



---

# *NETePay XML*

## *Installation & Configuration Guide*

---

*Version 4.10*

***For Alliance Data Host***  
***Supporting U.S. Debit and Dial Backup***

***Part Number: 8660.47 (ML)***  
***8660.48 (SL)***

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

Copyright © 2008 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.

Datacap, Datacap Systems, NETePay, DSIClient, DSIClientX, ePay Administrator, WinPop, IPTran, DialTran, TwinTran, Tran Management Software and DataTran are trademarks of the Datacap Systems Inc.

Microsoft, Windows NT 4.0, Windows 2000 Professional, Windows XP and Windows 98 are either trademarks or registered trademarks of the Microsoft Corporation.

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

Printed in the United States of America

Revised: 29 February 2007

## ***Version Support***

This document supports the following application versions:

NETePay ML/XML or NETePay SL/XML, Version 4.10

DSIClientX, Version 3.80

DSIClient Transaction Utility, Version 2.50

## ***Payment Processor Support***

This document supports the following payment processor:

***Alliance Data Host (US Debit with Dial Backup)***

---

# CONTENTS

<b>Overview.....</b>	<b>5</b>
Introduction .....	5
About NETePay with Dial Backup.....	5
About Datacap .....	5
What's Included on your CD .....	5
How it works.....	6
<b>Security Considerations.....</b>	<b>7</b>
Introduction .....	7
NETePay Compliance.....	8
POS System Considerations.....	8
Networking Considerations .....	8
What's at Stake for Merchants .....	8
Security Action Plan .....	9
More Information.....	9
<b>Installation.....</b>	<b>10</b>
Introduction .....	10
Requirements.....	10
Baseline System Configuration .....	10
Network Requirements .....	11
Installation Procedures .....	11
Accessing the NETePay CD-ROM .....	11
Installing/Upgrading Microsoft Internet Explorer .....	13
Installing NETePay .....	14
Installing DSIClientX .....	14
Installing Datacap DialLink modem (Required for Dial Operations) .....	14
<b>NETePay Configuration &amp; Testing.....</b>	<b>16</b>
Introduction .....	16
Activation .....	16
Configuration.....	17
Testing .....	20
Important! - Before You Start .....	20
<b>Using the DSIClient Transaction Utility .....</b>	<b>22</b>
Introduction .....	22
Supported Transaction Types.....	22
DSIClient Transaction Utility Setup .....	23
Verifone PINpad 2000 Setup .....	24
PDC Setup.....	25
Processing Transactions.....	27
<b>Index .....</b>	<b>30</b>



# **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* also incorporates automatic dialup backup direct to the processing host in the event of an Internet outage. The dial backup operation is completely automatic and switches back to Internet operation without operator intervention.

*NETePay* 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.

*NETePay* is available in two versions: SL and ML. The SL (Single Lane) version is designed for single station, non-LAN POS systems; the ML (Multi Lane) version is designed for multiple POS stations on a LAN. This User Guide is applicable to both versions.

### **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.

## **What's Included on your CD**

The *NETePay* CD-ROM includes client and server applications for Windows NT/2000/XP 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 XML ActiveX control that integrates into a Point of Sale or Restaurant 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 payment transactions
- ***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 or PSTN dialup direct 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.

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

# **SECURITY CONSIDERATIONS**

## **Introduction**

Systems which process payment transactions necessarily handle sensitive cardholder account information. The card associations (VISA, MasterCard) have developed security standards for handling cardholder information in a published document named *Payment Card Industry (PCI) Data Security Standard*.

The security requirements defined in the standard apply to all members, merchants, and service providers that store, process or transmit cardholder data.

The PCI Data Security Requirements apply to all **system components** which is defined as any **network component, server, or application** included in, or connected to, the cardholder data environment. Network components, include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, Web, database, authentication, Domain Name Service (DNS), mail, proxy, and Network Time Protocol (NTP). Applications include all purchased and custom applications, including internal and external (Web) applications.

The following **12 Requirements** comprise the Payment Card Industry Data Security Standard.

### **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

## ***NETePay Compliance***

All versions of **NETePay** at or above Version 4.00 implement all of the PCI Data Security Standard requirements which are applicable to a payment processing application.

- **NETePay** does not store any magnetic stripe (Track 1 or 2), card verification (CVV, CVV2, etc.) or PIN data, ever.
- **NETePay** truncates all account and expiration date information for transactions which have been settled in every area where it is either stored or displayed.
- **NETePay** encrypts account numbers and expiration dates for transactions which have not yet been settled.
- **NETePay** logs only record truncated account number and expiration date information and never record any magnetic stripe (Track 1 or 2), card verification (CVV, CVV2, etc) or PIN data, ever.
- **NETePay** utilities which present data in a user interface (display or print) always truncate account number and expiration date data and never display magnetic stripe (Track 1 or 2), card verification (CVV, CVV2, etc) or PIN data, ever.
- **NETePay** encrypts all transmissions which contain cardholder data.

## ***POS System Considerations***

Although **NETePay** implements all of the PCI Data Security Standard requirements which are applicable to a payment processing application, your POS application may not handle cardholder information in such a secure fashion.

PCI Data Security requirements must be implemented in all the components of a system which handle cardholder data in order to provide comprehensive security. The PCI Data Security requirements *must* be implemented in your POS system and any other applications which handle cardholder data. You should verify with your POS system provider that the version of the POS software you are using is compliant.

## ***Networking Considerations***

**NETePay** is designed to operate on a local area network (LAN). Your store LAN can be vulnerable to attempts to steal data, particularly if it is connected to an outside network (Internet, WAN, VPL, etc.) in either a wired or wireless manner. The PCI Data Security requirements which apply to networks must be implemented to provide comprehensive data security.

## ***What's at Stake for Merchants***

Most merchants do not design and create their own store POS systems. However, the PCI Data Security Standard specifically includes the merchant in the chain of responsibility for secure data handling. This responsibility includes the possibility of significant fines and compensation payments for any security breaches tracked to a merchant. The possible fines are considerable (up to \$500,000) and the compensation for losses is essentially unbounded. Compared to the possible liabilities, the implementation of compliant security systems and practices is a bargain.

## Security Action Plan

A comprehensive approach to assessing the security compliance of your entire system is necessary to protect you and your data. The following is a basic plan every merchant should adopt.

1. Read the PCI Standard in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
2. Create an action plan for on-going compliance and assessment. Once the gaps are identified, companies must determine the steps needed to close the gaps and protect cardholder data. It could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
3. Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities must complete annual self-assessments using the PCI Self Assessment Questionnaire.
4. Call in outside experts as needed. Visa has published a Qualified Security Assessor List of companies that can conduct on-site CISP compliance audits for Level 1 Merchants, and Level 1 and 2 Service Providers. MasterCard has a Compliant Security Vendor List of SDP-approved scanning vendors.

## More Information

You may download a copy of the *Payment Card Industry (PCI) Data Security Standard* from VISA's security website at the following Internet address:

[http://usa.visa.com/business/accepting\\_visa/ops\\_risk\\_management/cisp.html](http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html)

Additional information for merchants from VISA is available at the following Internet address:

[http://usa.visa.com/business/accepting\\_visa/ops\\_risk\\_management/cisp\\_merchants.html?it=ill/business/accepting\\_visa/ops\\_risk\\_management/cisp.html|Merchants](http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_merchants.html?it=ill/business/accepting_visa/ops_risk_management/cisp.html|Merchants)

Listing of qualified security assessors from VISA is available at the following Internet address:

[http://usa.visa.com/business/accepting\\_visa/ops\\_risk\\_management/cisp\\_accessors.html?it=|2|/business/accepting\\_visa/ops\\_risk\\_management/cisp\\_merchants%2Ehtml|Assessors](http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_accessors.html?it=|2|/business/accepting_visa/ops_risk_management/cisp_merchants%2Ehtml|Assessors)

# **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 that *DSIClientX* 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 2000 Professional with Service Pack 4 or, Windows XP Pro with Service Pack 2. All latest updates and hotfixes should be applied. It is strongly recommended that Windows Automatic Updates be enabled.
- 1GB of RAM minimum, 2GB or higher recommended
- 10 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.
- Available COM port (if using dial backup or dial primary communications)
- Datacap DialLink modem (if using dial backup or dial primary communications)
- 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.

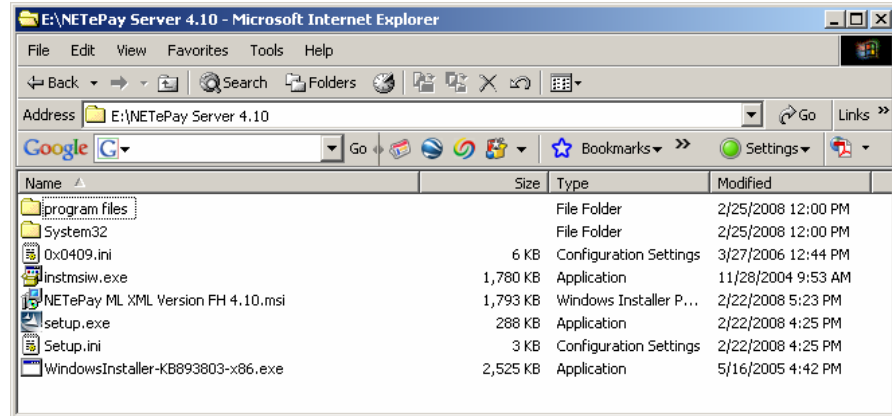
Use either of the following procedure to access the folders that contain the setup programs for *NETePay* and its components:

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:

datacap systems, inc.		Reliable Integrated E-Payment Solutions
	<a href="#">Open Installation &amp; Configuration Guide</a>	This document (ReadMe.pdf) describes the installation and setup of NETePay for Fifth Third Processing. Requires Acrobat Reader
	<a href="#">Open Security Recommendations Guide</a>	This document (Security-ReadMe.pdf) describes the PCI/CISP security recommendations for systems using NETePay. Requires Acrobat Reader
STEP 1.	<a href="#">Install NETePay</a>	The NETePay Server communicates with Alliance Data's processing host via a public IP Gateway in order to process Credit and Debit Card transactions.
OPTIONAL	<a href="#">Install DSIClient</a>	DSIClient is a stand-alone application used to send test transactions to NETePay.
OPTIONAL	<a href="#">Install Internet Explorer 6.0</a>	NETePay requires 128-bit data encryption. If your browser does not currently support this level of encryption, your browser must be upgraded to high-encryption or IE 6.0 must be installed.

Copyright © 2008 Datacap Systems, Inc - All rights reserved.  
Revised: February 21, 2008.

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.



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

## ***Installing/Upgrading Microsoft Internet Explorer***

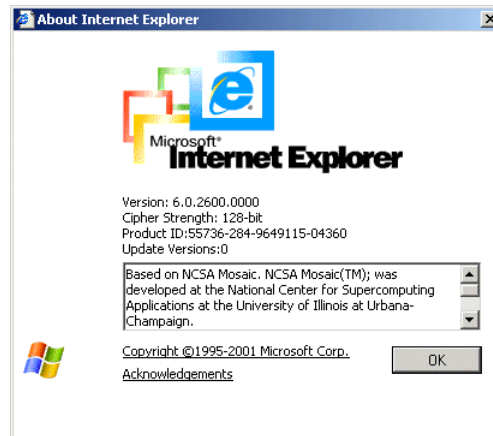
If needed, you can install or upgrade your server and each computer on the LAN with a version of Microsoft Internet Explorer that supports 128-bit encryption.

If needed, you can use the Windows Update on each PC to upgrade an existing version, or install a copy of Microsoft Internet Explorer 6.0 (or later) included on the *NETePay* CD-ROM.

### ***Determining the Encryption Strength***

To determine if a PC has the necessary encryption to run *NETePay*:

1. Launch **Internet Explorer**.
2. From the Internet Explorer menu bar, select **Help** and choose **About Internet Explorer**. The following window (or something similar), should appear:



3. The Cipher Strength should indicate 128-bit. If not, you must update your version of Internet Explorer.
4. Click **OK** to close the window.

### ***Installing Microsoft Internet Explorer***

To install Microsoft Internet Explorer 6.0:

1. Open the Microsoft Internet Explorer folder on the *NETePay* CD-ROM and double-click the **Microsoft Internet Explorer 60 High Encryption** folder.
2. Double-click the **i386** folder.
3. Double-click **setup.exe**.
4. Click **Install Internet Explorer 6 and Internet Tools**.
5. Follow the on-screen instructions.

## ***Installing NETePay***

To install the NETePay Server software:

1. Open the NETePay Server 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. 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.

## ***Installing DSIClientX***

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

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

**NOTE:** You may install *DSIClientX* (and the *DSIClient Transaction Utility*) on another computer(s) that are on a local area network with the computer running the *NETePay* server.

## ***Installing Datacap DialLink modem (Required for Dial Operations)***

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

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

1. Connect the uDIN8 connector of the interface cable to the *Datacap DialLink* modem to the PC/ECR port.
2. Connect the DB9 end of the interface cable to the intended COM port on the PC.

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

# **NETePay CONFIGURATION & TESTING**

## **Introduction**

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

*NETePay* is sent to you as a fully functional software application for 10 calendar days before requiring entry of an activation code by Datacap Systems.

If *NETePay* has not been activated by Datacap within those 10 days, it will decline all requests and return a “Must Activate NETePay” message to the POS terminal, indicating that the initial activation period has expired.

You will then have the option to extend the activation period for one additional 10-day period via the activation screen. If an activation code is not entered during the second activation period, *NETePay* will decline all requests and return a “Must Activate NETePay” message until an activation code is entered.

## **Activation**

During installation, *NETePay* generates a Session Code and Machine ID that are unique to that PC and required for permanent operation of *NETePay* on that machine.

Simply submit those numbers to Datacap by using one of the following methods to obtain an activation code:

- Contact the Sales Department at (215) 997-8989 and provide the two uniquely generated numbers. Datacap will register your software and provide you an individualized activation code.
- E-mail the numbers to Datacap and receive your activation code via return E-mail.

Send an email message to [activate@dcap.com](mailto:activate@dcap.com) with **NETePay Activation** in the Subject line. The body of the message should contain:

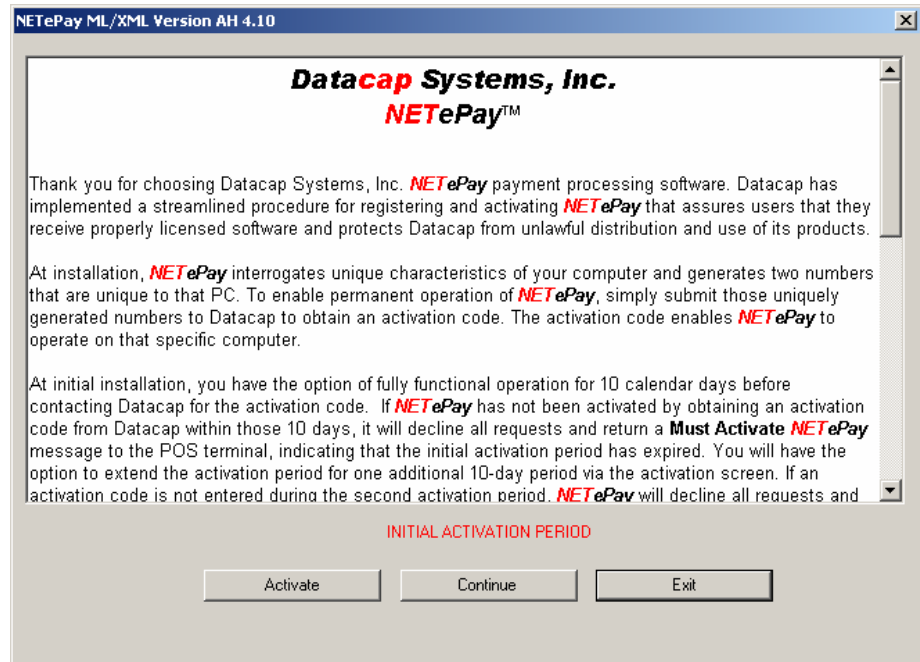
2. Your Name
3. Telephone Number
4. Serial Number
5. Session Code
6. Machine ID

The Serial Number, Session Code and Machine ID appear in the Activation dialog box and can be copied and pasted into the body of the E-mail message.

# Configuration

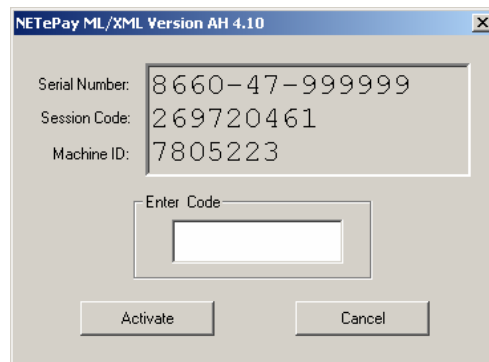
To activate and set up *NETePay* for use:

1. From the Desktop, double-click the **NETePay icon** The Initial Activation dialog box appears.

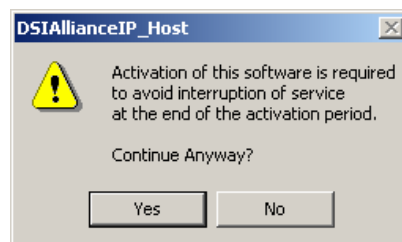


**NOTE:** The Initial Activation dialog box will appear each time you start *NETePay* until you activate it.

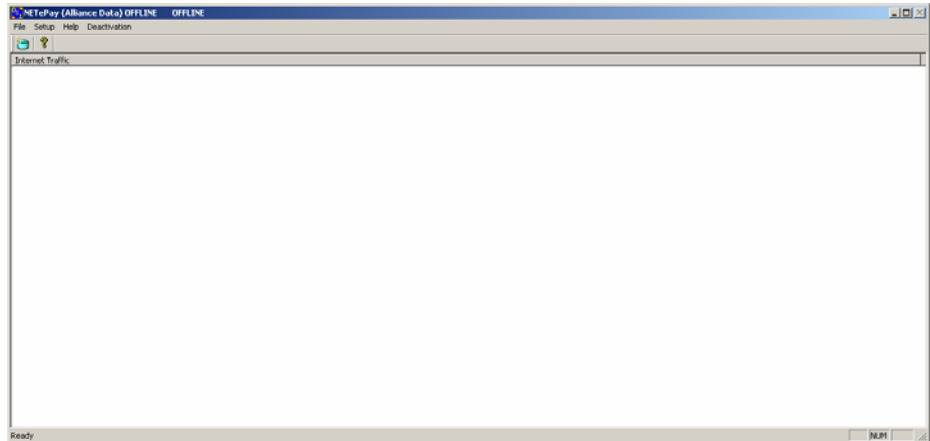
2. To enter the activation code, click **Activate**. When the activation dialog box appears, type the activation code in the box provided and click **Activate**



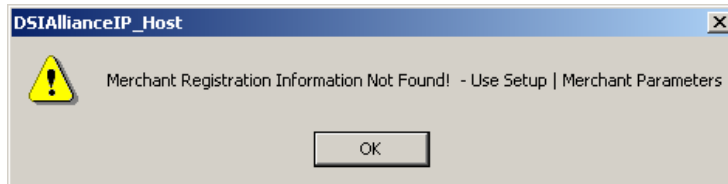
3. To proceed without activation, click **Continue**. When the message indicating that activation is required to avoid interruption of service appears, click **Yes** to continue.



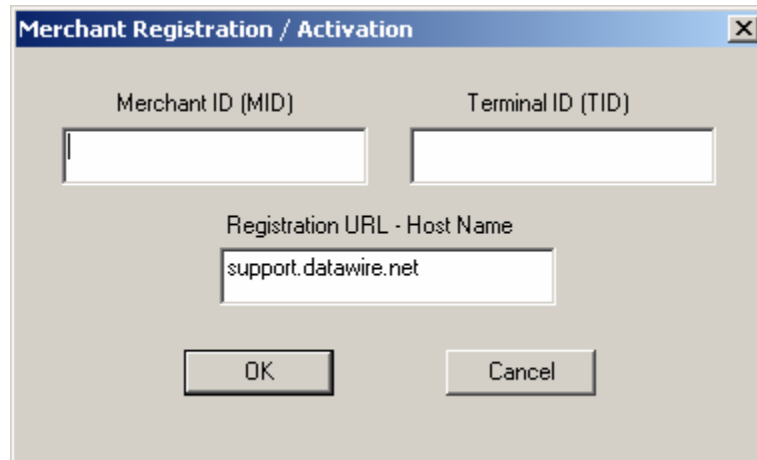
4. In either case, *NETePay* appears.



**NOTE:** During your initial access of *NETePay*, the following message will appear indicating that merchant registration information HAS NOT YETBEEN OBTAINED FROM Datawire. Click **OK** to continue.



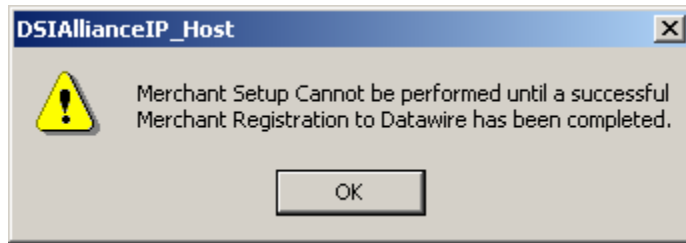
5. From the *NETePay* menu bar, select **Setup** and choose **Merchant Parameters**. The **Merchant Registration/Activation** dialog box appears.



6. In the **Merchant Registration/Activation** dialog, enter the Alliance Data Merchant information including **Merchant ID** (1-8 characters) and the **Terminal ID** (1-15 characters).

The Merchant Information required for this section is supplied by Alliance Data or your merchant services provider.

7. *NETePay* will use the entered Merchant ID and Terminal ID to download a merchant profile from Alliance Data's Internet gateway operator (Datawire) over the internet. If there is an error during the Datawire registration process, the following dialog will be displayed:



This indicates that NETePay attempted to finish automatic completion of the merchant programming but encountered an error. Check the Internet connection and verify the Merchant ID and Terminal ID entered in the setup screen. If this does not rectify the problem, contact your alliance Data or Datawire representative.

8. If the Datawire registration process is successful, then the following setup screen will be displayed:

11. In the Merchant Information section, the profile is automatically provided by the download from Datawire. The settings in this section are not changeable by the user but are displayed for verification purposes.
12. Under the **NETePay Information** section, you may select whether you want to use a password protection on communications between clients and the server. If you are using *NETePay* in a Wide Area Network (WAN) that uses an Internet connection, you should enable Client/Server password protection to prevent unauthorized use of *NETePay*. If you want to enable Client/Server Password operation, click the **Client/Server Password** box and enter the password to be used by the server in the box below the checkbox.

**NOTE:** You must also configure *DSIClientX* and *ePay Administrator* for Client/Server password protection using the same password to use this function.

The available Merchant Category setting is Retail.

13. Under the **Transport** section, you can select the method of communications to the Alliance Data processing host.
  - **IP Only** – Select this option if you want NETePay to use only the Internet to process transaction with the Alliance Data host.
  - **IP with Dial Backup** – Select this option if you want to use the Internet as the primary means of communication with Alliance Data and to have automatic direct dial backup operation occur when Internet service is interrupted. This option requires that you install a Datacap DialLink modem on an available COM port. *NETePay only operates with a Datacap DialLink modem for backup operations – third party modems are not supported.*
  - **Dial Only** – Select this option if you want to use the Datacap DialLink modem and phone line as the primary means of communication with Paymentech. This option requires that you install a Datacap DialLink modem on an available COM port. *NETePay only operates with a Datacap DialLink modem for dialup operations – third party modems are not supported.*
14. Under the **Dial Backup Information** section, you set parameters related to dial backup.
  - **Comm Port** – Select the COM port number where the Datacap DialLink modem is attached. Make sure not to use a port number used by another device. Allowable ports are 1-255.
  - **Dial Prefix** – If the phone system being used with the Datacap DialLink modem requires dialing a prefix to get an outside or long distance line, enter it here. A ‘W’ (wait for dial tone) or a ‘,’ (comma – wait 2 seconds before dialing next digit) are the most common along with 8 or 9. For example “8,” would wait two seconds after going off hook before dialing the number in the Alliance Authorization Phone Number text box.
  - **Alliance Authorization Phone Number** – This number will automatically be filled in for the recommended access number to Alliance Data. You may change this number if you are having problems reliably communicating with the host. Contact your merchant service provider or Alliance Data directly to obtain alternate access phone number(s).
15. Under the **IP Connection Information** section, you set the time in seconds to attempt an IP connection for each transaction before switching to dial for processing (if enabled). Allowable values are 3 to 40 seconds.
16. After completing the configuration settings, click **OK** to save the settings and exit the dialog box. If you want to quit without any changes being applied, click **Cancel**.

## 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.

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

**You should only process actual payments *after* verifying that all test transactions have been successfully deposited.**

Datacap Systems is not responsible for typographical errors, data entry errors or any other inaccuracies arising out of the creation and/or downloading of merchant data.

Furthermore, Datacap Systems shall not be liable for any errors or for incidental or consequential damages in connection with the use of the software or other programmed information, including customer supplied or Datacap supplied information.

# ***USING THE DSIClient TRANSACTION UTILITY***

## ***Introduction***

This chapter explains how to use the *DSIClient Transaction Utility* program as a stand-alone application to process retail payment transactions either at the server or a client machine.

**NOTE:** Before you process any transactions using the *DSIClient Transaction Utility*, you should have *NETePay* running.

## ***Supported Transaction Types***

DSIClient supports the following types of credit transactions via the keyboard, and/or an optional Verifone PINpad 2000:

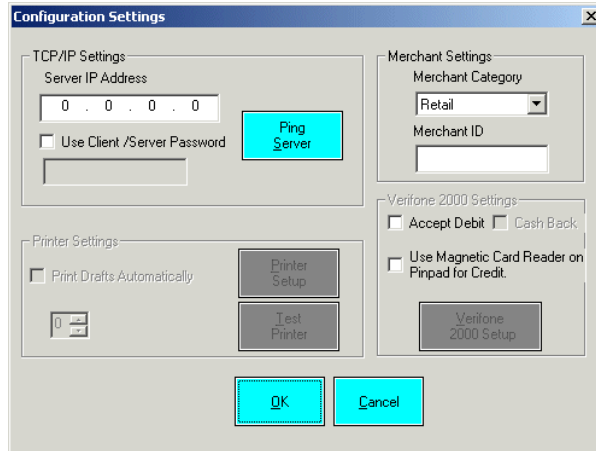
- **Credit Sale** – enables you to process a transaction for a payment for goods or services using a credit card (VISA, MasterCard, American Express, Discover, etc.).
- **Credit Refund** – enables you to issue a credit to the cardholder for the return or credit of goods or services using a credit card.
- **Credit Post Authorization** – enables you to process a transaction for which voice authorization code was obtained due to the payment-processing network being unavailable and places the transaction in the current batch for settlement and payment.
- **Credit Authorization Only** – enables you to authorize a credit card without settlement. In most cases, this transaction is used to determine if a credit card has sufficient remaining credit to process a sale.
- **Credit Void** – enables you to cancel a previously completed sale transaction in the current batch via a keyboard, PIN pad or magnetic card reader.
- **Override Duplicate** – enables you to force a network to authorize a transaction, when the first attempt for authorization resulted in a duplicate transaction error (such as “AP DUP”).

# DSIClient Transaction Utility Setup

Before you can use the *DSIClient Transaction Utility*, you must configure it for use.

To setup the *DSIClient Transaction Utility*:

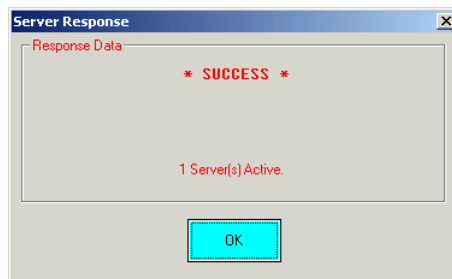
1. Launch *DSIClient*, then select **File** from the *DSIClient* menu bar, and choose **Setup**. The Configuration Settings dialog box appears.



15. Under **TCP/IP Settings** in the **Server IP Address** box, type the **IP Address** of the PC where *NETePay* is installed.

**NOTE:** If the *DSIClient Transaction Utility* and the *NETePay* are both installed on the same PC, use 127.0.0.1.

16. Under **Merchant Settings**, in the **Merchant ID** box, type “Local”.
17. If you enabled *NETePay* for client/server password usage, then under **TCP/IP**, check the **Use Client / Server Password** box and type the client/server password in the box provided.
18. To test a connection to the server (the PC where *NETePay* is installed), click **Ping Server**. If a successful connection is made, a response message appears. It should show at least one active server.

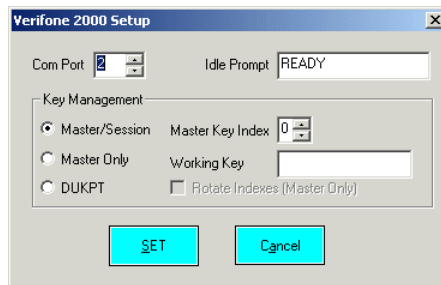


19. Click **OK** to continue.
20. If you enabled *NETePay* for client/server password usage, then under **TCP/IP**, check the **Use Client / Server Password** box and type the client/server password in the box provided.
21. To configure the Verifone PINpad 2000 for use with the *DSIClient Transaction Utility*, proceed to the next section.
22. To save the settings and exit the Configurations Settings, click **OK**.

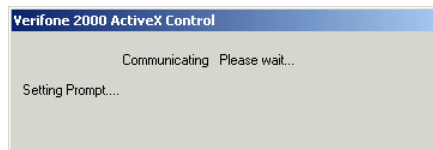
## Verifone PINpad 2000 Setup

If you will be processing Debit transactions then you need to install the optional Verifone PIN pad driver. To configure the *DSIClient Transaction Utility* to utilize an optional Verifone PINpad 2000 to process debit transactions:

1. Connect the Verifone PINpad 2000 to an available serial port and record the serial port number for later reference.
23. Under **Verifone 2000 Settings**, make the following choices:
- a. To process debit transactions, check the **Accept Debit** box that appears
  - b. If you selected to accept debit and will offer cash back to the customer, check the **Cash Back** box.
  - c. To use the Verifone PINpad 2000's magnetic card reader to process credit card transactions, check the **Use the Magnetic Card Reader on Pinpad for Credit** box.
- NOTE:** By making a selection, the *Verifone 2000 Setup* button becomes active.
24. Click **Verifone 2000 Setup**. The Verifone 2000 Setup dialog box appears.



25. In the **Comm Port** box, select the number of the serial port that is connected to the Verifone PINpad 2000.
26. If needed, you can change the prompt (up to 16 uppercase characters) that appears at the Verifone PINpad 2000's idle state.
27. Under **Key Management**, select one of the following options:
- For all networks (except Nova), select **DUKPT**
  - For Nova, select **Master Only** and check the **Rotate Indexes** box
28. Click **Set**. The *DSIClient Transaction Utility* will then attempt to communicate with the Verifone PINpad 2000.



If the *DSIClient Transaction Utility* successfully communicates with the Verifone PINpad 2000, the following message appears:



29. Click **OK** to continue.
30. To save the settings and exit the Configurations Settings, click **OK**.

## PDC Setup

To configure a PDC (Peripheral Device Controller) attached to a PC serial port to process transactions with the *DSIClient Transaction Utility*:

1. Connect the PDC to an available serial port and record the serial port number for later reference.
2. In the DSIClient Settings window, in the **PDC Settings** section, make the following choices:

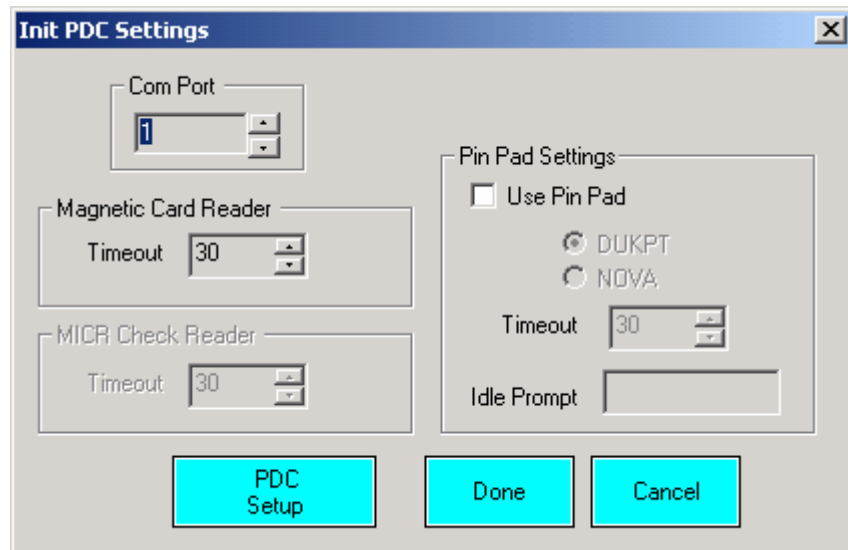
To process debit transactions, check the **Accept Debit** box.

If you selected to accept debit and will offer cash back to the customer, check the **Cash Back** box.

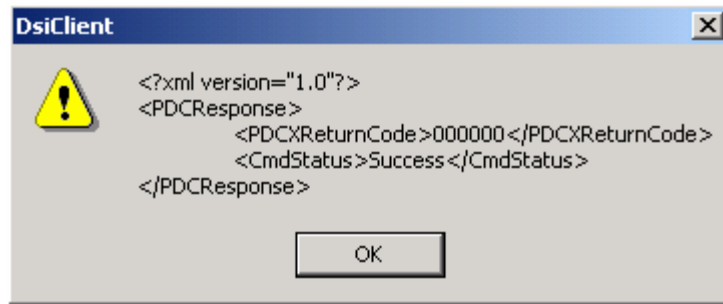
To use an optional magnetic card reader attached to the PDC to process credit card transactions, check the **Use Card Reader for Credit** box.

**NOTE:** By making a selection, the **PDC Setup** button becomes active.

3. Click the **PDC Setup** button. Init PDC Settings dialog box appears.



4. In the **Comm Port** box, select the number of the serial port that is connected to the PDC (1-255).
5. If an optional magnetic card reader is attached to the PDC, in the **Magnetic Card Reader** section, set the **Timeout** box to the desired value.
6. If an optional PIN pad is attached to the PDC, in the **PIN Pad Settings** section, check the **Use PIN Pad** box and select the **DUKPT** radio button. Set the **Timeout** to the desired value. If desired, you can change the prompt (up to 16 uppercase characters) that appears at the PIN pad's idle state.
7. Click the **PDC Setup** button to initialize the attached PDC with the new settings. If the PDC is successfully initialized, a response as follows will be displayed:



If you receive a response where the `<CmdStatus>` is other than `Success`, recheck all connections to the PDC and try again. If you continue to experience problems, refer to the PDC Integration Guide which is in the Documentation folder within the `DSIClient` folder.

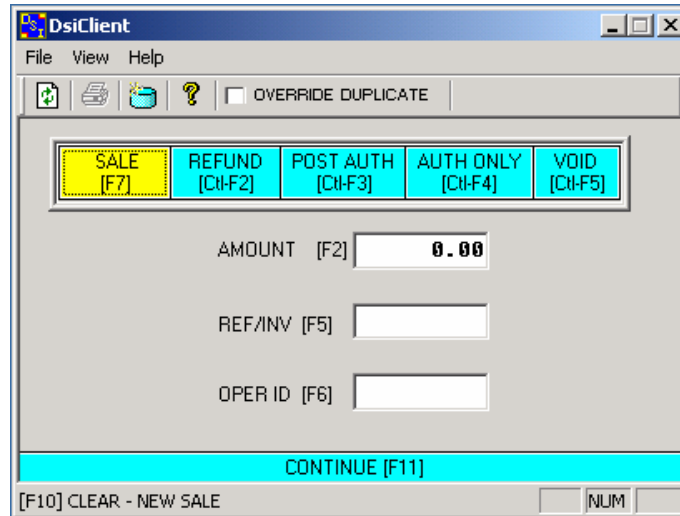
8. Click **OK** on the response.
9. Click **Done** on the **Init PDC Settings** window.
10. Click **OK** on the **Configuration Settings** window to get back to the *DSIClient Transaction Utility* main window.

# Processing Transactions

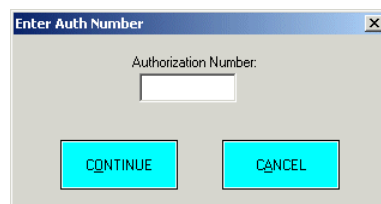
In order to process a transaction using the *DSIClient Transaction Utility*, *NETePay* must be running on the server.

To process a transaction using the *DSIClient Transaction Utility*:

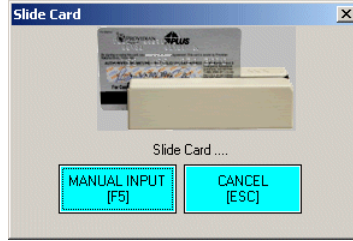
1. Launch *DSIClient*:



31. Using your mouse or action key(s), select the transaction type. The selected transaction type is then highlighted. The default transaction type is Sale (F7).
32. Type the transaction amount in the **AMOUNT** field
33. If needed (typically in Restaurant applications), type the check and/or the receipt number in the **REF NO/INV** box.  
**NOTE: NETePay does not currently support Restaurant applications**
34. If needed (this is a reference only field), type your name or ID number in the **OPER ID** box. (Operator ID).
35. If you want to force a network to authorize a transaction, when the first attempt for authorization resulted in a duplicate transaction error, check the **OVERRIDE DUPLICATE** box.
36. Click **CONTINUE** or press **F11**.
37. If required, the *DSIClient Transaction Utility* will prompt you for the entry of an authorization number.



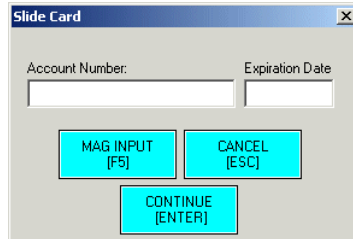
38. Type the number in the field provided, then click **CONTINUE** to proceed. The Slide Card dialog box appears.



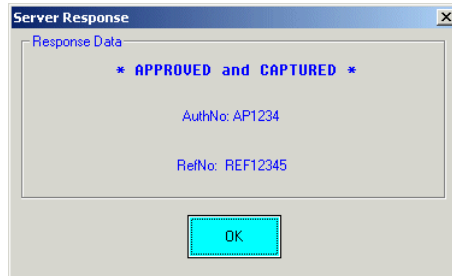
39. Either slide the credit card through the Verifone PINpad 2000's card reader or click **MANUAL INPUT**.

When using manual entry, the Slide Card dialog box will prompt you to enter an **Account Number** and **Expiration Date**.

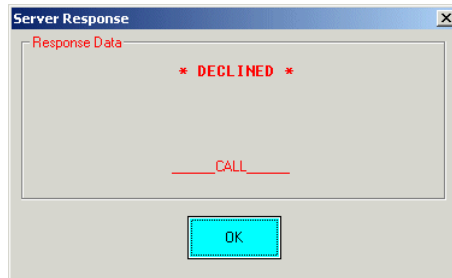
**NOTE:** When entering the date use the format: MMY (Month, Year).



40. After entering the account number and expiration date, click **CONTINUE** to process the transaction.
41. The system will then generate a response message either approving or declining the transaction



OR



42. In either case, click **OK** to continue.
43. You can now process another transaction. Press **F10** to clear the form.



---

# INDEX

About		
Datacap .....	5	
NETePay .....	5	
Credit Authorization Only .....	22	
Credit Post Authorization .....	22	
Credit Refund .....	22	
Credit Sale .....	22	
Credit Void .....	22	
Determining the Encryption Strength .....	13	
DSIClient Transaction Utility		
Installation .....	14	
Processing Transactions .....	27	
Setup .....	23	
Supported Transaction Types .....	22	
DSIClientX Installation .....	14	
ePay Administrator Installation .....	14	
How it works .....	6	
Installation .....	10	
Installation Procedures .....	11	
Accessing the NETePay CD-ROM .....	11	
DSIClient Transaction Utility .....	14	
DSIClientX .....	14	
ePay Administrator .....	14	
Microsoft Internet Explorer .....	13	
NETePay .....	14	
Microsoft Internet Explorer		
Determining the Encryption Strength .....	13	
Installation .....	13	
NETePay		
Activation .....	16	
Configuration .....	17	
Installation .....	14	
Testing .....	20	
Network Requirements .....	11	
Override Duplicate .....	22	
Overview .....	5	
Requirements		
Network .....	11	
Server .....	10	
Server Requirements .....	10	
Upgrading Microsoft Internet Explorer .....	13	
Using the DSIClient Transaction Utility .....	22	
Verifone PINpad 2000 Setup .....	24, 25	
What's Included on your CD .....	5	