

---

***DIALePay XML***  
***Installation & Configuration Guide***

---

***Version 4.10***

***Part Number: 8604-20 (ML)***  
***8604-30 (SL)***

# ***DIALePay XML Installation & Configuration Guide***

Copyright © 2007 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, DIALePay, DSIClient, ePay Administrator, WinPop 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 - Rev 20070130

## ***Version Support***

This document supports the following application versions:

DIALePay XML, Version 4.10

DSIClientX, Version 3.60

DSIClient Transaction Utility, Version 2.50

ePay Administrator for DIALePay, Version 4.00

DataTran Setup Software, Version 2.01

---

# CONTENTS

Chapter 1. <b>Overview</b> .....	<b>4</b>
Introduction.....	4
About DIALePay.....	4
About DataTran.....	4
What's Included on your CD.....	4
How it works.....	5
Chapter 2. <b>Security Recommendations for Systems Using DIALePay</b> .....	<b>6</b>
Introduction.....	6
Access Control.....	7
Remote Access Control.....	7
Wireless Access Control.....	8
Network Encryption.....	8
Network Security.....	8
DIALePay Compliance.....	9
Baseline System Configuration.....	9
Chapter 3. <b>Installation</b> .....	<b>10</b>
Introduction.....	10
Requirements.....	10
Baseline System Configuration.....	10
Network Requirements.....	11
Installation Procedures.....	11
Accessing the DIALePay CD-ROM.....	11
Installing/Upgrading Microsoft Internet Explorer.....	13
Installing DIALePay Server (Required).....	14
Installing DSIClient Application (Optional).....	14
Installing ePay Administrator for DIALePay (Required).....	14
Installing DataTran Setup Software (Optional).....	15
Installing Windows 98 Y2K Updates (As Needed).....	15
Chapter 4. <b>DIALePay Configuration</b> .....	<b>16</b>
Introduction.....	16
Activation.....	16
Configuration.....	17
Chapter 5. <b>Testing DIALePay</b> .....	<b>20</b>
LAN Test.....	20
Live Testing.....	23
Before You Start.....	23
DataTran Parameter Verification.....	23
DataTran Setup and Initialization.....	23
Entering Test Transactions.....	24

# OVERVIEW

## Introduction

### **About DIALePay**

Developed by Datacap Systems, *DIALePay* enables retail, restaurant and other businesses to perform reliable electronic payment authorizations via dial, wireless, and satellite communications through a DataTran 162 ML.

*DIALePay* is scalable, enabling customers to configure their store and enterprise system to fit their requirements and get the most favorable rates from their payment service.

*DIALePay* 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 DataTran**

The DataTran 162 ML is a self-contained payment processing system that can authorize and settle transactions with a wide variety of payment-processing centers.

It handles all message formatting, protocol, communications (via an integrated modem or external IPTran IP adapter) and transaction storage functions.

## What's Included on your CD

The *DIALePay* CD-ROM includes client and server applications for Windows NT/2000/XP operating systems for both single and multi pay-point users.

- ***DIALePay*** – server-side software that enables you to process payment authorization requests from client machines on a Local Area Network (LAN) to bankcard processors via dial, or wireless.
- ***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 *DIALePay* for processing. *DSIClientX* also includes a utility program to enter test payment transactions called ***DSIClient***.
- ***ePay Administrator for DIALePay*** – a software application that provides payment transaction batch management. You can also use *ePay Administrator* to enter and process payment transactions.

For information about using *ePay Administrator*, refer to the *ePay Administrator User Guide*.

- ***DataTranSetup*** – A utility program that enables Datacap Systems to enable loading of payment processor applications and merchant parameters into DataTran.

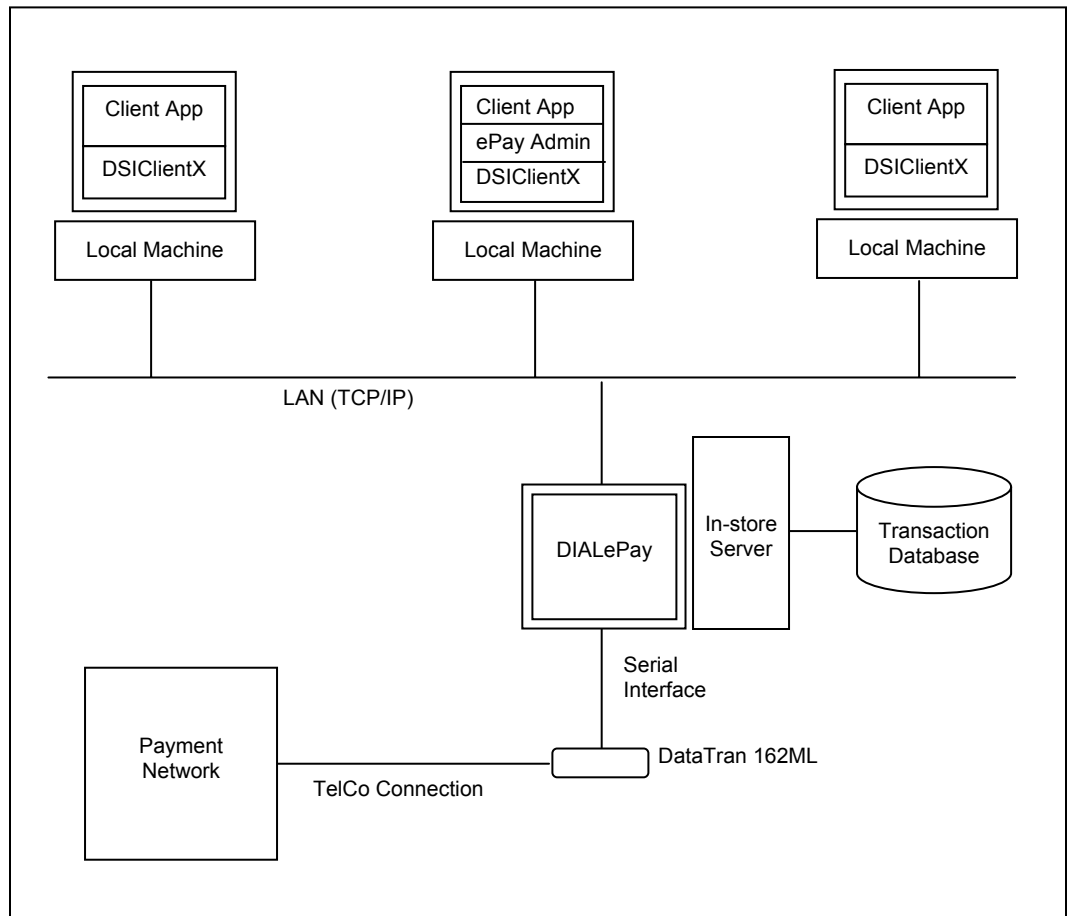
- **Microsoft Internet Explorer 6.0** – this latest version of Microsoft Internet Explorer will ensure that you can install the necessary cyber strength required for *DIALePay*.
- **Windows 98 Y2K Updates** – Windows 98 users must have the latest updates in order to install and use *DIALePay*.

## How it works

*DIALePay* is an application that executes on a server in a TCP/IP network and monitors encrypted transaction requests from client machines using a POS application integrated with *DSIClientX*, Datacap's XML ActiveX control.

When *DIALePay* receives an encrypted transaction request from a client machine, it sends the request to the bankcard processor for approval using a DataTran ML. The transactions are then stored in a database that resides on the server.

By using *ePay Administrator for DIALePay*, you can view the transactions, settle and close batches, generate reports and process payment transactions.



# ***SECURITY RECOMMENDATIONS FOR SYSTEMS USING DIALEPAY***

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

## ***DIALePay Compliance***

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

- **DIALePay** does not store any magnetic stripe (Track 1 or 2), card verification (CVV, CVV2, etc.) or PIN data, ever.
- **DIALePay** truncates all account and expiration date information for transactions which have been settled in every area where it is either stored or displayed.
- **DIALePay** encrypts account numbers and expiration dates for transactions which have not yet been settled.
- **DIALePay** 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.
- **DIALePay** 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.
- **DIALePay** encrypts all IP transmissions which contain cardholder data.

## ***Baseline System Configuration***

To realize the maximum security from *DIALePay*, the server on which it is installed 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 tested and applied.
- 512MB of RAM minimum, 1GB or higher recommended
- 2 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.
- DataTran 162 ML (purchased and installed separately)
- Serial port for DataTran interface

# **INSTALLATION**

## **Introduction**

This chapter explains how to set up and install the following *DIALePay* components.

- *DIALePay*
- *DSIClientX* (and *DSIClient* application)
- *ePay Administrator for DIALePay*
- *DataTran Setup Software*
- *Microsoft Internet Explorer 6.0 with High Encryption*
- *Windows 98 Y2K Updates*

You will need to install all the above components on the server (the PC connected to the DataTran).

Each client machine will require *DSIClientX* installed.

You can optionally install *ePay Administrator* on one or more client machines. For information about using *ePay Administrator*, refer to the *ePay Administrator User Guide*.

If you are using an older version of Microsoft Internet Explorer that already has high encryption, installation of Microsoft Internet Explorer 6.0 with High Encryption is optional.

## **Requirements**

### **Baseline System Configuration**

To successfully install and run *DIALePay* 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.
- 512MB of RAM minimum, 1GB or higher recommended
- 2 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.
- DataTran 162 ML (purchased and installed separately)
- Serial port for DataTran interface

## Network Requirements

Before installing *DIALePay* or any of its components, you should know the name and IP address of the server that will be receiving transaction requests.

You should also make port 9000 on the server available for incoming traffic if you are behind a firewall and connected to the default port. If you will process gift or prepaid cards, you should also enable port 9001. If you are using a port other than the default IP port (9000), make sure you know the port on which the server is listening.

## Installation Procedures

### Accessing the DIALePay CD-ROM

Before you begin installing *DIALePay* 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 *DIALePay* and its components:

1. Insert the *DIALePay* CD-ROM 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:

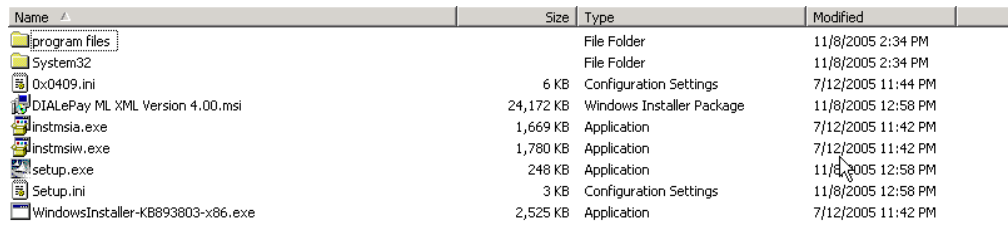
**datacap**  
systems, inc.

Reliable Integrated  
E-Payment Solutions

	<a href="#">Open Installation &amp; Configuration Guide</a>	This document (ReadMe.pdf) describes the installation and setup of DIALePay. Requires Acrobat Reader
STEP 1.	<a href="#">Install DIALePay</a>	DIALePay Server accepts electronic payment requests from a DSIClientX enabled POS application and communicates with a DataTran 162 ML in order to process Credit card, Debit card, EET card, Gift card and Check authorization transactions.
STEP 2.	<a href="#">Install EPay Admin for DIALePay</a>	EPay Admin is a stand-alone application that provides batch management and reporting by communicating with DIALePay.
OPTIONAL	<a href="#">Install DSIClient</a>	DSIClient is a stand-alone application used to send test transactions to DIALePay.
OPTIONAL	<a href="#">Install DataTran Setup</a>	This unregistered copy of DataTran setup utility is a stand-alone application used to verify proper operation of a DataTran and modify DataTran merchant specific profile settings (phone numbers and access methods).
OPTIONAL	<a href="#">Install Internet Explorer 6.0</a>	DIALePay 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.
OPTIONAL	<a href="#">Windows 98 Y2K Updates</a>	For Windows 98 users, installation of MDAC 2.7 requires Y2K updates to be installed. Install the original Y2K update first, then install update 2.

Copyright © 2003,2004 Datacap Systems, Inc - All rights reserved.  
Revised: November 08, 2005 .

2. If AUTORUN is not enabled on your system, then you should open **My Computer**, and then double-click the drive that contains the *DIALePay* CD-ROM. The following window appears:



Name	Size	Type	Modified
program files		File Folder	11/8/2005 2:34 PM
System32		File Folder	11/8/2005 2:34 PM
0x0409.ini	6 KB	Configuration Settings	7/12/2005 11:44 PM
DIALePay ML XML Version 4.00.msi	24,172 KB	Windows Installer Package	11/8/2005 12:58 PM
instmsia.exe	1,669 KB	Application	7/12/2005 11:42 PM
instmsiw.exe	1,780 KB	Application	7/12/2005 11:42 PM
setup.exe	248 KB	Application	11/8/2005 12:58 PM
Setup.ini	3 KB	Configuration Settings	11/8/2005 12:58 PM
WindowsInstaller-KB893803-x86.exe	2,525 KB	Application	7/12/2005 11:42 PM

From this window, you can install *DIALePay* by double clicking on SETUP (or SETUP.EXE).

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

*A version of Microsoft Internet Explorer that supports 128-bit encryption must be installed on both the client(s) and server PCs.*

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 DIALePay Server (Required)***

To install *DIALePay*:

1. Open the *DIALePay* Server folder on the *DIALePay* 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**.
5. If the option is available, make the application available to all users.
6. To begin installing the necessary files on your computer, click **Next**, then click **Install**.
7. To complete the installation process, click **Finish**. A pop-up message will then appear and inform you to restart the computer.
8. Click **Yes** to restart the computer.

Note: *It is very important to restart at this time to avoid possible configuration problems!*

## ***Installing DSIClient Application (Optional)***

The DSIClient application provides a convenient means to test operation of the DIALePay server and the store LAN configuration. It is not suitable for normal transaction processing since it cannot print drafts or receipts. Your POS system should be used for normal transaction processing through DIALePay.

To install the *DSIClient application* (includes the DSIClientX ActiveX control):

1. Open the DSIClient folder on the *DIALePay* 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.

## ***Installing ePay Administrator for DIALePay (Required)***

*Note: The ePay Administrator for DIALePay software is designed to use the LAN to perform transaction editing and reporting. Best security practices advise that you to install the ePay Administrator for DIALePay software on a workstation on the LAN, not on the server.*

To install *ePay Administrator for DIALePay*:

1. Open the ePayAdmin folder on the *DIALePay* 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**.
5. If the option is available, make the application available to all users.
6. To begin installing the necessary files on your computer, click **Next**, then click **Install**.
7. To complete the installation, click **Finish**. A pop-up message will then appear and inform you to restart the computer.
8. Click **Yes** to restart the computer.

For information about using *ePay Administrator*, refer to the *ePay Administrator User Guide*.

## ***Installing DataTran Setup Software (Optional)***

To install *DataTran Setup Software*:

1. Open the *DataTran Setup Software* folder on the *DIALePay* CD-ROM and double-click **setup.exe**.
2. The installation wizard will start. When the Welcome screen appears, click **Next**.
3. Enter your **User Name** and **Organization** and click **Next**.
4. To select the default destination directory (recommended), click **Next**. To select a different directory, click **Browse**.
5. To add the *DataTran Setup Software* program icons to the Program Folder shown (recommended), click **Next**.

**NOTE:** You can also enter a new Program Folder name or select another existing folder name.

6. The installation wizard will then display your selections, Click **Next** to begin the installation process.
7. After installation is complete, you will be prompted to restart your computer.
8. Select **Yes**, then click **Finish**.
9. To complete the installation, click **Finish** again.

## ***Installing Windows 98 Y2K Updates (As Needed)***

**Note:** The *DIALePay* server software is not designed for operation on Windows98. Windows98 systems should install only the *DSIClient* or *ePay Administrator* for *DIALePay* software.

For Windows 98 users, installation of MDAC 2.7 requires Y2K updates to be installed. Install the original Y2K update first, then install the update.

1. Open the **Windows 98 Y2K Updates** folder on the *DIALePay* CD-ROM and double-click **setup.exe**.
2. The installation wizard will start. Follow the on screen instructions.
3. After installation is complete, you will be prompted to restart your computer.
4. Select **Yes** then click **Finish**.

---

# ***DIALePay* CONFIGURATION**

## ***Introduction***

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

*DIALePay* is provided as a fully functional software application for 10 calendar days before requiring entry of an activation code by Datacap Systems.

If *DIALePay* has not been activated by Datacap within those 10 days, it will decline all requests and return a “Must Activate *DIALePay*” 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, *DIALePay* will decline all requests and return a “Must Activate *DIALePay*” message until an activation code is entered.

## ***Activation***

During program launch, *DIALePay* generates a Session Code and Machine ID that are unique to that PC and required for permanent operation of *DIALePay* 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 **DIALePay Activation** in the Subject line. The body of the message should contain:

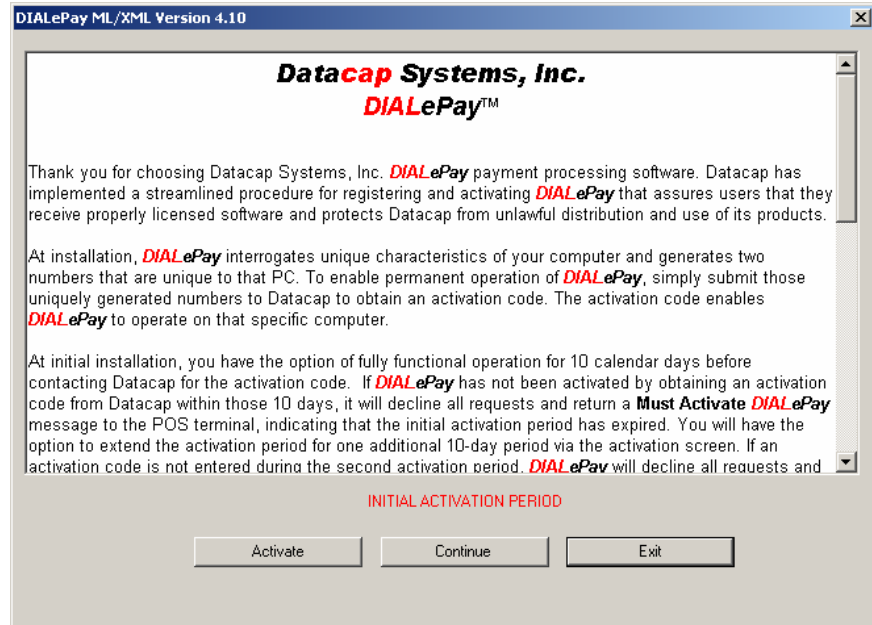
- a) Your Name
- b) Telephone Number
- c) Serial Number
- d) Session Code
- e) Machine ID

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

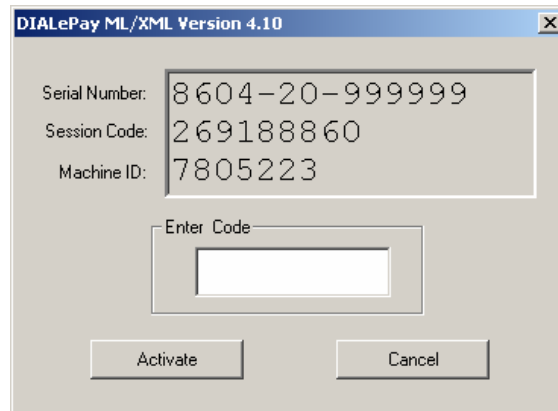
To activate and set up *DIALePay* for use:

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

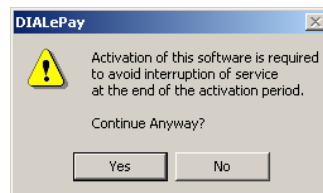


**NOTE:** The Initial Activation dialog box will appear each time you start *DIALePay* until you activate it.

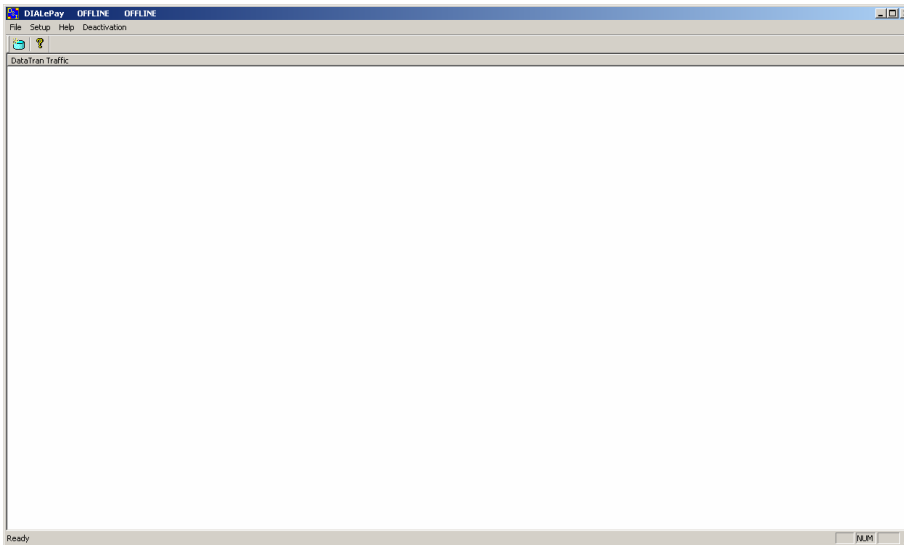
2. To enter the activation code, click **Activate**. When the activation dialog box appears, type the activation code in the box provided and click **Activate**



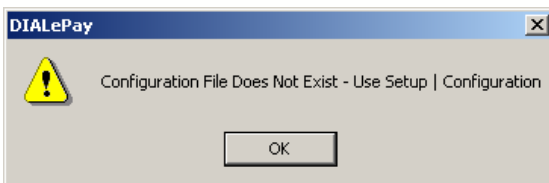
3. To proceed without activation, click **Continue**. When the message indicating that activation is required to avoid interruption of service appears, click **Yes** to continue.



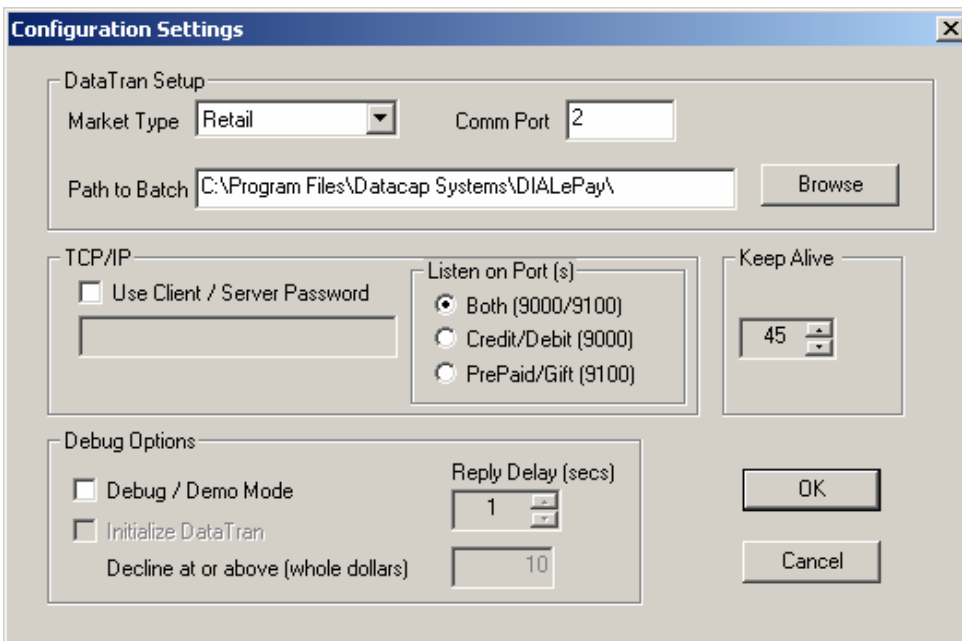
4. In either case, the *DIALePay* status screen appears.



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



5. From the *DIALePay* menu bar, select **Setup** and choose **Configuration**. The Configuration Settings dialog box appears.



6. Under **DataTran Setup**, make the following choices:
- Select one of the following **Market Types** (it must match the Merchant Category programmed into the DataTran):

- Retail
- Restaurant
- Direct Marketing
- eCommerce

**NOTE:** *Not all market types may be available from your payment processor.*

- b) In the **Comm Port** box, type the number of the serial port that you will use to connect the DataTran.
7. If you installed DIALePay in its default location

**C:\Program Files\Datacap Systems\DIALePay\**

then the entry in the **Path to Batch** box should be correct. If the Path to Batch box is empty, then click the Browse button to navigate to the file **dtbatch.mdb** which is inside the DIALePay folder.

8. Under **TCP/IP**, make the following choices:
  - a) If you are using *DIALePay* in a Wide Area Network (WAN) that uses an Internet connection, you should enable Client/Server password protection to prevent unauthorized use of *DIALePay*.  
  
To enable client/server password usage, under **TCP/IP**, check the **Use Client / Server Password** box, then type the client/server password in the box provided.  
  
**NOTE:** *You must also configure DSIClientX and ePay Administrator for Client/Server password protection with the same password to use this function.*
  - b) In the **Listen on Port(s)** box, the option Both (9000/9100) should normally be selected. The exception to this is if you will be using a GIFTePay server on the same hardware. In this case one DIALePay would be used to process credit/debit cards on port 9000 and the other would process gift or prepaid card transactions on port 9100.
9. The **Keep Alive** box should be left at the default value of 45 (sec). In rare situations of high transaction load or slow processor communications, it may be necessary to set this value lower to eliminate lost TCP socket errors.
10. The **Debug/Demo Mode** checkbox should *only* be checked for *testing*. When Debug/Demo Mode is selected, transactions are not actually processed by the DataTran. ***It is very important that Debug/Demo Mode is unchecked for actual production use, because transactions will not be paid to the merchant's account!***
11. After completing the configuration settings, click **OK** to save the settings and exit the dialog box.

# Testing DIALePay

After you configure *DIALePay*, you can perform the following tests using the *DSIClient Transaction Utility* to determine if the system is working properly.

## LAN Test

This test enables you to test *DIALePay* in a Local Area Network without DataTran dialing out and connecting to a payment processor.

### To perform a LAN test:

#### A. At the server:

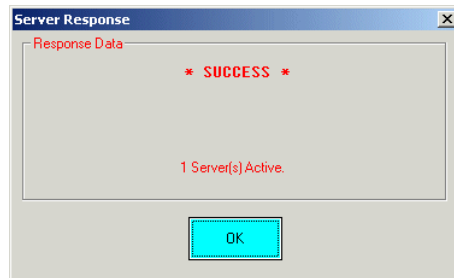
1. Launch *DIALePay* and enable Debug Mode from the Setup menu.
2. Retrieve the Server's IP address.

**NOTE:** If the IP Address is unknown, start the DOS Command Prompt and enter **IPCONFIG**.

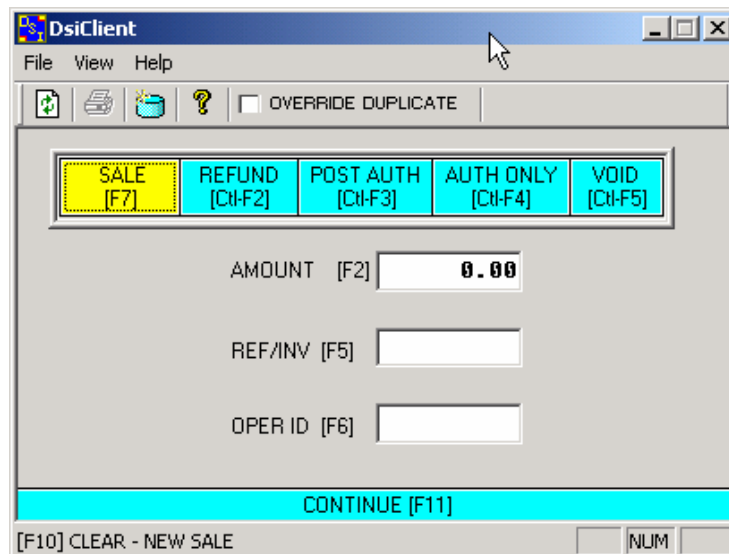
#### B. At the client machine:

1. Install *DSIClient* (refer to the installation of *DSIClient* application section in Chapter 3).
2. Launch the *DSIClient* application.
3. When the *DSIClient* dialog box appears, select **File** from the *DSIClient* menu bar, and choose **Setup**. The Configuration Settings dialog box appears.

4. Under **TCP/IP Settings** in the **Server IP Address** box, type the IP address of the server (the PC where *DIALePay* is installed).
5. Under **Merchant Settings**, select **Retail** as the **Merchant Category** and type `LocalServer` in the **Merchant ID** box and 0001 in the TerminalID box.  
*NOTE: The DSIClient Transaction Utility only supports the Retail Merchant Category.*
6. If you enabled *DIALePay* 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.
7. Click **Ping Server**. If a successful connection is made, a response message appears. It should show at least one active server.

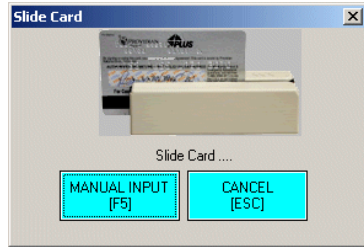


8. Click **OK** to continue.
9. To save the settings and exit the Configurations Settings, click **OK**, The DSIClient dialog box reappears.



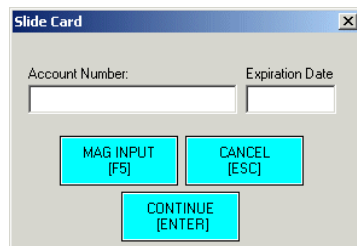
10. Enter the following information, then click **CONTINUE**:
  - a) **AMOUNT** – enter a dollar amount, such as \$1.00. If the amount equals or exceeds the “decline” amount entered in the *DIALePay* Configuration settings, the system will decline the transaction.
  - b) **REF/INV** – the Reference/Invoice number is optional, you can enter any number, up to 10-digits.
  - c) **OPER ID** – the Operator ID is optional, you can enter any number, up to 10-digits.

The Slide Card dialog box appears.

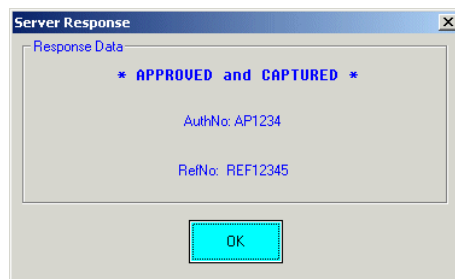


11. Click **MANUAL INPUT**. The Slide Card dialog box will then prompt you to enter an **Account Number** and **Expiration Date**.

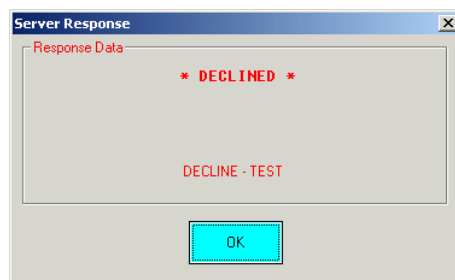
**NOTE:** You can use any 16-digit number for the account number. For the date, enter a 4-digit number using the format: MMY (Month, Year) for this test.



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



**NOTE:** If you enter an amount that meets or exceeds the whole dollar amount entered in the DIALePay Configuration Setting, DIALePay will decline the transaction.



In either case, you have verified that the LAN is set up properly for DIALePay operation.

13. Click **OK** to continue.

# Live Testing

## Before You Start

You should arrange with your bank and payment processor for testing *DIALePay* 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.

**It is the sole responsibility of the merchant account holder to verify that the merchant information loaded into their DataTran, or systems utilizing DataTran, 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.**

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 into DataTran devices or systems utilizing DataTran devices.

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.

## DataTran Parameter Verification

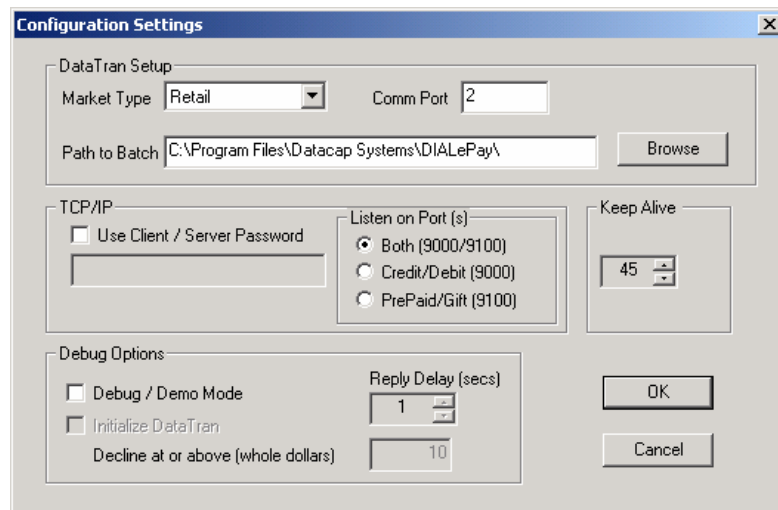
You should verify that the DataTran has the proper payment application network and merchant parameters loaded before you perform test transactions. Contact your Datacap dealer for information on the DataTran load configuration. Most Datacap resellers arrange to have the DataTran configured prior to installation.

## DataTran Setup and Initialization

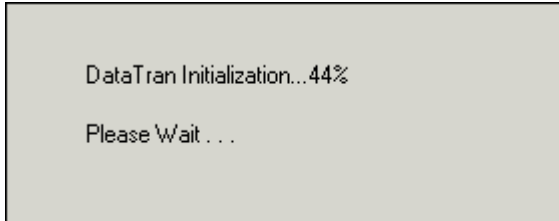
Once you verified the DataTran has the correct parameters, you can set up the DataTran to work with the *DIALePay* server.

To set up your DataTran to work with the *DIALePay* server:

1. Connect your DataTran to an available serial port on your server
2. Launch *DIALePay*.
3. From the *DIALePay* menu bar, select **Setup** and choose **Configuration**. The Configuration Settings dialog box appears.



4. Assure that Debug Mode is off by clearing the **Debug/Demo Mode** box. ***It is very important that Debug/Demo Mode is unchecked for actual production use, because transactions will not be paid to the merchant's account.***
5. Verify that all other inputs are correct according to the installation performed in Chapter 4.
6. Click **OK** to save the settings and exit the Configuration Settings dialog box.
7. *DIALePay* will then attempt to initialize the DataTran.



8. After a successful initialization attempt, the main *DIALePay* dialog box will reappear.
9. Close *DIALePay*.

## ***Entering Test Transactions***

Before using DataTran or systems utilizing DataTran to process live payments, you should first verify your merchant parameters for proper operation using the following procedure:

10. At the server, launch *DIALePay*.
11. On a client machine, enter a sale and return test transaction of \$1.00 for each card type you will be accepting. You should use your POS system to enter these transactions if possible. This will validate that your POS software is correctly configured to use *DIALePay*. If you are unable to use your POS software, you should use the *DSIClient* application as described in the LAN Test portion of this chapter.
12. Settle the batch containing the test transactions using *ePay Administrator*.
13. Verify with the merchant service provider that all the test transactions are processed to the merchant's account (this may require one to three business days).