



IP/Dial Bridge XML™

Installation & Configuration Guide

Version 4.26

***IP/Dial Bridge XML for
Mercury Payment Systems***

Part Number: 8660.30

IP/Dial Bridge 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 98, Windows 2000 Professional, Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista and Windows 7 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.

Printed in the United States of America

Revised: 21 January 2010

Version Support

This document supports the following application versions:

IP/Dial Bridge for Mercury Payment Systems, Version 4.26

DSIClientX, Version 3.85

DSIClient Transaction Utility, Version 2.50

Payment Processor Support

This document supports the following payment processor:

Mercury Payment Systems

CONTENTS

Overview	5
Introduction	5
About IP/Dial Bridge for Mercury	5
About Datacap	5
What's Included on your CD	5
How it works	5
Security Considerations.....	7
Introduction	7
IP/Dial Bridge Compliance	8
POS System Considerations.....	8
Networking Considerations	8
What's at Stake for Merchants	8
Security Action Plan	8
More Information	9
Installation	10
Introduction	10
Requirements.....	10
Server Requirements	10
Network Requirements	11
Installation Procedures.....	11
Accessing the IP/Dial Bridge CD-ROM.....	11
Installing/Upgrading Microsoft Internet Explorer.....	13
Installing IP/Dial Bridge (Required).....	14
Installing DSIClientX (As Required).....	14
IP/Dial Bridge Configuration & Testing.....	15
Introduction	15
Activation.....	15
Configuration.....	16
Testing	19
Important! - Before You Start.....	19
Using the DSIClient Transaction Utility	20
Introduction	20
Supported Transaction Types.....	20
DSIClient Transaction Utility Setup	21
Verifone PINpad 2000 Setup	22
PDC Setup	23
Processing Transactions.....	25
Index.....	28

OVERVIEW

Introduction

About *IP/Dial Bridge for Mercury*

Developed by Datacap Systems, *IP/Dial Bridge* enables Windows-based POS systems to add dial backup capability to the IP processing through *DSIClientX* for Mercury Payment Systems.

IP/Dial Bridge is multi-threaded to accept simultaneous requests from multiple clients, and supports automatic failover to dial when IP services are disrupted.

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

- ***IP/Dial Bridge*** – server-side software that enables you to process payment authorization requests via the Internet and dial phone lines to Mercury Payment Systems..
- ***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 *IP/Dial Bridge* 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 *IP/Dial Bridge*.

How it works

IP/Dial Bridge is an application that executes on a server at the store level and monitors transaction requests from client machines using a POS application integrated with *DSIClientX*, Datacap's XML ActiveX control.

When *IP/Dial Bridge* receives an encrypted transaction request from a client machine, it sends the request to Mercury Payment Systems for approval via the Internet or other TCP/IP Virtual Private Network (VPN) services.

If the *IP/Dial Bridge* system cannot deliver the transactions to Mercury due to some IP related failure, it will automatically utilize an attached **DialLink**[™] modem from Datacap to communicate directly over normal phone lines to Mercury's dial processing system. Datacap's *DialLink* modem is a DataTran but rather a V.22bis modem which has been optimized for use with Datacap's *IP/Dial Bridge* software for fast connections to Mercury.

IP/Dial Bridge supports multitransaction operation which allows multiple transactions to be processed during a single phone connection with Mercury. When transactions are waiting on the POS system, this feature can provide processing throughput close to IP speeds.

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

IP/Dial Bridge Compliance

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

- **IP/Dial Bridge** does not store any magnetic stripe (Track 1 or 2), card verification (CVV, CVV2, etc.) or PIN data, ever.
- **IP/Dial Bridge** logs only record truncated account number and expiration date information and never records any magnetic stripe (Track 1 or 2), card verification (CVV, CVV2, etc.) or PIN data, ever.
- **IP/Dial Bridge** encrypts all transmissions which contain cardholder data.

POS System Considerations

Although **IP/Dial Bridge** 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

IP/Dial Bridge 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 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

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

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=I2/business/accepting_visa/ops_risk_management/cisp_merchants%2Ehtml|Assessors

INSTALLATION

Introduction

This chapter explains how to install and configure the following *IP/Dial Bridge* components.

- *IP/Dial Bridge*
- *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 – see your POS documentation for the specific requirements for your implementation.

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

Server Requirements

To successfully install and run *IP/Dial Bridge* 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 Server 2003 or 2008 or Windows 7. All latest updates and hotfixes should be applied.
- 1 GB of RAM minimum, 2 GB 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
- Datacap DialLink modem
- Persistent Internet Connection (DSL, cable, frame relay, etc.)

Network Requirements

Before installing *IP/Dial Bridge* 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 *IP/Dial Bridge* server available for incoming traffic if you are behind a firewall and connected to the default port.

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.

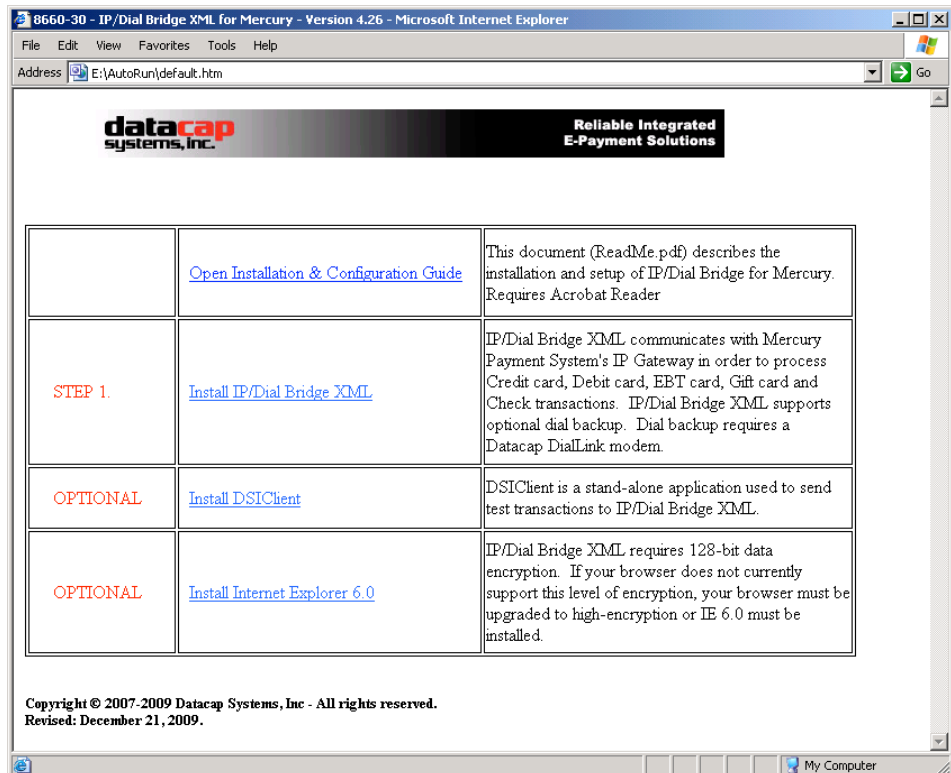
Installation Procedures

Accessing the IP/Dial Bridge CD-ROM

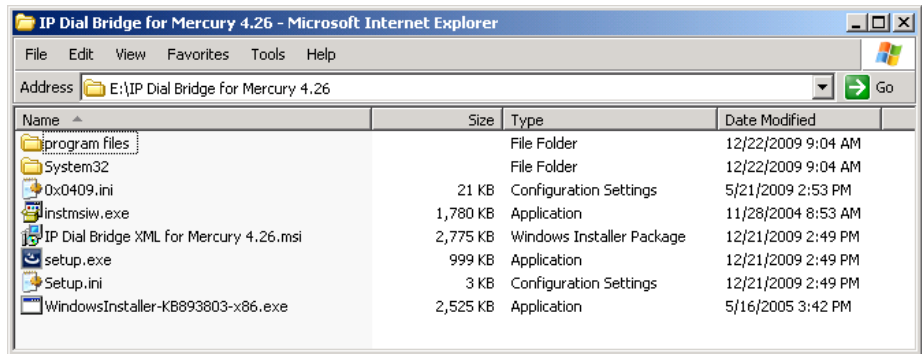
Before you begin installing *IP/Dial Bridge* and its components, you should close all unnecessary programs and disable any anti-virus software.

Use either of the following procedure to access the folders that contain the setup programs for *IP/Dial Bridge* and its components:

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



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



From either of these windows, you can install *IP/Dial Bridge* and its components.

Installing/Upgrading Microsoft Internet Explorer

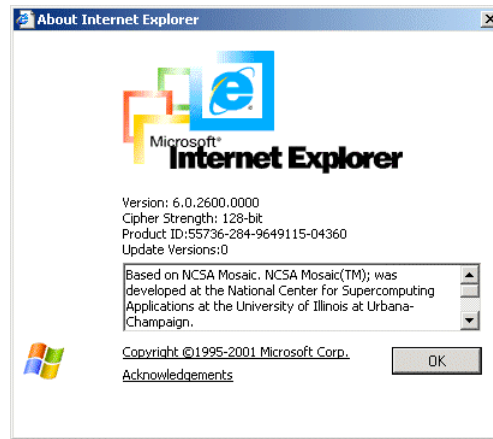
If needed, you can install or upgrade your server and each computer on the LAN with a version of Microsoft Internet Explorer that supports 128-bit encryption.

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 *IP/Dial Bridge* CD-ROM.

Determining the Encryption Strength

To determine if a PC has the necessary encryption to run *IP/Dial Bridge*:

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:

1. Open the Microsoft Internet Explorer folder on the *IP/Dial Bridge* 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 IP/Dial Bridge (Required)

To install the IP/Dial Bridge Server software:

1. Open the IP/Dial Bridge Server folder on the *IP/Dial Bridge* 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 (As Required)

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

1. Open the DSIClient folder on the *IP/Dial Bridge* 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.
If available on your operating system, make the application available to all users.
6. Click **Next**, then click **Install**. The installation wizard will then begin installing the necessary files on your computer.
7. Click **Finish** to complete the installation. A pop-up message will then appear and inform you to restart the computer.
8. Click **Yes** to restart the computer.

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 *IP/Dial Bridge* server.

IP/Dial Bridge CONFIGURATION & TESTING

Introduction

This chapter explains how to activate and configure *IP/Dial Bridge* for use.

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

Activation

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

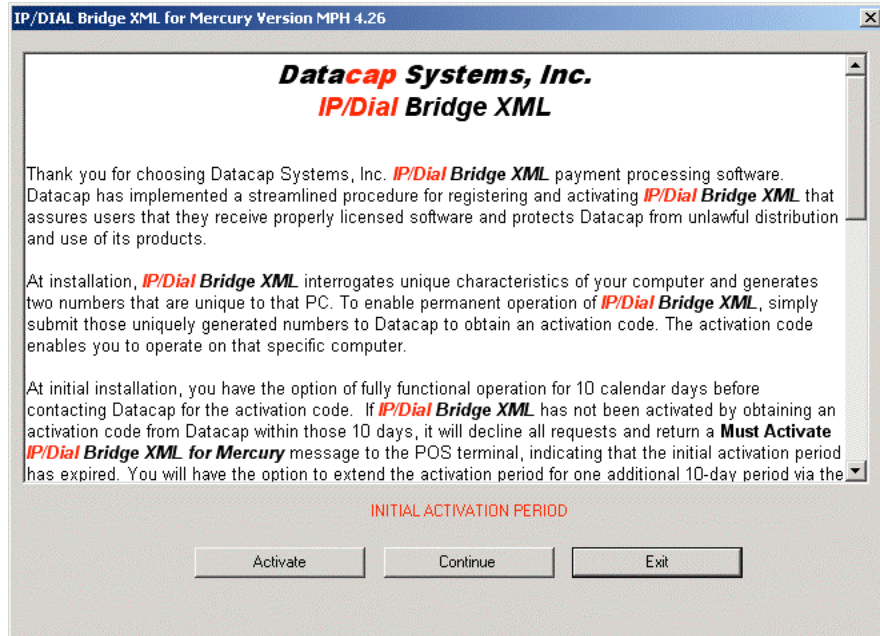
1. Your Name
2. Telephone Number
3. Serial Number
4. Session Code
5. Machine ID

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

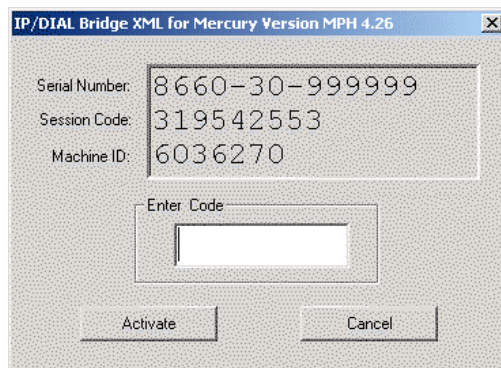
To activate and set up *IP/Dial Bridge* for use:

1. From the Desktop, double-click the **IP/Dial Bridge icon** The Initial Activation dialog box appears.

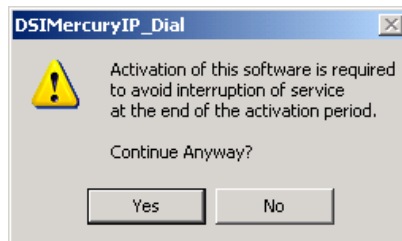


NOTE: The Initial Activation dialog box will appear each time you start *IP/Dial Bridge* until you activate it.

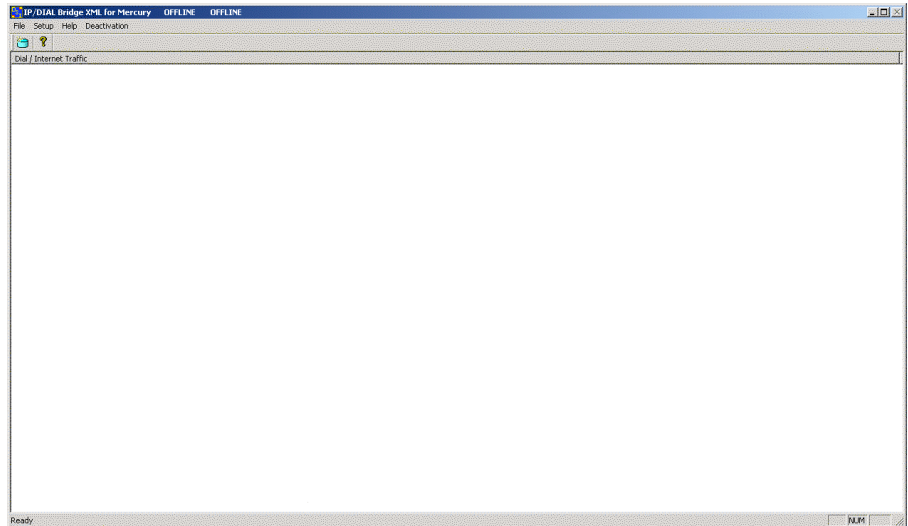
2. To enter the activation code, click **Activate**. When the activation dialog box appears, type the activation code in the box provided and click **Activate**



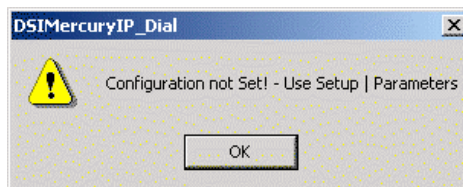
3. To proceed without activation, click **Continue**. When the message indicating that activation is required to avoid interruption of service appears, click **Yes** to continue.



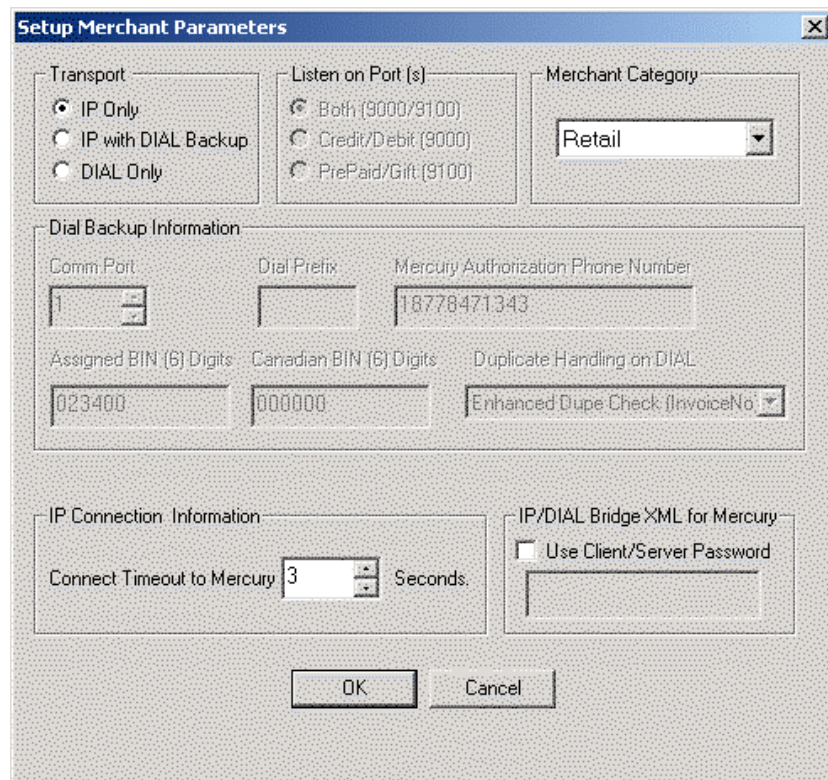
4. In either case, *IP/Dial Bridge* appears.



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



5. From the *IP/Dial Bridge* menu bar, select **Setup** and choose **Merchant Parameters**. The Setup IP/Dial Bridge Parameters dialog box appears.



6. Under the **Transport** section, select the desired mode of communications from the store to Mercury. If **IP Only** is selected, *IP/Dial Bridge* will not use dial up phone line to send transactions to Mercury even if it is operational; all transactions will go via IP on the Internet connection. If **Dial Only** is selected, *IP/Dial Bridge* will not use the Internet connection to send transactions to Mercury even if it is operational; all transactions will go via dial up. If **IP with Dial Backup** is selected, *IP/Dial Bridge* will attempt to use the Internet connection first on every attempt to send transactions to Mercury; if the Internet connection is down, *IP/Dial Bridge* will use dial up via the *DialLink* modem.
7. Under the **Listen on Port(s)** section, ports 9000 and 9100 are selected by default and cannot be changed.
8. Under the **Merchant Category** section, select the category assigned by Mercury Payment Systems. The possible choices supported are:
 - Retail
 - Restaurant
9. The **Dial Backup Information** section contains information required to use the phone line if you have selected either **Dial Only** or **IP with Dial Backup** as the transport option.

In the **Comm Port** box, select the PC serial port to which the DialLink modem is attached.

In the **Dial Prefix** box, enter any required dialing sequences to get an outside line. Typical values are 8, or 9, but you should verify your specific requirements with your phone equipment provider.

The **Mercury Authorization Phone Number** is set at the default value of 18778471343. Do not change this number unless instructed to do so by Mercury Payment Systems support personnel.

The **Assigned BIN 6 digits** is set at the default value from of 023400. Do not change this number unless instructed to do so by Mercury Payment Systems support personnel.

The **Canadian BIN 6 digits** is only required if you will be processing Canadian debit card transactions. The value must be entered and will be supplied to you by Mercury Payment Systems support personnel if required.

The **Duplicate Handling on Dial** section allows the selection of the method of duplication transaction screening or to disable duplicate check completely. The default value for **Duplicate Handling on Dial** is set to **Enhanced Dupe Checking {Invoice No.}**. Do not change this method unless instructed to do so by Mercury Payment Systems support personnel.
10. Under the **Security** section, you may select whether you want to use a password protection on communications between clients and the server. If you are using *IP/Dial Bridge* in a Wide Area Network (WAN) that uses an Internet connection, you should enable Client/Server password protection to prevent unauthorized use of *IP/Dial Bridge*. 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.
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 Mercury Payment Systems for testing *IP/Dial Bridge* 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 *IP/Dial Bridge* 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.

Operational Considerations

Important!

IP/Dial Bridge 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 IP/Dial Bridge operation and prevent possible loss and/or corruption of transaction data.**

The following operational guidelines **must** be observed to ensure reliable IP/Dial Bridge operation:

- *Always* quit IP/Dial Bridge from the File|Exit pull down menu before restarting or shutting down Windows.
- *Always* quit IP/Dial Bridge and then shut down Windows before turning off the computer power. Never turn off the computer power without first quitting IP/Dial Bridge and shutting down Windows.
- *Always* quit IP/Dial Bridge 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 IP/Dial Bridge, you **must** procure unique terminal and/or merchant account information for each copy of IP/Dial Bridge from your processing provider. Operation of multiple copies of IP/Dial Bridge with identical merchant setup information may cause transactions to be lost or duplicated at your processing provider.

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 IP/Dial Bridge running.*

Supported Transaction Types

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

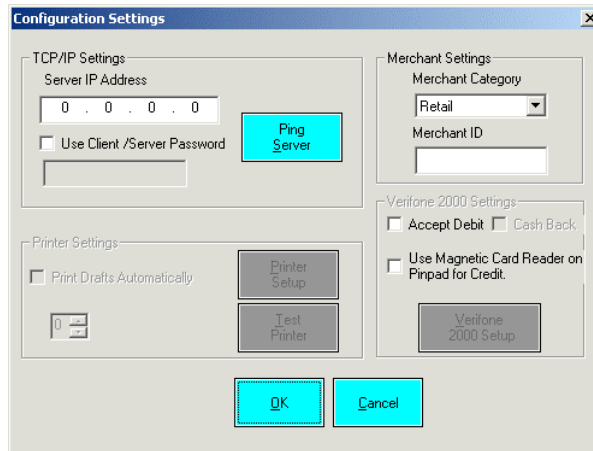
- **Credit Sale** – enables you to process a transaction for a payment for goods or services using a credit card (VISA, MasterCard, American Express, Discover, etc.).
- **Credit Refund** – enables you to issue a credit to the cardholder for the return or credit of goods or services using a credit card.
- **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

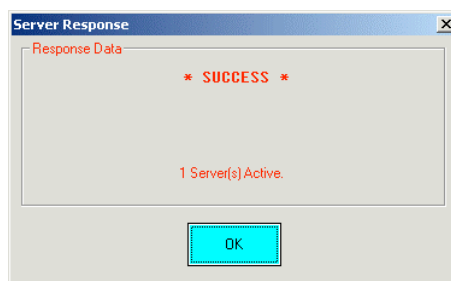
Before you can use the *DSIClient Transaction Utility*, you must configure it for use.

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.



2. Under **TCP/IP Settings** in the **Server IP Address** box, type the **IP Address** of the PC where *IP/Dial Bridge* is installed.
NOTE: If the *DSIClient Transaction Utility* and the *IP/Dial Bridge* are both installed on the same PC, use 127.0.0.1.
3. Under **Merchant Settings**, in the **Merchant ID** box, type “Local”.
4. If you enabled *IP/Dial Bridge* 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.
5. To test a connection to the server (the PC where *IP/Dial Bridge* is installed), click **Ping Server**. If a successful connection is made, a response message appears. It should show at least one active server.

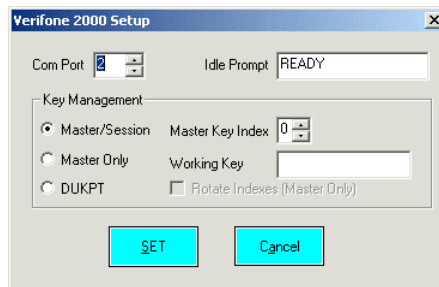


6. Click **OK** to continue.
7. If you enabled *IP/Dial Bridge* for client/server password usage, then under **TCP/IP**, check the **Use Client / Server Password** box and type the client/server password in the box provided.
8. To configure the Verifone PINpad 2000 for use with the *DSIClient Transaction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

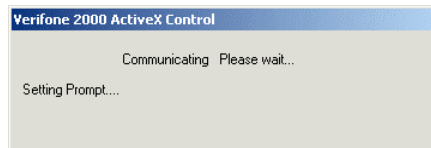
Verifone PINpad 2000 Setup

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.
 2. Under **Verifone 2000 Settings**, make the following choices:
 - A.1. To process debit transactions, check the **Accept Debit** box that appears
 - A.2. If you selected to accept debit and will offer cash back to the customer, check the **Cash Back** box.
 - A.3. 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.
3. Click **Verifone 2000 Setup**. 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.
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:
 - For all networks (except Nova), select **DUKPT**
 - For Nova, select **Master Only** and check the **Rotate Indexes** box
7. 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:

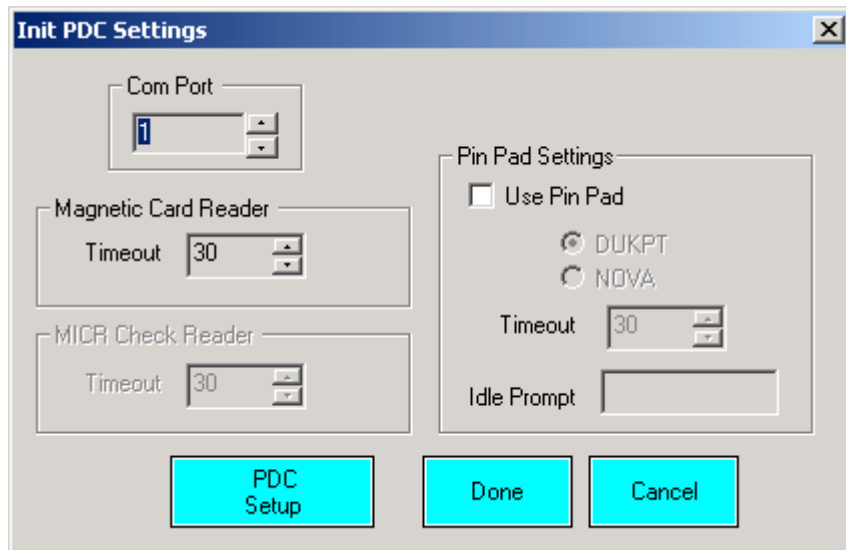


8. Click **OK** to continue.
9. To save the settings and exit the Configurations Settings, click **OK**.

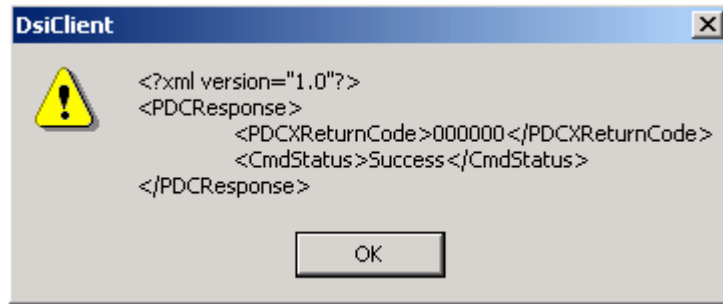
PDC Setup

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

- A.3.1.1.1.1.1. Connect the PDC to an available serial port and record the serial port number for later reference.
 - A.3.1.1.1.1.2. In the DSIClient Settings window, in the **PDC Settings** section, make the following choices:
 - A.4. To process debit transactions, check the **Accept Debit** box.
 - A.5. If you selected to accept debit and will offer cash back to the customer, check the **Cash Back** box.
 - A.6. 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.
2. Click the **PDC Setup** button. Init PDC Settings dialog box appears.



3. In the **Comm Port** box, select the number of the serial port that is connected to the PDC (1-255).
4. 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.
5. 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.
6. 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.

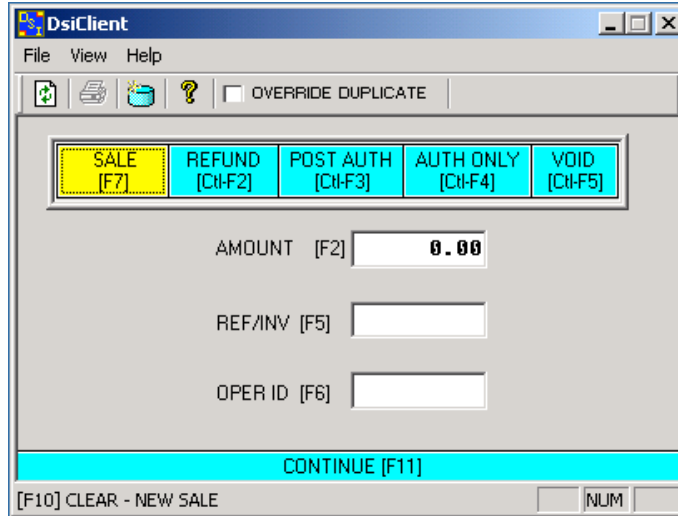
7. Click **OK** on the response.
8. Click **Done** on the **Init PDC Settings** window.
9. Click **OK** on the **Configuration Settings** window to get back to the *DSIClient Transaction Utility* main window.

Processing Transactions

In order to process a transaction using the *DSIClient Transaction Utility*, *IP/Dial Bridge* must be running on the server.

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

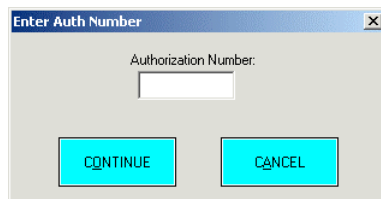
1. Launch *DSIClient*:



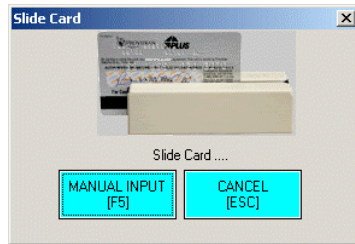
2. Using your mouse or action key(s), select the transaction type. The selected transaction type is then highlighted. The default transaction type is Sale (F7).
3. Type the transaction amount in the **AMOUNT** field
4. If needed (typically in Restaurant applications), type the check and/or the receipt number in the **REF NO/INV** box.

NOTE: *IP/Dial Bridge* does not currently support Restaurant applications

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 Transaction Utility* will prompt you for the entry of an authorization number.



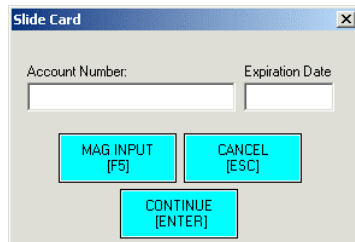
9. Type the number in the field provided, then click **CONTINUE** to proceed. The Slide Card dialog box appears.



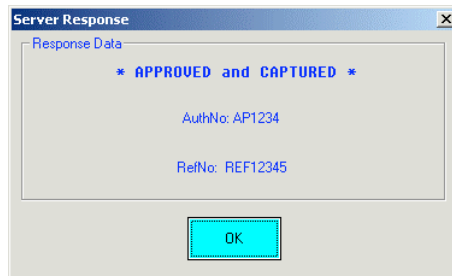
10. Either slide the credit card through the Verifone PINpad 2000's card reader or click **MANUAL INPUT**.

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

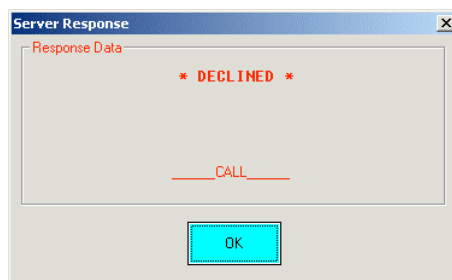
NOTE: When entering the date use the format: *MMYY (Month, Year)*.



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.
14. You can now process another transaction. Press **F10** to clear the form.

INDEX

About		
Datacap	5	
IP/Dial Bridge	5	
Credit Authorization Only	20	
Credit Post Authorization	20	
Credit Refund.....	20	
Credit Sale	20	
Credit Void	20	
Determining the Encryption Strength.....	13	
DSIClient Transaction Utility		
Installation	14	
Processing Transactions.....	25	
Setup	21	
Supported Transaction Types	20	
DSIClientX Installation	14	
How it works.....	5	
Installation	10	
Installation Procedures.....	11	
Accessing the IP/Dial Bridge CD-ROM.....	11	
DSIClient Transaction Utility.....	14	
DSIClientX	14	
Microsoft Internet Explorer	13	
IP/Dial Bridge	14	
Microsoft Internet Explorer		
Determining the Encryption Strength	13	
Installation.....	13	
IP/Dial Bridge		
Activation.....	15	
Configuration	16	
Installation.....	14	
Testing.....	18	
Network Requirements	11	
Override Duplicate.....	20	
Overview	5	
Requirements		
Network.....	11	
Server	10	
Server Requirements.....	10	
Upgrading Microsoft Internet Explorer	13	
Using the DSIClient Transaction Utility.....	20	
Verifone PINpad 2000 Setup	22, 23	
What's Included on your CD	5	