



NETePay 5.0

Installation & Configuration Guide

Heartland Portico Host

Part Number: 8715.67

NETePay Installation & Configuration Guide

Copyright © 2015 Datacap Systems Inc. All rights reserved.

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

Notice:

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

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

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

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

Revised: 16 Mar 2015

Version Support

This document supports the following application versions:

NETePay 5 (Heartland Portico Host) - Version 5.05

DSIClientX, Version 3.86

dsiPDCX, Version 1.41

DSIClient Transaction Utility, Version 2.50

Payment Processor Support

This document supports the following payment processor:

Heartland Portico Host

CONTENTS

OVERVIEW	5
INTRODUCTION	5
<i>About NETePay with Dial Backup</i>	<i>5</i>
WHAT'S INCLUDED ON YOUR CD	5
HOW IT WORKS	5
PA DSS 2.0 - IMPLEMENTATION GUIDE	6
ABOUT THIS GUIDE	6
NOTICE	6
REVISION INFORMATION	7
EXECUTIVE SUMMARY	7
<i>Typical Network Implementation</i>	<i>8</i>
<i>NETePay 5 – Network Diagram</i>	<i>8</i>
<i>The 12 Requirements of the PCI DSS:</i>	<i>10</i>
<i>Considerations for the Implementation of Payment Application in a PCI-Compliant Environment.....</i>	<i>11</i>
<i>Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4.a)</i>	<i>11</i>
<i>Sensitive Authentication Data requires special handling (PA-DSS 1.1.5.c).....</i>	<i>11</i>
<i>Purging of Cardholder Data (PA-DSS 2.1).....</i>	<i>12</i>
<i>Disable System Restore Settings</i>	<i>12</i>
<i>Disabling System Restore – Windows 7</i>	<i>12</i>
<i>Encrypt the System PageFile.sys</i>	<i>13</i>
<i>Encrypting PageFile.sys – Windows 7</i>	<i>13</i>
<i>Clear the System Pagefile.sys on shutdown</i>	<i>13</i>
<i>Disable System Management of Pagefile.sys.....</i>	<i>14</i>
<i>Disable Windows Error Reporting.....</i>	<i>14</i>
<i>Disabling Windows Error Reporting – Windows 7.....</i>	<i>14</i>
<i>Cardholder Data Encryption Key Management (PA-DSS 2.5.c and 2.6.a).....</i>	<i>14</i>
<i>Removal of Cryptographic material (PA-DSS 2.7.a)</i>	<i>15</i>
<i>Set up Strong Access Controls (3.1.a and 3.2).....</i>	<i>16</i>
<i>Properly Train and Monitor Admin Personnel.....</i>	<i>18</i>
<i>Log settings must be compliant (PA-DSS 4.1.b, 4.4.b).....</i>	<i>19</i>
<i>Services and Protocols (PA-DSS 5.4.c).....</i>	<i>19</i>
<i>PCI-Compliant Wireless settings (PA-DSS 6.1.f and 6.2.b)</i>	<i>19</i>
<i>Never store cardholder data on internet-accessible systems (PA-DSS 9.1.b).....</i>	<i>20</i>
<i>PCI-Compliant Remote Access (10.2).....</i>	<i>20</i>
<i>PCI-Compliant Delivery of Updates (PA-DSS 10.3.1).....</i>	<i>20</i>
<i>PCI-Compliant Remote Access (10.3.2.b)</i>	<i>21</i>
<i>Data Transport Encryption (PA-DSS 11.1.b)</i>	<i>22</i>
<i>PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2.b).....</i>	<i>22</i>
<i>Network Segmentation.....</i>	<i>23</i>
<i>Maintain an Information Security Program</i>	<i>23</i>
<i>Application System Configuration</i>	<i>23</i>
<i>Payment Application Initial Setup & Configuration</i>	<i>24</i>
INSTALLATION	25

INTRODUCTION	25
REQUIREMENTS	25
<i>Baseline System Configuration</i>	25
<i>Network Requirements</i>	26
INSTALLATION PROCEDURES	26
<i>Accessing the NETePay CD-ROM</i>	26
<i>Installing/Upgrading Microsoft Internet Explorer</i>	28
<i>Installing NETePay (Required)</i>	28
<i>Installing DSIClient Application (Conditional)</i>	28
NETEPAY CONFIGURATION	30
INTRODUCTION	30
ACTIVATION AND PARAMETER DOWNLOAD	30
VERIFYING YOUR SERIAL NUMBER AND ACTIVATION	39
TESTING	39
OPERATIONAL CONSIDERATIONS	40
INDEX	41

OVERVIEW

Introduction

About NETePay with Dial Backup

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.

What's Included on your CD

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

- ***NETePay*** – server-side software that enables you to process payment authorization requests via the Internet or other TCP/IP Virtual Private Network (VPN) services.
- ***DSIClientX*** – an ActiveX control that integrates with a Point of Sale application and sends encrypted payment authorization requests from client machines on a LAN to *NETePay* for processing. *DSIClientX* also includes a utility program to enter test payment transactions called ***DSIClient***.
- ***Microsoft Internet Explorer 6.0*** – this version (or later) of Microsoft Internet Explorer will ensure that you can install the necessary encryption capability required for *NETePay*.

How it works

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

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

PA DSS 2.0 - IMPLEMENTATION GUIDE

About this Guide

This Guide 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 Guide is based on PCI Security Standards Council Payment Application Data Security Standards program (version 2.0 dated October, 2010).

Datacap Systems Inc. instructs and advises its dealers and customers to deploy Datacap Systems Inc. applications in a manner that adheres to the PCI Data Security Standard (v2.0). Subsequent to this, best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various “Benchmarks”, should be followed in order to enhance system logging, reduce the chance of intrusion and increase the ability to detect intrusion, as well as other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, the disabling of infrequently-used or frequently vulnerable networking protocols and the implementation of certificate-based protocols for access to servers by users and vendors.

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

Notice

THE INFORMATION IN THIS GUIDE 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, 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.

Revision Information

Name	Title	Date of Update	Summary of Changes
NETePay 5	PA-DSS 2.0 Implementation Guide	29 April 2013	Guide Creation

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

Executive Summary

NETePay 5 version 5.05 has been PA-DSS (Payment Application Data Security Standard) certified, with PA-DSS Version 2.0. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):



Coalfire Systems, Inc. 361 Centennial Parkway Suite 150 Louisville, CO 80027	Coalfire Systems, Inc. 150 Nickerson Street Suite 106 Seattle, WA 98109
--	---

This Guide also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The Guide then provides specific installation, configuration, and ongoing management best practices for using Payment Application as a PA-DSS validated Application operating in a PCI Compliant environment.

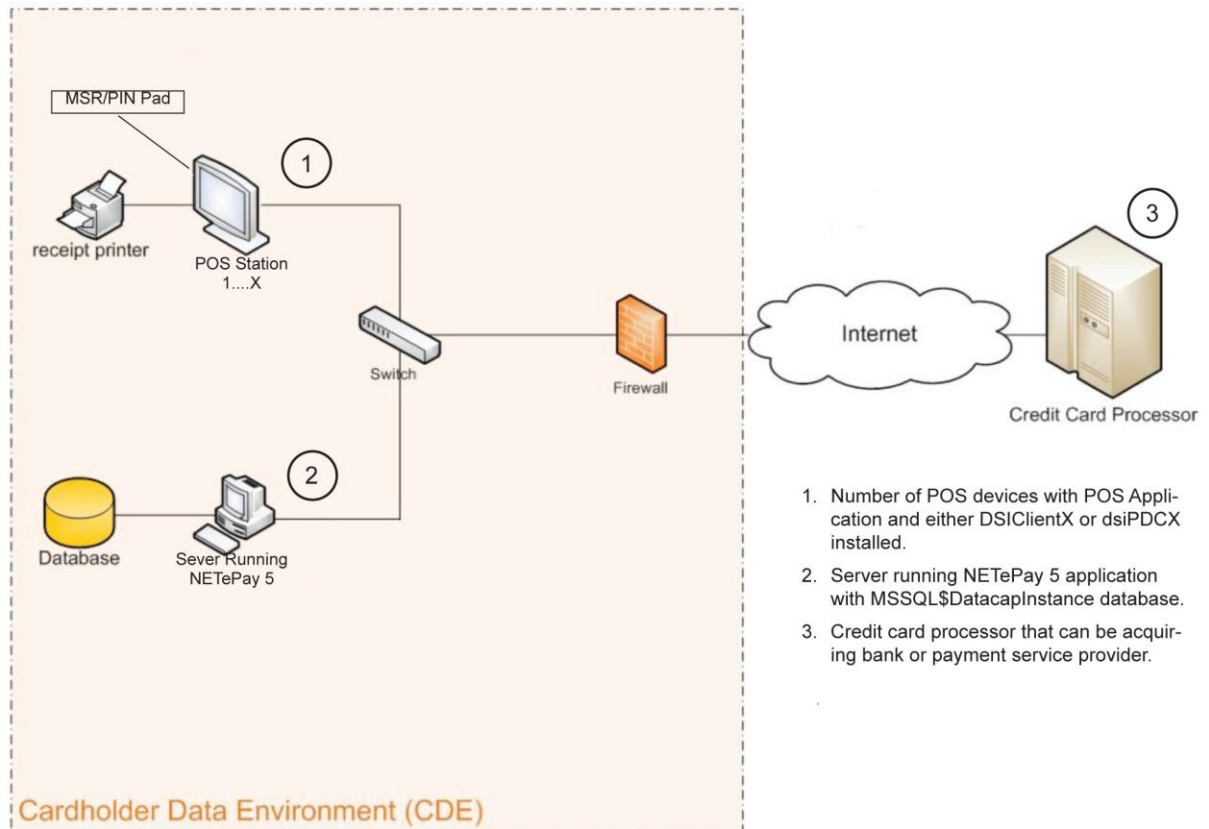
PCI Security Standards Council Reference Documents

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

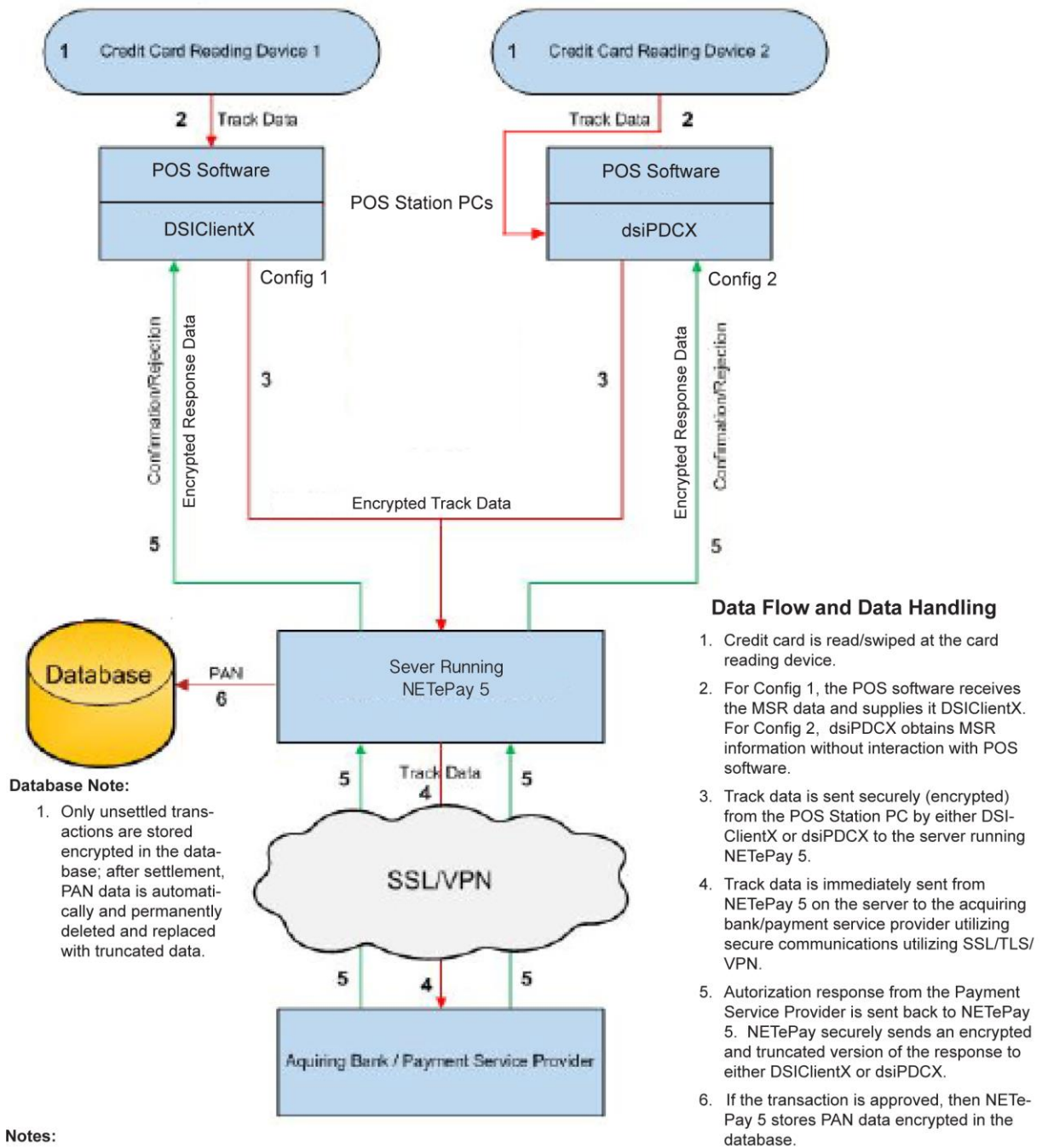
- Payment Applications Data Security Standard (PA-DSS)
https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml
- Payment Card Industry Data Security Standard (PCI DSS)
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- Open Web Application Security Project (OWASP)
<http://www.owasp.org>

Typical Network Implementation

NETePay 5 – Network Diagram



NETePay 5 – Data Flow and Data Handling Diagram



Notes:

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

Difference between PCI Compliance and PA-DSS Validation

As a software vendor, our responsibility is to be “PA-DSS Validated.”

We have performed an assessment and certification compliance review with our independent assessment firm, to ensure that our platform does conform to industry best practices when handling, managing and storing payment related information.

PA-DSS 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.

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

The PA-DSS Validation is intended to ensure that the Payment Application will help you achieve and maintain PCI Compliance with respect to how 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

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

Protect Cardholder Data

- 3. Protect Stored Data*
- 4. Encrypt transmission of cardholder data and sensitive information across public networks*

Maintain a Vulnerability Management Program

- 5. Use and regularly update anti-virus software*
- 6. Develop and maintain secure systems and applications*

Implement Strong Access Control Measures

- 7. Restrict access to data by business need-to-know*
- 8. Assign a unique ID to each person with computer access*
- 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

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.

- * Sensitive Authentication Data requires special handling
- * Remove Historical Cardholder Data
- * Set up Good Access Controls
- * Properly Train and Monitor Admin Personnel
- * Key Management Roles & Responsibilities
- * PCI-Compliant Remote Access
- * Use SSH, VPN, or SSLV3/TLS 1.0 or higher for encryption of administrative access
- * Log settings must be compliant
- * PCI-Compliant Wireless settings
- * Data Transport Encryption
- * PCI-Compliant Use of Email
- * Network Segmentation
- * Never store cardholder data on internet-accessible systems
- * Use SSLV3 for Secure Data Transmission
- * Delivery of Updates in a PCI Compliant Fashion

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4.a)

Previous versions of NETePay 5 did not store sensitive authentication data. Therefore, there is no need for secure removal of this historical data by the application as required by PA-DSS v2.0.

Sensitive Authentication Data requires special handling (PA-DSS 1.1.5.c)

Datacap Systems Inc. does not store Sensitive Authentication data for any reason, and we strongly recommend that you do not do this either. However, if for any reason you should do so, the following guidelines must be followed when dealing with sensitive authentication data (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

Purging of Cardholder Data (PA-DSS 2.1)

The following guidelines must be followed when dealing with cardholder data (PAN alone or with any of the following: expiry date, cardholder name or service code):

- ✦ A customer defined retention period must be defined with a business justification.
- ✦ Cardholder data exceeding the customer-defined retention period must be purged.
- ✦ Here are the locations of the cardholder data you must purge:
 - Files: dbnetepay.mdf and dbnetepay.ldf
 - Tables: MSSQL\$DatacapInstance – Tables: batch, version
- ✦ To purge the cardholder data you must do the following two things:
 1. The application automatically and permanently purges (truncates) settled transactions. Unsettled transactions are stored in encrypted form. A user may manually purge all transactions by removing the database using the Datacap Systems Inc supplied *NETePay Database Utility* as to delete the previous NETePay database, any backups and all logs:
 1. Shut down **NETePay**
 2. Using Windows Control Panel, select Add/Remove Programs
 3. Select **NETePay** and remove it
 4. Locate the **NETePay** folder in <bootdrive>:\Program Files\Datacap Systems and use a secure file deletion utility to remove it. (Such as Eraser {<http://eraser.heidi.ie>} or Microsoft SDelete {<http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx>})
 5. Install **NETePay 5.0**
 6. From the **Programs/Software from Datacap** group, run the **NETePay Database Manager**
 7. Select Connect
 8. Select Create New Database
 9. Shut down **NETePay Database Manager**
 10. Start **NETePay 5.0**

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

2. In the operating system you must configure appropriate settings to prevent inadvertent retention of cardholder data. The following items should be configured in Windows:

Disable System Restore Settings

Disabling System Restore – Windows 7

- Right Click on Computer > Select “Properties”

- Select “System Protection” on the top left list.
- Select Configure.
- 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

Encrypt the System PageFile.sys

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

Disable System Management of Pagefile.sys

Disabling System Management of PageFile.sys – Windows 7

- Right Click on Computer > Select “Properties”
- Select “Advanced System Settings” on the top left list.
- Under performance select “Settings” and go to the “Advanced” tab.
- Select “Change” under Virtual Memory.
- Uncheck “Automatically manage page file size for all drives”
- Select “Custom Size”
- Enter the following for the size selections:
 - Initial Size – as a good rule of thumb, the size should be equivalent to the amount of memory in the system.
 - Maximum Size – as a good rule of thumb, the size should be equivalent to 2x the amount of memory in the system.
- Click “Ok”, “OK”, and “OK”
- You will be prompted to reboot your computer.

Disable Windows Error Reporting

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”

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.

Cardholder Data Encryption Key Management (PA-DSS 2.5.c and 2.6.a)

NETePay 5 incorporates an automatic key generation methodology that creates a unique dynamic key for each stored PAN and expiry date stored in the database. This function cannot be disabled by a user and requires no user key management or custodial functions.

The following key management functions normally required to be performed per PCI DSS are automatically addressed by the NETePay 5 automatic key generation and usage methodology:

- Generation of strong cryptographic keys.
- Secure cryptographic key distribution.
- Secure cryptographic key storage.

- Cryptographic key changes for keys that reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of ciphertext has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).
- Retire keys when the integrity of the key has been weakened.
- Replace known or suspected compromised keys.
- If retired or replaced cryptographic keys are retained, the application cannot use these keys for encryption operations.
- Manual clear-text key-management procedures require split knowledge and dual control of keys.
- Prevention of unauthorized substitution of cryptographic keys.

Removal of Cryptographic material (PA-DSS 2.7.a)

NETePay 5 has the following versions that previously encrypted cardholder data: Version 5.04 or earlier and the following must be done:

NETePay 5 automatically and permanently purges (truncates) settled transactions. Unsettled transactions are stored in encrypted form; encrypted data includes PAN's and expiration dates. A user may manually purge all transactions by removing the database using the Datacap Systems Inc supplied *NETePay Database Utility* as to delete the previous NETePay database, any backups and all logs:

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

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

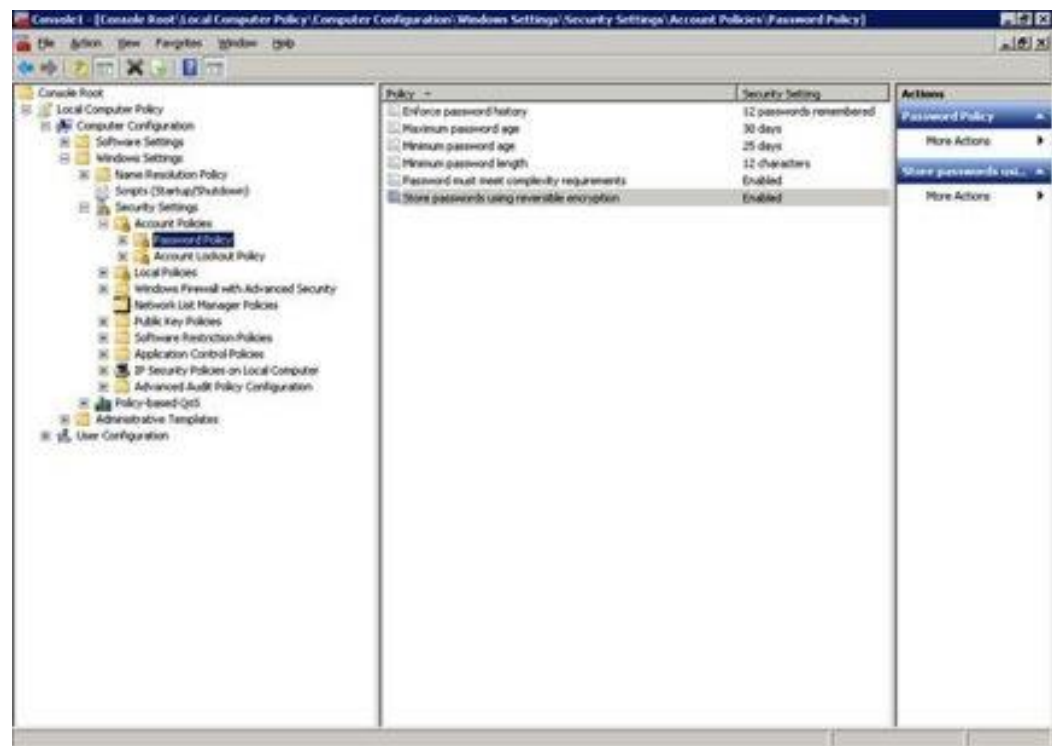
- * This removal is absolutely necessary for PCI DSS Compliance
- * It will not be possible to re-encrypt historic data since the deletion of the database permanently removes cryptographic information and *all* data simultaneously.

Set up Strong Access Controls (3.1.a and 3.2)

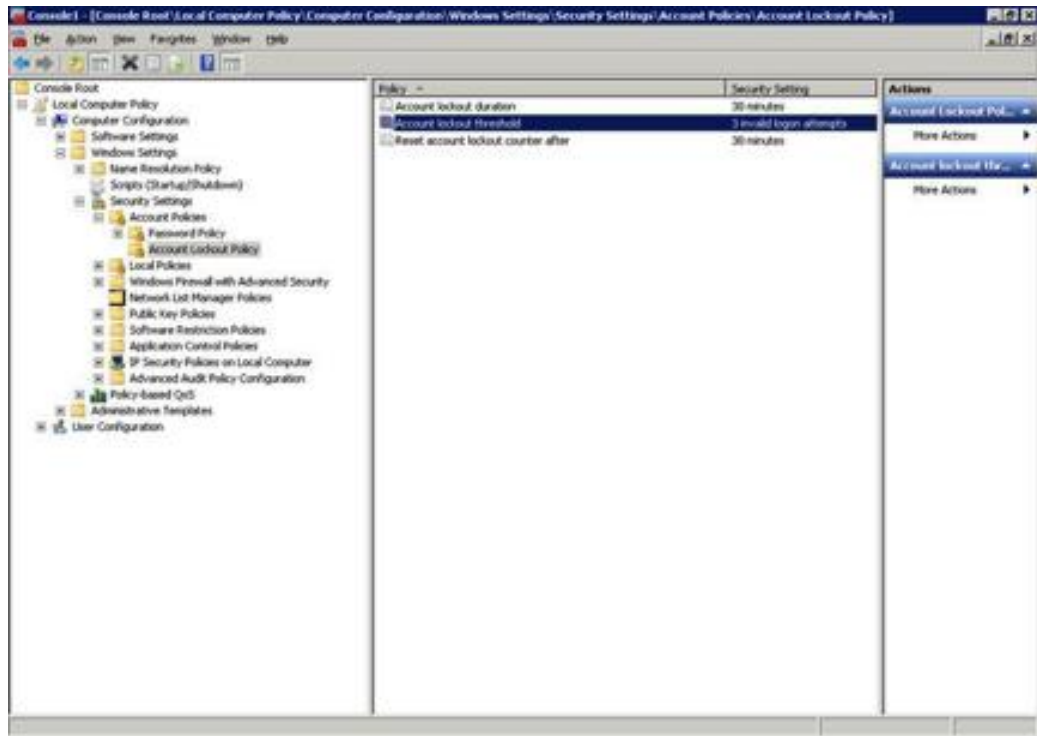
The PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by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

3.1.a: 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. NETePay 5 does not support user account access directly. However, a user should configure a Windows secure group access policy on the machine on which NETePAY 5 is installed.

Your Windows Server operating system environment must be modified to comply with the above requirement. 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:



All authentication credentials are provided by the application. For both the completion of the initial installation and for any subsequent changes (for example, any changes that result in user accounts reverting to default settings, any changes to existing account settings, or changes that generate new accounts or recreate existing accounts), the following 10 points must be followed per PCI 8.1, 8.2, and 8.5.8-15:

1. The application must assign unique IDs for user accounts. (8.1). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated above.*
2. The application must provide at least one of the following three methods to authenticate users: (8.2). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated above.*
 - 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
3. The application must NOT require or use any group, shared, or generic accounts or passwords.(8.5.8). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated above.*
4. The application requires passwords to be changed at least every 90 days (8.5.9). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated above.*
5. The application requires passwords must to be at least 7 characters (8.5.10). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated above.*
6. The application requires passwords to include both numeric and alphabetic characters (8.5.11). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated above.*
7. The application keeps password history and requires that a new password is different than any of the last four passwords used. (8.5.12). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated above.*
8. The application limits repeated access attempts by locking out the user account after not more than six logon attempts. (8.5.13). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated above.*
9. The application sets the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (8.5.14). *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated above.*
10. The application requires the user to re-authenticate to re-activate the session if the application session has been idle for more than 15 minutes. *NETePay 5 does not support user account access directly; a Windows Group access policy should be established as indicated above.*

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

SQLExpress 2008

[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 servers with cardholder data, and for access controlled by the application.]

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

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

/Program Files/Datacap Systems/NETePay/DATACAP_LOGS

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

DSIMMDDYYYY.log

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

Services and Protocols (PA-DSS 5.4.c)

NETePay 5 does not require nor permit the use of any insecure services or protocols. Here are the services and protocols that NETePay 5 does require:

- SSL 3.0
- TLS 1.0
- HTTPS

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

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

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

1. Encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions Refer to wireless device manufacturer's documentation for change instructions.
2. Default SNMP community strings on wireless devices must be changed. Refer to wireless device manufacturer's documentation for change instructions.
3. Default passwords/passphrases on access points must be changed. Refer to wireless device manufacturer's documentation for change instructions.
4. Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks. Refer to wireless device manufacturer's

documentation for firmware update instructions. Firmware updates should be performed for any wireless networking device which is capable, including routers, access points, gateways and switches.

5. Other security-related wireless vendor defaults, if applicable, must be changed. Refer to wireless device manufacturer's documentation for change instructions. Changes to vendor defaults settings should be performed for any wireless networking device which is capable, including routers, access points, gateways and switches.

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

4.1.1: Industry best practices (for example, IEEE 802.11.i) must be used to implement strong encryption for authentication and transmission of cardholder data.

Note: The use of WEP as a security control was prohibited as of June 30, 2010.

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

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 (10.2)

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

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

PCI-Compliant Delivery of Updates (PA-DSS 10.3.1)

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

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

Our continuing security education activities are comprised of the following:

- Participating in Microsoft E-Learning Security Clinics and Hands-On Labs
- Attendance of live Microsoft security seminars
- Encourage recommendations for technical library purchases on security subjects
- Regular review of OWASP (Open Web Application Security Project) website (<http://www.owasp.org>)
- Regular review of US-CERT (United States Computer Emergency Readiness Team) Current Activity (<http://www.us-cert.gov/current/>)
- Regular review of SecurityTracker 's Weekly Vulnerability Summary Newsletter distributed via email

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

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

PCI-Compliant Remote Access (10.3.2.b)

NETePay 5 does not natively support any remote access functionality.

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 SSLV3 or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments).

PCI DSS requirement 4.1: Use strong cryptography and security protocols such as secure sockets layer (SSLV3) / transport layer security (TLS 1.0 or higher) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

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

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

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

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

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

Non-console administration (PA-DSS 12.1)

Although NETePay 5 does not support non-console administration and we do not recommend using non-console administration, should you ever choose to do this, must use SSH, VPN, or SSLV3/TLS 1.0 or higher for encryption of this non-console administrative access.

Network Segmentation

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

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

Maintain an Information Security Program

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

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

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

Application System Configuration

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

- Microsoft Windows 2000 Professional with Service Pack 4, Windows XP Pro with Service Pack 3, Windows Vista Business Edition with Service Pack 2, Windows Server 2003 or 2008, Windows 7 or Windows 8. All latest updates and hotfixes should be applied.
- 2 GB of RAM minimum, 4 GB or higher recommended
- 50 GB of available hard-disk space
- Microsoft Internet Explorer with 128-bit encryption, Microsoft Internet Explorer 6.0 or higher recommended

- TCP/IP network connectivity. (Persistent Internet connection recommended)
- SQLExpress2008 - (for Windows XP Pro, Windows Server 2003 or 2008, Windows Vista, Windows 7, Windows 8)
- MSDE (for Windows 2000)

Payment Application Initial Setup & Configuration

*Installation of NETePay 5 and associated database and utilities requires Administrator access in Windows. Datacap advises users to change default password and manage Windows passwords according to PCI DSS 2.1

INSTALLATION

Introduction

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

- *NETePay*
- *DSIClientX*
- Microsoft Internet Explorer 6.0 (or later) with High Encryption

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

Each client machine will require *DSIClientX* 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 2000 Professional with Service Pack 4, Windows XP Pro with Service Pack 3, Windows Vista Business Edition with Service Pack 2, Windows Server 2003 or 2008, Windows 7 or Windows 8. All latest updates and hotfixes should be applied.
- 2 GB of RAM minimum, 4 GB or higher recommended
- 50 GB of available hard-disk space
- Microsoft Internet Explorer with 128-bit encryption, Microsoft Internet Explorer 6.0 or higher recommended
- TCP/IP network connectivity.
- Persistent Internet Connection (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.

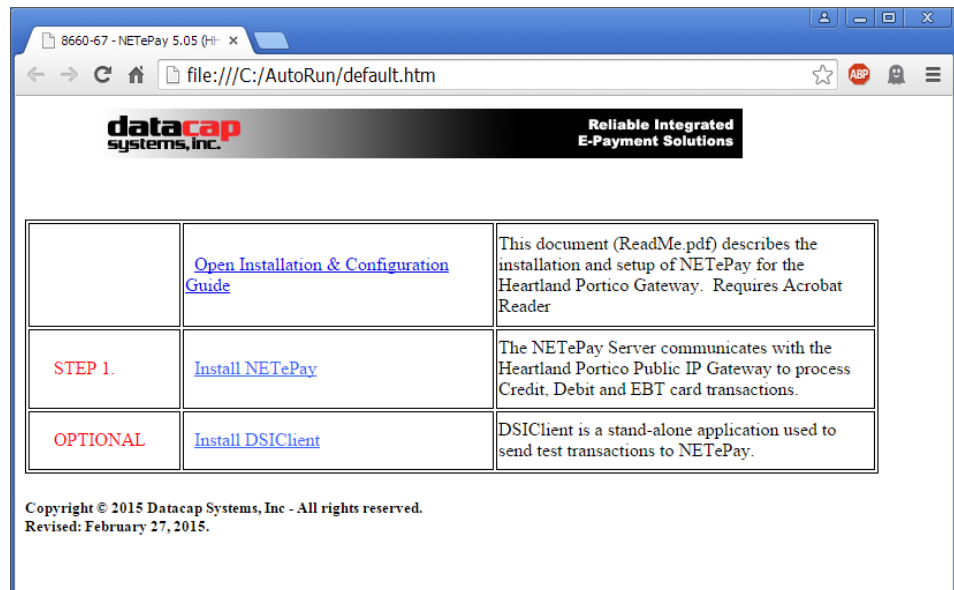
Installation Procedures

Accessing the NETePay CD-ROM








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

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

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



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

Name ^	Date modified	Type	Size	
 program files	3/3/2015 6:30 PM	File folder		
 System32	3/3/2015 6:30 PM	File folder		
 0x0409.ini	3/23/2010 5:44 PM	Configuration settings	22 KB	
 NETePay 5.05 (HH 5.05) Heartland Host.msi	2/28/2015 2:20 PM	Windows Installer Package	2,828 KB	
 setup.exe	2/28/2015 2:19 PM	Application	1,206 KB	
 Setup.ini	2/28/2015 2:19 PM	Configuration settings	6 KB	
 WindowsInstaller-KB893803-x86.exe	5/16/2005 5:42 PM	Application	2,525 KB	

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

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

Installing DSIClient Application (Conditional)

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

The DSIClient application provides a convenient means to test operation of the NETePay 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 which 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 on the *NETePay* CD-ROM and double-click, **setup.exe**.

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

NETePay CONFIGURATION

Introduction

This chapter explains how to activate and configure *NETePay 5.0* for use.

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

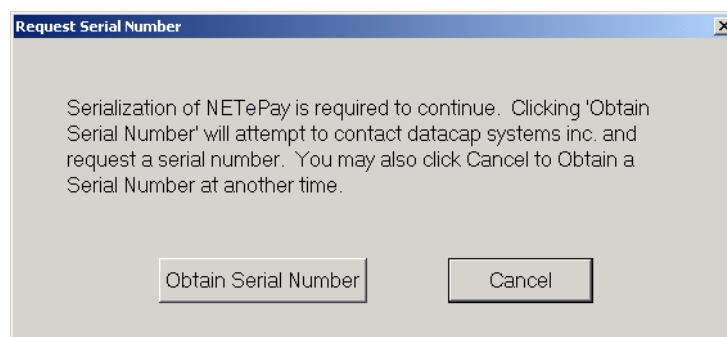
Note

Firewalls, routers or other systems which can block IP network traffic must allow NETePay 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.

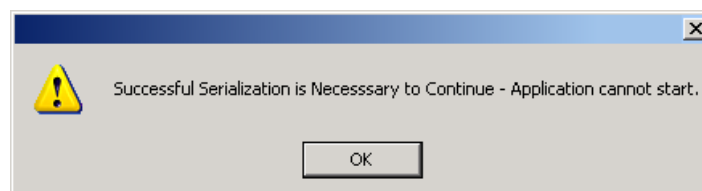
Activation and Parameter Download

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:



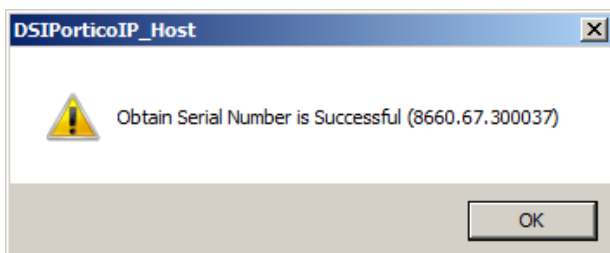
Click 'Obtain Serial Number' to enable NETePay to contact PSCS for a serial number.

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

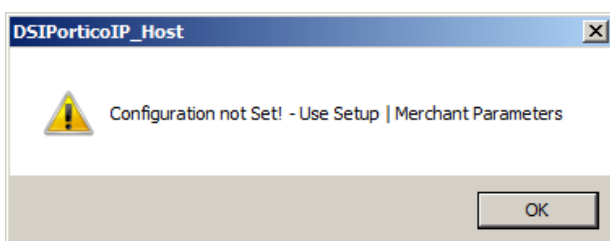


Click 'OK' and NETePay will close. Failure to successfully obtain a serial number means that NETePay was not able to contact Datacap's PSCS server over the Internet to obtain a serial number. Assure that the Internet connection is operating properly by using the default web browser on the machine where 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.

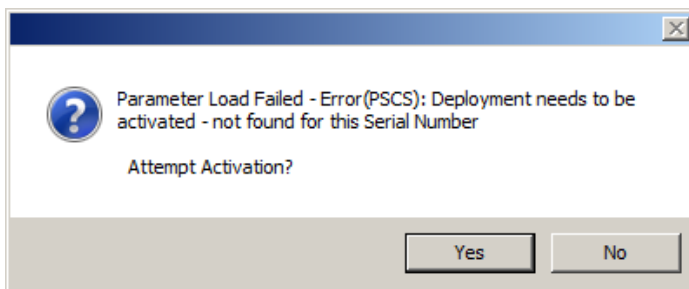
If a parameter file has been created on Datacap's PSCS server for the merchant account, then select 'Merchant Parameters' from the 'Setup' drop down menu. You will then see the following screen:

 A screenshot of a complex configuration window titled "Setup NETePay Parameters". The window is divided into several sections:

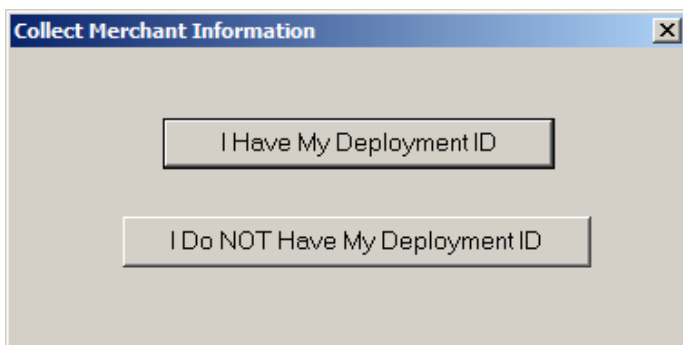
- Merchant Information:** Includes fields for License ID, Site ID, Portico Device ID, and a Merchant Category dropdown menu (set to "Retail"). There are also checkboxes for "Do Not Connect to Host on Startup" and "Verify Portico SSL Certificate".
- Portico Information:** Includes fields for User Name and Password.
- Security:** Includes a checkbox for "Use Client / Server Password" and an associated text field.
- Transport:** Includes radio buttons for "IP Only", "IP with DIAL Backup", and "DIAL Only".
- Dial Backup Information:** Includes fields for Comm Port, Dial Prefix, and Host Authorization Phone No.
- IP Connection Information:** Includes a field for Connect Timeout to Portico (set to 3 seconds) and a Max Lanes field (set to 1).

 At the bottom of the window are three buttons: "OK", "Load New Parameters", and "PSCS".

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

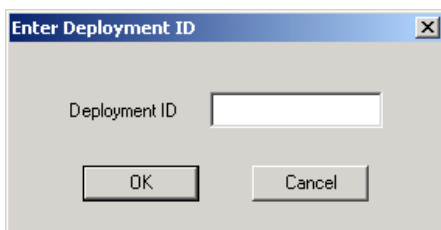


Click 'Yes' to attempt activation and you will see the following screen:



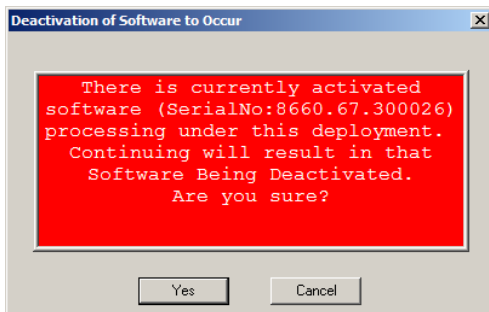
To continue, you must verify that you or someone else has created a Merchant Deployment on Datacap's PSCS server. If a deployment was created you may have been given a Deployment ID, which is typically an eight character code that has been assigned to the merchant's parameters. If you have a Deployment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

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



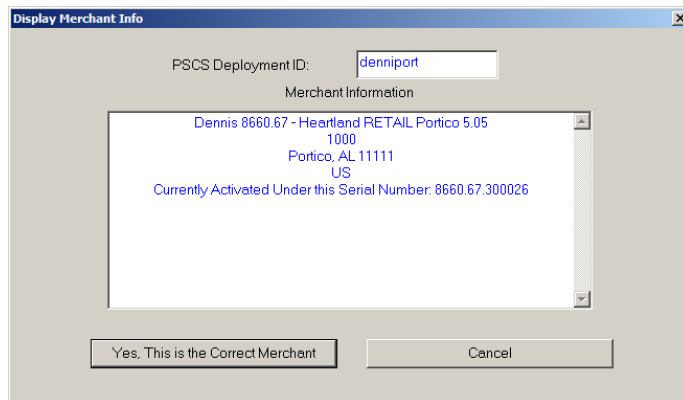
Enter the Deployment ID for the merchant parameter file and click 'OK'.

If NETePay 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.

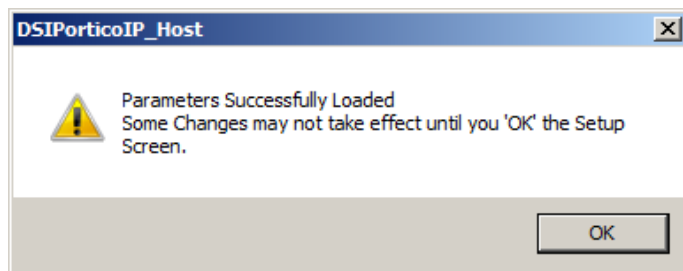
NETePay will display a screen with merchant demographic data for you to verify as follows:



The 'Display Merchant Info' dialog box shows the PSCS Deployment ID as 'denniport'. The Merchant Information section displays: 'Dennis 8660.67 - Heartland RETAIL Portico 5.05', '1000', 'Portico, AL 11111', 'US', and 'Currently Activated Under this Serial Number: 8660.67.300026'. At the bottom are 'Yes, This is the Correct Merchant' and 'Cancel' buttons.

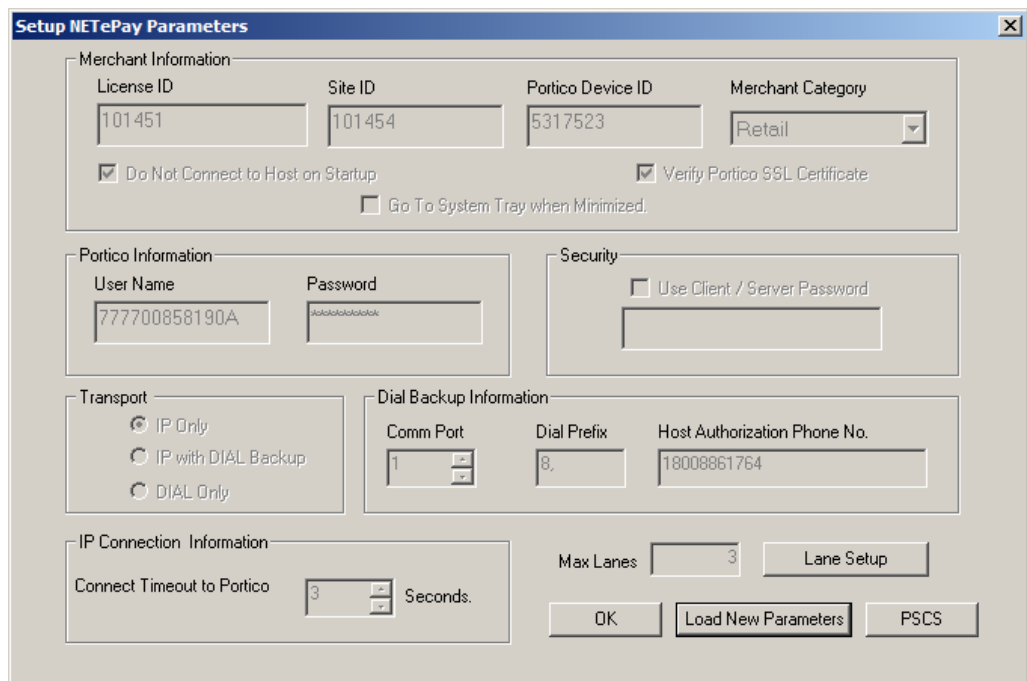
If the displayed information is not correct for the merchant site, click 'Cancel' and retry entry from the beginning of step 4. If the displayed information correctly identifies the merchant site, click 'Yes, This is the Correct Merchant'.

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



The 'DSIPorticoIP_Host' dialog box displays a warning icon and the text: 'Parameters Successfully Loaded. Some Changes may not take effect until you 'OK' the Setup Screen.' An 'OK' button is at the bottom right.

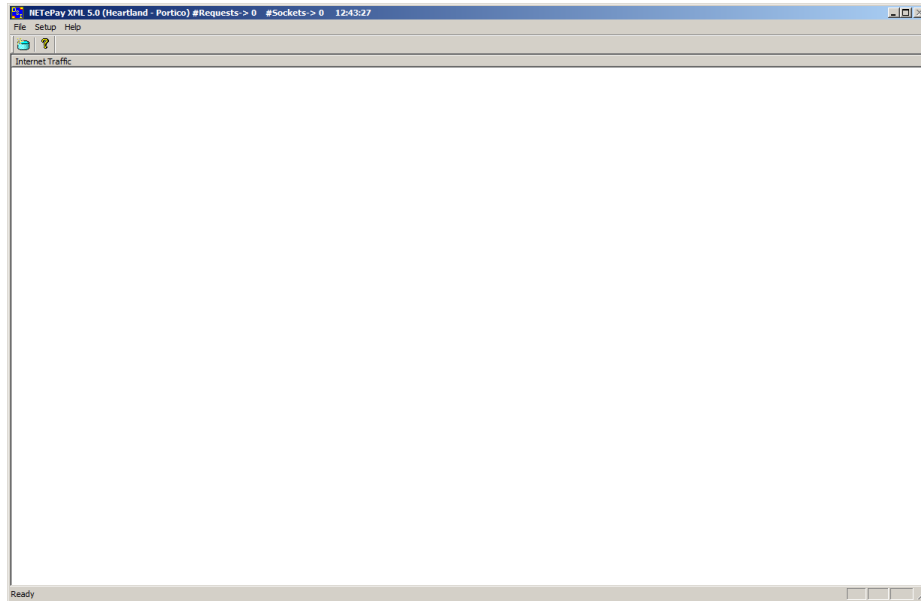
Click 'OK' and will then again see the setup screen as follows:



The 'Setup NETePay Parameters' dialog box contains several sections: 'Merchant Information' with fields for License ID (101451), Site ID (101454), Portico Device ID (5317523), and Merchant Category (Retail); checkboxes for 'Do Not Connect to Host on Startup', 'Verify Portico SSL Certificate', and 'Go To System Tray when Minimized'; 'Portico Information' with User Name (777700858190A) and Password; 'Security' with 'Use Client / Server Password' checkbox; 'Transport' with radio buttons for IP Only, IP with DIAL Backup, and DIAL Only; 'Dial Backup Information' with Comm Port (1), Dial Prefix (8), and Host Authorization Phone No. (18008861764); 'IP Connection Information' with Connect Timeout to Portico (3) seconds; and 'Max Lanes' (3) with a 'Lane Setup' button. At the bottom are 'OK', 'Load New Parameters', and 'PSCS' buttons.

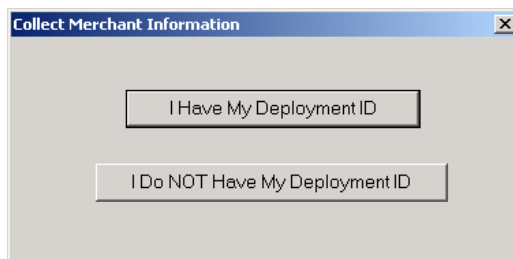
Lane Setup allows you to optionally change the description associated with each lane that was authorized in the PSCS parameter file. You cannot alter the number of lanes in NETePay; changes to the number of lanes must be done by editing the deployment file in PSCS.

The 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.

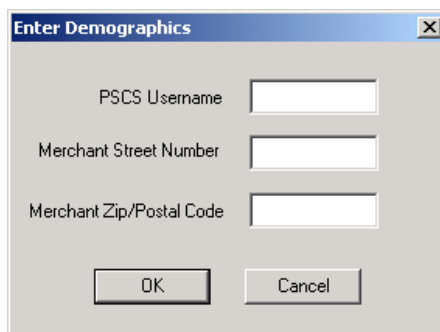


NETePay setup is complete.

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:

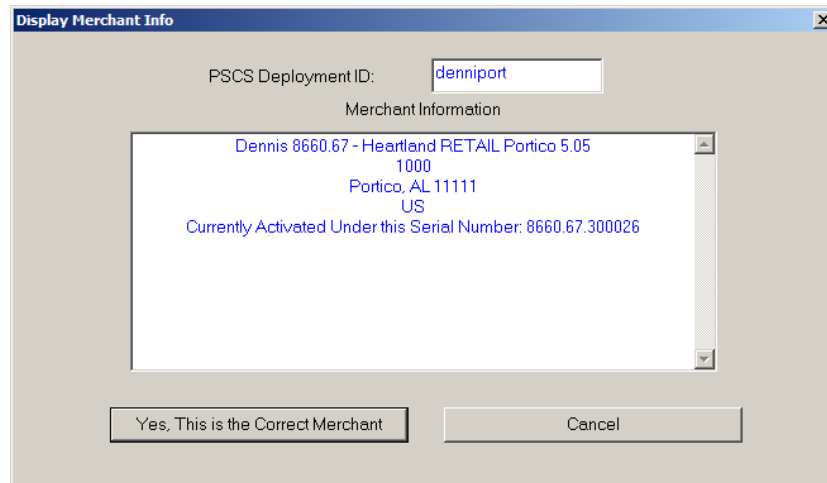


You need the following information to complete the demographics dialog entries:

- 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

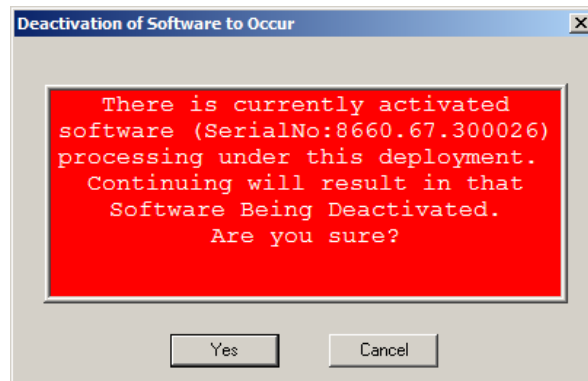
After entering this information, click 'OK'.

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



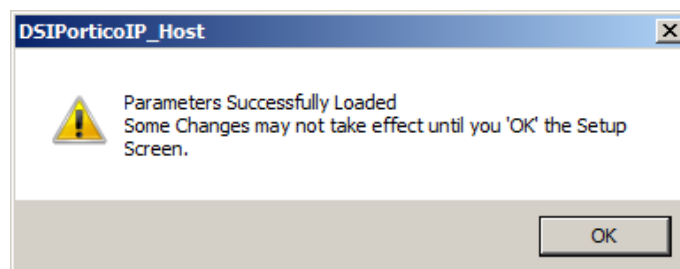
If the displayed information is not correct for the merchant site, click 'Cancel' and retry entry from the beginning of step 4. If the displayed information correctly identifies the merchant site, click 'Yes, This is the Correct Merchant'.

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:

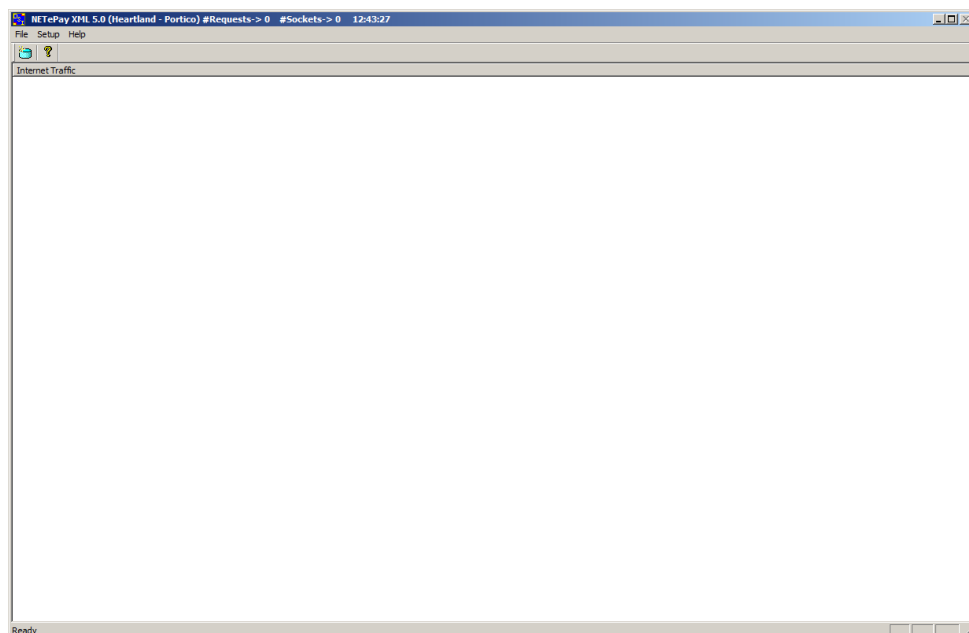
The screenshot shows the 'Setup NETePay Parameters' dialog box with the following fields and values:

- Merchant Information:**
 - License ID: 101451
 - Site ID: 101454
 - Portico Device ID: 5317523
 - Merchant Category: Retail (dropdown)
 - ☒ Do Not Connect to Host on Startup
 - ☒ Verify Portico SSL Certificate
 - ☐ Go To System Tray when Minimized.
- Portico Information:**
 - User Name: 777700858190A
 - Password: [masked]
- Security:**
 - ☐ Use Client / Server Password
- Transport:**
 - ☒ IP Only
 - ☐ IP with DIAL Backup
 - ☐ DIAL Only
- Dial Backup Information:**
 - Comm Port: 1
 - Dial Prefix: 8
 - Host Authorization Phone No.: 18008861764
- IP Connection Information:**
 - Connect Timeout to Portico: 3 Seconds.
- Max Lanes:** 3
- Buttons:** OK, Load New Parameters, PSCS, Lane Setup

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.

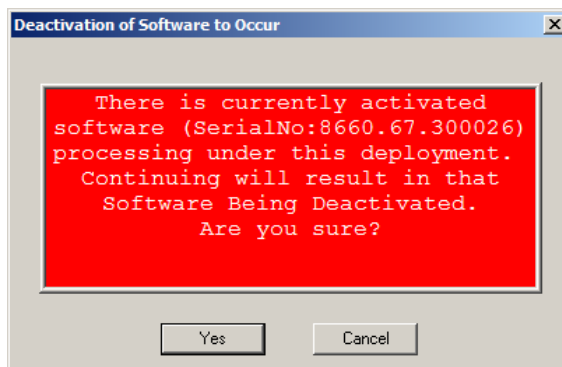
Lane Setup allows you to optionally change the description associated with each lane that was authorized in the PSCS parameter file. You cannot alter the number of lanes in NETePay; changes to the number of lanes must be done by editing the deployment file in PSCS.

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.

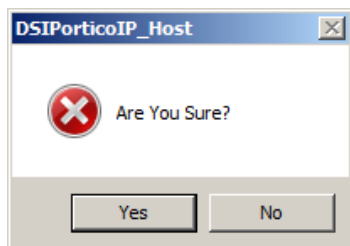
If the Deployment ID or merchant demographic information is correct and you want to force the parameters to load into NETePay, you should be aware that the NETePay with the serial number listed in the dialog box will be deactivated and will no longer be able to process transactions.

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.

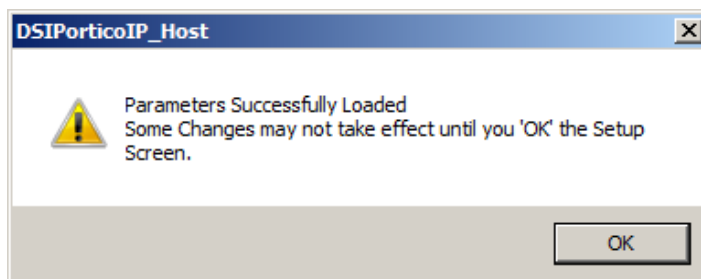
WARNING:

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 which 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:

Setup NETePay Parameters

Merchant Information

License ID: 101451 Site ID: 101454 Portico Device ID: 5317523 Merchant Category: Retail

☒ Do Not Connect to Host on Startup ☒ Verify Portico SSL Certificate
☐ Go To System Tray when Minimized.

Portico Information

User Name: 777700858190A Password: XXXXXXXXXXXX

Security

☐ Use Client / Server Password

Transport

☒ IP Only
☐ IP with DIAL Backup
☐ DIAL Only

Dial Backup Information

Comm Port: 1 Dial Prefix: 8 Host Authorization Phone No.: 18008861764

IP Connection Information

Connect Timeout to Portico: 3 Seconds.

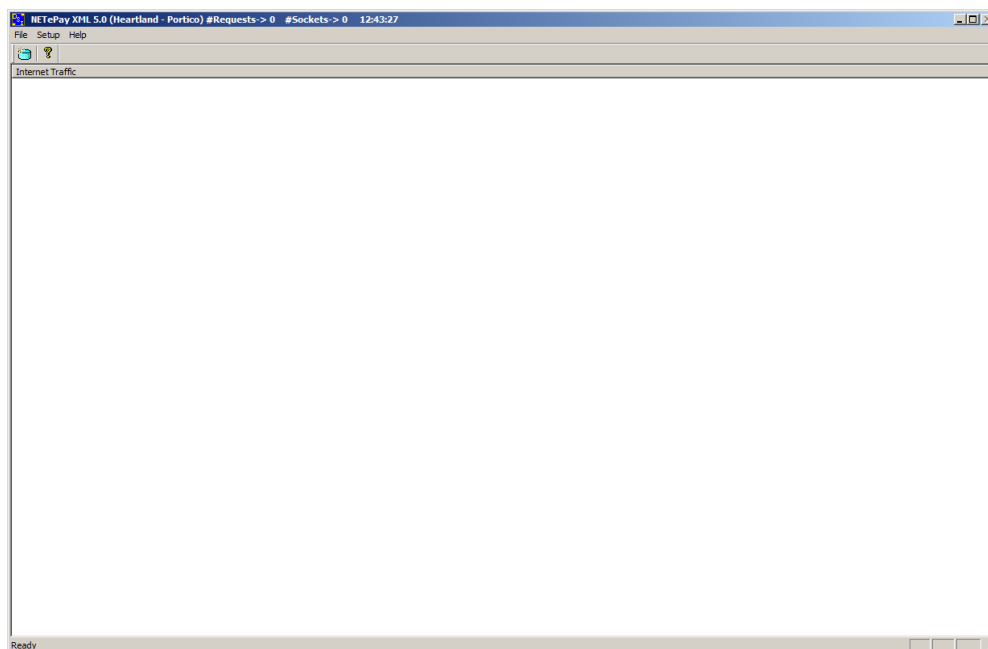
Max Lanes: 3 Lane Setup

OK Load New Parameters PSCS

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

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

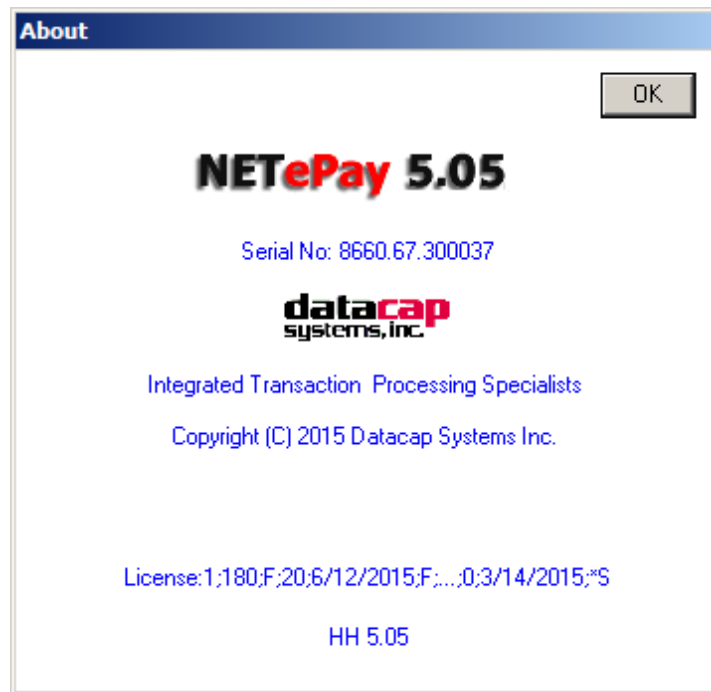
You will then see the NETePay main status window indicating that NETePay is now programmed and ready to process transactions.



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 item in the main status window. 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 such as MSDE or SQLExpress 2005. **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.

INDEX

A

About
NETePay, 5

H

How it works, 5

I

Installation, 25
Installation Procedures, 26
 Accessing the NETePay CD-ROM, 26
 NETePay, 28

N

NETePay
 Installation, 28
 Testing, 39, 40
Network Requirements, 26

O

Overview, 5

R

Requirements
 Network, 26
 Server, 25

S

Server Requirements, 25

U

Upgrading Microsoft Internet Explorer, 28

W

What's Included on your CD, 5