datacap systems, inc.

NETePay 5

Installation & Configuration Guide

Datacap Hosted For Canada

Includes PA-DSS V3.2 Implementation Guide

Version 5.07

Part Number: 8730.20

NETePay Installation & Configuration Guide

Revised: 07 Jan 2021

Version Support

This document supports the following application versions:

NETePay 5 (Datacap Hosted for Canada - Rental) - Version 5.07.XX

NETePay 5 Director - Version 5.07.XX

NETePayService – V 1.1.0.0

DSIEMVClientX, Version 1.33

DSIClientX, Version 3.86

dsiPDCX, Version 1.59

dsiEMVUS, Version 1.31

Payment Processor Support

This document supports the following payment processor:

Datacap Hosted for Canada

CONTENTS

OVERVIEW

Introduction

About NETePay

Developed by Datacap Systems, *NETePay* enables retail, restaurant and other businesses to perform fast electronic payment authorizations via the Internet.

NETePay 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.

About Datacap

Datacap Systems, Inc. develops and markets electronic payment interfaces that enable cash register and business systems developers to add electronic payment acceptance to their systems.

Datacap has various solutions that interface to virtually any hardware or software platform and send transactions to all major payment processors via most common communications technologies including dial, wireless, and Internet.

How it works

NETePay is an application that executes on a server at the store level and monitors transaction requests from client machines using a POS application integrated with one of Datacap's client ActiveX controls, DSIEMVClientX, DSIClientX, dsiPDCX or dsiEMVX.

When *NETePay* receives an encrypted transaction request from a client control integrated with POS software, it sends the request to the processing host for approval via the Internet or other TCP/IP Virtual Private Network (VPN) services.

CHAPTER 2

PA DSS 3.2 - 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 3.2 dated May 2016).

Datacap Systems instructs and advises its customers to deploy Datacap Systems applications in a manner that adheres to the PCI Data Security Standard (v3.2). 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 INC 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 Inc. 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 retailer may undertake activities that may affect compliance. For this reason, Datacap Systems Inc. is required to be specific to only the standard software provided by it.

About this Document

This document describes the steps that must be followed in order for your NETePay 5 installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application - Data Security Standards program (version 3.2 dated June 2016). Datacap Systems Inc. instructs and advises its customers to deploy Datacap Systems Inc. applications in a manner that adheres to the PCI Data Security Standard (v3.2). 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.

Revision Information

Name	Title	Date of Update	Summary of Changes
NETePay 5	PA-DSS 2.0 Implementation Guide	29 April 2013	Document Creation for PA-DSS 2.0 - Version 1.00
NETePay 5	PA-DSS 2.0 Implementation Guide	18 Mar 2014	Annual Review – No Updates - Version 1.00
NETePay 5	PA-DSS 2.0 Implementation Guide	12 Nov 2014	Revised Application Description – Version 1.01
NETePay 5	PA-DSS 3.1 Implementation Guide	24 Sept 2015	Document Update for PA-DSS 3.1 – Version 1.01
NETePay 5	PA-DSS 3.1 Implementation Guide	02 Aug 2016	Annual Review – No Updates - Version 1.01
NETePay 5	PA-DSS 3.1 Implementation Guide	08 Jan 2017	Document for Update – Windows Service Support - Version 1.02
NETePay 5	PA-DSS 3.2 Implementation Guide	15 Jun 2017	Document Update for PA-DSS 3.2 – Version 1.03

Note: This PA-DSS Implementation Guide must be reviewed on a yearly basis, whenever the underlying application changes or whenever the PA-DSS requirements change. Updates should be tracked and reasonable accommodations should be made to distribute or make the updated guide available to users. Datacap Systems Inc. will distribute the IG to new customers as a file included with the software distribution and via Datacap's website.

Executive Summary

NETePay 5 Version 5.07.XX has been Payment Application - Data Security Standard (PA-DSS) validated, in accordance with PA-DSS Version 3.2. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Coalfire Systems, Inc. 11000 Westmoor Circle, Suite 450, Westminster, CO 80021	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 Inc.'s NETePay 5 Version 5.07.XX 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)
- Payment Card Industry Data Security Standard (PCI DSS)
- Open Web Application Security Project (OWASP)
- Center for Internet Security (CIS) Benchmarks (used for OS Hardening)

Application Summary

<table>
<tr><td>Payment Application Name</td><td>NETePay 5</td><td>Payment Application Version</td><td>5.07.XX</td></tr>
<tr><td>Application Description</td><td colspan="3">NETePay is client-server based payment middleware designed to integrate with POS systems needing payment capabilities for a wide variety of transaction types, markets and processing providers.

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

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

NETePay can remove the need for POS software to have any interaction with or visibility to cardholder data. By eliminating the need to handle, transmit or store any type of cardholder information, NETePay may provide POS software systems with a streamlined path to achieve PA-DSS compliance.</td></tr>
<tr><td>Typical Role of Application</td><td colspan="3">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, and MOTO industry segments.</td></tr>
<tr><td>Target Market for Payment Application</td><td colspan="3">
<table>
<tr><td colspan="6">Target Market for Payment Application (check all that apply):</td></tr>
<tr><td>X</td><td>Retail</td><td></td><td>Processors</td><td></td><td>Gas/Oil</td></tr>
<tr><td></td><td>e-Commerce</td><td>X</td><td>Small/medium merchants</td><td></td><td></td></tr>
<tr><td>X</td><td colspan="5">Others (please specify): Restaurant, MOTO</td></tr>
</table>
</td></tr>
<tr><td rowspan="3">Stored Cardholder Data</td><td colspan="3">The following is a brief description of files and tables that store cardholder data:</td></tr>
<tr><td colspan="2">File or Table Name</td><td>Description of Stored Cardholder Data</td></tr>
<tr><td colspan="2">File:
DSIVitalTNSIP_Host_5_07_xxxxxxx.db
where 'xxxxxxx' is the Build designation.

Tables:
batch
store_and_forward
store_and_forward_detail</td><td>Temporarily:

Full track data, card verification codes and values (CAV2, CID, CVC2, CVV2), PINs and PIN blocks</td></tr>
</table>

	Individual access to cardholder data is logged as follows: NETePay 5 does not log full text PAN's or expiration dates in any context - only truncated data (i.e. last 4 digits, of PAN's) are recorded. Since NETePay 5 only logs truncated cardholder data, it does not track or record log access activity.
Components of the Payment Application	The following are the application-vendor-developed components which comprise the payment application: **NETePay.exe:** Windows desktop application that provides transaction processing services for requests received from DSIClientX, dsiPDCX or dsiEMVX direct to Payment Service Provider using secure protocols over the Internet. **DSIClientX.ocx, dsiPDCX.ocx or dsiEMVX.ocx:** Windows ActiveX controls integrated with third party POS software on primary POS terminals that communicate transactions requests securely to NETePay application. **NETePayService.exe:** Windows executable that allows the NETePay 5 application (NETePay.exe) to be optionally started as a service for desktop versions of Windows (excludes Win CE7)
Required Third Party Payment Application Software	The following are additional third party payment application components required by the payment application: None
Database Software Supported	The following are database management systems supported by the payment application: None
Other Required Third Party Software	The following are other required third party software components required by the payment application: None
Operating System(s) Supported	The following are Operating Systems supported or required by the payment application: Latest Supported Versions of: • Windows 7 SP1 • Windows 10 • Windows Server 2012 R2 • Windows Server 2016 • Windows Compact Edition 7 For Microsoft Windows Compact Edition 7, NETePay 5 on executes on only Datacap proprietary Tran Series hardware which are preloaded with a customized, headless core version Windows CE 7. The Tran models supported are: TranServer IPTran IPTranLT TwinTran TranCloud

<table>
<tr><td></td><td>Tran devices are equipped with Ethernet interfaces for connection to the CDE – they do not support any type of wireless connection directly. The NETePay 5 executable for CE 7 is designed to validate a unique Tran identity built into each hardware example during manufacture. NETePay 5 activation based on the unique ID of each hardware example is required and therefore it cannot be loaded into or execute from any other CE 7 based systems.</td></tr>
<tr><td>Application Authentication</td><td>During installation with desktop versions of Windows, NETePay installs an encrypted license file that contains data whereby Datacap knows the product has been successfully activated and therefore is valid to use for processing. The same license file contains the merchant settings. There is no other authentication data required. The license file is encrypted and proprietary to Protection Plus.

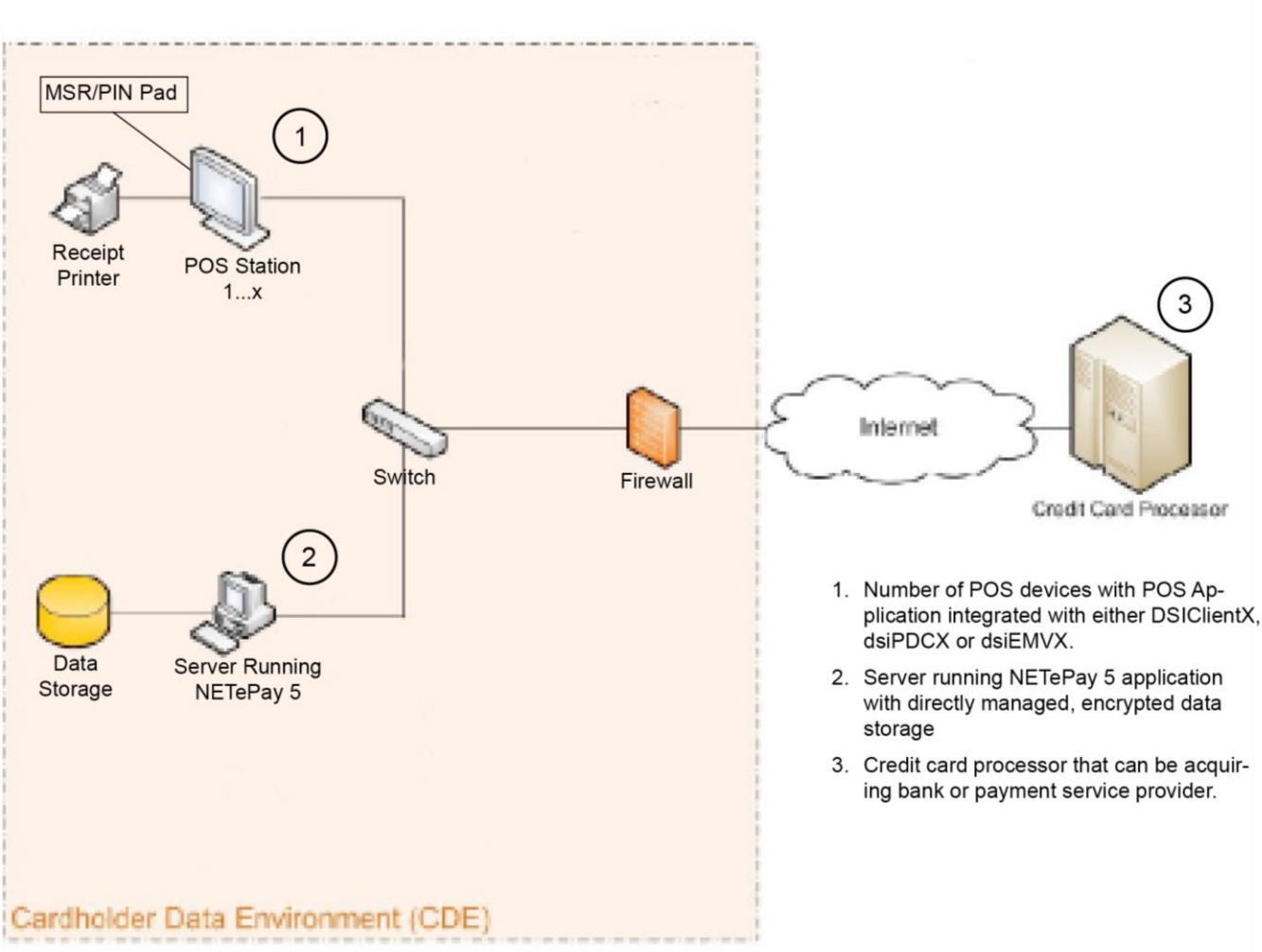
For Windows CE7 deployments on compatible Tran hardware, the NETePay 5 executable for CE 7 is designed to validate a unique proprietary Tran identity built into each hardware example during manufacture. NETePay 5 activation based on the unique ID of each hardware example is required and therefore it cannot be loaded into or execute from any other CE 7 based systems. NETePay 5 executables loaded to Tran compatible hardware are signed and verified with a VeriSign certificate.</td></tr>
<tr><td>Application Encryption</td><td>Client connections from DSIClientX, dsiPDCX or dsiEMVX to NETePay 5 are validated by an encrypted proprietary process to assure that only a Datacap client can communicate with NETePay. After the client connection is validated, data transfers containing transaction requests are encrypted using a public/private key exchange and RSA full strength 1024 bit keys.

Data storage is directly managed from within the NETePay 5 application code on the server where NETePay 5 is installed. Data store encryption is based on unique per-record automatically generated hashed 128bits keys which are used to encrypt the random data using a 3DES 192bit Cipher.</td></tr>
<tr><td>Application Functionality Supported</td><td>Payment Application Functionality (check only one):
<table>
<tr><td></td><td>Automated Fuel Dispenser</td><td></td><td>POS Kiosk</td><td></td><td>Payment Gateway/Switch</td></tr>
<tr><td></td><td>Card-Not-Present</td><td></td><td>POS Specialized</td><td>X</td><td>Payment Middleware</td></tr>
<tr><td></td><td>POS Admin</td><td></td><td>POS Suite/General</td><td></td><td>Payment Module</td></tr>
<tr><td></td><td>POS Face-to-Face/POI</td><td></td><td>Payment Back Office</td><td></td><td>Shopping Cart & Store Front</td></tr>
</table></td></tr>
<tr><td>Payment Processing Connections:</td><td>NETePay 5 is an application that resides on a computer running a version of the Windows operating system that monitors encrypted transaction requests via IP from client machines using a POS or restaurant application exclusively integrated with one of DSIClientX, dsiPDCX or dsiEMVX, Datacap’s ActiveX controls.

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

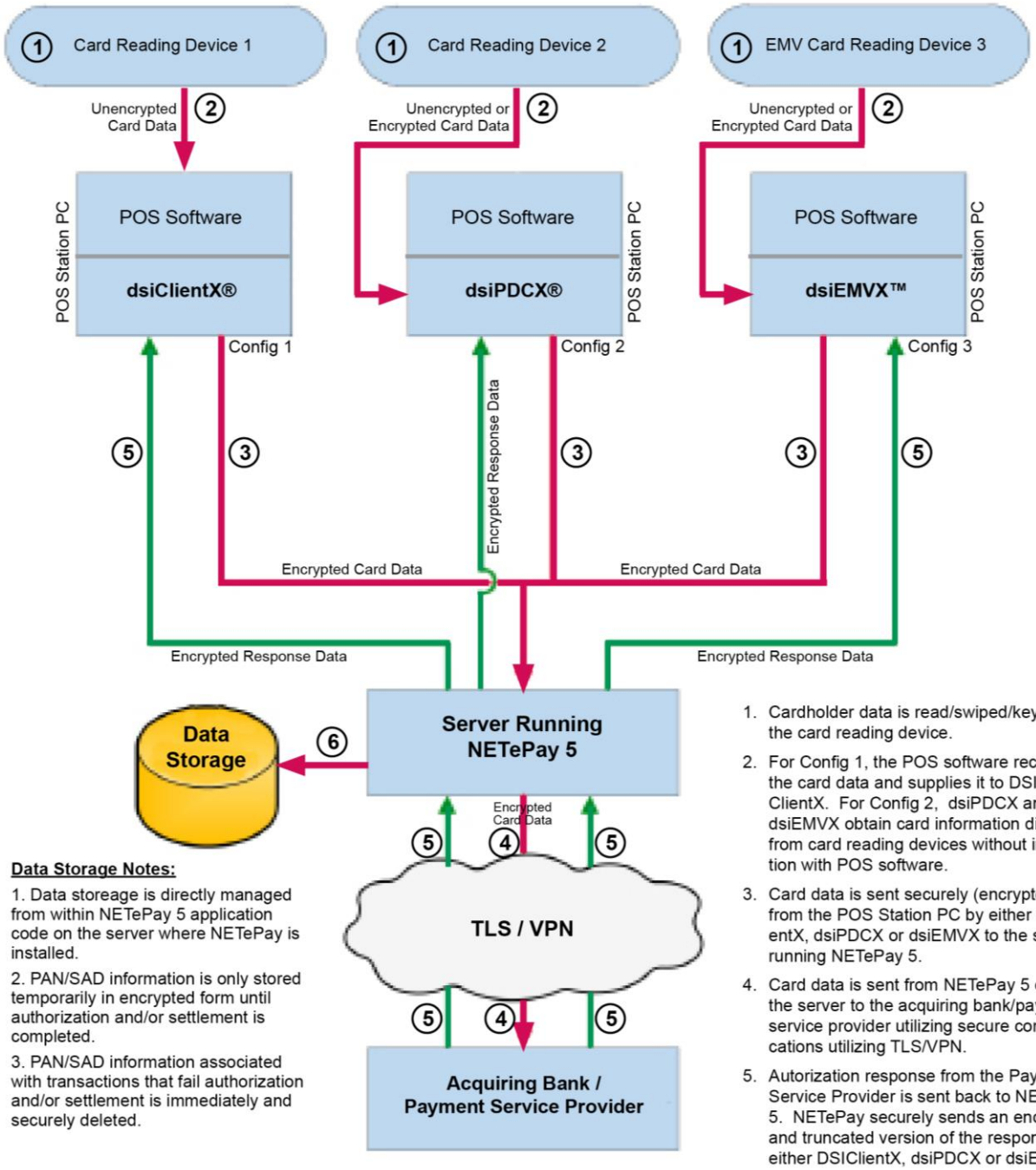
	The processing host returns a reply directly to NETePay 5 using the processor's specified secure protocol via the Internet. NETePay 5 reformats the response and returns the reply to the requesting client control using a secure connection.
Description of Listing Versioning Methodology	NETePay 5 versioning has three levels, Major, Minor, and Build: • **Major** changes include significant changes to the application and would have an impact on PA-DSS requirements. • **Minor** changes include small changes such as minor enhancements and may or may not have an impact on PA-DSS requirements. • **Build** changes include bug fixes or rollups and would have no negative impact on PA-DSS requirements and are indicated by the WILDCARD (X). Based on the above versioning methodology the application version being listed with the PCI SSC is: 5.07.XX

Typical Network Implementation



1. Data Storage is directly managed from within the NETePay 5 application code on the server where NETePay 5 is installed.

Credit/Debit Cardholder Dataflow Diagram



Data Storage Notes:

1. Data storeage is directly managed from within NETePay 5 application code on the server where NETePay is installed.
2. PAN/SAD information is only stored temporarily in encrypted form until authorization and/or settlement is completed.
3. PAN/SAD information associated with transactions that fail authorization and/or settlement is immediately and securely deleted.

1. Cardholder data is read/swiped/keyed at the card reading device.
2. For Config 1, the POS software receives the card data and supplies it to DSIClientX. For Config 2, dsiPDCX and dsiEMVX obtain card information directly from card reading devices without interaction with POS software.
3. Card data is sent securely (encrypted) from the POS Station PC by either DSIClientX, dsiPDCX or dsiEMVX to the server running NETePay 5.
4. Card data is sent from NETePay 5 on the server to the acquiring bank/payment service provider utilizing secure communications utilizing TLS/VPN.
5. Autorization 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 DSIClientX, dsiPDCX or dsiEMVX.
6. If the transaction is approved, then NETePay 5 securely deletes PAN/SAD data from the data storage.

Notes:

1. DSIClientX, dsiPDCX and dsiEMVX have no persistent data storage capability and never retain any type of 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 3.2 is the standard against which Payment Application has been tested, assessed, and validated.

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

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

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

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

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

The 12 Requirements of the PCI DSS:

Build and Maintain a Secure Network and Systems

1. *Install and maintain a firewall configuration to protect cardholder data*
2. *Do not use vendor-supplied defaults for system passwords and other security parameters*

Protect Cardholder Data

3. *Protect stored cardholder data*
4. *Encrypt transmission of cardholder data across open, public networks*

Maintain a Vulnerability Management Program

5. *Protect all systems against malware and regularly update anti-virus software or programs*
6. *Develop and maintain secure systems and applications*

Implement Strong Access Control Measures

7. *Restrict access to cardholder data by business need-to-know*
8. *Identify and authenticate access to system components*
9. *Restrict physical access to cardholder data*

Regularly Monitor and Test Networks

10. *Track and monitor all access to network resources and cardholder data*
11. *Regularly test security systems and processes*

Maintain an Information Security Policy

12. *Maintain a policy that addresses information security for all personnel*

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

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

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

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4)

Previous versions of NETePay 5 did not store sensitive authentication data. Therefore, there is no need for secure deletion of this historical data by the application as required by PA-DSS v3.2.

Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

NETePay 5 temporarily stores Sensitive Authentication Data to enable off-line operation when network connectivity to the payment processing provider is unavailable. When network communications are restored, transactions are processed and all associated SAD is immediately and securely deleted. The following guidelines are followed when dealing with Sensitive Authentication Data used for pre-authorization (swipe data, validation values or codes, PIN or PIN block data):

- NETePay 5 temporarily stores sensitive authentication data only when needed to provide off-line processing capability when network connectivity to the payment processing provider is unavailable. NETePay 5 collects only the minimum sensitive authentication data required to process off-line transactions when network communications are restored to the payment processing provider. Upon re-establishing network communications, all off-line transactions are processed and all associated sensitive authentication data is immediately and securely deleted. In the event that network connectivity cannot be established within 48 hours of the time that sensitive authentication data is collected for an unprocessed transaction, the associated sensitive authentication data is automatically and securely deleted.

- Sensitive authentication data is only stored in specific, known locations with limited access. NETePay 5 implements file handling and management internally and does not use an external database system. Sensitive authentication data is stored in a single file installed on the same computer by NETePay 5 which contains the equivalent of three tables.

  File: DSIVitalTNSIP_Host_5_07_xxxxxxx.db

  where ‘xxxxxxx’ is the Build designation

  Tables: batch
  store_and_forward
  store_and_forward_detail

  NETePay always stores sensitive authentication data in its tables in encrypted and/or truncated form.

- NETePay 5 collects only the minimum amount of sensitive authentication data required to successfully process a particular type of transaction.

- NETePay always stores sensitive authentication data in encrypted and/or truncated form.
  The NETePay encryption starts by generating a unique session code based on an encrypted license file and other version specific data. Encryption starts by taking this value and hashing it using SHA hashing algorithm and then using the hash to generate a 128-bit key and then destroys the hash in memory. NETePay 5 then uses the generated key to encrypt the sensitive authentication data using a 3DES 192bit cipher.

- NETePay 5 securely deletes (SAD) sensitive authentication data immediately after use by masking it completely with 'X's and re-encrypting the data. PAN data is masked with X's in all but the last 4 positions wherever stored or displayed.

We strongly recommend that you do not store Sensitive Authentication Data for any reason. However, if you should do so, the following 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)

NETePay 5 does not permanently store cardholder data and therefore there is no data to be purged by the application as required by PA-DSS v3.2.

Any cardholder data you store outside of the application must be documented and you must define a retention period at which time you will securely delete (render irretrievable) the stored cardholder data. When defining a retention period you must take into account legal, regulatory, or business purpose.
All underlying software (this includes operating systems and/or database systems) must be configured to prevent the inadvertent capture of PAN. Instructions for configuring the underlying operating systems and/or databases can be found in **Appendix A**.

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 is no configuration details to be provided as required for PA-DSS v3.2. PAN data is masked with X's in all but the last 4 positions wherever stored or displayed.

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

NETePay 5 does temporarily 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 merchant's environment for any reason, therefore there are no location or configuration details to provide as required by PA-DSS v3.2.
NETePay 5 does not have a debugging mode that could write PAN to debugging logs.

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
- Version 5.06
- NETePay 5 uses previously validated encryption algorithms that are PCI compliant. Therefore there is no need to render historical cryptographic keys 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:

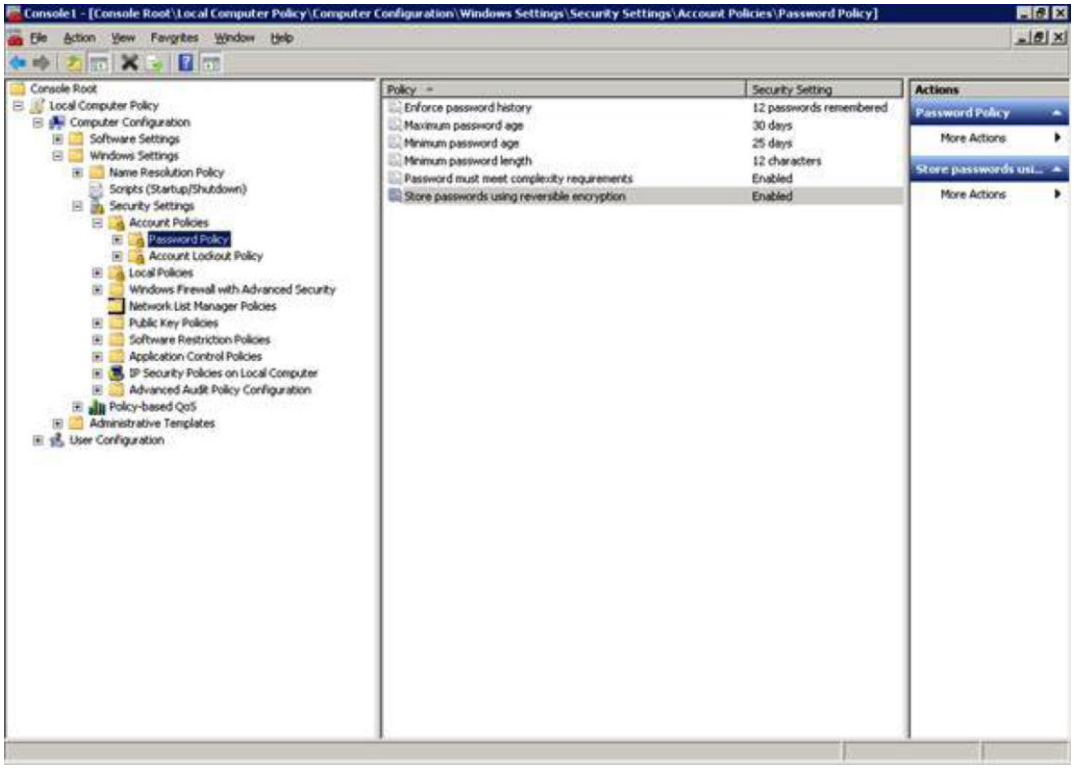
- You must not use or require the use of default administrative accounts for other necessary or required software (for example, database default administrative accounts) (PCI DSS 2.1 / PA-DSS 3.1.1)
- You must assign unique IDs for all user accounts. (PCI DSS 8.1.1 / PA-DSS 3.1.3). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated below.*

- 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
- 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.*
- 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.*
- 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.*
- 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.*
- 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.*
- 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.*
- 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.*

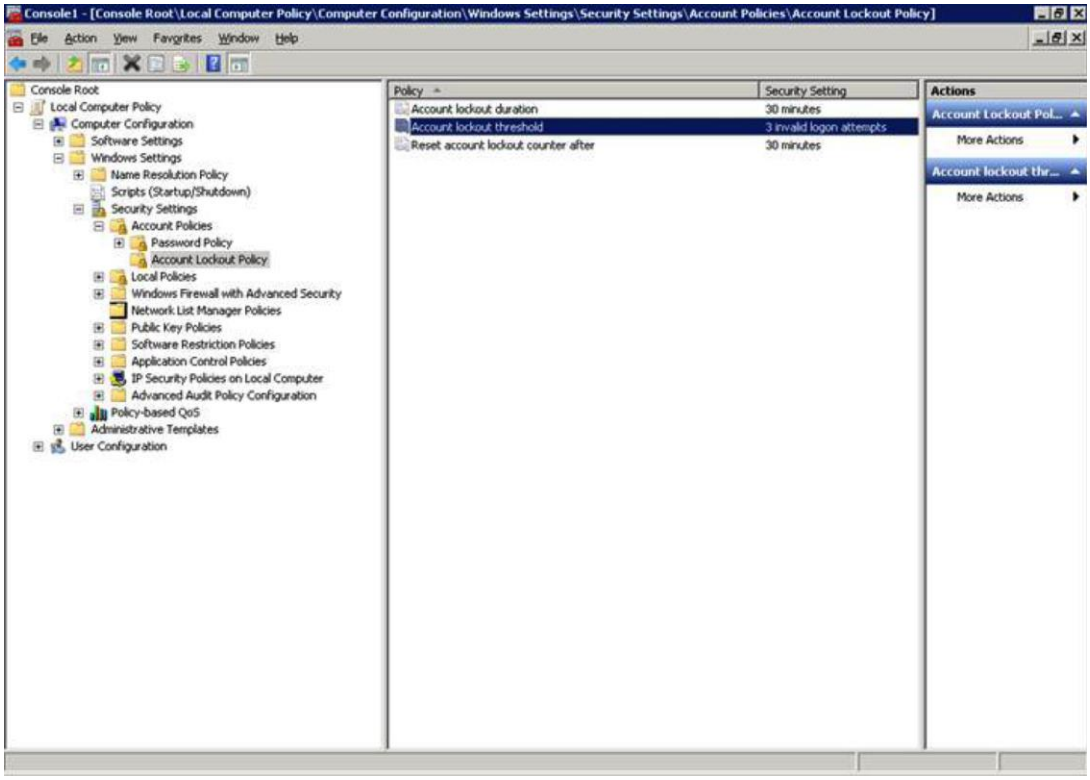
Establishing a Windows Secure Group Access Policy

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

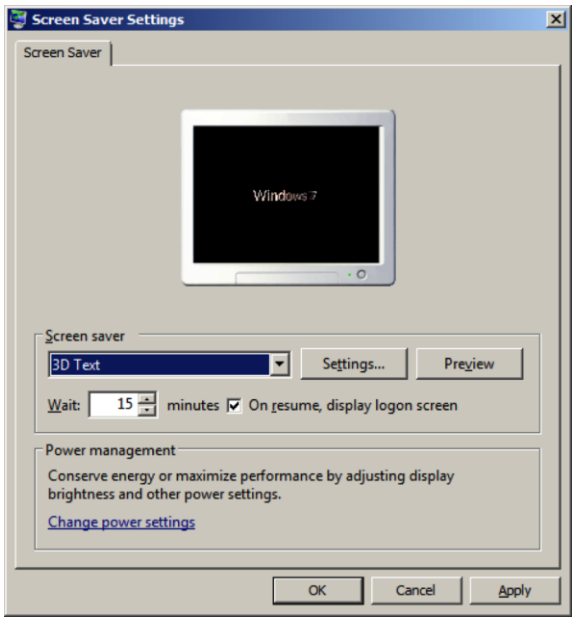
Your Windows operating system environment must be modified to comply with the above requirements. Access these settings by going to Start/Run and type MMC. Add the snap-in for Group Policy Editor and change the security settings as shown below. Under Account Policies select Password Policy and change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



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 requirements must also be applied to any applications or databases included in payment processing to be PCI compliant.

[**Note:** These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to systems with cardholder data, and for access controlled by the application.

The requirements apply to the payment application and all associated tools used to view or access cardholder data.]

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

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.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.

The NETePay 5 application 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

NETePay 5 application log files are recorded by date in individual ASCII files named as follows:

DSIMMDDYYYY.log

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

NETePayService.exe records its own log in addition to the NETePay application logs. This log records when the NETePay application was started/stopped as a service and the service account used. The NETePay service log files are written in the same install volume location as the NETePay 5 application logs.

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

SERVICE_DSIMMDDYYYY.log

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

The format of the log files is plain text that 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:

- 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
- Default SNMP community strings on wireless devices must be changed <
- Default passwords/passphrases on access points must be changed
- Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks
- 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 1.2 and will automatically use the most secure version supported by the payment processing service.

NETePay 5 must be installed on a Windows desktop system that supports TLS 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). Versions of Windows Compact 7 installed on Tran hardware support only TLS 1.2.

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 (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 to of the above. No configuration of NETePay 5 is required to accomplish this.

PCI-Compliant Delivery of Updates (PA-DSS 10.2.1.a, 7.2.3)

NETePay 5 delivers patches and updates in a secure manner:

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.

NETePay 5 incorporates an automatic update function which periodically and automatically checks Datacap's website using HTTPS to determine if an update is available. During installation, desktop Windows versions of NETePay 5 may be configured to automatically install updates without user intervention as they become available from Datacap or install updates based on user input to permit installation as conditions allow. Users who defer a prompted update are prompted again when NETePay is relaunched.

In addition, Datacap will notify users of the availability and advisability of installing updated applications via email and its website and will supply a download link to obtain the updated application installer if the user requires.

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

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

Our continuing security education activities are comprised of the following:

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

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

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

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

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

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

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

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

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

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

PCI-Compliant Remote Access (10.2.3.a)

NETePay 5 does not natively support any remote access functionality.

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

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

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

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

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

- Change default settings (such as usernames and passwords) on remote access software (e.g. VNC)

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

Data Transport Encryption (PA-DSS 11.1.b)

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with TLS 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 1.2) 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 and Multi-Factor Authentication (PA-DSS 12.1, 12.2)

Although NETePay 5 does not support non-console administration and we do not recommend using non-console administration, should you ever choose to do this, must use SSH, VPN, or TLS 1.1 or higher for encryption of this non-console administrative access along with a multi-factor authentication solution.

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.

<u>For desktop/server versions of Microsoft Windows:</u>

- Microsoft Windows Server 2012 R2, Windows Server 2016, Windows 7 SP1, 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
- TCP/IP network connectivity. (Persistent Internet connection recommended)

<u>For Microsoft Windows Compact Edition 7:</u>

- Datacap supplied Tran Series hardware with preloaded Windows Compact Edition 7
- Tran models supported:
    - TranServer
    - IPTran
    - IPTranLT
    - TwinTran
    - TranCloud

Payment Application Initial Setup & Configuration

For desktop/server versions of Microsoft Windows:

- Installation of NETePay 5 and associated utilities requires Administrator access in Windows. Datacap advises users to change default password and manage Windows passwords according to PCI DSS 3.2

For Microsoft Windows Compact Edition 7:

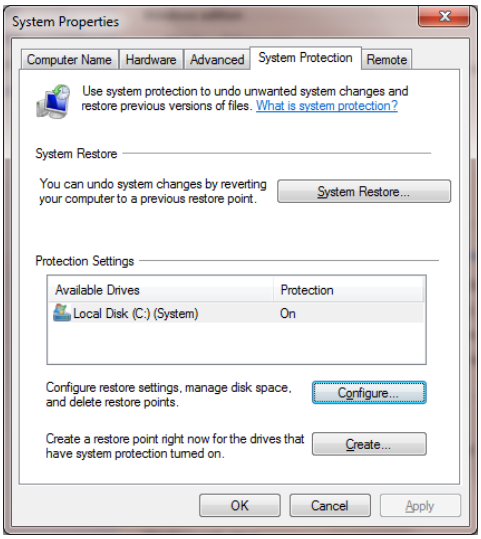
- Datacap supported Tran Series hardware with preloaded Windows Compact Edition 7

Appendix A: Addressing Inadvertent Capture of PAN

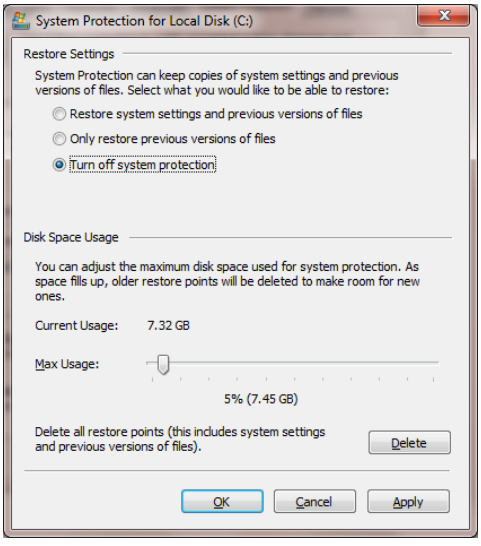
Addressing Inadvertent Capture of PAN on WINDOWS 7

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:

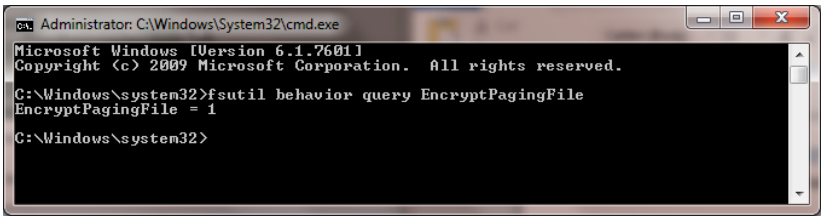


- Select "Turn off system protection"
- Click apply, and OK to shut the System Protection window
- Click OK again to shut the System Properties window
- Reboot the computer

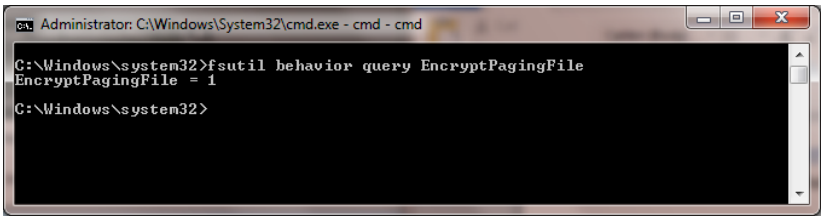
Encrypting PageFile.sys – Windows 7

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

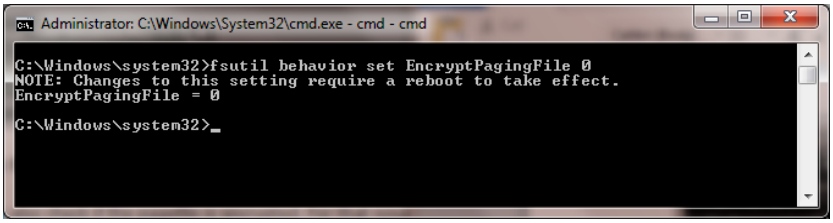
- Click on the Windows "Orb" and in the search box type in "cmd".
- Right click on cmd.exe and select "Run as Administrator"
- To Encrypt the Pagefile type the following command: fsutil behavior set EncryptPagingFile 1



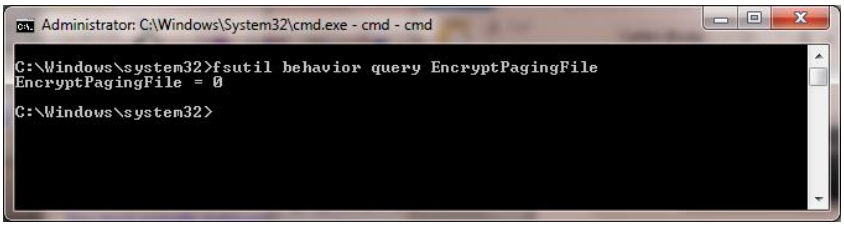
- To verify configuration type the following command: fsutil behavior query EncryptPagingFile



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



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



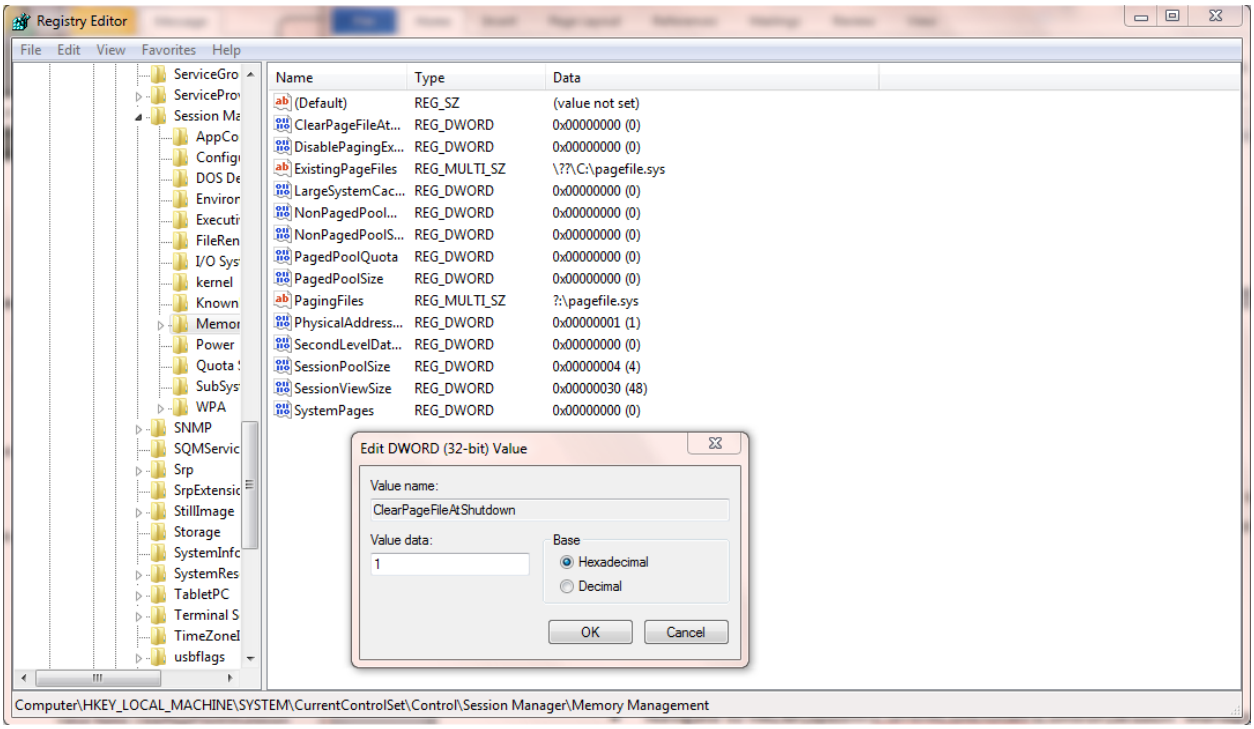
- If encryption is disabled EncryptPagingFile = 0 should appear

Clear the System Pagefile.sys on shutdown

Windows 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.

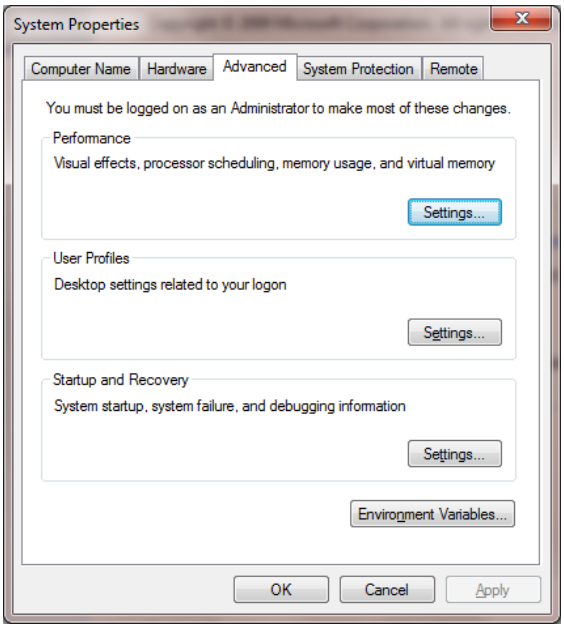
- Click on the Windows "Orb" and in the search box type in "regedit".
- Right click on regedit.exe and select "Run as Administrator"
- Navigate to HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
- Change the value from 0 to 1
- Click OK and close Regedit



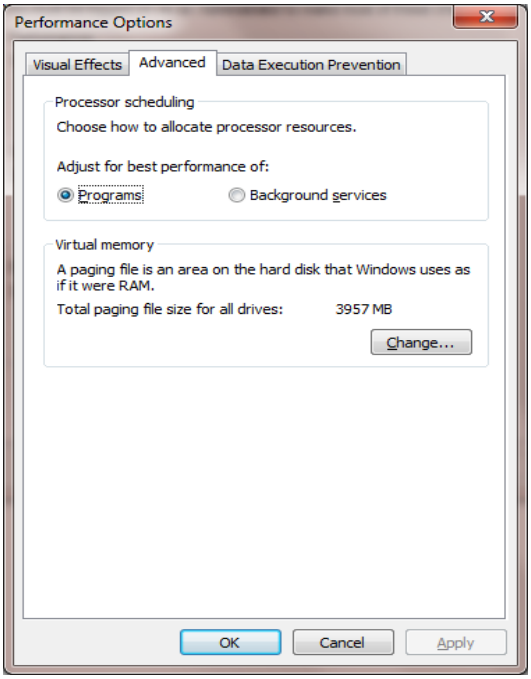
- If the value does not exist, add the following:
  - Value Name: ClearPageFileAtShutdown
  - Value Type: REG_DWORD
  - Value: 1

Disabling System Management of PageFile.sys – Windows 7

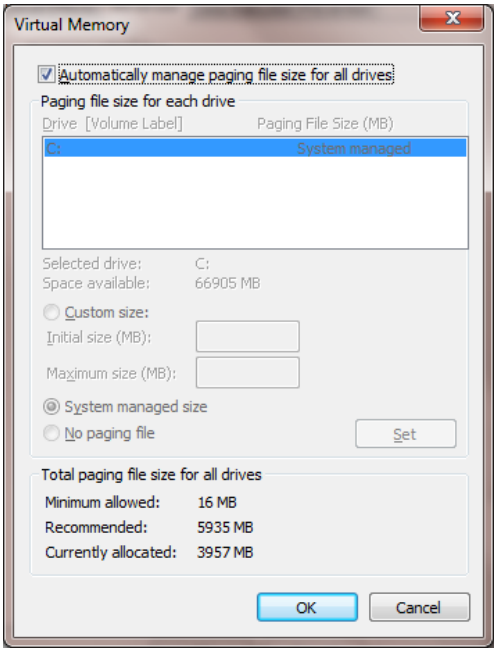
- Right Click on Computer > Select “Properties”
- Select “Advanced System Settings” on the top left list, the following screen will appear:



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



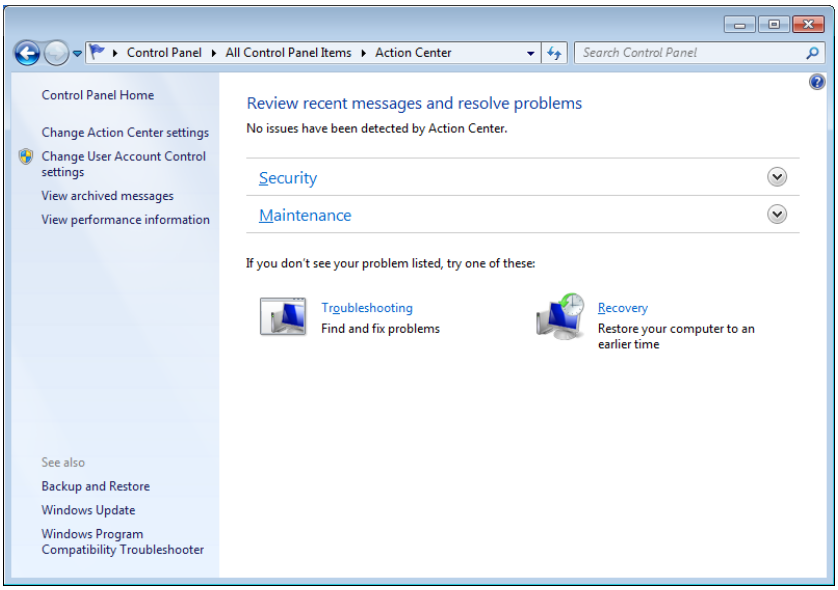
- Select “Change” under Virtual Memory, the following screen will appear:



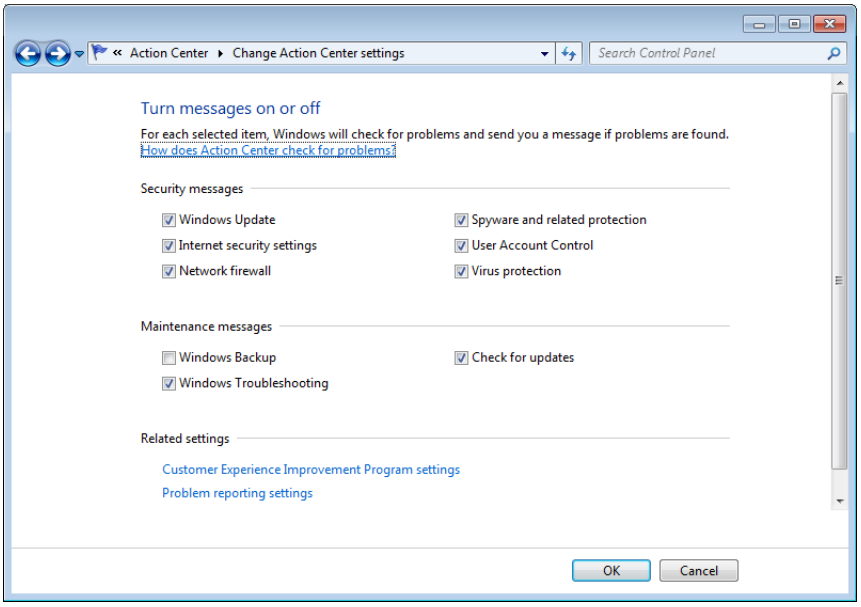
- Uncheck “Automatically manage page file size for all drives”
- Select “Custom Size”
- Enter the following for the size selections:
    - Initial Size – as a good rule of thumb, the size should be equivalent to the amount of memory in the system.
    - Maximum Size – as a good rule of thumb, the size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

Disabling Windows Error Reporting – Windows 7

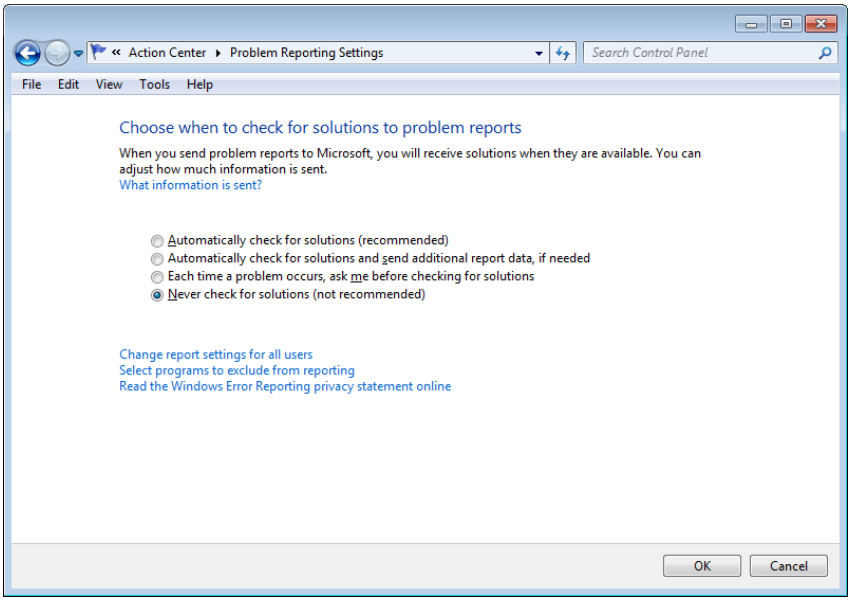
- Open the Control Panel
- Open the Action Center
- Select “Change Action Center Settings”



- Select “Problem Reporting Settings”



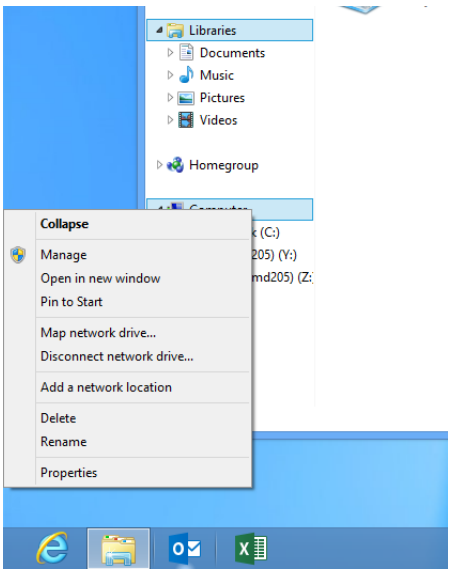
- Select “Never Check for Solutions”



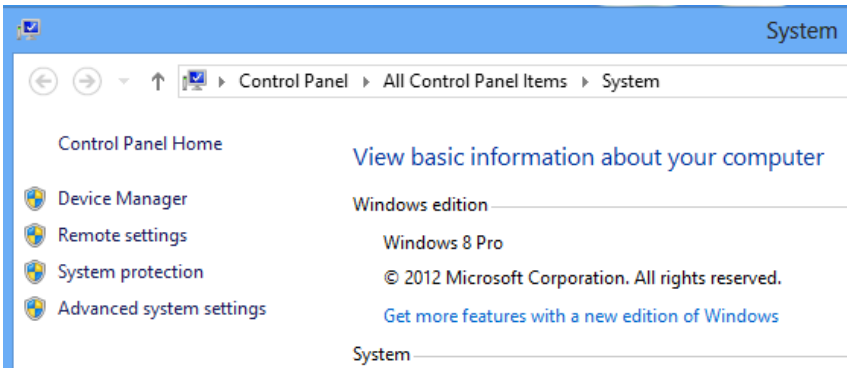
To Address Inadvertent Capture of PAN on Windows 8, 10, Server 2012 or 2016:

1. Disable System Restore – Windows 8, 10, Server 2012 or 2016

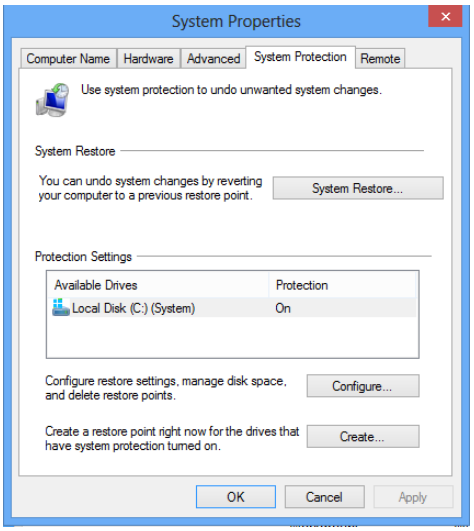
Right Click on Computer > Select "Properties":



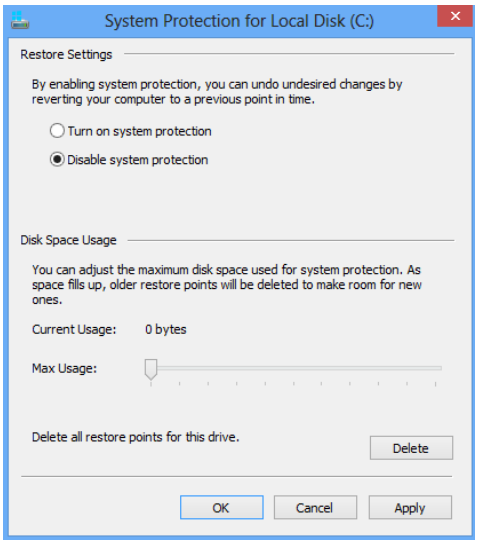
Select "Advanced System Settings" from the System screen:



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



- Select Configure, the following screen will appear:



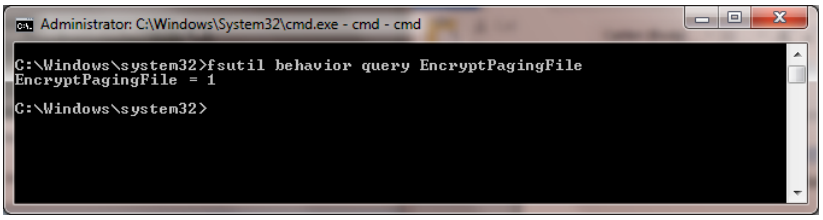
- Select "Disable system protection"
- Click apply, and OK to shut the System Protection window

- Click OK again to shut the System Properties window
- Reboot the computer

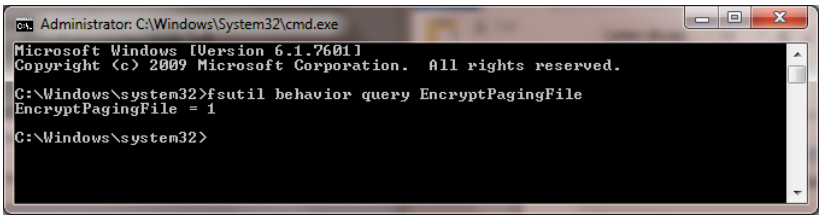
2. Encrypt PageFile.sys – Windows 8, 10, Server 2012 or 2016

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

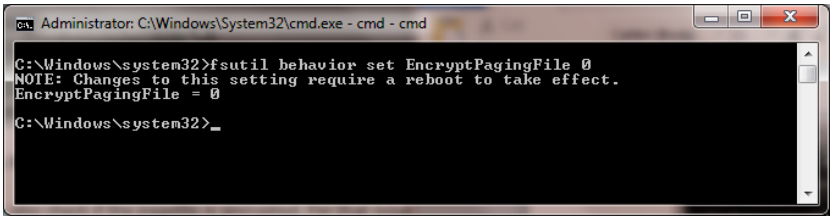
- From the desktop hold down the "Windows" key and type "F" to bring up the "Search" charm, select "Apps" in the "Apps" box type in "cmd".
- Right click on "Command Prompt" icon located on the left side of your screen, a selection bar will appear at the bottom of the screen, select "Run as Administrator"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



- If encryption is enabled EncryptPagingFile = 1 should appear
- If encryption is disabled EncryptPagingFile = 0 should appear
- To Encrypt the Pagefile type the following command: fsutil behavior set EncryptPagingFile 1



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

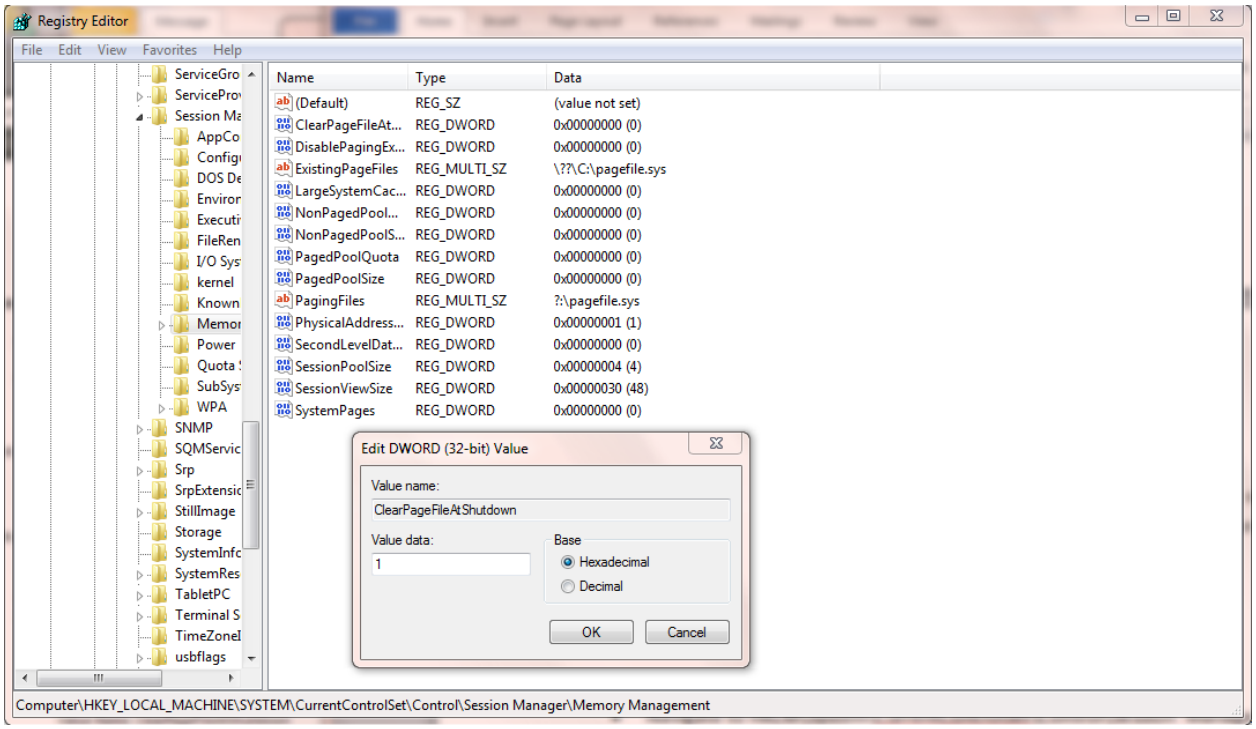


3. Clear the System Pagefile.sys on shutdown – Windows 8, 10, Server 2012 or 2016

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.

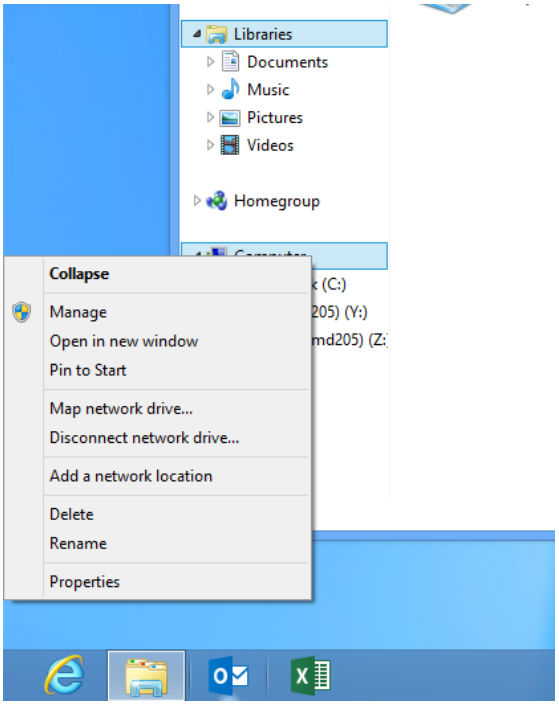
- From the desktop hold down the “Windows” key and type “F” to bring up the “Search” charm, select “Apps” in the “Apps” box type in “regedit”.
- Right click on regedit.exe and select “Run as Administrator”
- Navigate to HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
- Change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



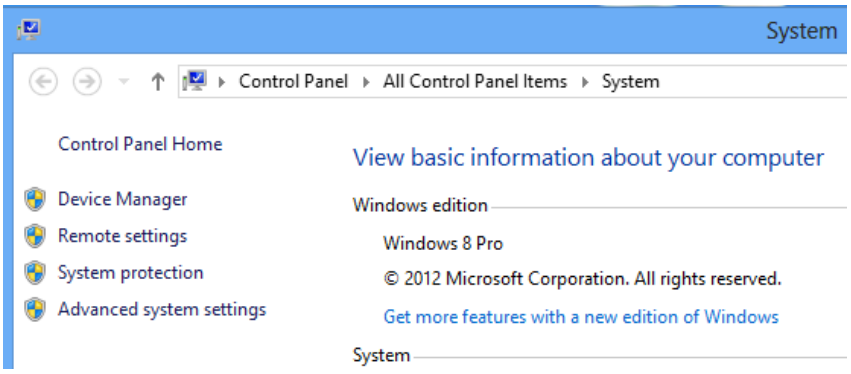
- If the value does not exist, add the following:
  - Value Name: ClearPageFileAtShutdown
  - Value Type: REG_DWORD
  - Value: 1

4. Disable System Management of PageFile.sys – Windows 8, 10, Server 2012 or 2016

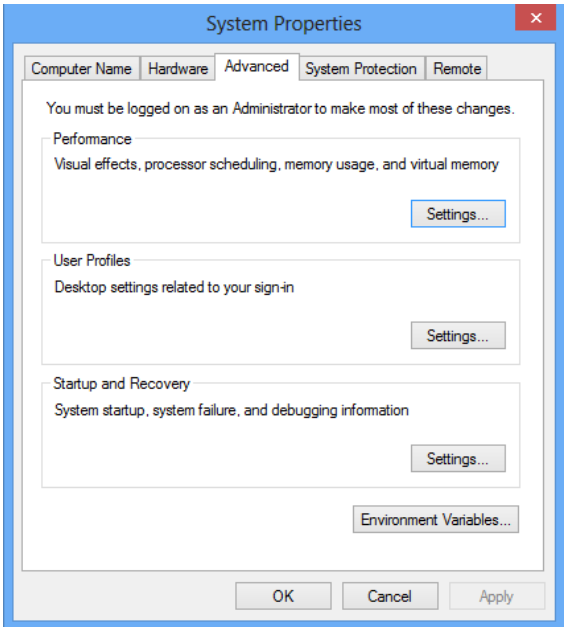
- Right Click on Computer > Select “Properties”:



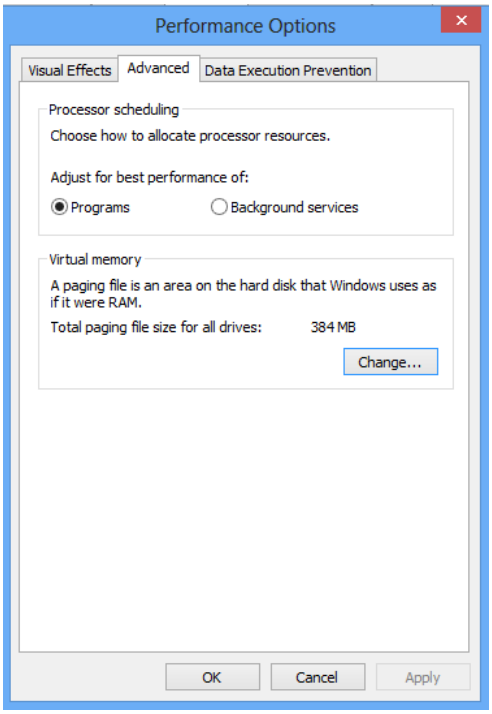
- Select “Advanced System Settings” from the System screen:



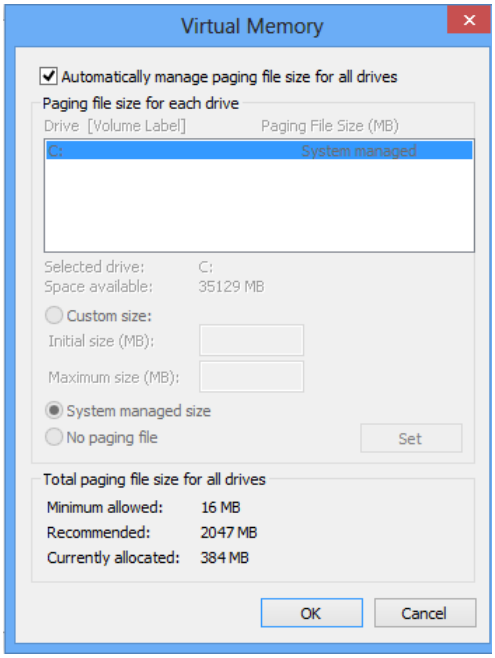
- Select the “Advanced” tab:



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



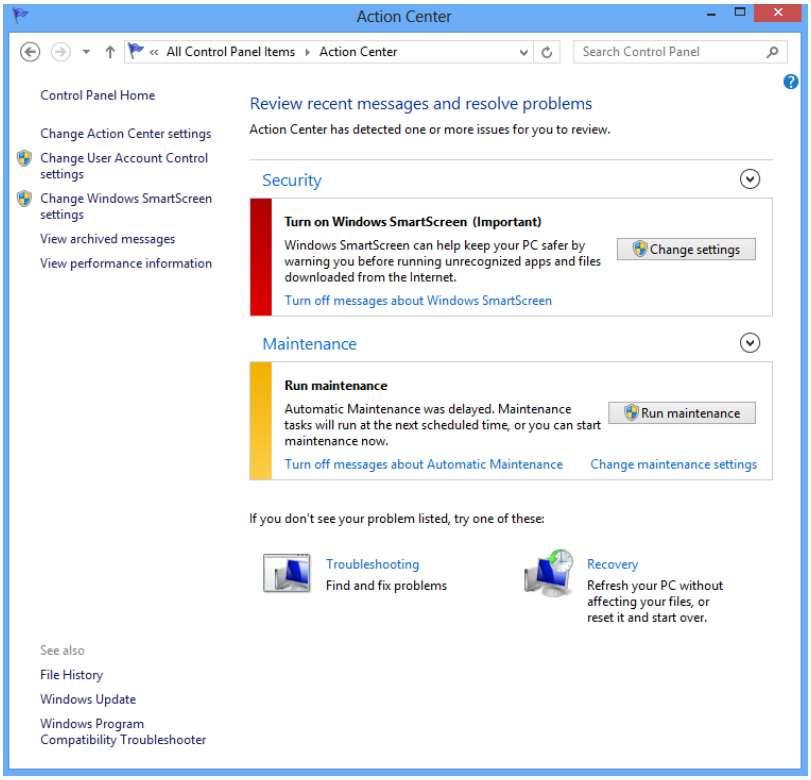
- Select “Change” under Virtual Memory, the following screen will appear:



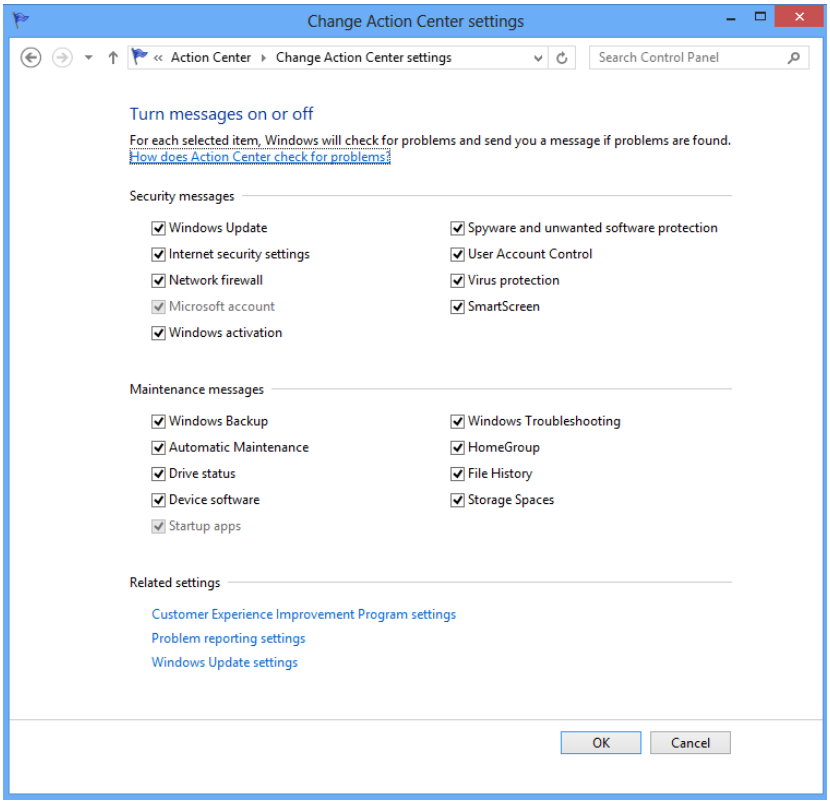
- Uncheck “Automatically manage page file size for all drives”
- Select “Custom Size”
- Enter the following for the size selections:
  - Initial Size – as a good rule of thumb, the size should be equivalent to the amount of memory in the system.
  - Maximum Size – as a good rule of thumb, the size should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

5. Disable Windows Error Reporting – Windows 8, 10, Server 2012 or 2016

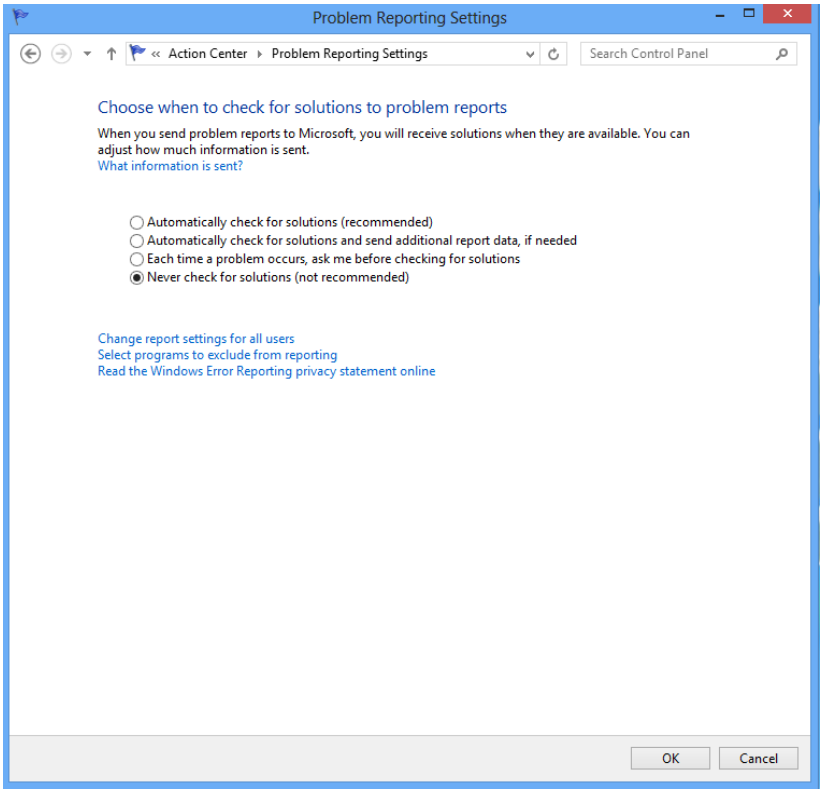
- From the desktop hold down the “Windows” key and type “I” to bring up the “Settings” charm, select “Control Panel”.
- Open the Action Center
- Select “Change Action Center Settings”:



- 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.

INSTALLATION

Introduction

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

- *NETePay*
- *DSIEMVClientX or DSIClientX or dsiPDCX or dsiEMVX*
- 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 one of either *DSIClientX or dsiPDCX or dsiEMVX* to be installed.

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* on your server, it should meet or exceed the following system requirements:

- Microsoft Windows Server 2012 R2, Windows Server 2016, Windows 7 SP1, or Windows 10. All latest service packs, updates and hotfixes must be applied. *Refer to Chapter 2 – PA-DSS 3.2 Implementation Guide for complete instructions for PCI compliant installation.*
- 4 GB of RAM minimum, 8 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 (DSL, cable, frame relay, etc.)

Network Requirements

Before installing *NETePay* 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* server available for incoming traffic if you are behind a firewall and connected to the default port.

If you are using a port other than the default IP port (9000), make sure you know the port on which the server is listening.

Installation Procedures

Downloading the NETePay Software

All components required for a NETePay 5 installation are available for download from Datacap's Software Download website at:

http://www.datacapepay.com

After agreeing with the Terms of Use, select **Proceed to Software Download Menu**. Select **NETePay 5**. From the **HOST** based section of downloads, select the appropriate ActiveX client for your installation (DSIEMVClientX, **DSIClientX, dsiPDCX or dsiEMVX**). Then select the appropriate NETePay 5 from the table. Each download is an automatic self-extracting installer, just double click to install each required component and follow on-screen instructions.

Note: After installation, your copy of NETePay 5 must be activated before it can be used to process transactions. Chapter 4 details the steps for activation.

What's Included in the NETePay Installer Package

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

The *NETePay* installer package is supplied as a self-extracting executable and includes the NETePay server application for Windows 7 SP1, Windows 10, Windows Server 2012 R2 or Windows Server 2016 operating systems for both single and multi-pay point users.

- ***DSIEMVClientX, DSIClientX, dsiPDCX, dsiEMVX***– XML ActiveX controls downloaded separately integrate into a Point of Sale or Restaurant application and sends encrypted payment authorization requests from client machines on a LAN to *NETePay* for processing. *Which ActiveX client to install depends upon the requirements of your processor and/or POS software vendor.* DSIClientX is an in-scope client control that allows the POS software to manage cardholder data. (*DSIClientX* also includes a utility program to enter payment transactions). dsiPDCX is an out-of-scope client control that manages payment peripherals. dsiEMVX is an out-of-scope client control that manages EMV capable POS peripherals.
- ***You must be logged in as an 'Administrator' to install NETePay and all of it's components.*** Installations performed when logged on as another user with rights less than 'Administrator' will not operate correctly.

Installing/Upgrading Microsoft Internet Explorer

NETePay 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 NETePay (Required)

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

To install the NETePay Server software:

1. Open the NETePay Server folder 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 a client control (DSIClientX, dsiPDCX or dsiEMVX) (As Required)

To install ***DSIEMVClientX***:

1. Open the DSIEMVClientX folder 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 *DSIEMVClientX* installation and click **Next**.
5. Enter your User Name and Organization.
6. If available on your operating system, make the application available to all users.
7. Click **Next**, then click **Install**. The installation wizard will then begin installing the necessary files on your computer.
8. Click **Finish** to complete the installation. A pop-up message will then appear and inform you to restart the computer.
9. Click **Yes** to restart the computer.

To install ***DSIClientX*** (includes the DSIClient Transaction Utility):

10. Open the DSIClient folder and double-click, **setup.exe**.
11. The installation wizard will start. When the Welcome screen appears, click **Next**.
12. Read and accept the End User License agreement and click **Next**.
13. Read the notes pertaining to *DSIClientX* installation and click **Next**.
14. Enter your User Name and Organization.
15. If available on your operating system, make the application available to all users.
16. Click **Next**, then click **Install**. The installation wizard will then begin installing the necessary files on your computer.
17. Click **Finish** to complete the installation. A pop-up message will then appear and inform you to restart the computer.
18. Click **Yes** to restart the computer.

To install ***dsiPDCX***:

19. Open the dsiPDCX folder and double-click, **setup.exe**.
20. The installation wizard will start. When the Welcome screen appears, click **Next**.
21. Read and accept the End User License agreement and click **Next**.
22. Read the notes pertaining to *dsiPDCX* installation and click **Next**.
23. Enter your User Name and Organization.
24. If available on your operating system, make the application available to all users.
25. Click **Next**, then click **Install**. The installation wizard will then begin installing the necessary files on your computer.
26. Click **Finish** to complete the installation. A pop-up message will then appear and inform you to restart the computer.
27. Click **Yes** to restart the computer.

To install ***dsiEMVX***:

1. Open the dsiEMVX folder 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 *dsiEMVX* installation and click **Next**.
5. Enter your User Name and Organization.
28. If available on your operating system, make the application available to all users.
6. Click **Next**, then click **Install**. The installation wizard will then begin installing the necessary files on your computer.
7. Click **Finish** to complete the installation. A pop-up message will then appear and inform you to restart the computer.
8. Click **Yes** to restart the computer.

Installing DSIClient Application (Conditional)

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

The DSIClient application downloaded separately provides a convenient means to test operation of the NETePay 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.

Important Note:

The *DSIClient application* includes the DSIClientX ActiveX control that is required for NETePay 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 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 NETePay 5 Director (Optional)

About NETePay 5 Director

NETePay 5 Director is a unified software licensing and automatic upgrade system for use with Datacap's ePay server products, such as NETePay, GIFTePay and others.

Benefits of NETePay 5 Director

NETePay 5 Director streamlines installation, licensing and updates of Datacap ePay server products. Compared to standalone ePay server installs, *NETePay 5 Director* supports the following enhancements:

- Only one serial number and license to manage for all ePay products installed on a particular PC hardware platform.
- Automatic updates over the Internet for all installed ePay products without user intervention.
- Remote installation and management of ePay server configurations remotely using Datacap's PSCS (Payment System Configuration Server).

NETePay 5 Director is installed as a system service that starts automatically when Windows starts. The Director service automatically launches any installed and activated ePay software (e.g. NETePay, GIFTePay) servers(s) for processing transaction requests from clients.

The Director service also supports an interface in the Windows tray called Manager. The Manager application interoperates with the Director service to allow a user to suspend or restart the running ePay servers and provide access to the ePay server User Interface for running ePay software.

The Manager also supports installations automatically of ePay servers that are originated in Datacap's PSCS (Payment System Configuration Server). PSCS access over the Internet affords for the complete management of a merchant's ePay software environment, including installation, feature control and version updates.

Download NETePay 5 Director Software

The *NETePay 5 Director* installation is available for download from Datacap's Software Download website at:

http://www.datacapepay.com

Click **Get Started**, then Click **NETePay 5**, select **Director and Manager**.

Click the **Download** button for the Director and Manager.

After agreeing with the Terms of Use, the download of the install package will begin.

The *NETePay Director* installer package is supplied as a self-extracting executable and includes the NETePay Director application for Windows 7 SP1, Windows 10, Windows Server 2012 R2 or Windows Server 2016 operating systems. Double click on the downloaded file to start the installation.

CHAPTER 4

NETePay CONFIGURATION & TESTING

Introduction

This chapter explains how to activate and configure *NETePay for Heartland Portico Host*.

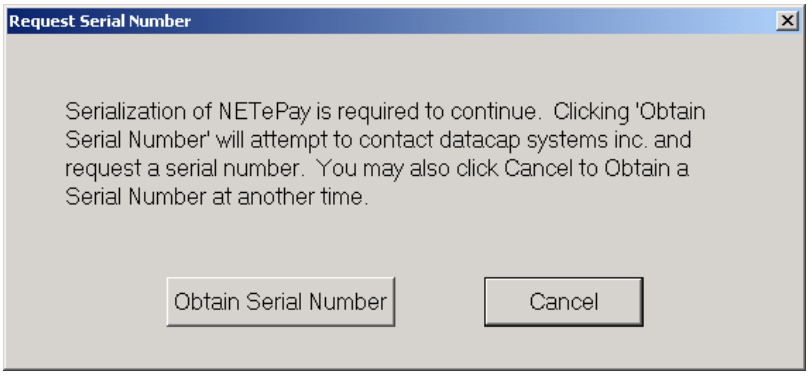
NETePay is activated and programmed over the Internet so a working Internet connection is required for the process.

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

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

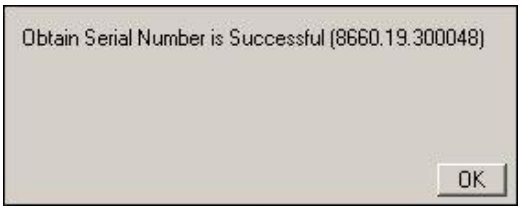


Click 'Obtain Serial Number' to enable NETePay to contact PSCS for a serial number.

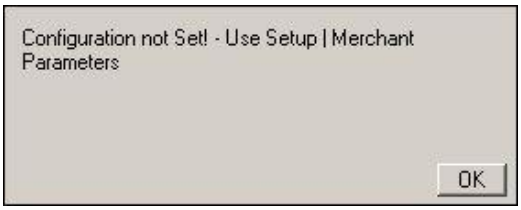
2. If NETePay is unsuccessful in obtaining a serial number, it will present the following dialog:

Click 'OK' and NETePay will close. Failure to successfully obtain a serial number means that NETePay 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 is installed to contact www.datacapsystems.com. If you are successful in contacting Datacap's website, close the browser, restart NETePay 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.

3. At this point, NETePay could present two possible responses. If *NETePay 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:

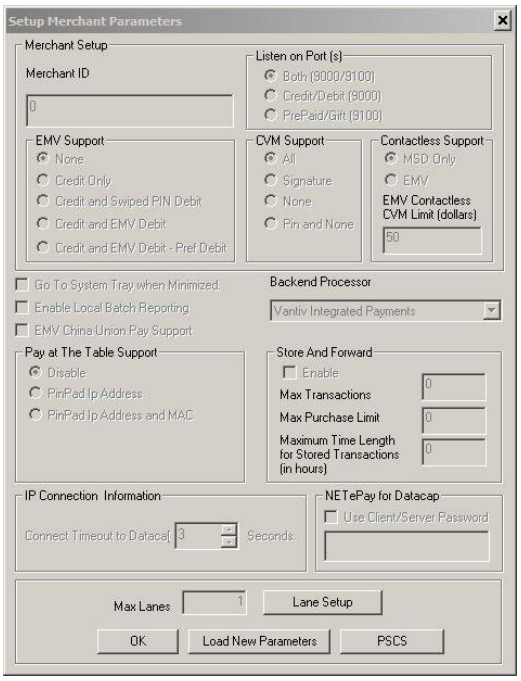


The dialog contains the 10-digit serial number that was automatically assigned to NETePay. Click 'OK' to continue and then you will see the following dialog:

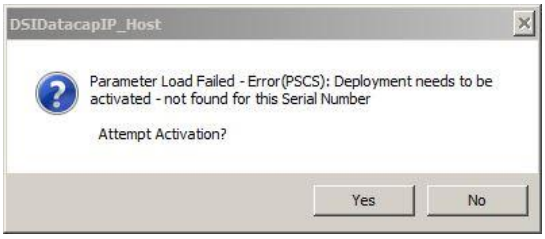


This dialog indicates that NETePay has not yet retrieved merchant parameters from Datacap's PSCS server and cannot operate until parameters are downloaded.

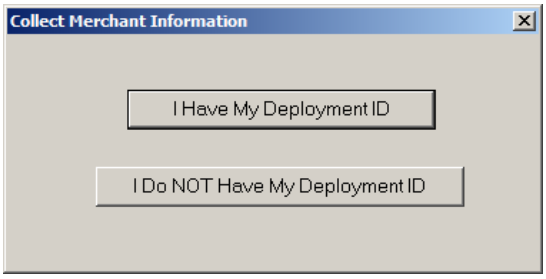
If a parameter file has been created on Datacap's PSCS server for the merchant account, then select 'Merchant Parameters' from the 'Setup' drop down menu. You will then see the following screen:



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:

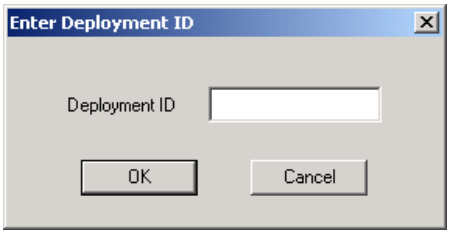


Click 'Yes' to attempt activation and you will see the following screen:



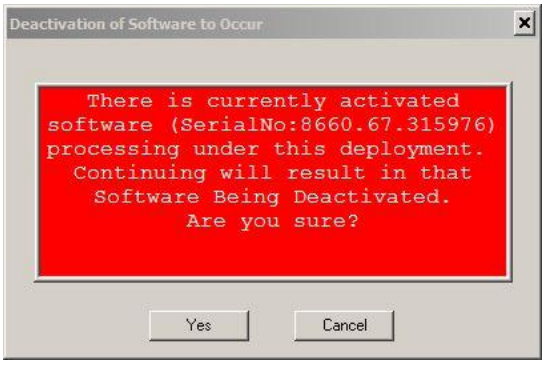
To continue, you must verify that you or someone else has created a Merchant Deployment on Datacap's PSCS server. If a deployment was created you may have been given a Deployment ID, which is typically an eight-character code that has been assigned to the merchant's parameters. If you have a Deployment 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:



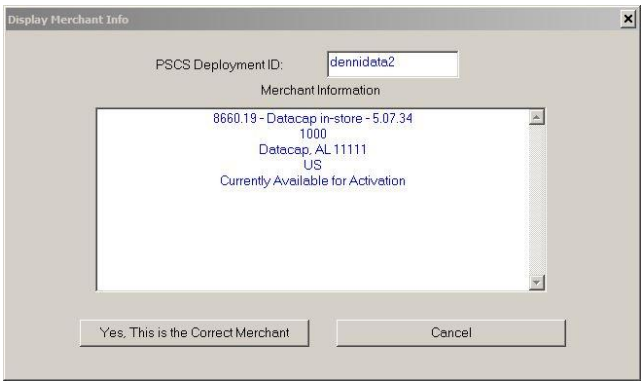
Enter the Deployment ID for the merchant parameter file and click 'OK'.

If NETePay 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.

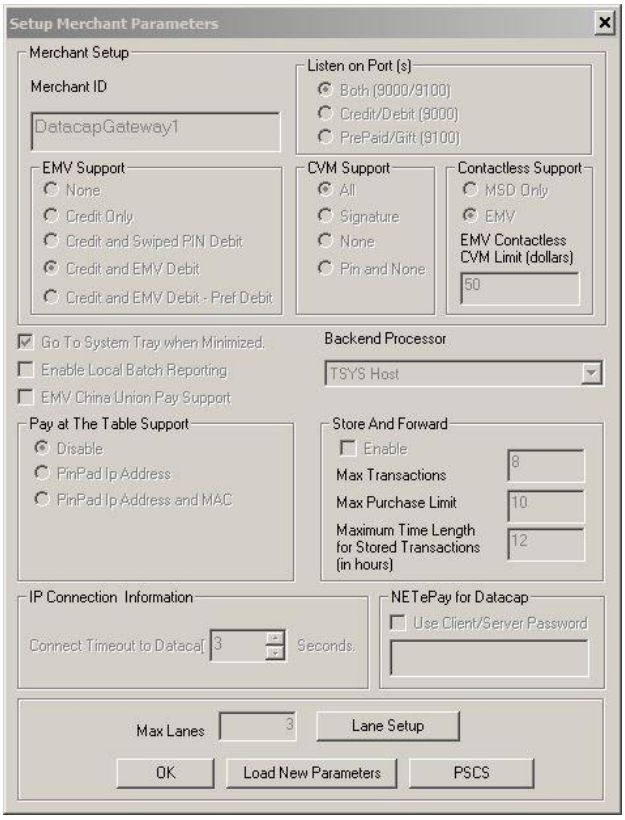
NETePay will display a screen with merchant demographic data for you to verify as follows:



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'.

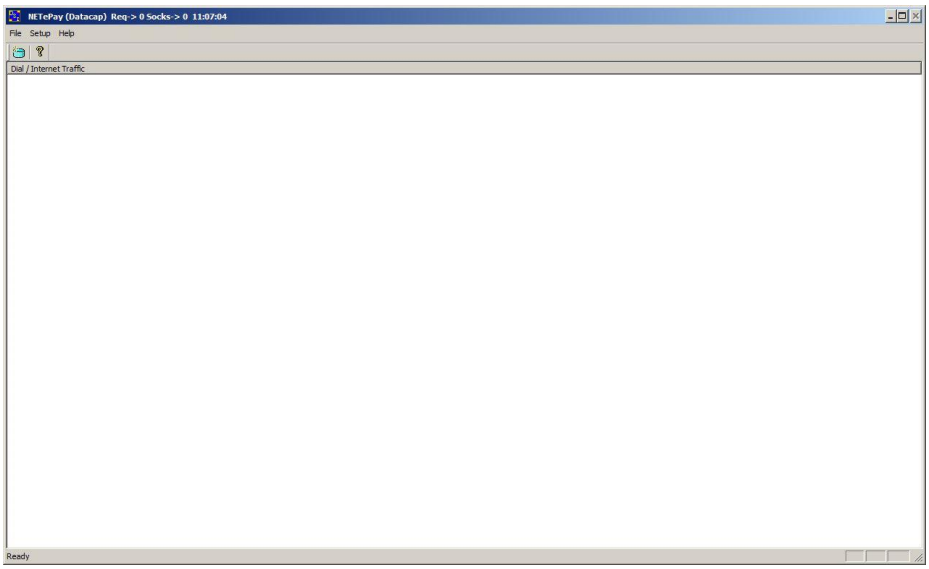
If NETePay successfully retrieves the parameters associated with the entered Deployment ID from the PSCS server, you will see the following dialog:

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



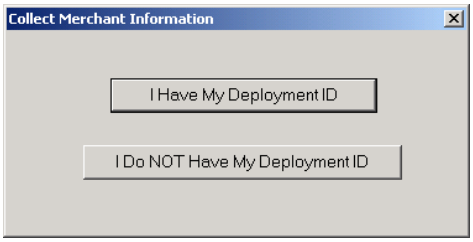
Lane Setup allows you to optionally change the description associated with each lane that was authorized in the PSCS parameter file. You cannot alter the number of lanes in NETePay; changes to the number of lanes must be done by editing the deployment file in PSCS. The Perform PDL button should only be used under direction of Heartland technical support personnel.

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 main status window indicating that NETePay is now programmed and ready to process transactions.

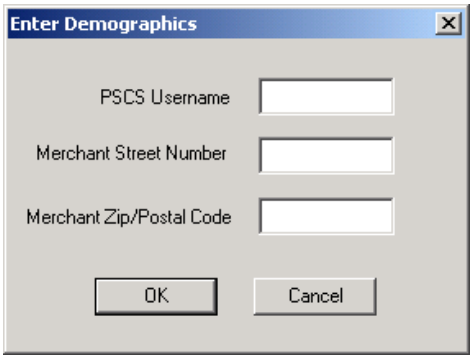


NETePay setup is complete.

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:

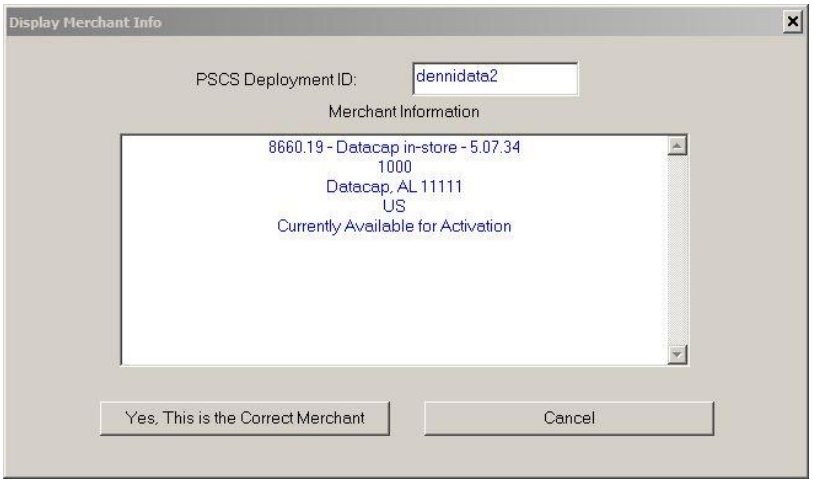


You need the following information to complete the demographics dialog entries:

- 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

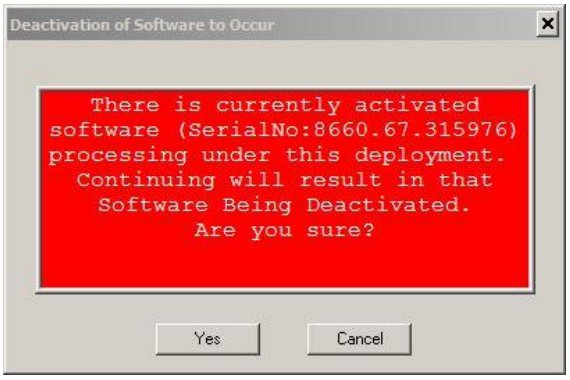
After entering this information, click 'OK'.

If NETePay 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'.

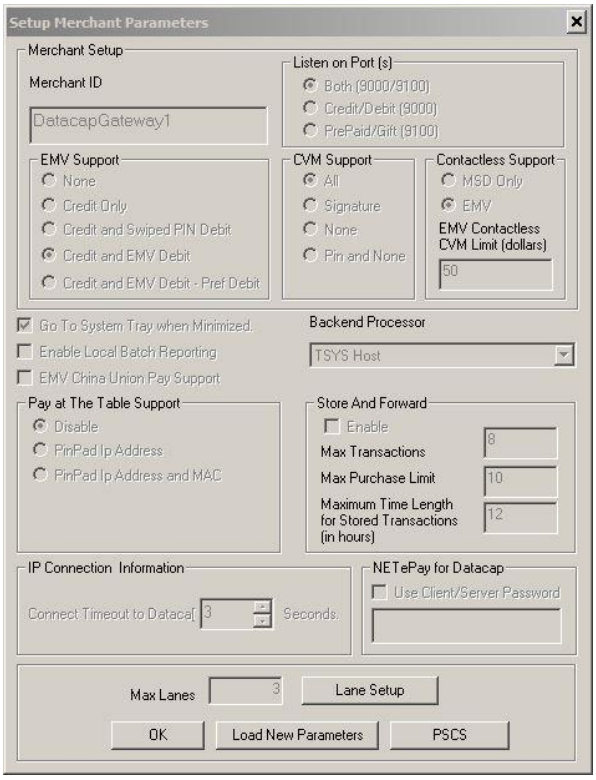
If NETePay detects that the selected merchant is already in use by another serial number, you will see the following dialog:



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

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

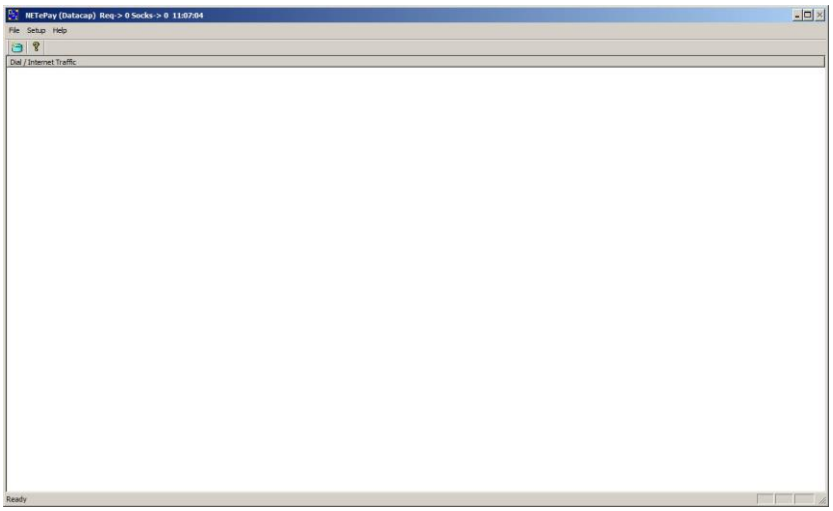
Click ‘OK’ and you will then see the setup screen as follows:



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.

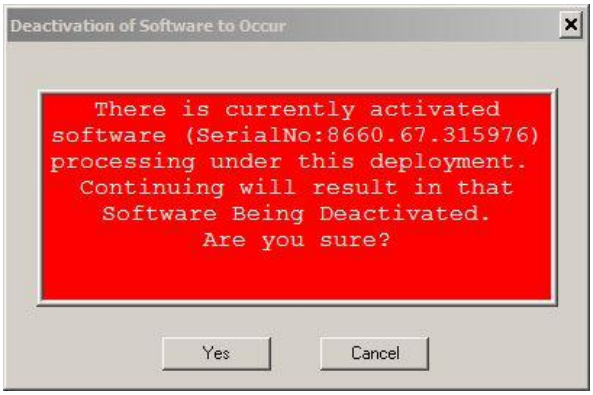
Lane Setup allows you to optionally change the description associated with each lane that was authorized in the PSCS parameter file. You cannot alter the number of lanes in NETePay; changes to the number of lanes must be done by editing the deployment file in PSCS. The Perform PDL button should only be used under direction of Heartland technical support personnel.

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



NETePay 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 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, you should be aware that the NETePay 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 is a replacement for a NETePay 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 installation. This process will allow the new NETePay 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.

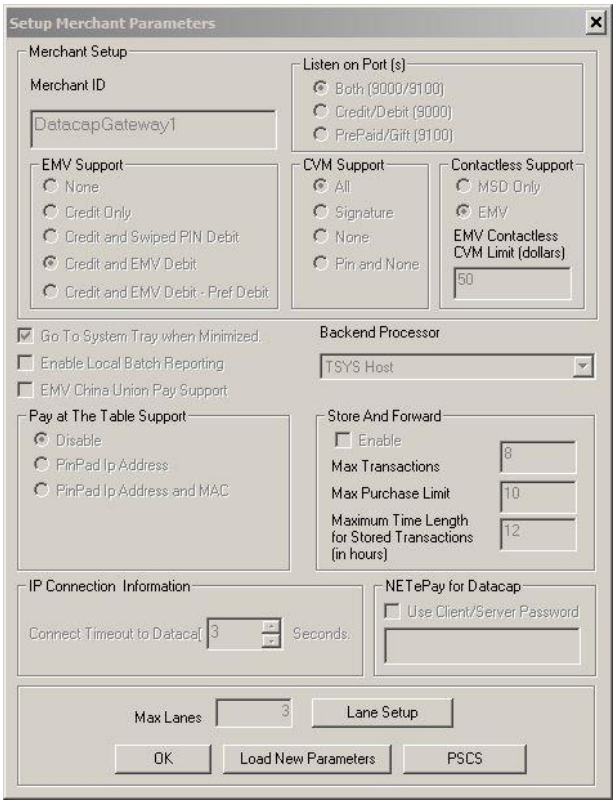
WARNING:

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

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

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

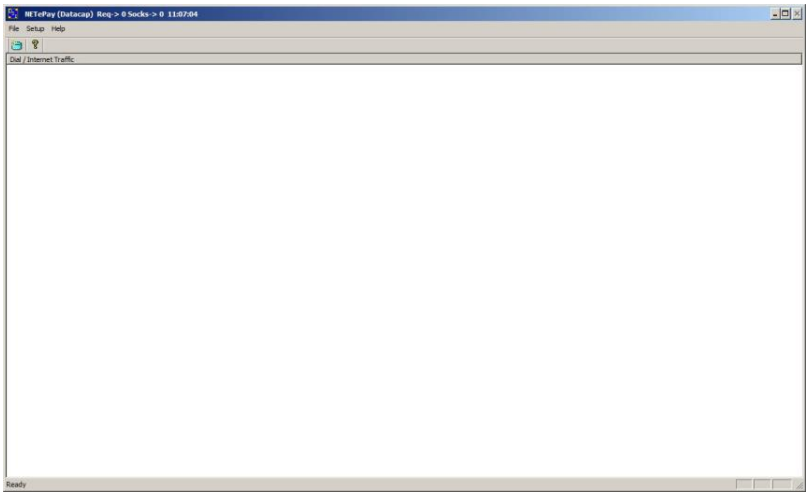
Click ‘OK’ and will then again see the setup screen as follows:



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; changes to the number of lanes must be done by editing the deployment file in PSCS. The Perform PDL button should only be used under direction of Heartland technical support personnel.

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



NETePay setup is complete.

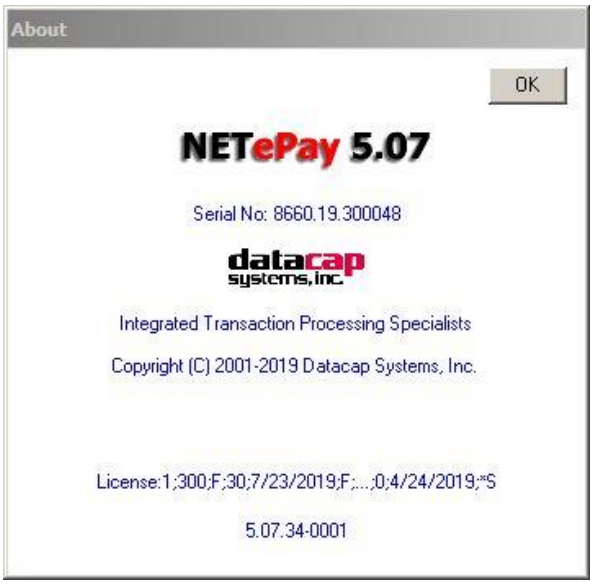
Verifying Your Serial Number and Activation

You can verify the serial number assigned to your copy of NETePay by selecting **About** from the **Help** menu in the main status window. You must start NETePay from the desktop to access the menus.

If NETePay was started by NETePayService.exe as a service, you must first stop the service with the Windows ServiceControl Manager (SCM).

Click the Windows 'Start' button; right-click the 'Computer' shortcut and select 'Manage' from the resulting context menu. Double-click to expand the 'Services and Applications' option from the left pane, and then select 'Services' from the options tree. Scroll to locate NETePay Service and double-click to launch its Properties menu. Click 'Stop' to halt the NETePayService (and the NETePay 5 application). Go to the Desktop (or 'All Programs' | 'Software from Datacap') and click 'NETePay' to start the application on the desktop. Select 'About' | 'Help' to view the About box.

You will see a dialog bog 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* 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 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 relies on numerous services provided by Windows and other Microsoft software. **Proper computer operation is imperative to ensure reliable NETePay operation and prevent possible loss and/or corruption of transaction data.**

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

- *Always* quit NETePay from the File|Exit pull down menu before restarting or shutting down Windows.
- *Always* quit NETePay and then shut down Windows before turning off the computer power. Never turn off the computer power without first quitting NETePay and shutting down Windows.
- *Always* quit NETePay 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, you *must* procure unique terminal and/or merchant account information for each copy of NETePay from your processing provider. Operation of multiple copies of NETePay with identical merchant setup information may cause transactions to be lost or duplicated at your processing provider.

CHAPTER 5

Starting NETePay AS A SERVICE

Introduction

NETePay 5 may be optionally configured to start as a Windows service for installations that want to have NETePay's payment processing services begin automatically when the computer is powered up or restarted without requiring a user console log on.

NETePay 5 must first be installed and successfully activated as described in Chapter 4.

NETePay 5 installation includes a Windows service named *NETePayService.exe* which is placed in the NETePay directory, typically C:/Program Files (x86)/Datacap Systems/NETePay. Upon completion of the NETePay installation, *NETePayService* is configured as 'Manual' and is 'Off'.

NETePay Service Windows Description

Name: NETePay Service

Description: Runs NETePay as a service. When NETePay Service's 'Startup Type' is configured as 'Automatic', there is no longer a requirement that someone has to log in to start NETePay. Once NETePay Service's 'Startup Type' has been changed to 'Automatic', every time the computer is started, NETePay will automatically start. If NETePay Service's 'Startup Type' has been changed to 'Manual', NETePay will no longer automatically start when the computer is started. NOTE: Even if the 'Startup Type' is currently 'Manual', NETePay can be run as a service without changing the 'Startup Type'. Use the 'Start the service' link when NETePay is selected in the Services control panel."

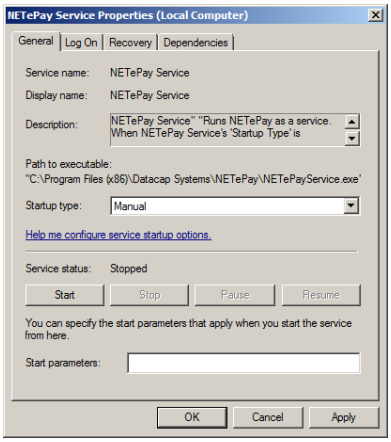
Activating Automatic NETePay Service Start

The Services panel within Windows Administrative Tools is used to configure the operation of NETePayService as follows:

Click the Windows 'Start' button; right-click the 'Computer' shortcut and select 'Manage' from the resulting context menu.

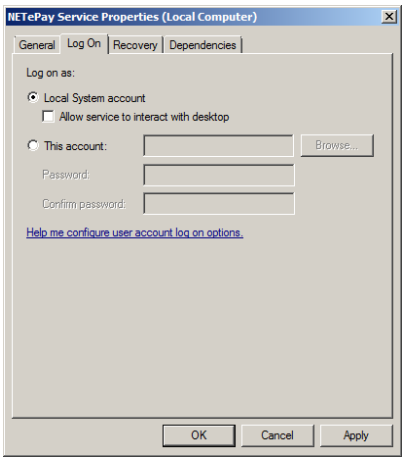
Double-click to expand the 'Services and Applications' option from the left pane, and then select 'Services' from the options tree.

Scroll to locate NETePay Service and double-click to launch its Properties menu, where you can set its execution options from the 'Startup Type' section.

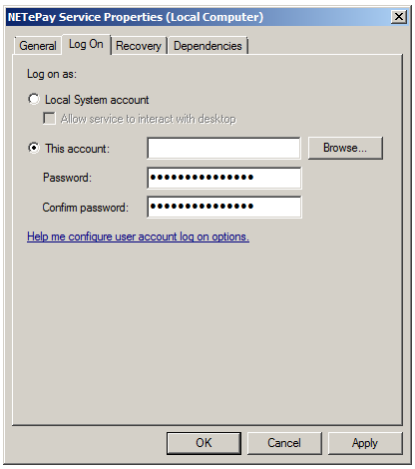


In the 'Start Type' drop down, select 'Automatic'. An Automatic startup launches the NETePayService service, which starts NETePay along with starting Windows; a Manual startup allows you to launch it only when necessary; the Disabled option deactivates the service entirely, requiring you to enable it prior to launching it.

Next, select the 'Log On' tab in the Properties dialog, which will display as follows:



Click the 'Use Account' radio button and the dialog will update as follows:

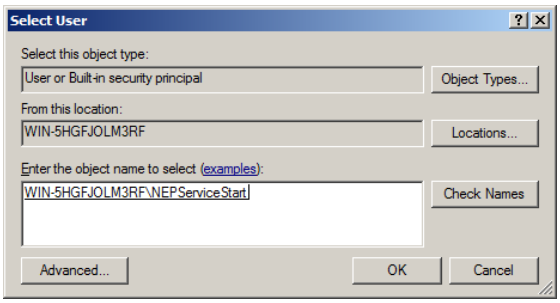


Important Note:
Prior to the next step, you should create an account from the User group specifically to launch the NETePayService service via Windows Management Console.

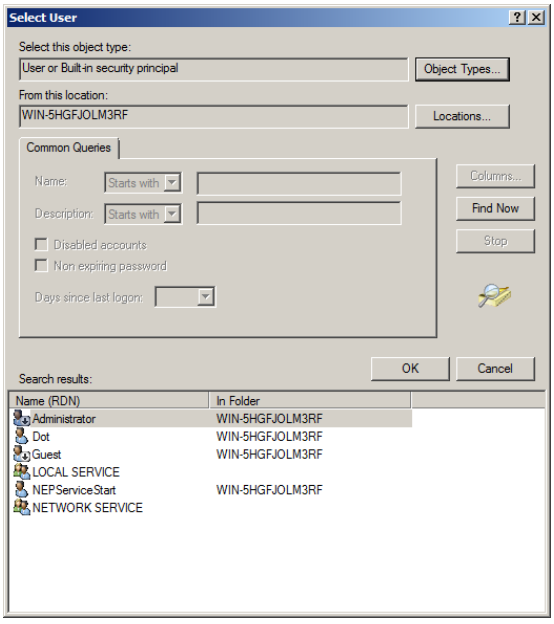
This User account will be reported in the NETePayService log files. For PA-DSS compliance, you should not use the SystemService default principal – it is anonymous and has the privileges of an Administrative account.

Follow the instructions in the PA-DSS 3.1 Implementation Guide - Chapter 2 to configure the account. The account properties should have 'Password never expires' selected to allow the process to start without interruption.

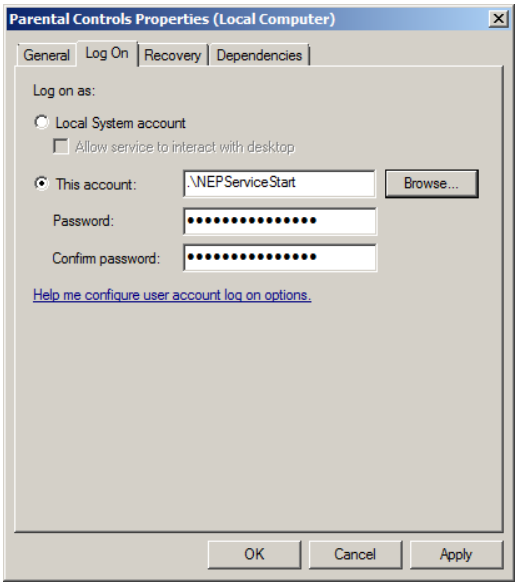
Click the 'Browse' button and the Select User dialog opens as follows:



Next, Click the 'Advanced' button, and the dialog will expand; then click the 'Find Now' button to see as list of Users and Service Accounts as follows:



Double click on a User account created to use to start the NETePayService then click 'OK' to accept the account. The dialog for the service properties will the display again with the account name. Enter (replace) the password with those of the selected account.



Click 'Apply' then 'OK' to complete the NETePayService setup for subsequent automatic start.

NETePay Application and Service Logging

The *NETePay 5* application 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 NETePay log file includes entries that indicate whether it was started as a service or as an application from the Desktop. The log files are in the following location on the install volume:

/Program Files/Datacap Systems/NETePay/DATACAP_LOGS

NETePay 5 application log files are recorded by date in individual ASCII files named as follows:

DSIMMDDYYYY.log

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

NETePayService.exe records its own log in addition to the NETePay application logs. This log records when the NETePay application was started/stopped as a service and the service account used. The NETePay service log files are written in the same install volume location as the NETePay 5 application logs.

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

SERVICE_DSIMMDDYYYY.log

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