
NETePay XML
Installation & Configuration Guide

For CEPAS
State of Michigan

Version 4.00

Part Number: 8660.58 (ML)
8660.59 (SL)

NETePay XML Installation & Configuration Guide

Copyright © 2010 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, DIALePay, DSIClient, DSIClientX, ePay Administrator, IPTran, TwinTran, DialTran, DataTran are trademarks of the Datacap Systems Inc.

Microsoft, Windows NT 4.0, Windows 2000 Professional, Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista 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: 20 February 2010

Version Support

This document supports the following application versions:

NETePay XML, Version 4.00 (CEPAS – State of Michigan)

DSIClientX, Version 3.85

DSIClient Transaction Utility, Version 2.50

Note: All components of the release package 20070525 are Windows 7™ and Windows Vista™ compliant.

Payment Processor Support

This document supports the following payment processor:

CEPAS – State of Michigan

CONTENTS

OVERVIEW	5
INTRODUCTION	5
<i>About NETePay.....</i>	<i>5</i>
WHAT'S INCLUDED ON YOUR CD	5
HOW IT WORKS	5
SECURITY RECOMMENDATIONS FOR SYSTEMS USING NETEPAY	7
INTRODUCTION	7
ACCESS CONTROL.....	8
REMOTE ACCESS CONTROL	8
WIRELESS ACCESS CONTROL	9
NETWORK ENCRYPTION.....	9
NETWORK SECURITY	9
NETEPAY COMPLIANCE	10
BASELINE SYSTEM CONFIGURATION	10
ADDITIONAL SYSTEM SECURITY RECOMMENDATIONS.....	11
POS SYSTEM CONSIDERATIONS	11
SECURITY ACTION PLAN.....	11
MORE INFORMATION	12
INSTALLATION	13
INTRODUCTION	13
REQUIREMENTS	13
<i>Baseline System Configuration</i>	<i>13</i>
<i>Network Requirements</i>	<i>14</i>
INSTALLATION PROCEDURES	14
<i>Accessing the NETePay CD-ROM</i>	<i>14</i>
<i>Installing/Upgrading Microsoft Internet Explorer</i>	<i>16</i>
<i>Installing NETePay (Required).....</i>	<i>17</i>
<i>Installing DSIClient Application (Optional).....</i>	<i>17</i>
NETEPAY CONFIGURATION.....	18
INTRODUCTION	18
ACTIVATION	18
CONFIGURATION.....	19
TESTING.....	21
<i>Important! - Before You Start</i>	<i>21</i>
OPERATIONAL CONSIDERATIONS.....	22
<i>Important!</i>	<i>22</i>
USING THE DSICLIENT TRANSACTION UTILITY TO TEST NETEPAY SERVER.....	23
INTRODUCTION	23
<i>Supported Transaction Types.....</i>	<i>23</i>
DSICLIENT TRANSACTION UTILITY SETUP	24

<i>Verifone 2000 PIN pad Setup</i>	26
<i>PDC Setup</i>	27
PROCESSING TEST TRANSACTIONS	29
INDEX	31

CHAPTER 1

OVERVIEW

Introduction

About NETePay

Developed by Datacap Systems, *NETePay* enables retail, restaurant and other businesses to perform reliable electronic payment authorizations via the Internet or other TCP/IP securely services in as little as two seconds or less.

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.

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 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 LAN. 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 RECOMMENDATIONS FOR SYSTEMS USING NETEPAY

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

Access Control

The PCI standard 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. Additionally any default accounts provided with operating systems, databases and/or devices should be removed/disabled/renamed if possible, or at least should have complex passwords and should not be used. Examples of such default administrator accounts include administrator (Windows systems), sa (SQL/MSDE), and root (UNIX/Linux).

The PCI standard requires the following password complexity for compliance:

- Passwords must be at least 7 characters
- Passwords must include both numeric and alphabetic characters
- Passwords must be changed at least every 90 days
- New passwords can not be the same as the last 4 passwords

Below are the other PCI account requirements beyond uniqueness and password complexity:

- If an incorrect password is provided 6 times the account should be locked out
- Account lock out duration should be at least 30 min. (or until an administrator resets it)
- Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session.

These same account and password criteria must also be applied to any applications or databases included in payment processing to be PCI compliant.

Remote Access Control

The PCI standard requires that if employees, administrators, or vendors can access the payment processing environment remotely; access should be authenticated using a 2-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate).

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

Access to hosts within the payment processing environment via 3rd party remote access software such as Remote Desktop (RDP)/Terminal Server, PCAnywhere, etc. requires that when such programs are used that these sessions are encrypted with at least 128 bit encryption (this requirement is in addition to the requirement for 2-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.

Wireless Access Control

The PCI standard requires the encryption of cardholder data transmitted over wireless connections. The following items identify the PCI standard requirements for wireless connectivity to the payment environment:

- Firewall/port filtering services should be placed between wireless access points and the payment processing environment with rules restricting access
- Use of appropriate encryption mechanisms such as **VPN, SSL/TLS at 128 bit, WEP at 128 bit, and/or WPA**
- If WEP is used the following additional requirements must be met:
 - Another encryption methodology must be used to protect cardholder data
 - If automated WEP key rotation is implemented key change should occur every 10-30 minutes
 - If automated key change is not used, keys should be manually changed at least quarterly and when key personnel leave the organization
- Vendor supplied defaults (administrator username/password, SSID, and SNMP community values) should be changed
- Access point should restrict access to known authorized devices (using MAC Address filtering)

Network Encryption

The PCI standard requires the use of strong cryptography and encryption techniques (at least 128 bit); such as Secure Sockets Layer (SSL) and Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks (like the Internet).

Additionally PCI requires that cardholder information never be sent via e-mail without strong encryption of the data.

Network Security

ePay Administrator and ePay Administrator for NETePay may be installed on other computers on the network rather than on the computer on which the NETePay server is installed. ***If either of these ePay Administrators is installed remotely in this manner, you should enable SSL encryption for the instance of MSDE by using Microsoft Management Console.***

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 IP transmissions which contain cardholder data.

Baseline System Configuration

To realize the maximum security from *NETePay*, the server on which it is installed should meet or exceed the following system requirements:

- Microsoft Windows 2000 Professional with Service Pack 4, Windows XP Pro with Service Pack 2, Windows Vista Business Edition, Windows Server 2003 or 2008. All latest updates and hotfixes should be applied.
- 1 GB of RAM minimum, 2 GB or higher recommended
- 5 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.
- 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.)

Additional System Security Recommendations

Although **NETePay** implements all of the PCI Data Security Standard requirements which are applicable to a payment processing application, additional overall security can be realized by implementing the following:

- Use a router which implements NAT (Network Address Translation).
- Use antivirus software with auto update capability, from vendors such as McAfee, Norton, Panda, Kaspersky, Trend Micro, etc.
- Enable firewall services (either software based like Windows Firewall or hardware based) between the payment processing environment and the internet access device (typically an ISP provided router/modem).
- Define and use strong passwords to restrict access to authorized personnel.
- Test and install security related Windows and SQL/MSDE updates, service packs and hotfixes promptly. Consider using automatic updating.

POS System Considerations

Although **NETePay** implements all of the PCI Data Security Standard (DSS) 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.

Security Action Plan

In addition to the preceding security recommendations, 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 the PCI Security Standards Council website at the following Internet address:

http://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.shtml

Additional information for merchants from the PCI Security Standards Council is available at the following Internet address:

http://www.pcisecuritystandards.org/education/fact_sheets.shtml

Listing of qualified security assessors from the PCI Security Standards Council is available at the following Internet address:

http://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

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. *ePay Administrator* is installed on one or more client machines (for more information about using *ePay Administrator*, see the *ePay Administrator User Guide*).

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

Requirements

Baseline System Configuration

To successfully install and run *NETePay* 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 2, Windows Vista Business Edition, Windows 7, Windows Server 2003 or 2008. All latest updates and hotfixes should be applied.
- 1 GB of RAM minimum, 2 GB or higher recommended
- 5 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 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:

	Open Installation & Configuration Guide	This document (ReadMe.pdf) describes the installation and setup of NETePay for CEPAS State of Mich. Requires Acrobat Reader
	Open Security Recommendations Guide	This document (Security-ReadMe.pdf) describes the PCI/CISP security recommendations for systems using NETePay. Requires Acrobat Reader
STEP 1.	Install NETePay	The NETePay Server communicates with CEPAS in order to process Credit card transactions.
OPTIONAL	Install DSIClient	DSIClient is a stand-alone application used to send test transactions to NETePay.
OPTIONAL	Install Internet Explorer 6.0	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 © 2010 Datacap Systems, Inc - All rights reserved.
Revised: February 17, 2010.

Done

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	Size	Type	Date Modified
program files		File Folder	2/18/2010 10:37 AM
System32		File Folder	2/18/2010 10:37 AM
0x0409.ini	21 KB	Configuration Settings	5/21/2009 2:53 PM
instmsiw.exe	1,780 KB	Application	11/28/2004 8:53 AM
NETePay XML 4.0 (ML CE 4.00) CEPAS Mich...msi	1,319 KB	Windows Installer Package	2/17/2010 4:48 PM
setup.exe	999 KB	Application	2/17/2010 4:48 PM
Setup.ini	3 KB	Configuration Settings	2/17/2010 4:48 PM
WindowsInstaller-KB893803-x86.exe	2,525 KB	Application	5/16/2005 3:42 PM

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

Installing/Upgrading Microsoft Internet Explorer

NETePay uses Windows encryption services and requires that Internet Explorer with 128 bit encryption strength is installed on each system in the LAN. 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, use the Windows Update on each PC to upgrade an existing version, or if an Internet connection is not available, install a copy of Microsoft Internet Explorer 6.0 included on the *DIALePay* CD-ROM.

Determining the Encryption Strength

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

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 (As Required)

To install Microsoft Internet Explorer 6.0 from the *DIALePay* CD-ROM:

1. Open the Microsoft Internet Explorer folder on the *DIALePay* 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 (Required)

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 (Optional)

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 cannot print drafts or receipts. Your POS system should be used for normal transaction processing through NETePay.

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* for use.

NETePay is provided 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 program launch, *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 with **NETePay Activation** in the Subject line. The body of the message should contain:

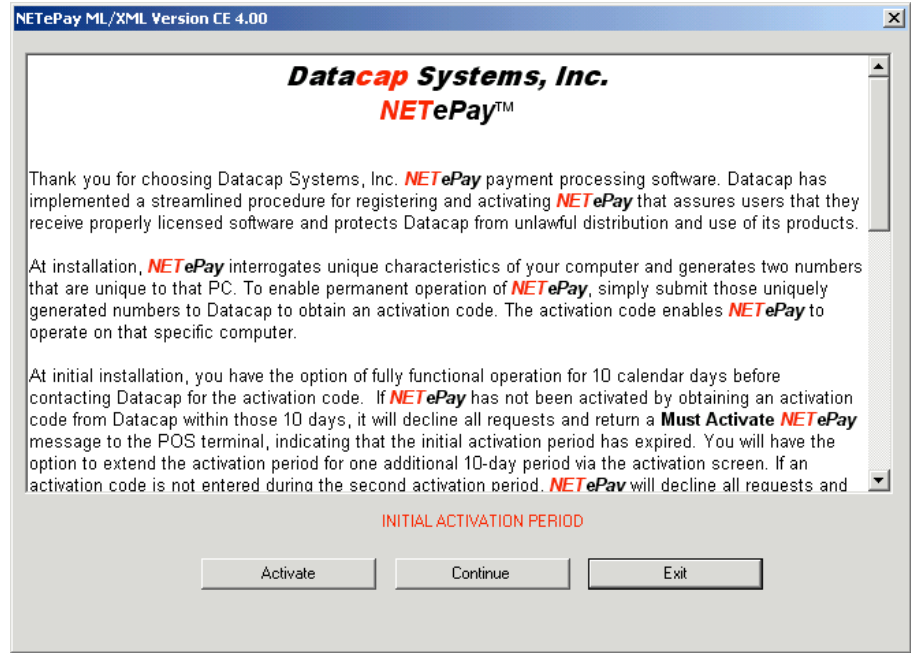
1. Your Name
2. Telephone Number
3. Serial Number
4. Session Code
5. Machine ID

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

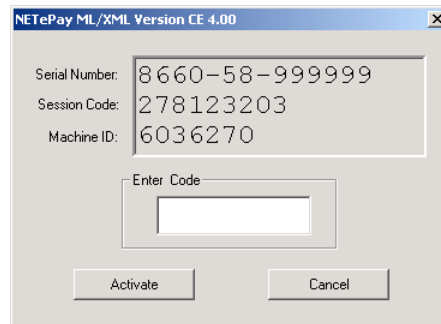
To activate and set up *NETePay* for use:

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

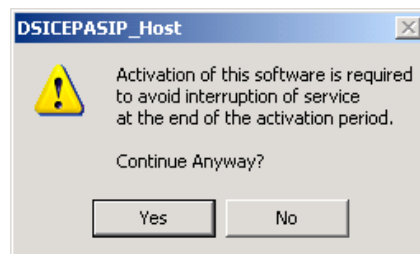


NOTE: The Initial Activation dialog box will appear each time you start *NETePay* until you activate it.

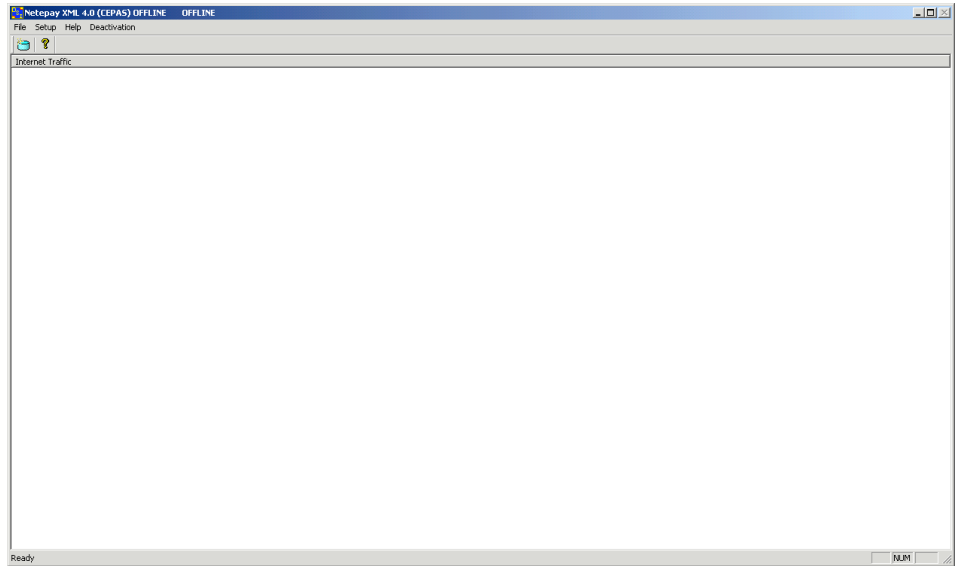
2. To enter the activation code, click **Activate**. When the activation dialog box appears, type the activation code in the box provided and click **Activate**. Contact Datacap at 215-997-8989 for your activation code Monday through Friday, 8:30AM to 5:30 PM Eastern time.



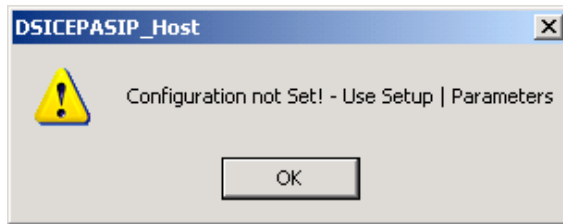
3. To proceed without activation, click **Continue**. When the message indicating that activation is required to avoid interruption of service appears, click **Yes** to continue.



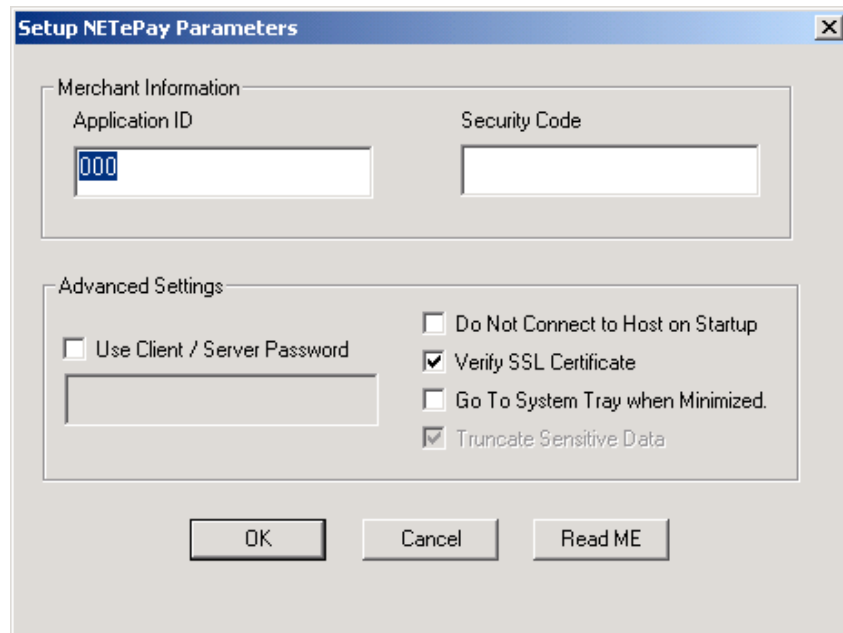
4. In either case, *NETePay* appears.



NOTE: During your initial access of *NETePay*, the following message will appear indicating that configuration is required. Click **OK** to continue.



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



NOTE: You may click the *Read Me* button at any time to view the *Read Me* file with additional information on setting your configuration.

6. Under **Merchant Information** section, enter each of the following fields which are supplied by your processing services provider.

**Application ID
Security Code**

Note that the merchant information is case sensitive and should be entered exactly as provided by your processing service provider.

7. Under **Advanced Settings** 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* for Client/Server password protection using the same password to use this function.

8. The selection box **Go To System Tray when Minimized** is unchecked by default. If you want to have the *NETePay* icon appear in the System Tray rather than in the Toolbar when minimized, check this option.
9. The selection box **Verify SSL Certificate** is checked by default. If you want to have the *NETePay* skip verification of the SSL certificate, you may uncheck this box. If you experience errors on startup with SLL certificate authentication, contact your processing service provider to determine if you should disable this feature.
10. The selection box **Do Not Connect to Host on Startup** is unchecked by default. When this option is unchecked, *NETePay* will check that it can establish a connection to the processing host before starting. If this box is checked, *NETePay* will start without testing the connection to the host. The selection box **Truncate Sensitive Data** is checked by default and cannot be changed, all log files generated by *NETePay* will truncate recorded account numbers to just the last 4 digits and remove all expiration data digits. No CVV, CVV2, CVC, PIN or magnetic stripe data is recorded in the logs.
11. 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. 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.

USING THE DSIClient TRANSACTION UTILITY TO TEST NETEPAY SERVER

Introduction

This chapter explains how to use the *DSIClient Transaction Utility* program as a stand-alone application to test the operation of the NETePay server.

It is strongly recommended that you test each card type with the *DSIClient Transaction Utility* and verify that the processor has received the transactions into your merchant account.

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 a 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 credit transaction, when the first attempt for authorization resulted in a duplicate transaction error (such as “AP DUP”).
- **Debit Sale** - enables you to process a transaction for a payment for goods or services using a bank ATM card.
- **Debit Refund** – enables you to issue a credit to the cardholder for the return or credit of goods or services using a bank ATM card.

DSIClient Transaction Utility Setup

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

To setup the *DSIClient Transaction Utility*:

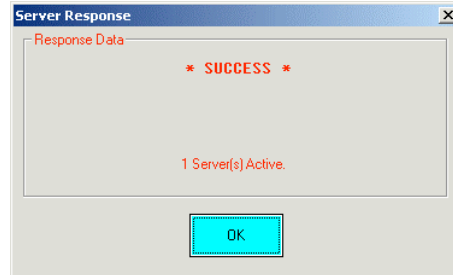
1. Launch *DSIClient* application, then select **File** from the *DSIClient* menu bar, and choose **Setup**. The Configuration Settings dialog box appears.

The screenshot shows the 'Configuration Settings' dialog box with the following details:

- TCP/IP Settings:** A text box for 'Host Name or IP Address', a checkbox for 'Use Client /Server Password', and a 'Ping Server' button.
- Merchant Settings:** A dropdown menu for 'Merchant Category' (set to 'Retail'), text boxes for 'Merchant ID' and 'Terminal ID'.
- Input Settings:** A checkbox for 'Use PDC/Verifone 2000 device' and two radio buttons for 'PDC' and 'Verifone 2000'.
- PDC Settings:** Checkboxes for 'Accept Debit', 'Cash Back', and 'Use Card Reader for Credit', and a 'PDC Setup' button.
- Verifone 2000 Settings:** Checkboxes for 'Accept Debit', 'Cash Back', and 'Use Magnetic Card Reader on Pinpad for Credit', and a 'Verifone 2000 Setup' button.
- Printer Settings:** A checkbox for 'Print Drafts Automatically', a printer icon, and 'Printer Setup' and 'Test Printer' buttons.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

2. Under TCP/IP Settings in the Server IP Address box, type the IP Address of the PC where NETePay is installed.
3. Under Merchant Settings, enter the Merchant Category, Merchant ID and Terminal ID entered during NETePay Configuration.
4. If you enabled NETePay for client/server password usage, then under TCP/IP, check the Use Client / Server Password box and type the same client/server password used when setting up NETePay in the box provided.
5. If you will be using a Datacap PDC (Peripheral Device Controller) or directly attaching a VeriFone 2000 PIN pad to your PC, then check the Use PDC/Verifone 200 Device box in the Input Settings section. This is only required if you will be testing Debit and/or EBT transactions.
6. If you checked the Use PDC/Verifone 2000 Device box, then you must select one of the radio buttons – check PDC if you have a Peripheral Device Controller attached to your PC or check Verifone 2000 if the pin pad will be directly attached to a PC serial port.

7. The Printer Settings section is not supported and requires no settings.
8. 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.



9. If you do not get at least 1 Server Active, then verify that the IP address for the server is correct and that the NETePay server is running and try again. You must have at least one server active to process transactions.
10. Click **OK** to continue.
11. To configure the Verifone 2000 PIN pad for use with the *DSIClient* application, proceed to the next section. If will not be processing debit, then you should skip the Verifone 2000 PIN Pad setup section.
12. To save the settings and exit the Configurations Settings, click **OK**.

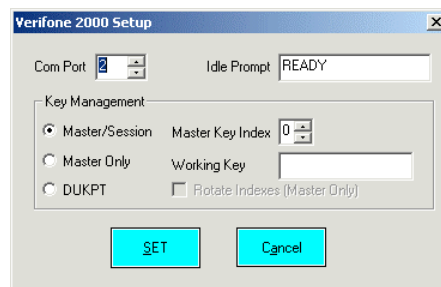
Verifone 2000 PIN pad Setup

To configure a Verifone 2000 PIN pad attached directly to a PC serial port to process debit and/or EBT transactions with the *DSIClient* application:

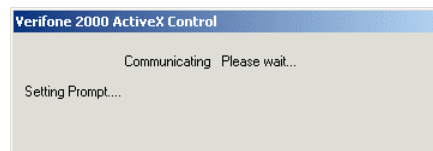
1. Connect the Verifone PINpad 2000 to an available serial port and record the serial port number for later reference.
2. In the DSIClient Settings window, in the **Verifone 2000 Settings** section, make the following choices:
 1. To process debit transactions, check the **Accept Debit** box.
 2. If you selected to accept debit and will offer cash back to the customer, check the **Cash Back** box.
 3. To use the Verifone PINpad 2000's magnetic card reader to process credit card transactions, check the **Use the Magnetic Card Reader on PIN pad for Credit** box.

NOTE: By making a selection, the **Verifone 2000 Setup** button becomes active.

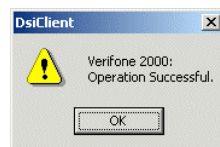
3. Click the **Verifone 2000 Setup** button. The Verifone 2000 Setup dialog box appears.



4. In the **Comm Port** box, select the number of the serial port that is connected to the Verifone PINpad 2000 (1-255).
5. If needed, you can change the prompt (up to 16 uppercase characters) that appears at the Verifone PINpad 2000's idle state.
6. Under **Key Management**, select one of the following options:
 - Select **DUKPT**
7. Click **Set**. The *DSIClient* application will then attempt to communicate with the Verifone PINpad 2000.



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



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

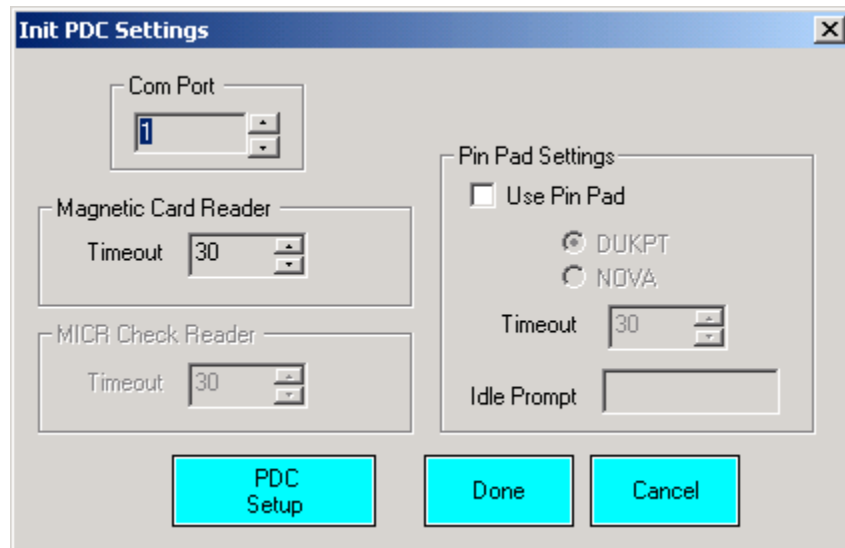
PDC Setup

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

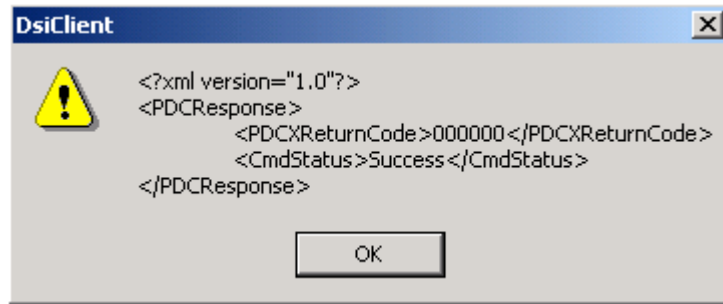
1. Connect the PDC to an available serial port and record the serial port number for later reference.
2. In the DSIClient Settings window, in the **PDC Settings** section, make the following choices:
 2. To process debit transactions, check the **Accept Debit** box.
 3. If you selected to accept debit and will offer cash back to the customer, check the **Cash Back** box.
 4. 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.

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



9. In the **Comm Port** box, select the number of the serial port that is connected to the PDC (1-255).
10. 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.
11. 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.
12. 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.

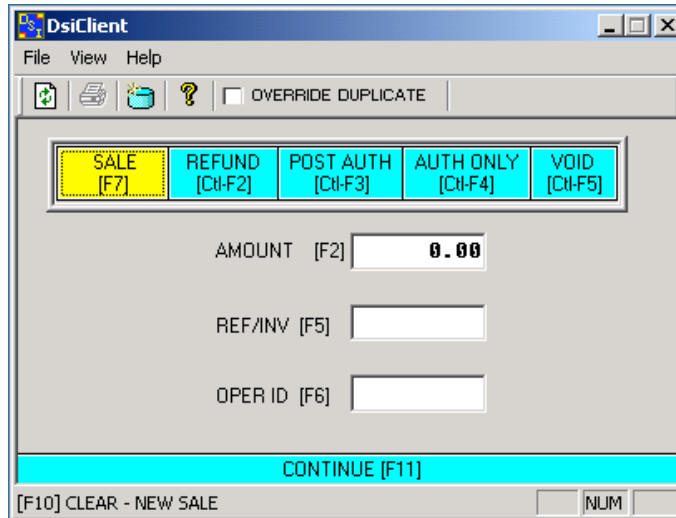
13. Click **OK** on the response.
14. Click **Done** on the **Init PDC Settings** window.
15. Click **OK** on the **Configuration Settings** window to get back to the *DSIClient Transaction Utility* main window.

Processing Test Transactions

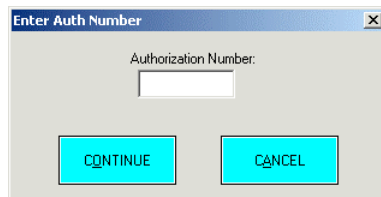
In order to process a transaction using the *DSIClient* application, *NETePay* must be running on the server.

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

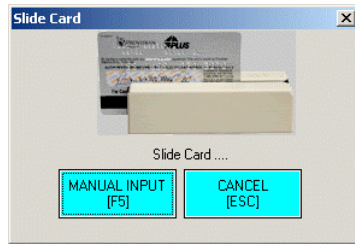
1. Launch *DSIClient*:



2. 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).
3. Type the transaction amount in the **AMOUNT** field
4. No entry is required for the **REF/INV** box.
NOTE: The *DSIClient* application only supports Retail category transactions.
5. If needed (this is a reference only field), type your name or ID number in the **OPER ID** box. (Operator ID).
6. 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.
7. Click **CONTINUE** or press **F11**.
8. If required, the *DSIClient* application will prompt you for the entry of an authorization number.



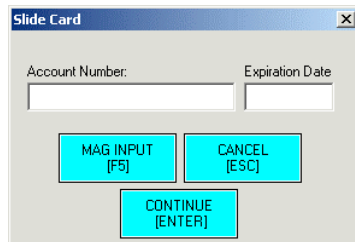
9. Type the number in the field provided, then click **CONTINUE** to proceed. The Slide Card dialog box appears.



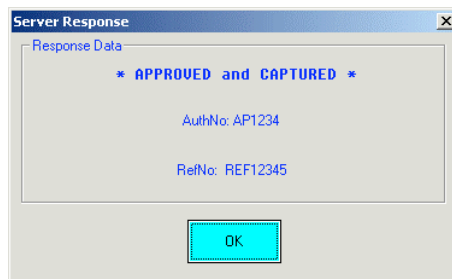
10. Either slide the credit card through the Verifone PINpad 2000's card reader or click **MANUAL INPUT**.

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

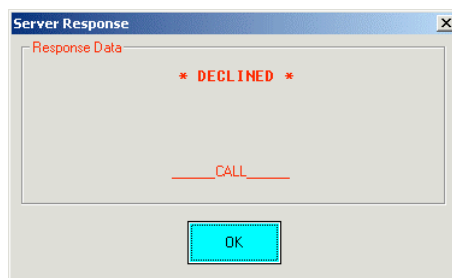
NOTE: When entering the date use the format: *MMYY (Month, Year)*.



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



OR



13. In either case, click **OK** to continue. If you receive a response with No Response from Any Server, verify that NETePay is running and that you have entered the correct IP address for the NETePay server in the DSIClient application setup.
14. You can now process another transaction. Press **F10** to clear the form.

INDEX

- A**
- About
 - NETePay, 5
- C**
- Credit Authorization Only, 23
 - Credit Post Authorization, 23
 - Credit Refund, 23
 - Credit Sale, 23
 - Credit Void, 23
- D**
- DSIClient Transaction Utility
 - Processing Transactions, 29
 - Setup, 24
 - Supported Transaction Types, 23
- H**
- How it works, 5
- I**
- Installation, 13
 - Installation Procedures, 14
 - Accessing the NETePay CD-ROM, 14
 - NETePay, 17
- N**
- NETePay
 - Configuration, 19
 - Installation, 17
 - Testing, 21, 22
 - Network Requirements, 14
- O**
- Override Duplicate, 23
 - Overview, 5
- R**
- Requirements
 - Network, 14
 - Server, 13
- S**
- Server Requirements, 13
- U**
- Upgrading Microsoft Internet Explorer, 16
 - Using the DSIClient Transaction Utility, 23
- V**
- Verifone PINpad 2000 Setup, 26, 27
- W**
- What's Included on your CD, 5