

---

***NETePay POSPAD***  
***Installation & Configuration Guide***

---

***Moneris***  
***Canadian EMV Host***

***V5.07***

***Part Number: 8729.83***

# ***NETePay Installation & Configuration Guide***

Copyright © 2006 - 2017 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™, NETePay POSPAD™, GIFTePay™, DIALePay™, DSIClient™, DSIClientX®, dsiPDCX®, dsiEMVX®, dsiEMVUS®, DSIEMVClientX™, ePay Administrator™, IPTran™, IPTran LT™, IPTran LT Mobile™, TwinTran™, TwinTran Server™, TranCloud™, DialTran™, DataTran™ are trademarks and/or registered trademarks of Datacap Systems Inc.

Microsoft, Windows NT 4.0, Windows 2000 Professional, Windows XP, Windows 98, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Vista, Windows 7, Windows 8, and Windows 10 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: 08 Nov 2017

## **Version Support**

This document supports the following application versions:

NETePay POSPAD – (Moneris Canadian EMV Host) - Rental - Version 5.07.XX

NETePayService – V 1.0.0.1

DSIEMVClientX, Version 1.30

## **Payment Processor Support**

This document supports the following payment processor:

***Moneris Canadian EMV Host (with POSPAD)***

---

# CONTENTS

<b>OVERVIEW .....</b>	<b>5</b>
INTRODUCTION .....	5
<i>About NETePay</i> .....	5
<i>About Datacap</i> .....	5
HOW IT WORKS .....	5
<b>SECURITY IMPLEMENTATION GUIDANACE .....</b>	<b>6</b>
ABOUT SECURITY .....	6
NOTICE .....	6
PCI DATA SECURITY STANDARD.....	7
THE 12 REQUIREMENTS OF THE PCI DSS:.....	7
<b>INSTALLATION .....</b>	<b>8</b>
INTRODUCTION .....	8
REQUIREMENTS .....	8
<i>Baseline System Configuration</i> .....	8
<i>Network Requirements</i> .....	9
INSTALLATION PROCEDURES .....	9
<i>Downloading the NETePay Software</i> .....	9
<i>What's Included in the NETePay Installer Package</i> .....	9
<i>Installing/Upgrading Microsoft Internet Explorer</i> .....	10
<i>Installing NETePay POSPAD (Required)</i> .....	10
<i>Installing the client control (DSIEMVClientX)</i> .....	10
<b>NETEPAY CONFIGURATION.....</b>	<b>11</b>
INTRODUCTION .....	11
ACTIVATION AND PARAMETER DOWNLOAD .....	11
VERIFYING YOUR SERIAL NUMBER AND ACTIVATION .....	20
TESTING .....	20
<i>Important! - Before You Start</i> .....	20
OPERATIONAL CONSIDERATIONS.....	20
<i>Important!</i> .....	20
<b>STARTING NETEPAY AS A SERVICE .....</b>	<b>22</b>
INTRODUCTION .....	22
NETEPAY SERVICE WINDOWS DESCRIPTION .....	22
ACTIVATING AUTOMATIC NETEPAY SERVICE START .....	22
NETEPAY APPLICATION AND SERVICE LOGGING.....	25
<b>NETEPAY AUTOMATIC UPDATES.....</b>	<b>26</b>
INTRODUCTION .....	26
AUTOMATIC UPDATES .....	26
PROMPTED UPDATES .....	26
NEVER UPDATE .....	28



# **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* POSPAD 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 Datacap's client ActiveX control, DSIEMVClientX.

*NETePay* POSPAD is designed to operate exclusively with a PIN device that is running the Moneris POSPAD application. A merchant must obtain the required PIN devices and POSPAD from Moneris who will guide the installation and testing processes.

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

---

# SECURITY IMPLEMENTATION GUIDANCE

## ***About Security***

Datacap Systems advises its customers to deploy Datacap Systems applications in a manner that adheres to the most current PCI Data Security Standard. 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.

## ***Notice***

**NETePay POASPAD exclusively utilizes an attached PIN pad device running the Moneris POSPAD application. The POSPAD application was developed by Moneris and all cardholder information and SAD (Sensitive Authentication Data) are managed by the POSPAD application. Since NETePay never handles, transmits or processes cardholder information, it is 'out of scope' from a PCI perspective.**

**Since payment applications that are 'out-of-scope' are not eligible for PA-DSS certification, NETePay POSPAD V5.07 has not been assessed to PA-DSS 3.2 standards as published by the PCI-SSC (Payment Card Industry- Security Standards Council).**

**The merchant must follow all guidance from Moneris during deployment and utilization of NETePay POSPAD and the Moneris POSPAD application to assure a secure payment environment.**

## **PCI Data Security Standard**

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 merchants, and service providers that store, process, or transmit cardholder data.

The PCI DSS requirements are applicable 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*

---

# **INSTALLATION**

## **Introduction**

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

- *NETePay POSPAD*
- *DSIEMVClientX*
- 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 *DSIEMVClientX* 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.
- 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.

## 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 POSPAD**. From the **HOST** based section of downloads, select the ActiveX client for your installation (**DSIEMVClientX**). 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 POSPAD 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 POSPAD 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** – 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.
- **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 POSPAD (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 the client control (DSIEMVClientX)***

To install *DSIEMVClientX*:

1. Separately download the *DSIEMVClientX* installer and double-click the **exe** to start installation.
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.  
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.

---

# 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.

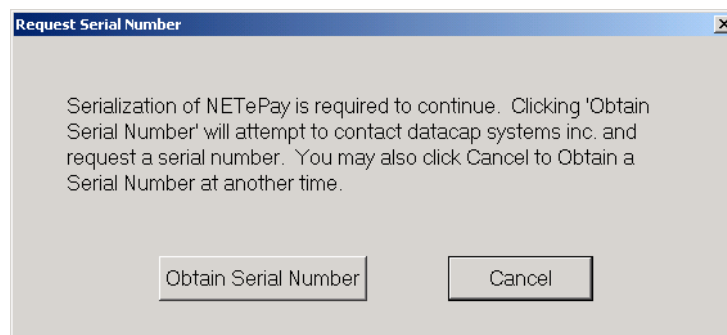
### Note

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.

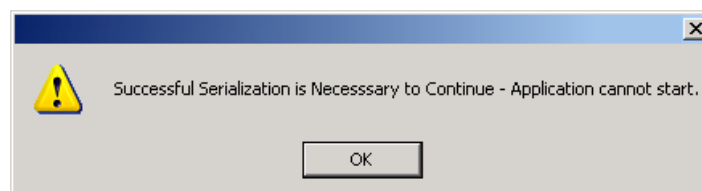
## Activation and Parameter Download

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:



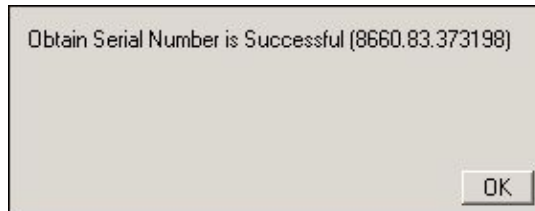
Click 'Obtain Serial Number' to enable NETePay to contact PSCS for a serial number.

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

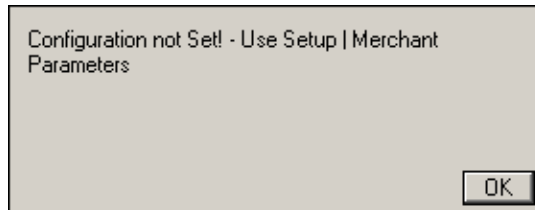


Click 'OK' and NETePay will close. Failure to successfully obtain a serial number means that NETePay was not able to contact Datacap's PSCS server over the Internet to obtain a serial number. Assure that the Internet connection is operating properly by using the default web browser on the machine where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

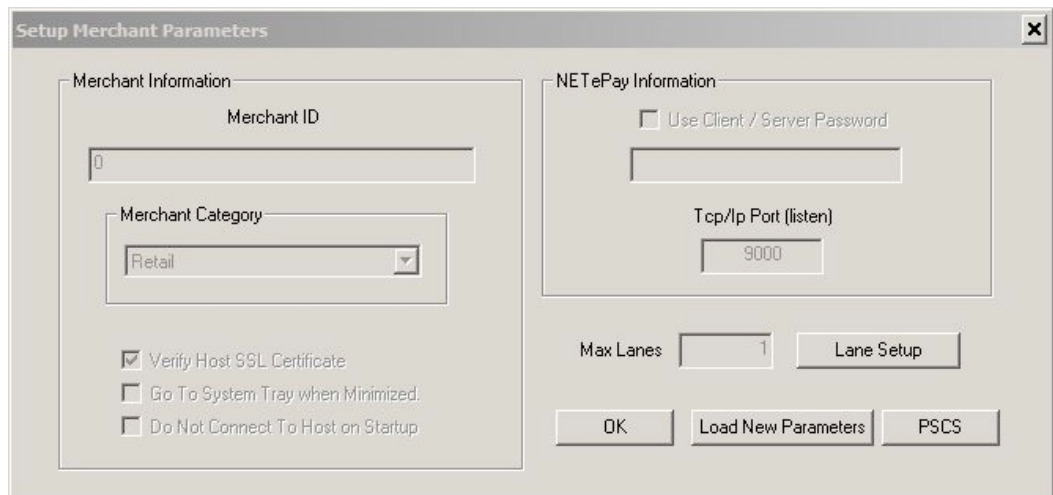


The dialog contains the 10 digit serial number that was automatically assigned to NETePay. Click 'OK' to continue and then you will see the following dialog:

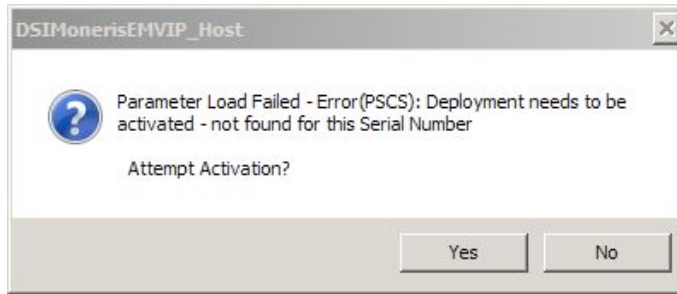


This dialog indicates that NETePay has not yet retrieved merchant parameters from Datacap's PSCS server and cannot operate until parameters are downloaded.

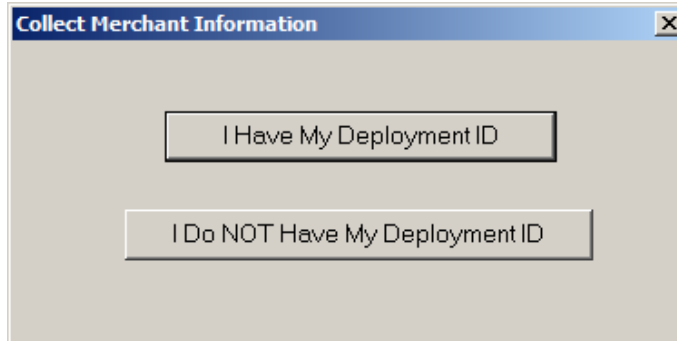
If a parameter file has been created on Datacap's PSCS server for the merchant account, then select 'Merchant Parameters' from the 'Setup' drop down menu. You will then see the following screen:



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:

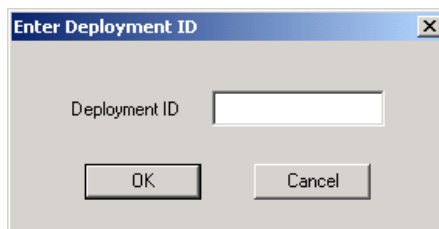


Click 'Yes' to attempt activation and you will see the following screen:



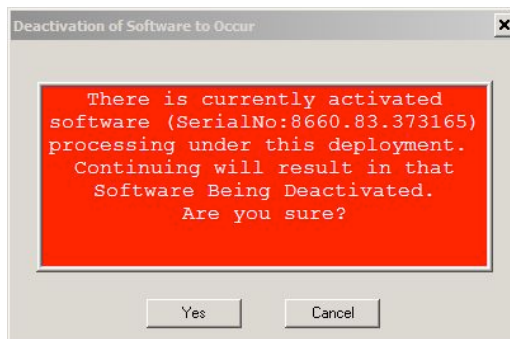
To continue, you must verify that you or someone else has created a Merchant Deployment on Datacap's PSCS server. If a deployment was created you may have been given a Deployment ID, which is typically an eight character code that has been assigned to the merchant's parameters. If you have a Deployment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



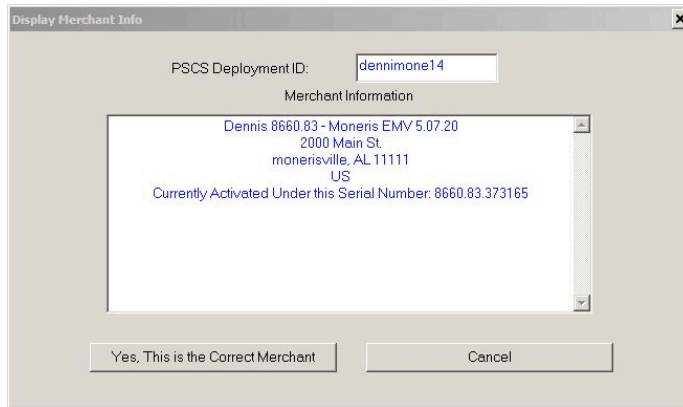
Enter the Deployment ID for the merchant parameter file and click 'OK'.

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



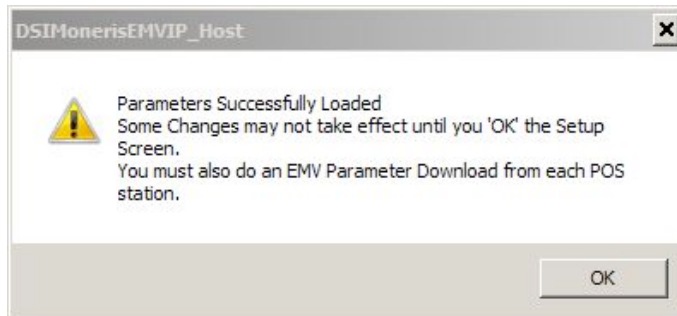
If you see this Deactivation Warning dialog, proceed to step 5.

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

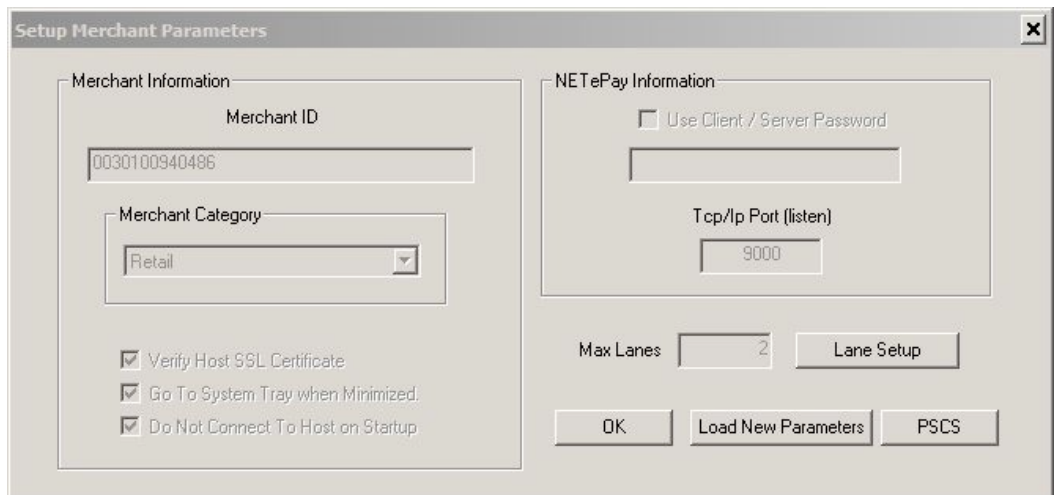


If the displayed information is not correct for the merchant site, click ‘Cancel’ and retry entry from the beginning of step 4. If the displayed information correctly identifies the merchant site, click ‘Yes, This is the Correct Merchant’.

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

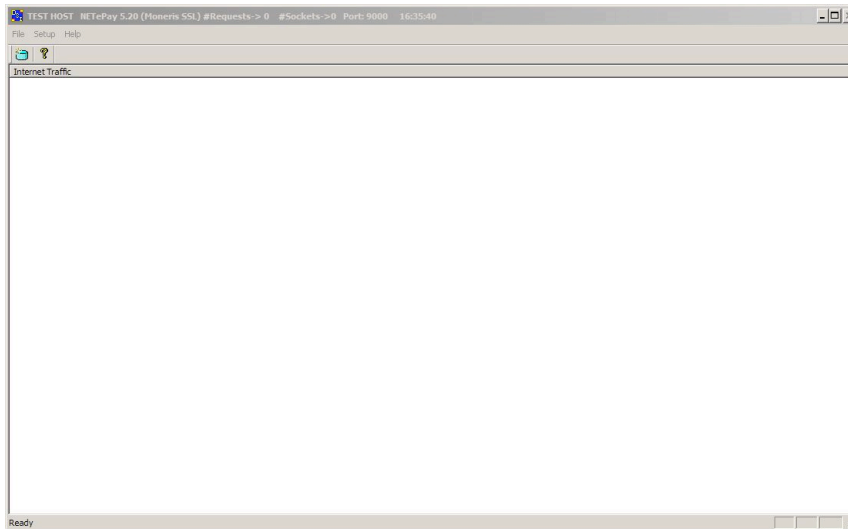


Click ‘OK’ and will then again see the setup screen as follows:



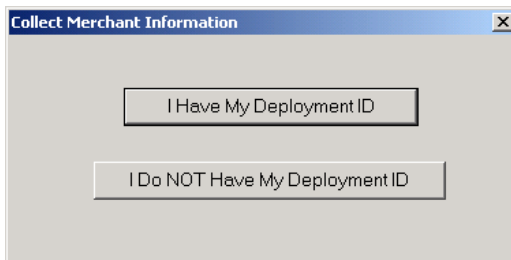
Lane Setup allows you to optionally change the description associated with each lane that was authorized in the PSCS parameter file. You cannot alter the number of lanes in NETePay; changes to the number of lanes must be done by editing the deployment file in PSCS.

The 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.

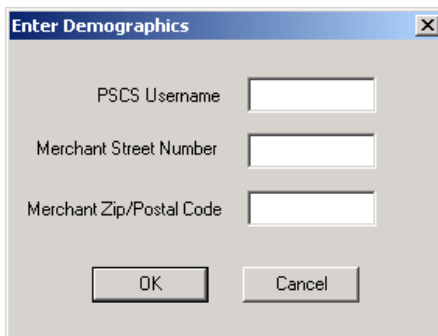


**NETePay setup is complete.**

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:

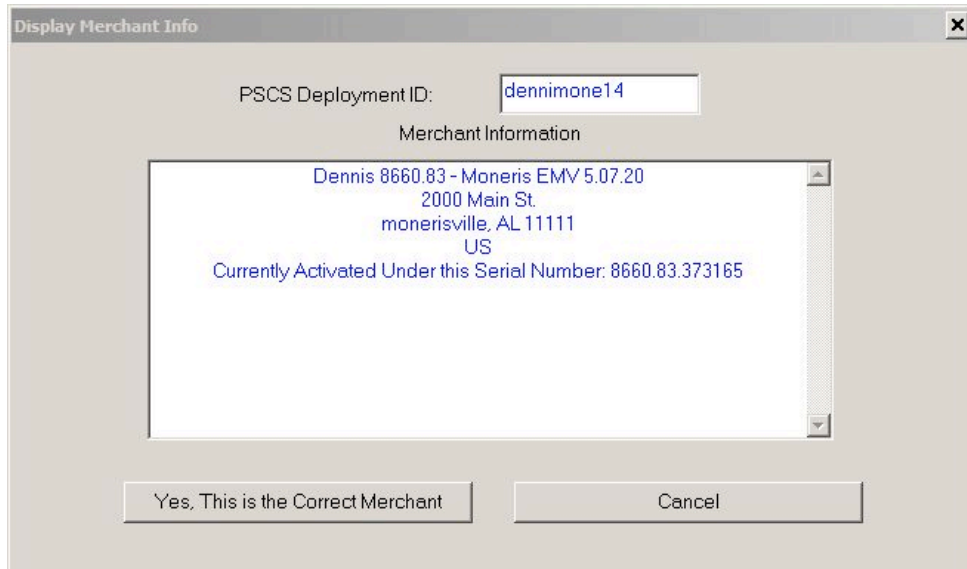


You need the following information to complete the demographics dialog entries:

- 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

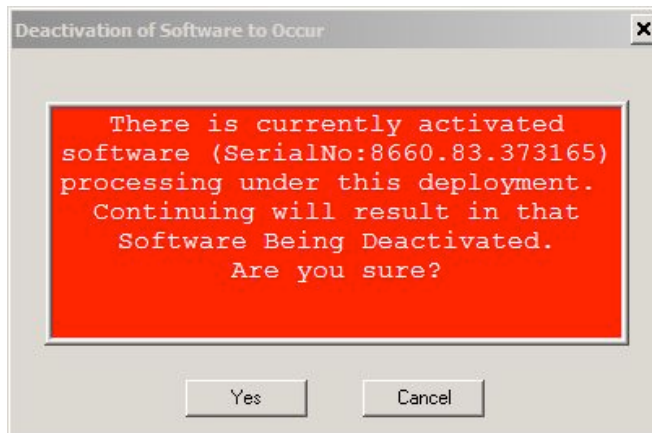
After entering this information, click 'OK'.

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



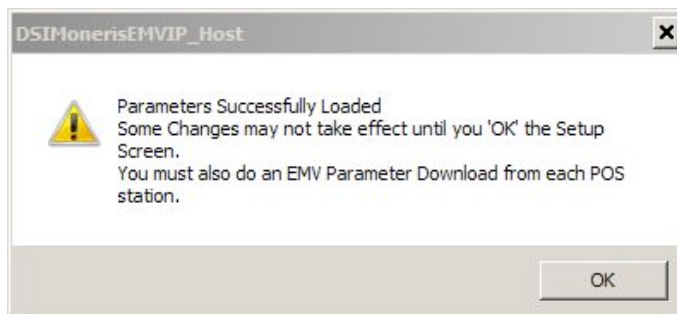
If the displayed information is not correct for the merchant site, click ‘Cancel’ and retry entry from the beginning of step 4. If the displayed information correctly identifies the merchant site, click ‘Yes, This is the Correct Merchant’.

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



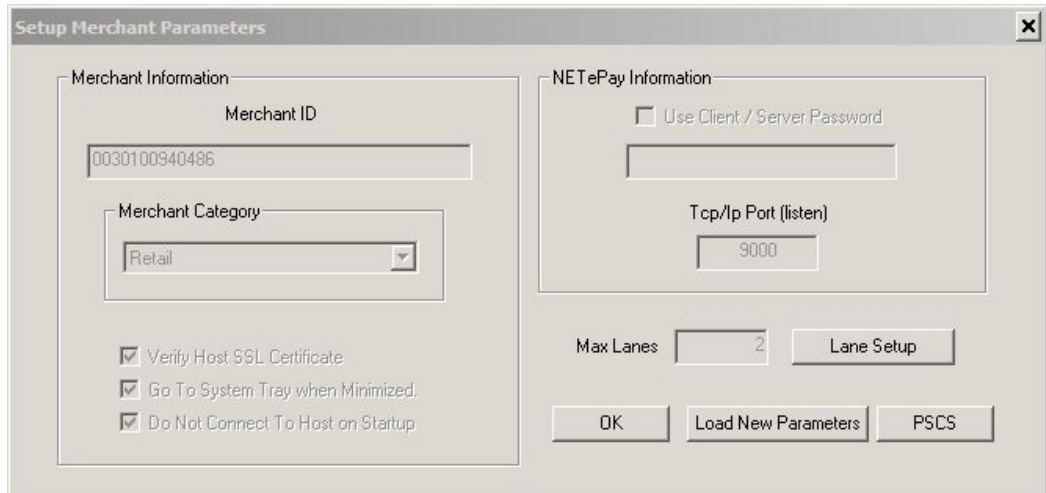
If you see this Deactivation Warning dialog, proceed to step 5.

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



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

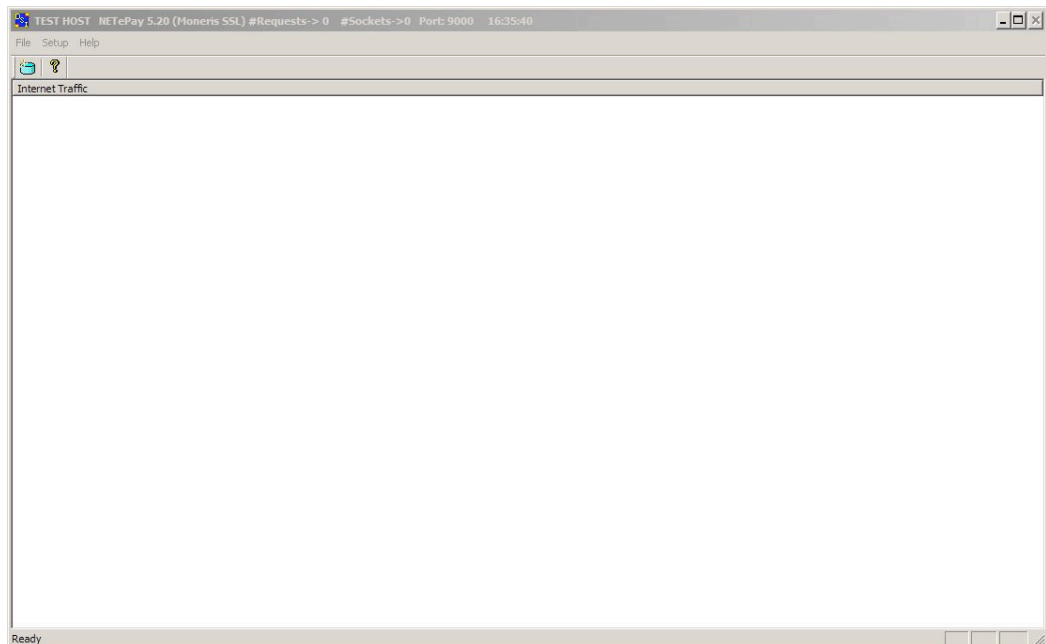




The setup screen now contains non-zero values in the text boxes throughout the screen indicating the values retrieved from Datacap's PSCS server. You should verify that the parameters are correct and then click 'OK' to complete the setup process.

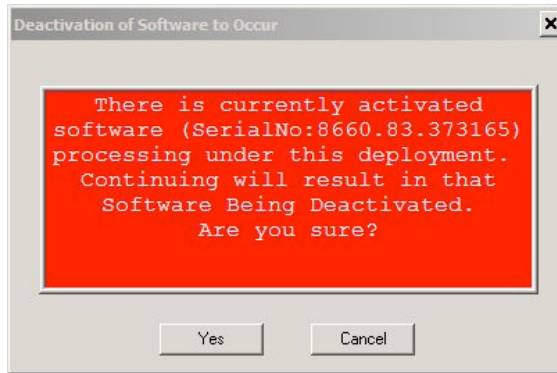
Lane Setup allows you to optionally change the description associated with each lane that was authorized in the PSCS parameter file. You cannot alter the number of lanes in NETePay; changes to the number of lanes must be done by editing the deployment file in PSCS.

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.

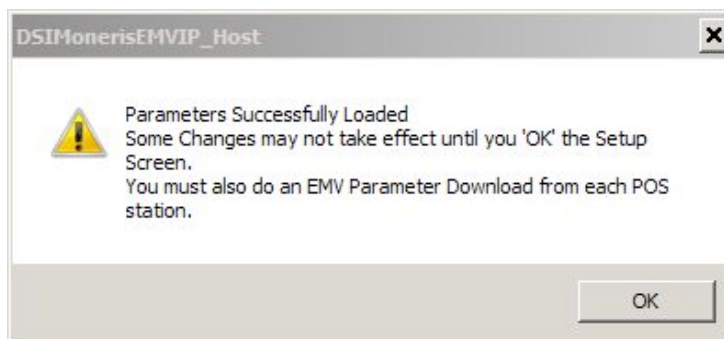
**WARNING:**

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

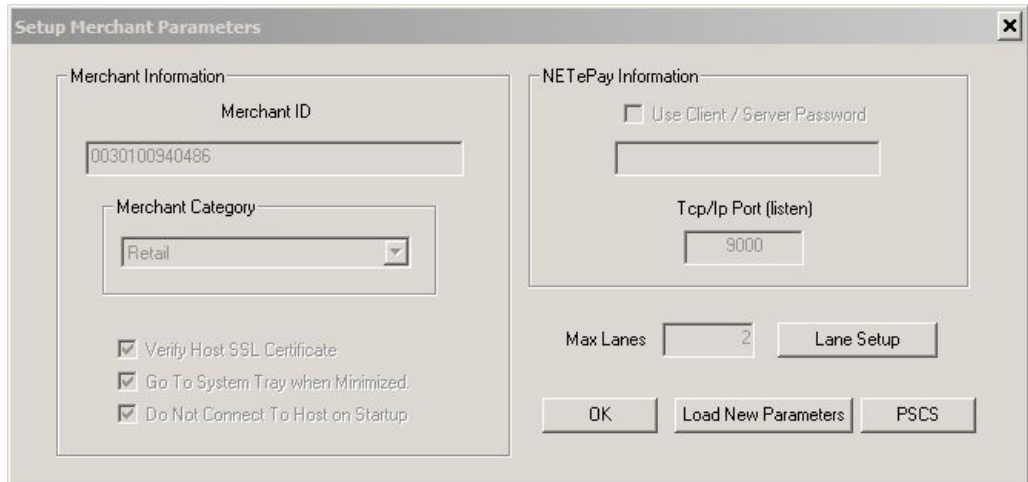
If you are certain that you want to deactivate the NETePay serial number listed in the Deactivation Warning dialog and use it with the new NETePay, then click 'OK'. You will see the following dialog which verifies your choice:



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:



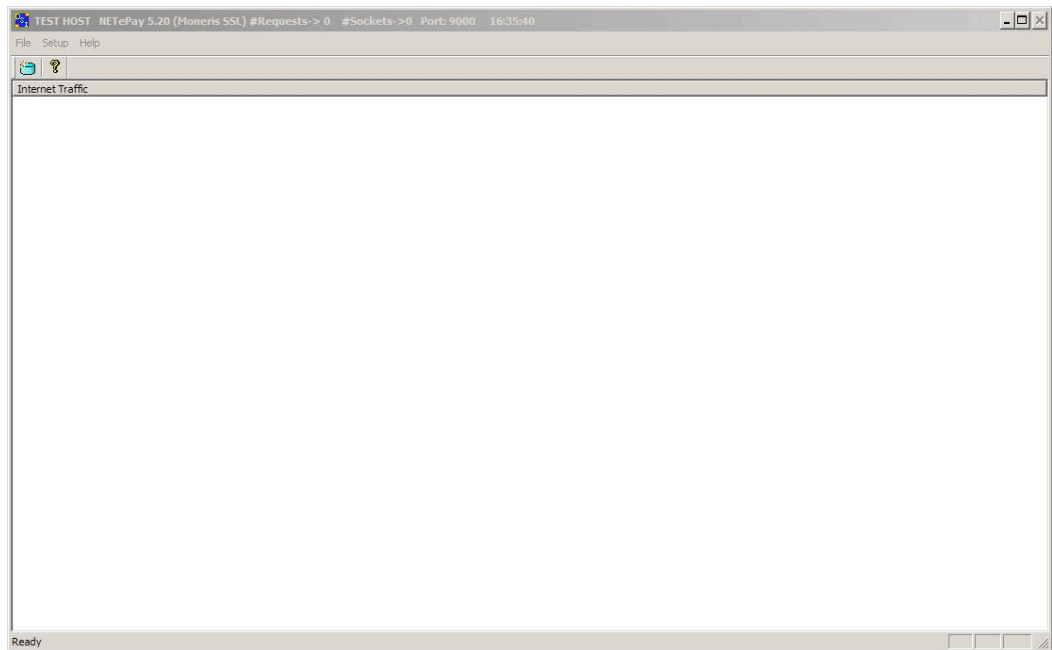
Click 'OK' and will then again see the setup screen as follows:



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.

# **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.”

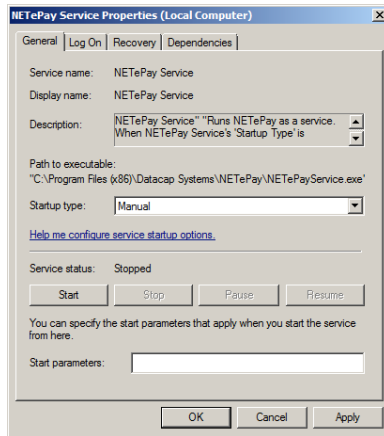
## **Activating Automatic NETePay Service Start**

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.

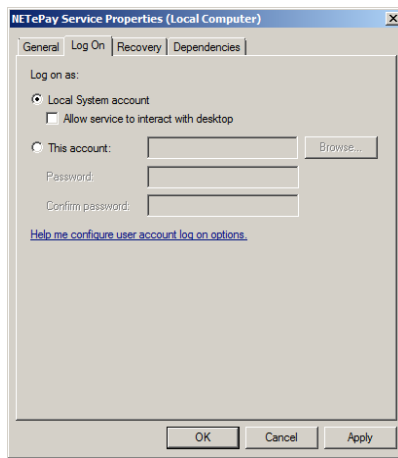
Double-click to expand the 'Services and Applications' option from the left pane, and then select 'Services' from the options tree.

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.

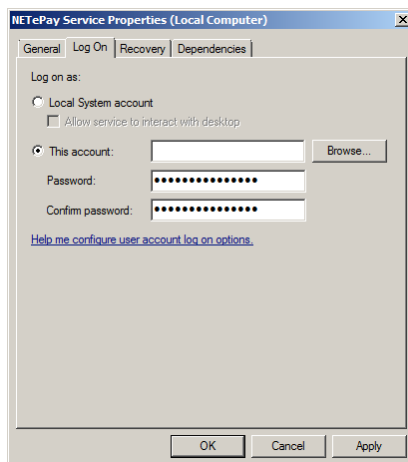


In the 'Start Type' drop down, select 'Automatic'. An Automatic startup launches the NETePayService service, which starts NETePay along with starting Windows; a Manual startup allows you to launch it only when necessary; the Disabled option deactivates the service entirely, requiring you to enable it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



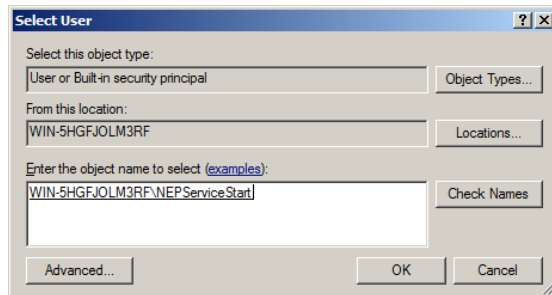
**Important Note:**

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

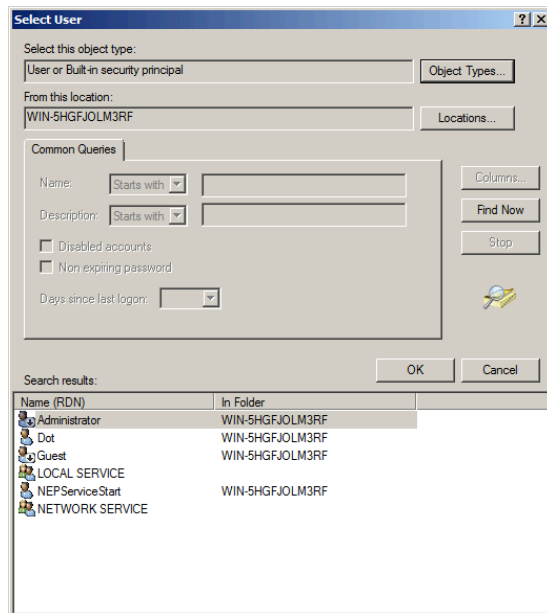
***This User account will be reported in the NETePayService log files. For PA-DSS compliance, you should not use the SystemService default principal – it is anonymous and has the privileges of an Administrative account.***

***Follow the instructions in the PA-DSS 3.2 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:

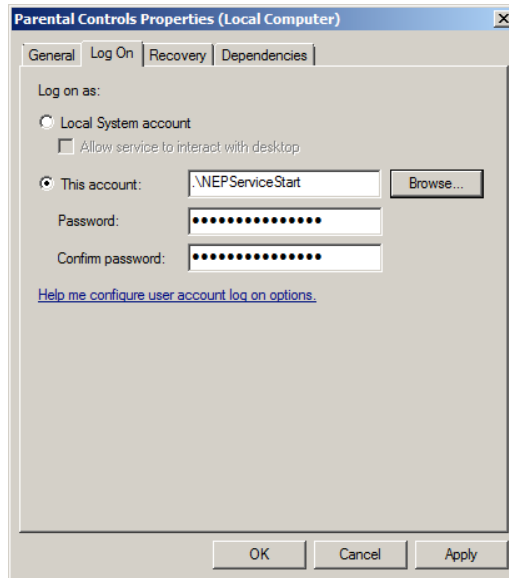


Next, Click the 'Advanced' button, and the dialog will expand; then click the 'Find Now' button to see as list of Users and Service Accounts as follows:



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.

# **NETePay AUTOMATIC UPDATES**

## **Introduction**

*NETePay 5* may be optionally configured to automatically retrieve and install a new version of the software which includes updates including patches and fixes as they become available from Datacap.

When *NETePay 5* is activated, configuration settings controlling automatic updates are defined in Datacap's PSCS (Payment System Configuration Server) system. The PSCS configuration settings control subsequent behavior of *NETePay 5* when it is launched.

There are three options which can be configured in PSCS prior to *NETePay 5* activation for controlling automatic updating:

1. Perform an ***Automatic*** update unconditionally when an updated version of *NETePay 5* is available when the program is launched.
2. ***Prompt*** the user for input to accept or bypass updated when an updated version of *NETePay 5* is available when the program is launched.
3. ***Never*** install an available updated version of *NETePay 5* when the program is launched.

## **Automatic Updates**

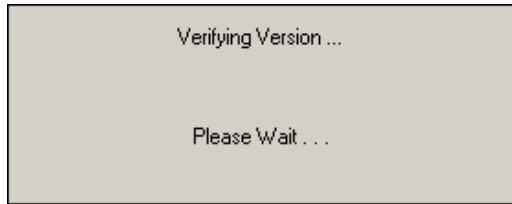
***Automatic*** updates require no intervention from an operator, regardless of how *NETePay 5* execution is started, either as an application or as a service.

## **Prompted Updates**

***Prompted*** updates behave differently depending on how *NETePay 5* is launched and whether updates are enabled in PSCS.

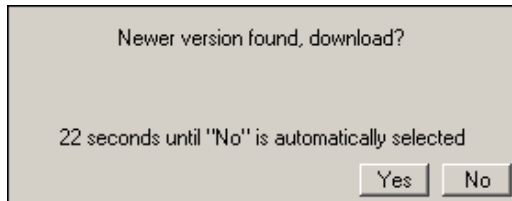
### ***When NETePay started as an application by a user:***

If the *NETePay 5* application is launched by a user from a menu or icon, the operator will first see the following dialog:



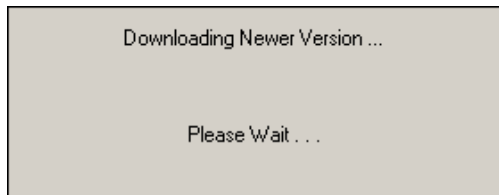
This dialog indicates that NETePay is checking to see if an updated version of NETePay 5 is available from PSCS. If there's no update, then NETePay starts executing its normal transaction processing operations.

If NETePay 5 determines that there is an update available from PSCS, the operator will see the following dialog:



If the operator selects **No** or lets the timeout expire, then NETePay starts its executing normal transaction processing operations.

If the operator selects **Yes** before the timeout, the update process will begin and while the update is in progress, the following is displayed:



If the update process completes successfully, then NETePay starts executing its normal transaction processing operations.

If there's an error during the update process, the following dialog will be displayed:



This dialog will remain until the timeout expires or the operator clicks OK (whichever occurs first) and then NETePay starts executing its normal transaction processing operations.

An operator who is presented with the update failure should quit NETePay 5 and relaunch to attempt another update. If that fails, the merchant should contact their dealer or Datacap Systems for assistance.

### **NETePay started as a service:**

If the NETePay 5 is started as a service, prompting for the operator is bypassed. Depending on whether PSCS is configured to enable updates in this case, NETePay 5 will verify whether an update is available and download it without dialogs. NETePay then starts executing it's normal transaction processing operations.

### ***Never Update***

Automated updating is the preferred method to keep NETePay up-to-date. Some installations may not be able to accommodate automated updates for a variety of reasons. Datacap makes NETePay 5 updates available via its software download website for these users.

Downloaded NETePay 5 updates are supplied as complete self-installation executables.. All NETePay 5 updates, whether delivered by automated processing or manual download, are code signed with a VeriSign certificate to assure integrity and authenticity.

#### **Note:**

Datacap strongly recommends that *automatic* updates be enabled on PSCS (Payment System Configuration Server) when the software is initially installed and configured.