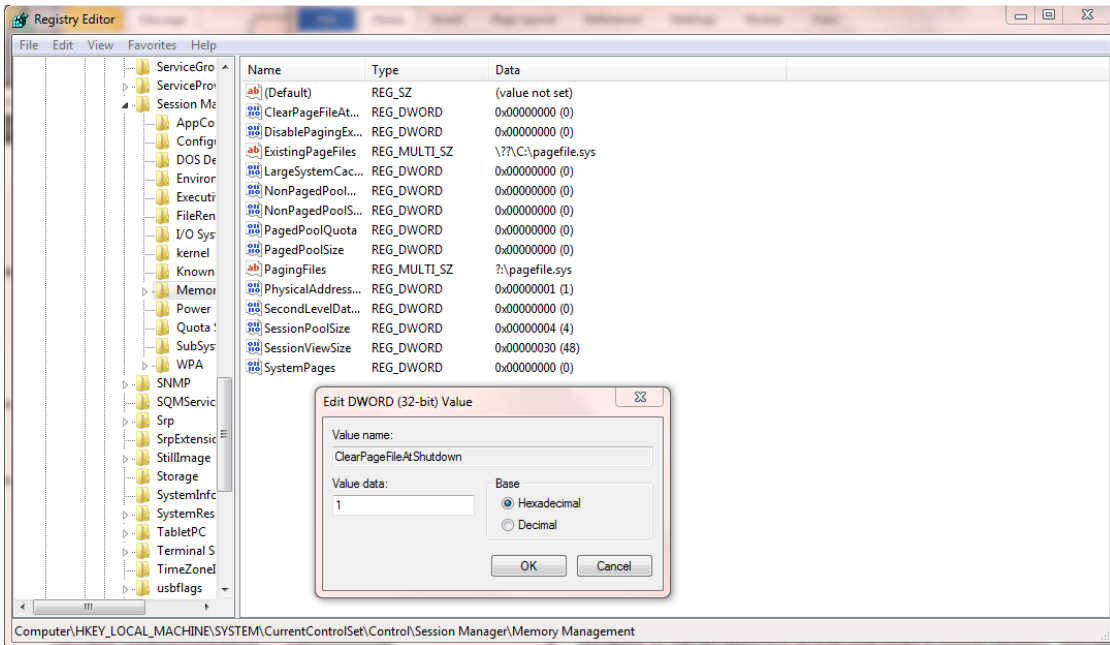
Clear the System Pagefile.sys on shutdown – Windows 8, 10, Server 2008 or 2012

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.

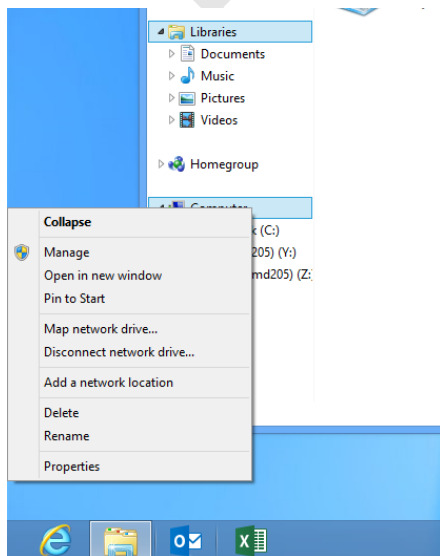
- Click OK and close Regedit



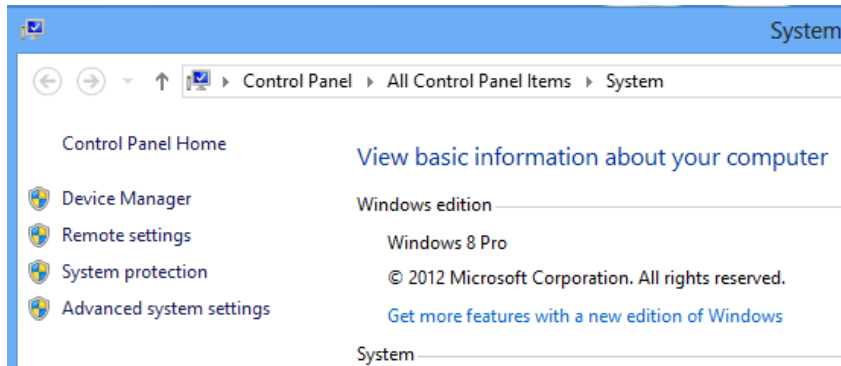
- If the value does not exist, add the following:
 - Value Name: ClearPageFileAtShutdown
 - Value Type: REG_DWORD
 - Value: 1

Disable System Management of PageFile.sys – Windows 8, 10, Server 2008 or 2012

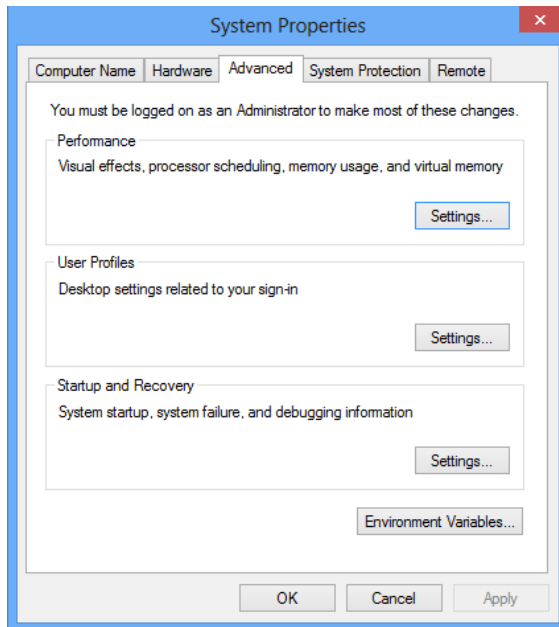
- Right Click on Computer > Select “Properties”:



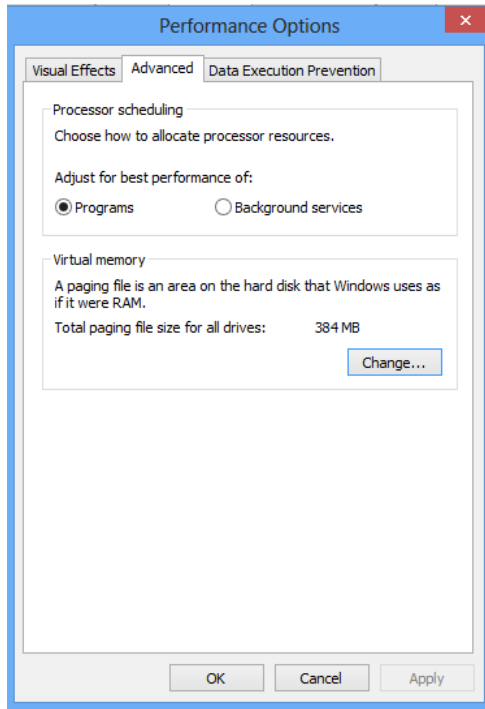
- Select “Advanced System Settings” from the System screen:



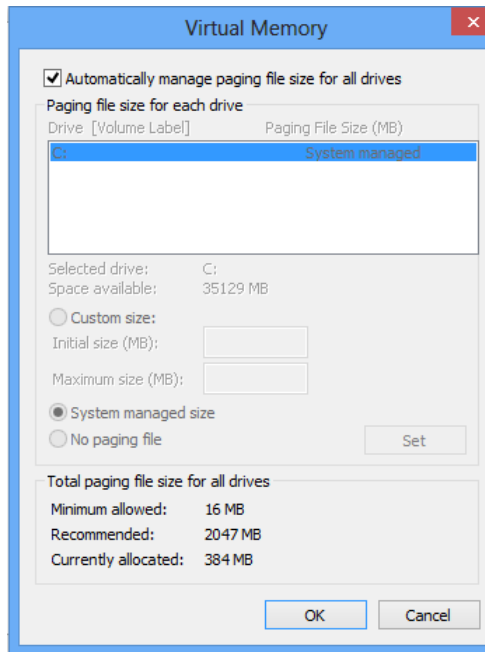
- Select the “Advanced” tab:



- 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:

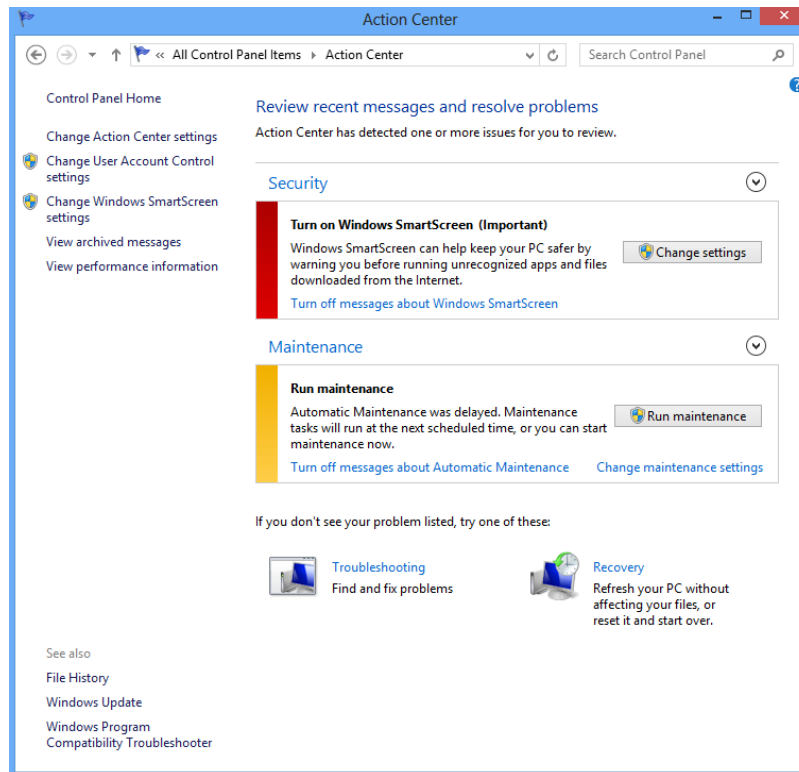


- Uncheck “Automatically manage page file size for all drives”
- Select “Custom Size”
- Enter the following for the size selections:
 - Initial Size – as a good rule of thumb, the size should be equivalent to the amount of memory in the system.

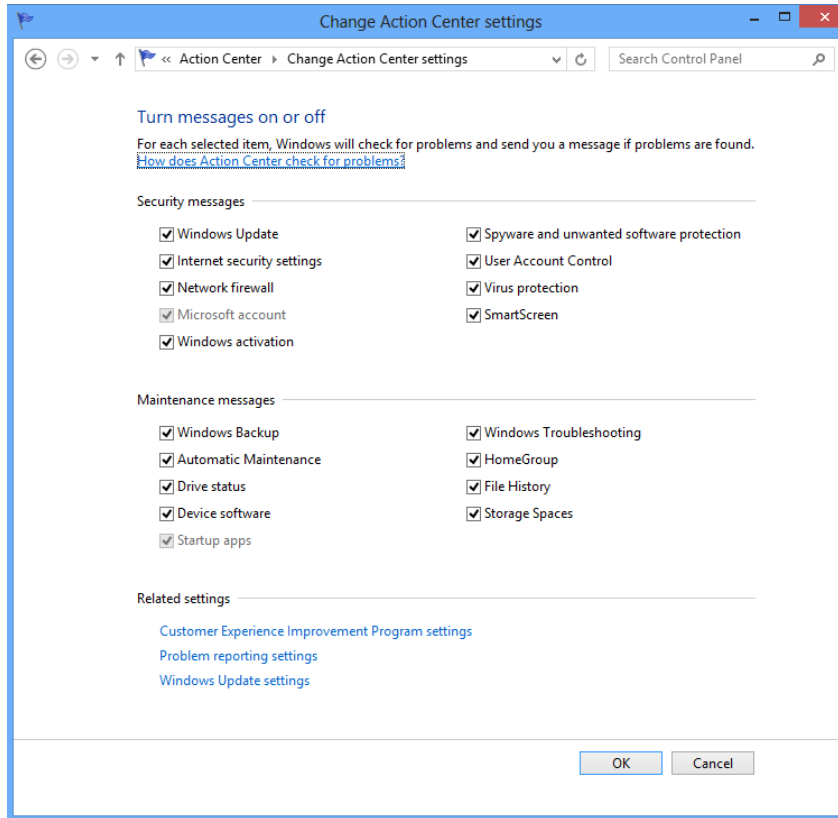
- Maximum Size – as a good rule of thumb, the size should be equivalent to 2x the amount of memory in the system.
- Click “Ok”, “OK”, and “OK”
- You will be prompted to reboot your computer.

Disable Windows Error Reporting – Windows 8, 10, Server 2008 or 2012

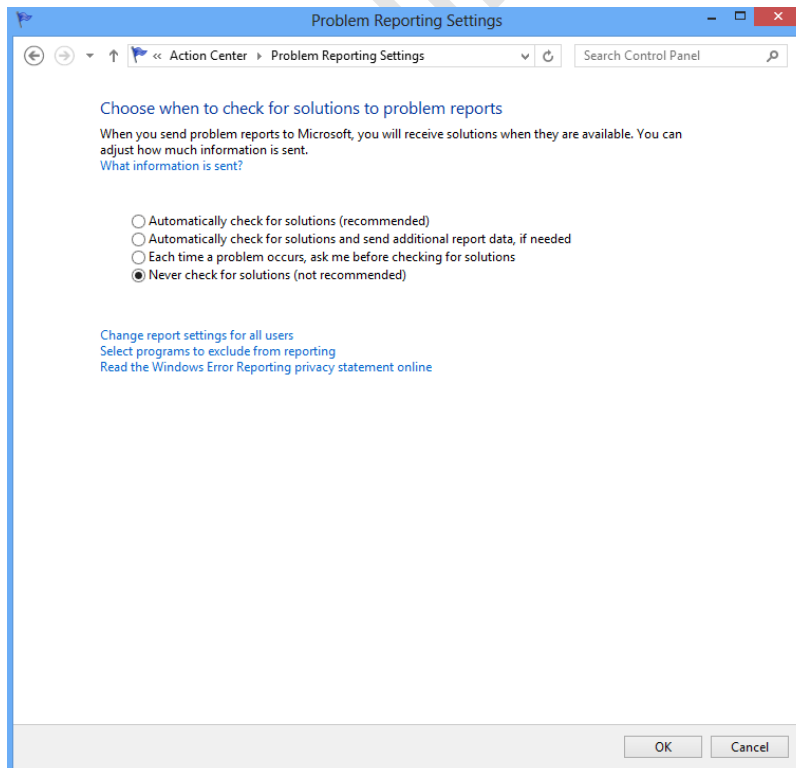
- From the desktop hold down the “Windows” key and type “I” to bring up the “Settings” charm, select “Control Panel”.
- Open the Action Center
- Select “Change Action Center Settings”:
-



- 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.*

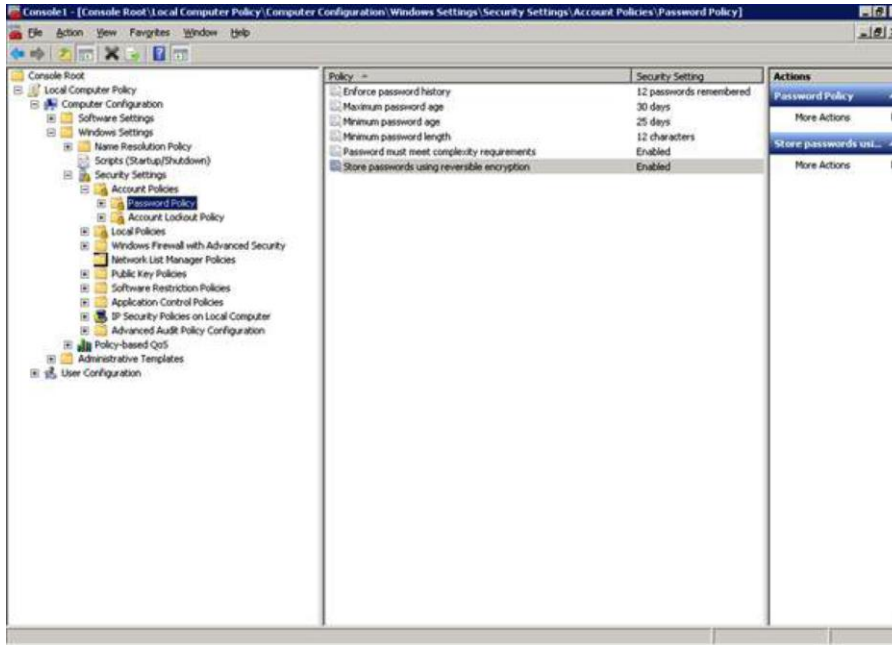
You must assign strong passwords to any default accounts (even if they won't be used), and then disable or do not use the accounts.

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.

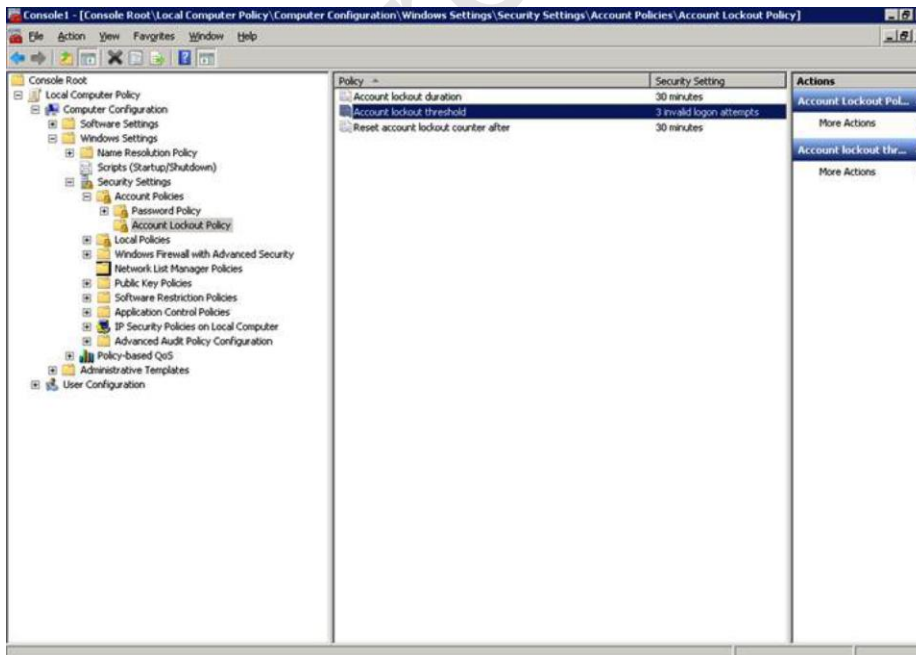
PA-DSS 3.2: Control access, via unique username and PCI DSS-compliant complex passwords, to any PCs or servers with payment applications and to databases storing cardholder data.

Establishing a Windows Secure Group Access Policy

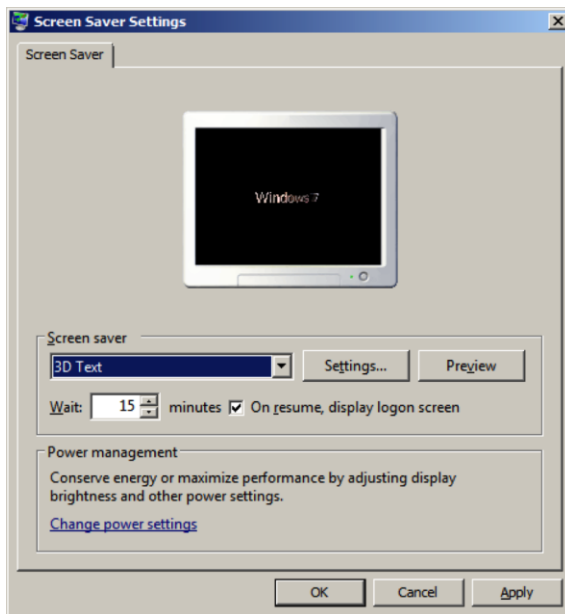
Users should configure a Windows secure group access policy on the machine on which NETePAY 5 is installed. Your Windows operating system environment must be modified to comply with the above requirements. Access these settings by going to Start/Run and type MMC. Add the snap-in for Group Policy Editor 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.

PCI-Compliant Wireless settings (PA-DSS 6.1.a and 6.2.b)

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.

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).

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)

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

NETePay 5 does not natively support any remote access functionality. NETePay 5 supports most types of two-factor remote solutions and does not require any specific one to be used. All two-factor vendor guidance should be followed to use that technology correctly and you should choose one that clearly uses two of the above. No configuration of NETePay 5 is required to accomplish this.

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

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 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 subscribes 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 10.2.3)

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)

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 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).

You must use strong cryptography and security protocols such as transport layer security (TLS 1.1 / TLS 1.2) 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.

NETePay 5 verifies the certificates of the payment processors it communicates with by verifying certificate ownership, expiration status and the acceptable signing authority.

NETePay 5 programmatically allows only secure versions of PCI-DSS acceptable protocols.

NETePay 5 has no configuration options that allow for a user to choose an improper encryption strength. The application does this programmatically with no user input.

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).

PCI requires that cardholder information sent via any end user messaging technology must use strong encryption of the data.

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, you 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, Windows 8, 10, Server 2008 or 2012 or Windows 10. 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

INSTALLATION

Introduction

This chapter explains how to install and configure the following *NETePay* components.

- *NETePay 5*
- *DSIClientX*, *dsiPDCX* or *dsiEMVX*
- *ePay Administrator*
- Microsoft SQL Express Database Engine
- Microsoft Internet Explorer 6.0 (or later) with High Encryption

You will need to install all the components on the server.

Each client machine will require *DSIClientX* or *dsiPDCX* be installed. *ePay Administrator* is installed on one or more client machines (for more information about using *ePay Administrator*, see the *ePay Administrator User Guide*).

If you are using version 5.1 (or later) of Microsoft Internet Explorer that already has high encryption, installation of Microsoft Internet Explorer 6.0 (or later) with High Encryption is optional. If you are using a version prior to 5.1, you must upgrade your Internet Explorer installation.

Requirements

Baseline System Configuration

To successfully install and run *NETePay 5* on your server, it should meet or exceed the following system requirements:

- Microsoft Windows Server 2008 or 2012, Windows 7, Windows 8 or Windows 10. All latest service packs, 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.
- TCP/IP network connectivity.
- Available COM port (if using dial backup)
- Datacap DialLink modem (if using dial backup)
- Persistent Internet Connection (DSL, cable, frame relay, etc.)

Network Requirements

- Before installing *NETePay 5* or any of its components, you should know the names and IP addresses of the servers receiving transactions. For remote servers or enterprise systems, it may be necessary to contact your network administrator or your merchant service provider
- You should also make port 9000 on the *NETePay 5* server available for incoming traffic if you are behind a firewall and connected to the default port.

Installation Procedures

Accessing the NETePay CD-ROM

Before you begin installing *NETePay 5* and its components, you should close all unnecessary programs and disable any anti-virus software.

Use either of the following procedures to access the folders that contain the setup programs for *NETePay 5* and its components:

1. Insert the CD-ROM labeled *NETePay 5* into the server's CD-ROM drive. If you have Window's AUTORUN feature enabled for your CD/DVD, then you will be presented with the following window:

The screenshot shows a web browser window titled "8660-92 - NETePay 5.05 (PT) x" with the address bar showing "file:///C:/AutoRun/default.htm". The page header includes the Datacap Systems, Inc. logo and the tagline "Reliable Integrated E-Payment Solutions". The main content is a table with four rows, each representing a step in the installation process. The first row is for the installation guide, the second for SQL server requirements, the third for installing NETePay, the fourth for EPay Admin, and the fifth for an optional DSIClient component. The footer contains copyright information for 2002-2013 Datacap Systems, Inc.

	Open Installation & Configuration Guide	This document (ReadMe.pdf) describes the installation and setup of NETePay for Paymentech Processing. Requires Acrobat Reader
STEP 1.	For Windows XP, 2003 Server, Install MSDE Datacap Instance OR For Windows Vista, 2008 Server (32-bit) Install SQL Express 2005 Datacap Instance OR For Windows 7 or 8 (32-bit) Install SQL Express 2008 Datacap Instance OR For Windows 7 or 8 (64-bit) or 2008 Server (64-bit) Install SQL Express 2008 (64-bit) Datacap Instance	For Windows XP or 2003 Server, NETePay requires this installation of SQL (MSDE) Server for batch management and reporting. If upgrading from an earlier version of NETePay where MSDE - Datacap Instance was previously installed, skip this step. For Windows Vista or 2008 Server (32-bit), NETePay requires this installation of SQL Express 2005 Server for batch management and reporting. If upgrading from an earlier version of NETePay where SQL Express 2005 - Datacap Instance was previously installed, skip this step. For Windows 7 or 8 (32-bit), NETePay requires this installation of SQL Express 2008 Server for batch management and reporting. If upgrading from an earlier version of NETePay where SQL Express 2008 - Datacap Instance was previously installed, skip this step. For Windows 7 or 8 (64-bit) or 2008 Server (64-bit), NETePay requires this installation of SQL Express 2008 Server for batch management and reporting. If upgrading from an earlier version of NETePay where SQL Express 2008 - Datacap Instance was previously installed, skip this step.
STEP 2.	Install NETePay	The NETePay Server communicates with Paymentech's NetConnect IP Gateway in order to process Credit card transactions.
STEP 3.	Install EPay Admin	EPay Admin is a stand-alone application that provides batch management and reporting by communicating with NETePay.
OPTIONAL	Install DSIClient	DSIClient is a stand-alone application used to send test transactions to NETePay.

Copyright © 2002-2013 Datacap Systems, Inc. - All rights reserved.
Revised: May 10, 2013.

2. If AUTORUN is not enabled on your system, then you should open **My Computer**, and then double-click the drive that contains the *NETePay* CD-ROM. The following window appears. Double click SETUP (or SETUP.EXE) to install NETePay 5.

Name ^	Date modified	Type	Size
program files	8/7/2013 1:10 AM	File folder	
System32	8/7/2013 1:10 AM	File folder	
Windows	8/7/2013 1:10 AM	File folder	
0x0409	3/23/2010 4:44 PM	Configuration settings	22 KB
instmsiw	11/28/2004 7:53 AM	Application	1,780 KB
NETePay 5.05 (PT 5.05) Paymentech Term	5/10/2013 2:45 PM	Windows Installer Package	2,863 KB
setup	5/10/2013 2:45 PM	Application	1,187 KB
Setup	5/10/2013 2:45 PM	Configuration settings	6 KB
WindowsInstaller-KB893803-x86	5/16/2005 4:42 PM	Application	2,525 KB

From either of these windows, you can install *NETePay 5* and its components.

3. ***You must be logged in as an 'Administrator' to install NETePay 5 and all of its components.*** Installations performed when logged on as another user with rights less than 'Administrator' will not operate correctly.

Preliminary

Installing/Upgrading Microsoft Internet Explorer

NETePay 5 uses Windows encryption services and requires that Internet Explorer with 128 bit encryption strength be installed on each system in the LAN. If needed, you must install or upgrade your server and each computer on the LAN with a version of Microsoft Internet Explorer that supports 128-bit encryption.

If needed, use the Windows Update on each PC to upgrade an existing version of IE to one that supports at least 128 bit encryption.

Installing SQL Express 2005 (Required for Windows Server 2008)

Note: You must be logged in as an 'Administrator' to install NETePay 5 and all of its components. Installations performed when logged on as another user with rights less than 'Administrator' will not operate correctly.

To install the SQL Express 2005:

1. Open the *SQL Express 2005 DatacapInstance 1.00* folder on the NETePay 5 CD-ROM and double-click **setup** (or setup.exe).
2. Accept all default values and click **NEXT** or **INSTALL** as requested.
3. Upon successful completion, you will be prompted to restart.
4. Click **Yes** to restart the computer. ***It is very important to restart at this time to avoid configuration problems!***

Note: When SQL Express 2005 DatacapInstance is installed, an application named **NETePay 5 Database Manager** is also installed in the Software from Datacap program group. This application provides basic maintenance functions, such as backup, restore and purge, and is covered in Chapter 5.

Installing SQL Express 2008 (Required for Windows Server 2012, Windows 7 & 8)

Note: You must be logged in as an 'Administrator' to install NETePay 5 and all of its components. Installations performed when logged on as another user with rights less than 'Administrator' will not operate correctly.

To install the SQL Express 2008:

1. Open the *SQL Express 2008 DatacapInstance 1.00* folder on the NETePay 5 CD-ROM and double-click **setup** (or setup.exe).
2. Accept all default values and click **NEXT** or **INSTALL** as requested.
3. Upon successful completion, you will be prompted to restart.
4. Click **Yes** to restart the computer. ***It is very important to restart at this time to avoid configuration problems!***

Note: When SQL Express 2008 DatacapInstance is installed, an application named **NETePay 5 Database Manager** is also installed in the Software from Datacap program group. This application provides basic maintenance functions, such as backup, restore and purge, and is covered in Chapter 5.

Installing NETePay 5 (Required)

Note: *You must be logged in as an 'Administrator' to install NETePay 5 and all of its components.* Installations performed when logged on as another user with rights less than 'Administrator' will not operate correctly.

To install the NETePay 5 Server software:

1. Open the NETePay 5 Server folder on the *NETePay 5* CD-ROM and double-click **setup** (or **setup.exe**).
2. The installation wizard will start. When the Welcome screen appears, click **Next**.
3. Read and accept the End User License agreement and click **Next**.
4. Enter your **User Name** and **Organization**. If available on your operating system, make the application available to all users.
5. Click **Next**, then click **Install**. The installation wizard will then begin installing the necessary files on your computer.
6. Click **Finish** to complete the installation. A pop-up message will then appear and inform you to restart the computer.
7. Click **Yes** to restart the computer. ***It is very important to restart at this time to avoid configuration problems!***

Installing DSIClient Application (Conditional)

Note: *You must be logged in as an 'Administrator' to install NETePay 5 and all of its components.* Installations performed when logged on as another user with rights less than 'Administrator' will not operate correctly.

The DSIClient application provides a convenient means to test operation of the NETePay 5 server and the store LAN configuration. It is not suitable for normal transaction processing since it does not print drafts or receipts. Your POS system should be used for normal transaction processing through NETePay 5.

Important Note:

The *DSIClient application* includes the DSIClientX ActiveX control which is required for NETePay 5 operation. If your POS system installs the DSIClientX ActiveX control, then installation of the DSIClient application is optional; if DSIClientX is not installed on your system, the installation of the DSIClient application is required.

To install the *DSIClient application* (includes the DSIClientX ActiveX control):

1. Open the DSIClient folder on the *NETePay 5* CD-ROM and double-click, **setup.exe**.
2. The installation wizard will start. When the Welcome screen appears, click **Next**.
3. Read and accept the End User License agreement and click **Next**.
4. Read the notes pertaining to *DSIClient* installation and click **Next**.
5. Enter your User Name and Organization.
6. If the option is available, make the application available to all users.
7. To begin installing the necessary files on your computer, click **Next**, then click **Install**.
8. To complete the installation process, click **Finish**. A pop-up message will then appear and inform you to restart the computer.
9. Click **Yes** to restart the computer.

Installing ePay Administrator for NETePay 5 (Required)

Note: You must be logged in as an 'Administrator' to install NETePay 5 and all of its components. Installations performed when logged on as another user with rights less than 'Administrator' will not operate correctly.

Note: The ePay Administrator for NETePay 5 software is designed to use the LAN to perform transaction editing and reporting. Best security practices advise that you to install the ePay Administrator for NETePay 5 software on a workstation on the LAN, not on the server.

To install *ePay Administrator for NETePay 5*:

1. Open the ePayAdmin folder on the *NETePay 5* CD-ROM and double-click **setup.exe**.
2. The installation wizard will start. When the Welcome screen appears, click **Next**.
3. Read and accept the End User License agreement and click **Next**.
4. Enter your **User Name** and **Organization**.
If available on your operating system, make the application available to all users.
5. Click **Next**, then click **Install**. The installation wizard will then begin installing the necessary files on your computer.
6. Click **Finish** to complete the installation. A pop-up message will then appear and inform you to restart the computer.
7. Click **Yes** to restart the computer.

For more information about using *ePay Administrator for NETePay 5*, see the *ePay Administrator for NETePay 5 User Guide*

Installing Datacap DialLink modem (Required for Dial Backup Operation)

Note: To use the dial capabilities of NETePay 5 (as backup communications), a Datacap DialLink modem (not a DataTran) must be attached to an available COM port on the PC.

To install the *Datacap DialLink modem* for *NETePay 5*:

1. Connect the uDIN8 connector of the interface cable to the Datacap DialLink modem PC/ECR port.
2. Connect the DB9 end of the interface cable to the intended COM port on the PC.
3. Connect one end of the RJ11 cable to the TELCO connector on the Datacap DialLink modem.
4. Connect the other end of the RJ11 cable to a working phone line jack. No other devices should be connected to this phone line and plain old telephone service (POTS) line is best.
5. Connect the transformer to the POWER connector on the Datacap DialLink modem.
6. Plug the transformer into a suitable 110VAC outlet. It is strongly recommended that a surge protector be used with the Datacap DialLink modem.

NETePay 5 CONFIGURATION

Introduction

This chapter explains how to activate and configure *NETePay 5* for use.

NETePay 5 is activated and programmed over the Internet so a working Internet connection is required for the process.

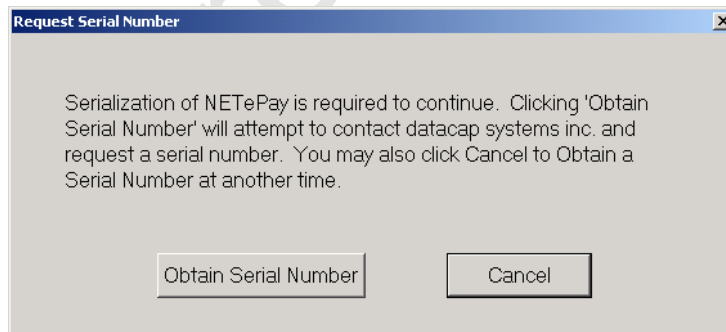
Note

Firewalls, routers or other systems which can block IP network traffic must allow *NETePay 5* to accept traffic on port 9000.

NETePay 5 must complete two actions on the Internet before it is ready to process transactions. The first is to obtain a license file from Datacap's PSCS (Payment Systems Configuration Server) system. The second is to retrieve merchant parameters from Datacap's PSCS server.

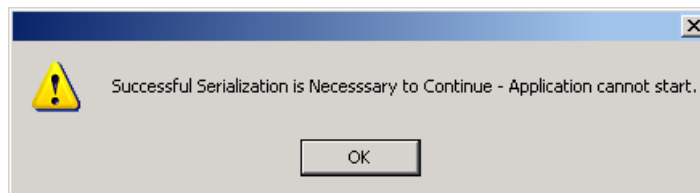
Activation and Parameter Download

1. On the first program launch after installation, *NETePay 5* must obtain a license file over the Internet from Datacap's PSCS (Payment Systems Configuration Server) system. When *NETePay 5* detects that a serial number is required, it presents the following dialog:



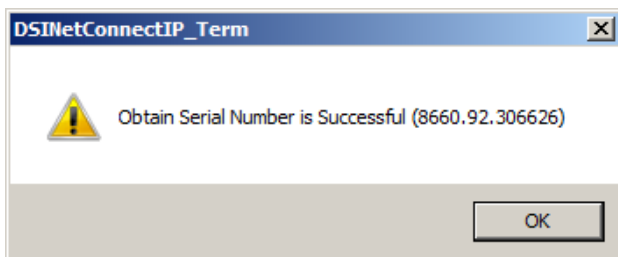
Click 'Obtain Serial Number' to enable *NETePay 5* to contact PSCS for a serial number.

2. If *NETePay 5* is unsuccessful in obtaining a serial number, it will present the following dialog:

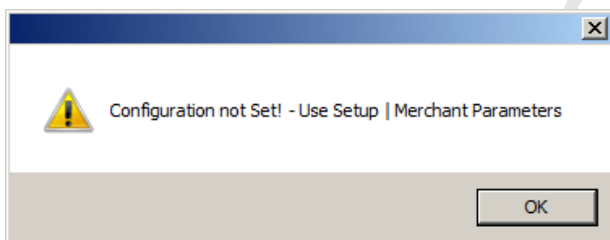


Click 'OK' and NETePay 5 will close. Failure to successfully obtain a serial number means that NETePay 5 was not able to contact Datacap's PSCS server over the Internet to obtain a serial number. Assure that the Internet connection is operating properly by using the default web browser on the machine where NETePay 5 is installed to contact www.datacapsystems.com. If you are successful in contacting Datacap's website, close the browser, restart NETePay 5 and click 'Obtain Serial Number' again. If you continue to experience difficulties in obtaining a serial number, contact your network administrator to assure that there are no firewall or DNS issues.

- At this point, NETePay 5 could present two possible responses. If *NETePay 5 is successful in obtaining a serial number but is unable to locate merchant parameters for the assigned serial number*, you will see the following dialog:



The dialog contains the 10 digit serial number that was automatically assigned to NETePay 5. Click 'OK' to continue and then you will see the following dialog:



This dialog indicates that NETePay 5 has not yet retrieved merchant parameters from Datacap's PSCS server and cannot operate until parameters are downloaded.

If a parameter file has been created on Datacap's PSCS server for the merchant account, then select 'Merchant Parameters' from the 'Setup' drop down menu. You will then see the following screen:

Setup NETePay Parameters

Merchant Information

Merchant ID: 000000000000 Terminal ID: 000 Client ID: 0000 Merchant Category: Retail

Contactless Capable Send <Memo> as Customer Data Verify NetConnect SSL Certificate

Do Not Connect to Paymentech on Startup Go To System Tray when Minimized.

NetConnect Information

User ID: 0 Password: *

Security

Use Client / Server Password Truncate Sensitive Data

Transport

IP Only IP with DIAL Backup DIAL Only

Dial Backup Information

Comm Port: 1 Dial Prefix: Paymentech Authorization Phone No.: 18775295688

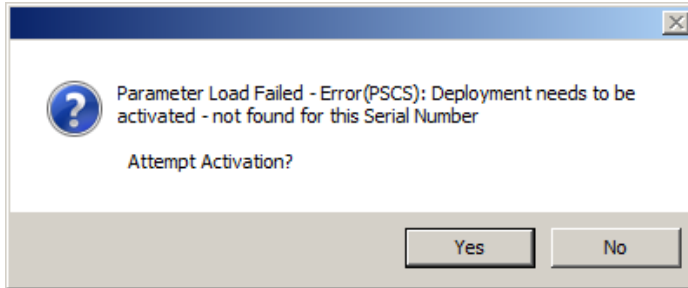
IP Connection Information

Connect Timeout to NetConnect: 3 Seconds.

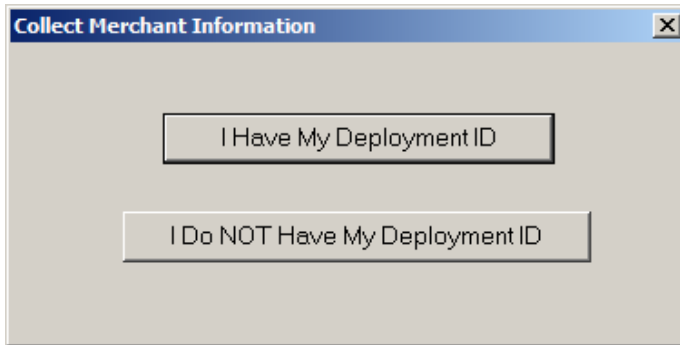
Max Lanes: 1 Lane Setup

OK Load New Parameters PSCS

This setup screen displays the current values for the merchant parameters which are all 0's indicating that merchant parameters have not yet been loaded from Datacap's PSCS server. Click 'Load New Parameters' and you will see the following screen:

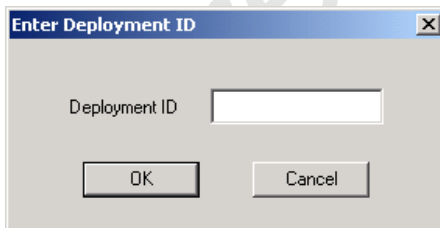


Click 'Yes' to attempt activation and you will see the following screen:



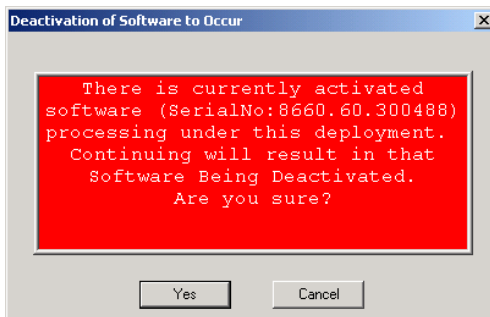
To continue, you must verify that you or someone else has created a Merchant Deployment on Datacap's PSCS server. If a deployment was created you may have been given a Deployment ID, which is typically an eight character code that has been assigned to the merchant's parameters. If you have a Deployment ID for the merchant, click 'I Have My Deployment ID'. If the merchant's parameters were created on PSCS but you do not have the Deployment ID, proceed to step 4.

When you click 'I Have My Deployment ID', you will see the following dialog:



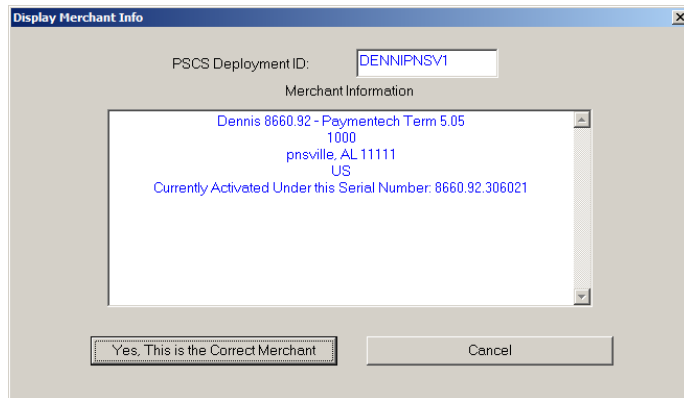
Enter the Deployment ID for the merchant parameter file and click 'OK'.

If NETePay 5 detects that the Deployment ID is already in use by another serial number, you will see the following dialog:



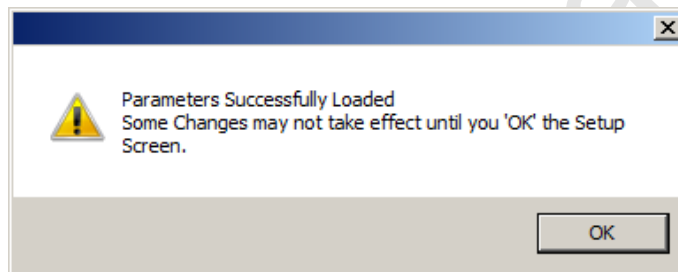
If you see this Deactivation Warning dialog, proceed to step 5.

NETePay 5 will display a screen with merchant demographic data for you to verify as follows:

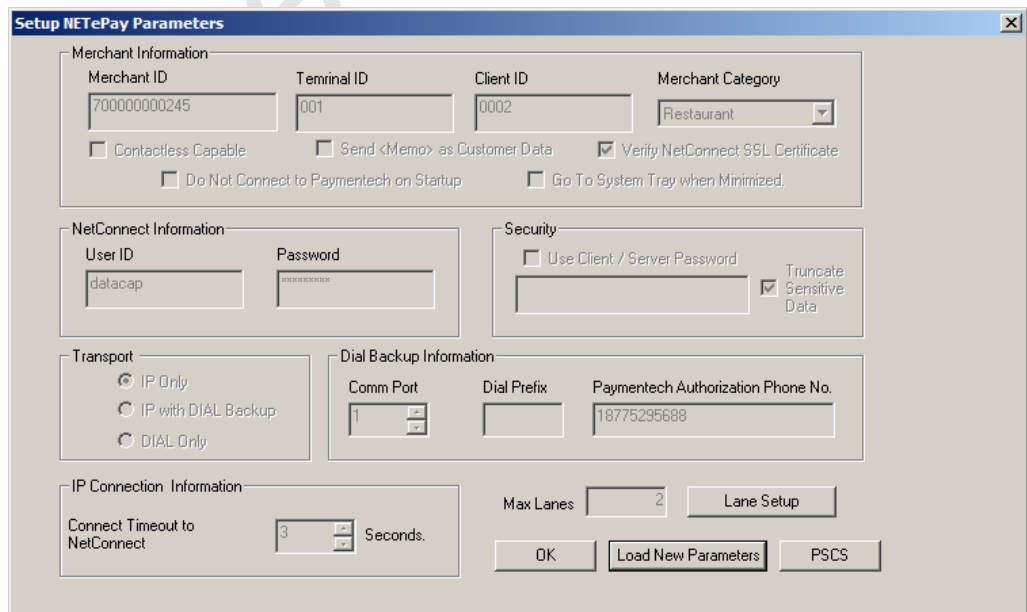


If the displayed information is not correct for the merchant site, click 'Cancel' and retry entry from the beginning of step 4. If the displayed information correctly identifies the merchant site, click 'Yes, This is the Correct Merchant'.

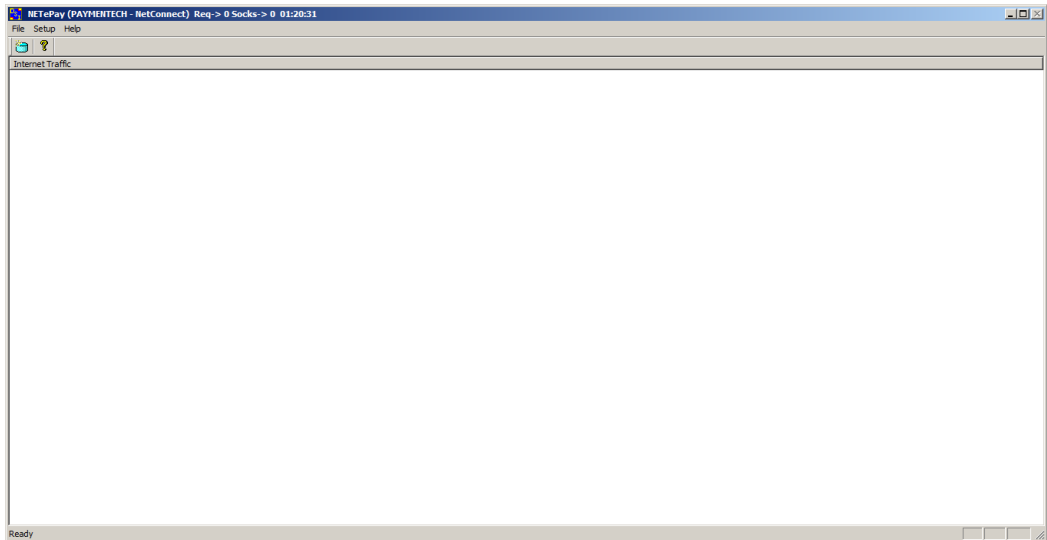
If NETePay 5 successfully retrieves the parameters associated with the entered Deployment ID from the PSCS server, you will see the following dialog:



Click 'OK' and will then again see the setup screen as follows:

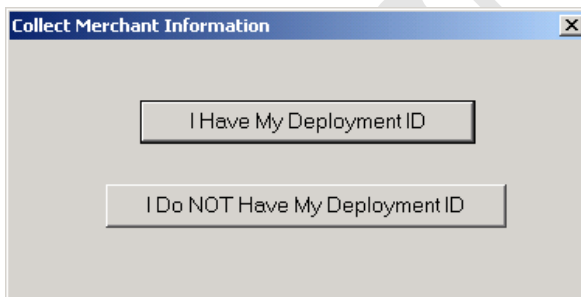


The setup screen now contains non-zero values in the text boxes throughout the screen indicating the values retrieved from Datacap's PSCS server. You should verify that the parameters are correct and then click 'OK' to complete the setup process. You will then see the NETePay 5 main status window indicating that NETePay 5 is now programmed and ready to process transactions.

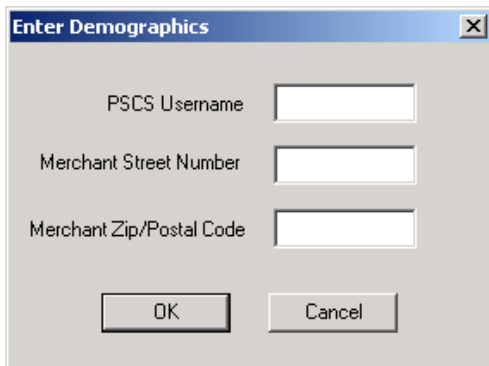


NETePay 5 setup is complete.

4. If you don't have the PSCS Deployment ID for the merchant, click 'I Do NOT Have My Deployment ID' in the following dialog:



You will then see a dialog that will allow you to retrieve the PSCS merchant parameters from Datacap's PSCS server using merchant demographic information as follows:



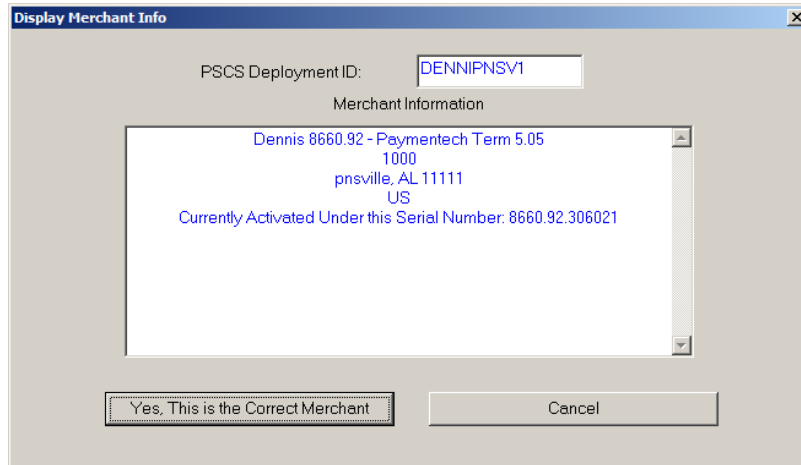
You need the following information to complete the demographics dialog entries:

- The PSCS user under which the merchant parameter file was created on the PSCS server

- The merchant location street number (e.g. enter '123' for 123 Main St.)
- The merchant location 5 digit zip code or 6 character Canadian postal code

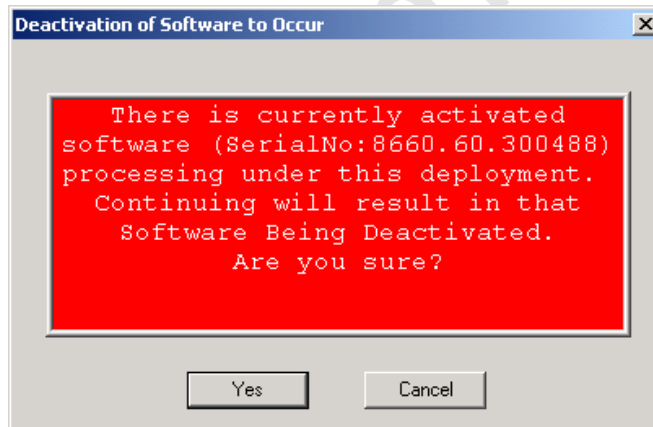
After entering this information, click 'OK'.

If NETePay 5 is successful in retrieving the merchant parameters from Datacap's PSCS server, then you will see the following screen:



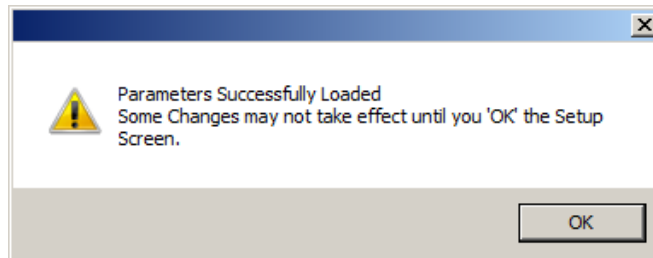
If the displayed information is not correct for the merchant site, click 'Cancel' and retry entry from the beginning of step 4. If the displayed information correctly identifies the merchant site, click 'Yes, This is the Correct Merchant'.

If NETePay 5 detects that the selected merchant is already in use by another serial number, you will see the following dialog:



If you see this Deactivation Warning dialog, proceed to step 5.

If the parameters are successfully loaded, you will see the following dialog:



Click 'OK' and you will then see the setup screen as follows:

Setup NETePay Parameters

Merchant Information

Merchant ID: 70000000245 Terminal ID: 001 Client ID: 0002 Merchant Category: Restaurant

Contactless Capable Send <Memo> as Customer Data Verify NetConnect SSL Certificate

Do Not Connect to Paymentech on Startup Go To System Tray when Minimized.

NetConnect Information

User ID: datacap Password: [REDACTED]

Security

Use Client / Server Password Truncate Sensitive Data

Transport

IP Only
 IP with DIAL Backup
 DIAL Only

Dial Backup Information

Comm Port: 1 Dial Prefix: [REDACTED] Paymentech Authorization Phone No.: 18775295688

IP Connection Information

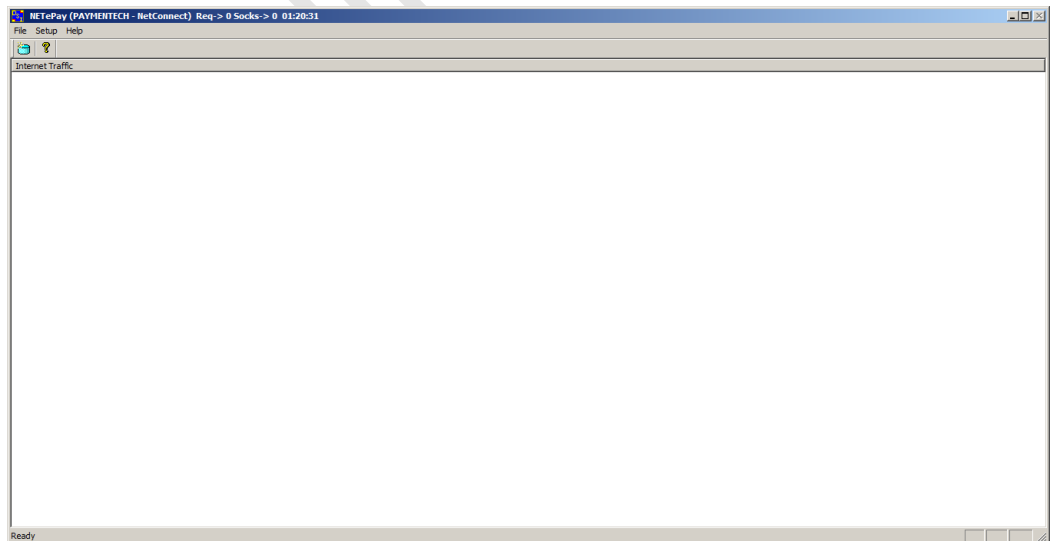
Connect Timeout to NetConnect: 3 Seconds. Max Lanes: 2 Lane Setup

OK Load New Parameters PSCS

The setup screen now contains non-zero values in the text boxes throughout the screen indicating the values retrieved from Datacap’s PSCS server. You should verify that the parameters are correct and then click ‘OK’ to complete the setup process.

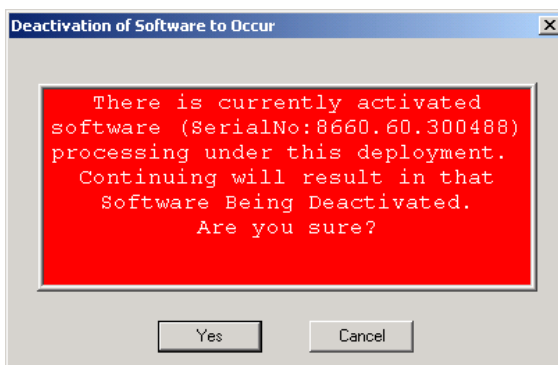
Lane Setup allows you to optionally change the description associated with each lane that was authorized in the PSCS parameter file. You cannot alter the number of lanes in NETePay 5; changes to the number of lanes must be done by editing the deployment file in PSCS.

You will then see the NETePay 5 main status window indicating that NETePay 5 is now programmed and ready to process transactions.



NETePay 5 setup is complete.

5. If you receive the following Deactivation Warning dialog when entering a Deployment ID or Merchant Demographic Information that means another installation of NETePay 5 is already using the merchant parameters associated with the Deployment ID or demographic information.



Verify that the Deployment ID or demographic information entered is correct; if not click 'Cancel' and retry the entry.

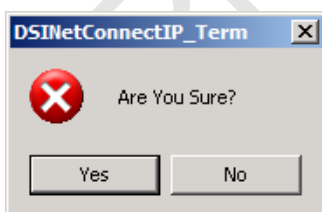
If the Deployment ID or merchant demographic information is correct and you want to force the parameters to load into NETePay 5, you should be aware that the NETePay 5 with the serial number listed in the dialog box will be deactivated and will no longer be able to process transactions.

This dialog is typically encountered when the current NETePay 5 is a replacement for a NETePay 5 already activated for the same merchant who may have had a computer problem or hard disk failure that no longer allows them to use that earlier NETePay 5 installation. This process will allow the new NETePay 5 installation to use the existing merchant parameters associated with the entered Deployment ID without the need to create a new parameter file on Datacap's PSCS server.

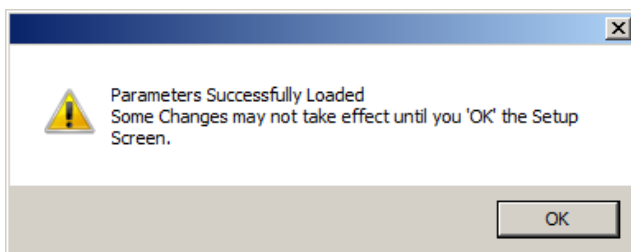
WARNING:

Do not select 'Yes' unless you are certain that the NETePay 5 with the serial number listed in the dialog box should be deactivated.

If you are certain that you want to deactivate the NETePay 5 serial number listed in the Deactivation Warning dialog and use it with the new NETePay 5, then click 'OK'. You will see the following dialog which verifies your choice:



Click 'Yes' to if you are certain that you want to deactivate the NETePay 5 serial number listed in the Deactivation Warning dialog and use it with the new NETePay 5. You will then see the following screen if the parameter download from Datacap's PSCS server is successful:



Click 'OK' and will then again see the setup screen as follows:

Setup NETePay Parameters

Merchant Information

Merchant ID: 70000000245 Terminal ID: 001 Client ID: 0002 Merchant Category: Restaurant

Contactless Capable Send <Memo> as Customer Data Verify NetConnect SSL Certificate

Do Not Connect to Paymentech on Startup Go To System Tray when Minimized.

NetConnect Information

User ID: datacap Password: [REDACTED]

Security

Use Client / Server Password Truncate Sensitive Data

Transport

IP Only IP with DIAL Backup DIAL Only

Dial Backup Information

Comm Port: 1 Dial Prefix: Paymentech Authorization Phone No.: 18775295688

IP Connection Information

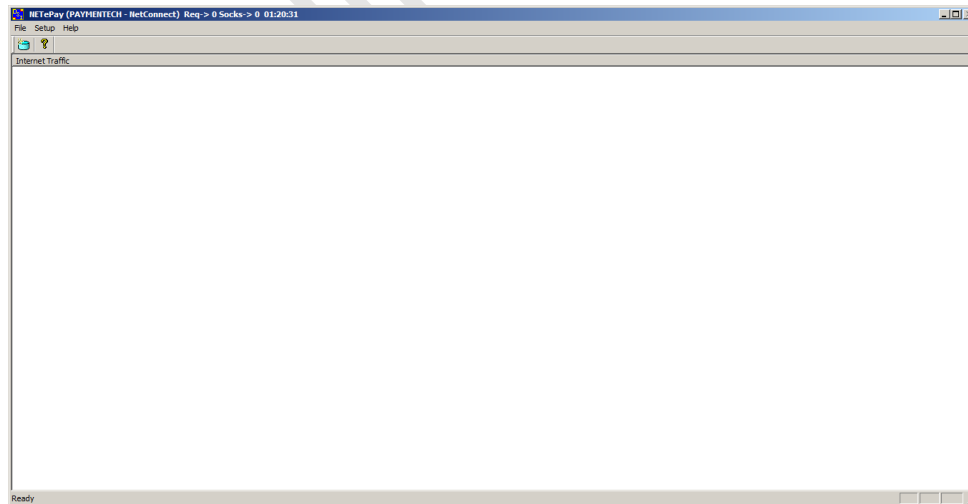
Connect Timeout to NetConnect: 3 Seconds. Max Lanes: 2 Lane Setup

OK Load New Parameters PSCS

The setup screen now contains non-zero values in the text boxes throughout the screen indicating the values retrieved from Datacap's PSCS server. You should verify that the parameters are correct and then click 'OK' to complete the setup process.

Lane Setup allows you to optionally change the description associated with each lane that was authorized in the PSCS parameter file. You cannot alter the number of lanes in NETePay 5; changes to the number of lanes must be done by editing the deployment file in PSCS.

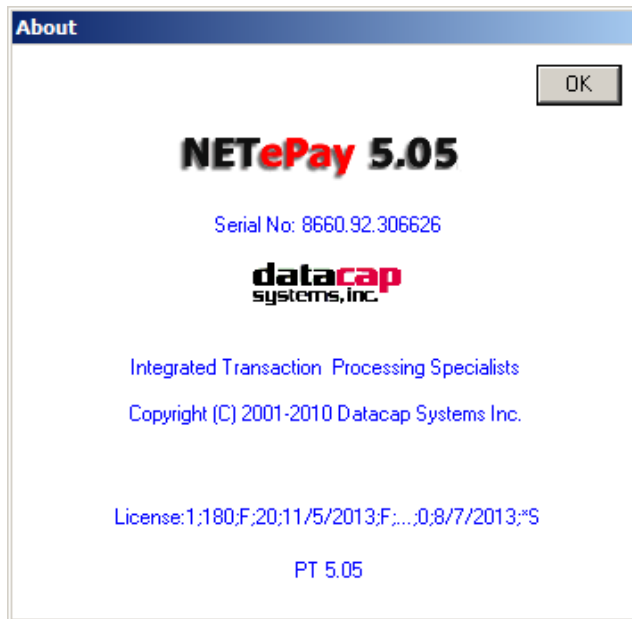
You will then see the NETePay 5 main status window indicating that NETePay 5 is now programmed and ready to process transactions.



NETePay 5 setup is complete.

Verifying Your Serial Number and Activation

You can verify the serial number assigned to your copy of NETePay 5 by selecting **About** from the **Help** menu item in the main status window. You will see a dialog box containing the serial number and some additional information of the activation that you may need to supply in certain support situations. An example of the dialog box information is as follows:



Testing

Important! - Before You Start

You should arrange with your bank and payment processor for testing *NETePay 5* and all other related components before going live. You should perform a sale and return transaction of \$1.00 for each card type you will be accepting using live credit cards. You should then verify with your processing provider that all transactions were credited properly.

It is the sole responsibility of the merchant account holder to verify that the merchant information entered into NETePay 5 is complete and correct.

You should only process actual customer payments after you have verified with your merchant account provider that all test transactions have been successfully processed.

Operational Considerations

Important!

NETePay 5 relies on numerous services provided by Windows and other Microsoft software such as MSDE or SQLExpress 2005. **Proper computer operation is imperative to ensure reliable NETePay 5 operation and prevent possible loss and/or corruption of transaction data.**

The following operational guidelines *must* be observed to ensure reliable NETePay 5 operation:

- *Always* quit NETePay 5 from the File|Exit pull down menu before restarting or shutting down Windows.
- *Always* quit NETePay 5 and then shut down Windows before turning off the computer power. Never turn off the computer power without first quitting NETePay 5 and shutting down Windows.
- *Always* quit NETePay 5 and shut down Windows before pressing the reset button on the computer.
- If the computer is subject to unplanned power losses, the use of an UPS (Uninterruptible Power Supply) is *highly recommended*.
- If you operate a backup copy of NETePay 5, you *must* procure unique terminal and/or merchant account information for each copy of NETePay 5 from your processing provider. Operation of multiple copies of NETePay 5 with identical merchant setup information may cause transactions to be lost or duplicated at your processing provider.

Preliminary

USING THE NETEPAY - DATABASE MANAGER

Introduction

This chapter explains how to use the *NETePay Database Manager* program to perform maintenance functions on NETePay's MSDE/SQL Express database. The *NETePay Database Manager* program is installed as part of the NETePay 5 installation. The *NETePay Database Manager* program is available in the Software from Datacap program group available under the Programs menu under the Windows Start button.

Maintenance Functions

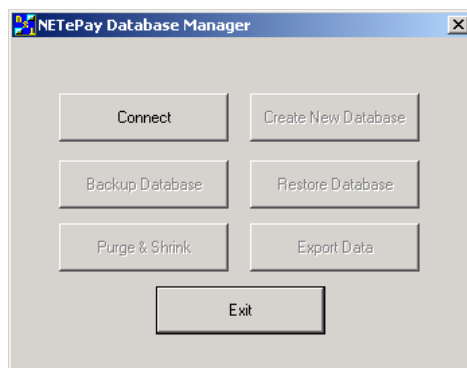
The *NETePay Database Manager* can perform the following functions:

- **Connect** – Before any of the maintenance functions can be performed, the NETePay Database Manager must be connected to the database.
- **Backup Database** – This function will backup the current database to a file that is automatically named with the current date (or a user defined name). These backup files can subsequently be Restored if there's a database problem. *It is strongly recommended that you regularly backup the database.*
- **Purge & Shrink** – This function allows you to control the size of the database by removing older transaction data based on its age. This function will prevent the database from growing too large and using disk storage inefficiently. *It is strongly recommended that you keep only the oldest transactions required by your processing provider and delete any older to save disk space.*
- **Create New Database** – This function allows you to create a new, empty database with no transactions. Normally, this type of function would be used only when instructed by a technical support person.
- **Restore Database** - This function allows you to restore a previously saved backup database file.
- **Export Database** – This function allows you to export a copy of the data to a CSV (comma separated value) format file. Note that only open records (i.e. transactions which have not been settled) are included in the export file.

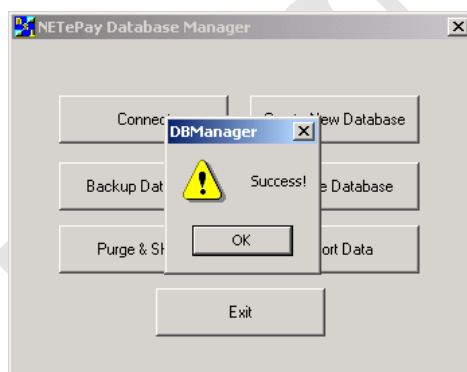
Using the NETePay Database Manager

To start, launch the program by selecting **NETePay Database Manager** from the **Software from Datacap** program group under **Start|Programs**. The following main screen will be presented:

Connecting to the Database



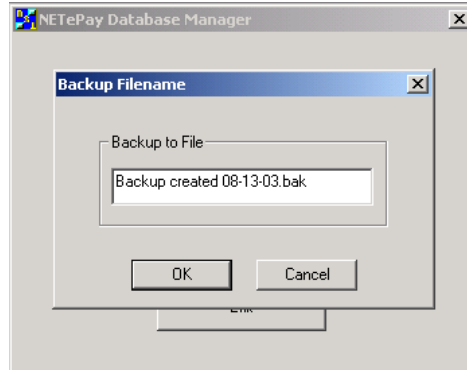
1. Before any of the maintenance functions can be performed, the NETePay Database Manager must be connected to the database. Click the **Connect** button.
2. If the NETePay 5 database is located and successfully opened, after a few moments, you will see the following:



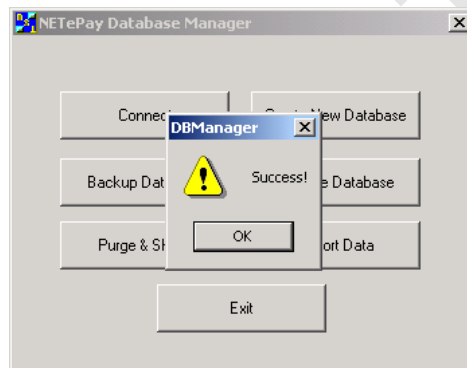
If the Database Manager cannot establish a connection to the database, make sure that MSDE was previously installed and note the error codes.

Backing Up Your Database

1. To backup the current database, click the **Backup Database** button. The following dialog will be displayed:



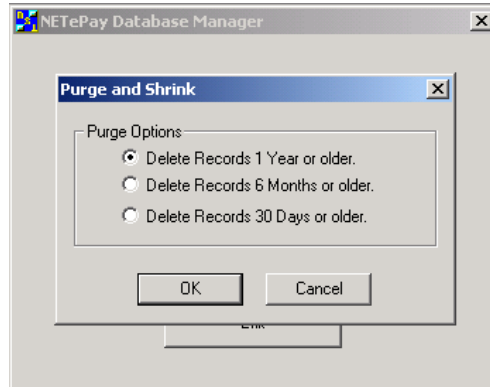
2. A file name with today's date will automatically be generated. If that is acceptable, click OK. If you want a different file name to be used for the backup file, you may type it in the text box and click OK.
3. If the backup operation is successful, after a few moments, you will see the following:



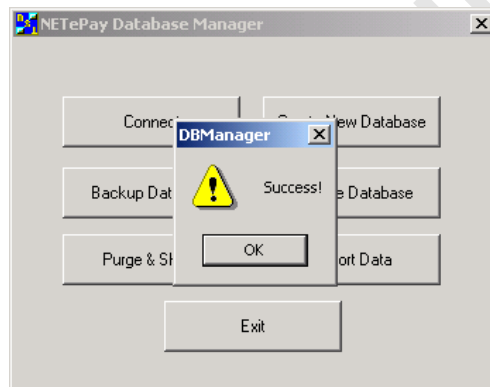
Note: This function will backup the current database with the most recent transactions. Backup files can subsequently be Restored if there's a database problem. *It is strongly recommended that you regularly backup the database file.*

Purging and Shrinking Your Database

1. To remove old transaction data from the database and save disk storage space, click the **Purge & Shrink** button. The following dialog will be displayed:



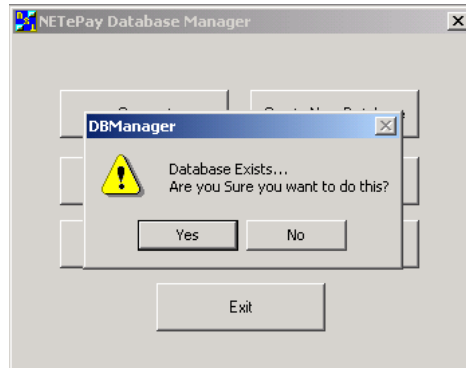
2. Select the age of transaction records that you want to remove from the database and click OK.
3. If the **Purge and Shrink** operation is successful, after a few moments, you will see the following:



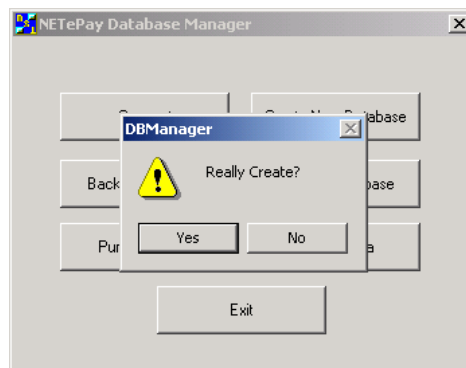
Note: This function will prevent the database from growing too large and using disk storage inefficiently. *It is strongly recommended that you keep only the oldest transactions required by you processing provider and delete any older to save disk space.*

Creating a New Database

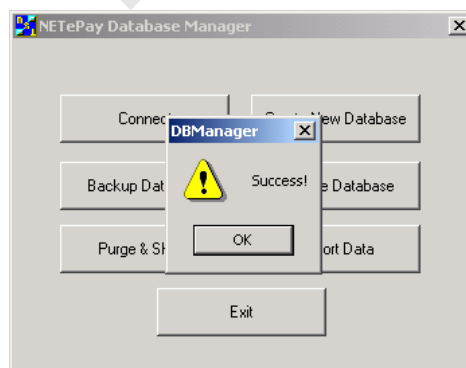
1. To create a new empty database, click the **Create Database** button. The following dialog will be displayed:



2. Since the **Create Database** operation replaces the current database with a new one, the dialog box will remind you that there's a current database. Click YES to proceed with create.
3. Since the current database will be lost, another dialog confirms the operation. Click YES to continue with the create.



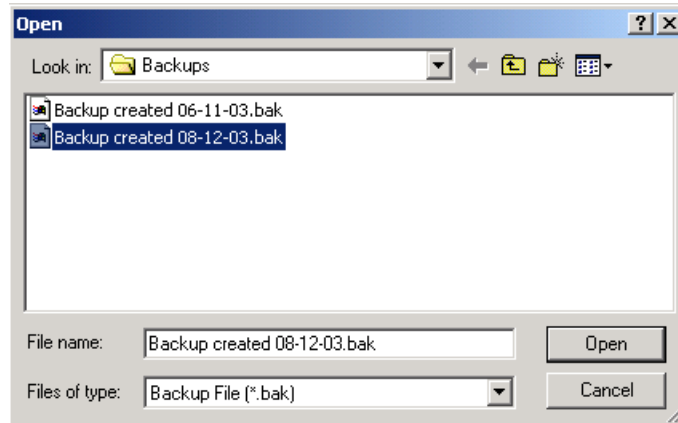
4. If the **Create Database** operation is successful, after a few moments, you will see the following:



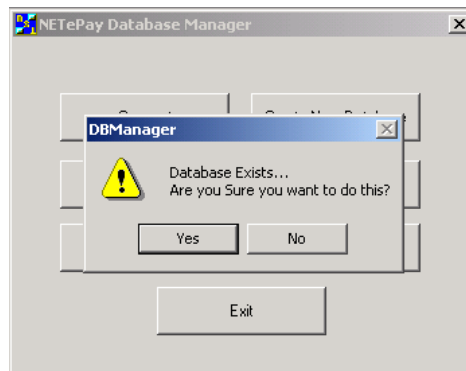
Note: This function is normally used by support personnel. *Caution! Since this operation destroys any current data, make sure you backup any current database before using!*

Restoring Your Database

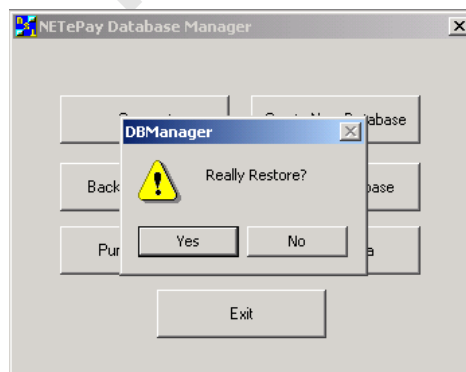
1. To restore and previously backed up database, click the **Restore Database** button. A file dialog will be presented and you should select the file that you want to restore to the current database:



2. Since the restore operation replaces the current database with an older one, the dialog box will remind you that there's a current database. Click YES to proceed with restore.



3. Since the current database will be lost, another dialog confirms the operation. Click YES to continue with the restore.



4. If the **Restore Database** operation is successful, after a few moments, you will see the following:

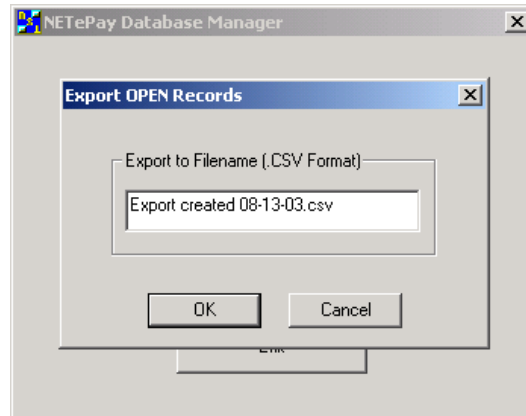


Note: This function will prevent the database from growing too large and using disk storage inefficiently. *It is strongly recommended that you keep only the oldest transactions required by you processing provider and delete any older to save disk space.*

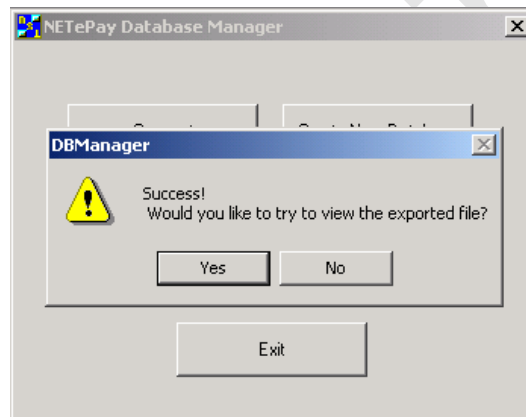
Preliminary

Exporting Your Database

1. To backup the current database, click the **Backup Database** button. The following dialog will be displayed:



2. An export file name with today's date and a ".csv" extension will automatically be generated. If that is acceptable, click OK. If you want a different file name to be used for the export file, you may type it in the text box and click OK.
3. If the export operation is successful, after a few moments, you will see the following:



If you select YES, then the exported file will open in an associated application (such as Microsoft Excel).

INDEX

A		N	
About		NETePay	
NETePay, 5		Installation, 45, 46	
		Testing, 58	
		Network Requirements, 43	
C		O	
Credit Sale, 60		Overview, 5	
D		R	
DSIClient Transaction Utility		Requirements	
Setup, 61		Network, 43	
Supported Transaction Types, 60		Server, 42	
E		S	
ePay Administrator Installation, 47, 48		Server Requirements, 42	
H		U	
How it works, 6		Upgrading Microsoft Internet Explorer, 45	
		Using the DSIClient Transaction Utility, 60	
I		W	
Installation, 42		What's Included on your CD, 5	
Installation Procedures, 43			
Accessing the NETePay CD-ROM, 43			
ePay Administrator, 47, 48			
NETePay, 45, 46			