datacap systems, inc.

IP/Dial Bridge

Installation & Configuration Guide

IP/Dial Bridge
for Mercury Payment Systems

V 5.04

Part Number: 8660.30

IP/Dial Bridge Installation & Configuration Guide

Printed in the United States of America

Revised: 11 March 2013

Version Support

This document supports the following application versions:

IP/Dial Bridge for Mercury Payment Systems, 5.04

DSIClientX, Version 3.86

Payment Processor Support

This document supports the following payment processor:

Mercury Payment Systems

CONTENTS

CHAPTER 1

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 not 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 multi-tran 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.

CHAPTER 2

SECURITY CONSIDERATIONS

Introduction

Systems that 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 (DSS)***.

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** that are 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 be 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 3 rd party remote access software such as Remote Desktop (RDP)/Terminal Server, PCAnywhere, etc. requires that when such programs are used that there 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.

IP/Dial Bridge does not directly support remote access for maintenance, monitoring, operation, troubleshooting or updates. Datacap Systems does not use remote access software to deliver any services, software, or support to users of IP/Dial Bridge. If merchants, integrators or resellers elect to use third party remote access independent of IP/Dial Bridge, they should observe the following remote access procedures:

- *Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).*
- *Allow connections only from specific (known) IP/MAC addresses.*
- *Use strong authentication and complex passwords for logins according to PCI DSS Requirements 8.1, 8.3, and 8.5.8–8.5.15*
- *Enable encrypted data transmission according to PCI DSS Requirement 4.1*
- *Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13*
- *Configure the system so a remote user must establish a Virtual Private Network "VPN") connection via a firewall before access is allowed.*
- *Enable the logging function.*
- *Restrict access to customer passwords to authorized reseller/integrator personnel.*
- *Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.*

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/TPS 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.

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 that 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** truncates all account and expiration date information for transactions that have been settled in every area where it is either stored or displayed.
- **IP/Dial Bridge** encrypts account numbers and expiration dates for transactions that have not yet been settled.
- **IP/Dial Bridge** 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. IP/Dial Bridge logs are fixed in function, format and contents and cannot be disabled or configured by any user.
- **IP/Dial Bridge** 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.
- **IP/Dial Bridge** encrypts all IP transmissions that contain cardholder data using current SSL/TLS standards.
- **IP/Dial Bridge** does not allow or facilitate sending of PANs (Primary Account Numbers) by end user messaging technologies; however if a merchant, integrator or reseller transmits information of this type, a solution that implements strong cryptography should be employed.

Baseline System Configuration

To realize the maximum security from *IP/Dial Bridge*, 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 7, Windows Server 2003 or 2008. All latest updates and hotfixes should be applied.
- 2 GB of RAM minimum, 4 GB or higher recommended

- 20 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 IP/Dial Bridge 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 that 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 IP/Dial Bridge 5.0 implements all of the PCI Data Security Standard (DSS) requirements that 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 that 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 that handle cardholder data. You should verify with your POS system provider that the version of the POS software you are using is compliant.

Removal of Historical Data

No released versions of IP/Dial Bridge have ever stored any historical transaction data however logs are maintained for diagnostic purposes and should be removed. The following procedure should be executed to delete all previous IP/Dial Bridge logs:

1. Shut down **IP/Dial Bridge**
2. Using Windows Control Panel, select Add/Remove Programs
3. Select **IP/Dial Bridge** and remove it
4. Locate the **IP/Dial Bridge** folder in **<bootdrive>:/Program Files/Datacap Systems** and use a secure file deletion utility to remove it
5. Install **IP/Dial Bridge**

Information Handling and Collection Criteria

IP/Dial Bridge and all of its components handle sensitive cardholder data in accordance with the PA-DSS 1.2 standard of the PCI Data Security Council. However, IP/Dial Bridge does not monitor the activities of users or other software to assure that they accord sensitive data the same standards. Merchant, and reseller/integrators should adhere to the following guidelines if they handle cardholder information:

- Collect sensitive authentication only when needed to solve a specific problem.
- Store such data only in specific, known locations with limited access.
- Collect only the limited amount of data needed to solve a specific problem.
- Encrypt sensitive authentication data while stored.
- Securely delete such data immediately after use.

IP/Dial Bridge only stores cardholder information only for unsettled transactions. Once IP/Dial Bridge settles transactions, all cardholder information is either deleted or truncated. The merchant, integrator or reseller does not need to manage retention of cardholder data in IP/Dial Bridge beyond assuring that transactions are settled in a timely manner.

IP/Dial Bridge logs are fixed in function, format and contents and cannot be disabled or configured by any user. IP/Dial Bridge 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.

IP/Dial Bridge does not allow or facilitate sending of PANs (Primary Account Numbers) by end user messaging technologies; however if a merchant, integrator or reseller transmits information of this type, a solution that implements strong cryptography should be employed.

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.

Implementation Guide Reviews and Updates

Datacap Systems reviews the IP/Dial Bridge Implementation Guide and issues updates to maintain compliance at least once per year or whenever a software change warrants. This implementation guide is also incorporated as part of every IP/Dial Bridge Installation and User Guide. The latest version, which is supplied on the distribution CD, may also be downloaded from Datacap's site at www.datacapepay.com in the IP/Dial Bridge section separately at any time.

Development and Deployment of Security Updates

Datacap is committed to timely development and deployment of security patches. When a vulnerability is detected, we will develop and deploy an updated IP/Dial Bridge executable within 30 days of discovery. These updates will be delivered using a known chain of trust. A technical notice will be sent out via email and the update will be made available on our web site. The update file can then be downloaded directly. The update files are digitally signed to verify their authenticity.

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:

https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.html

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

A listing in PDF format 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

CHAPTER 3

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 you 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.
- 2 GB of RAM minimum, 4 GB or higher recommended
- 20 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.

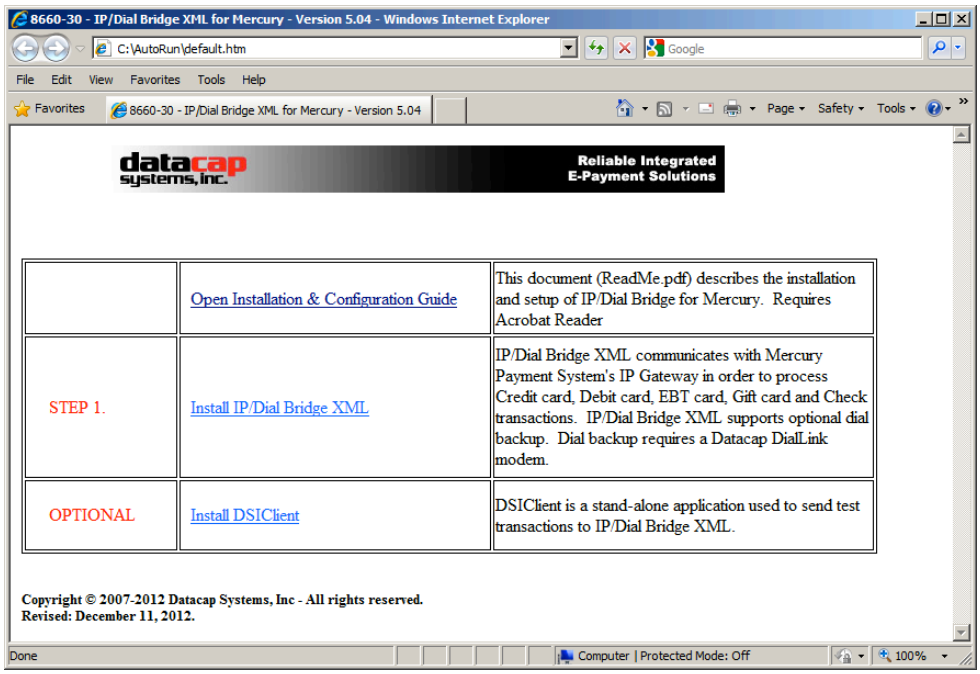
Installation Procedures

Accessing the IP/Dial Bridge CD-ROM

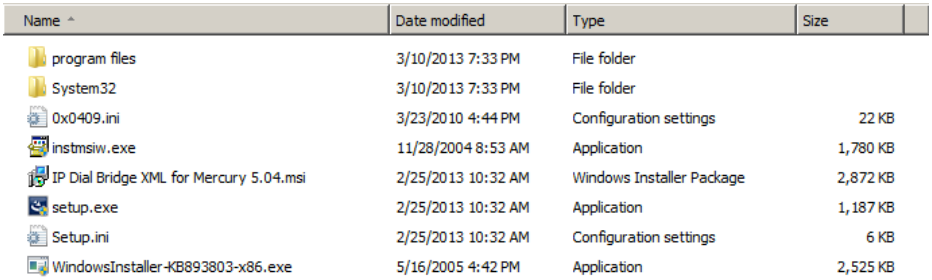
Before you begin installing *IP/Dial Bridge* and its components, you should close all unnecessary programs and disable any anti-virus software.

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.



Name	Date modified	Type	Size
program files	3/10/2013 7:33 PM	File folder	
System32	3/10/2013 7:33 PM	File folder	
0x0409.ini	3/23/2010 4:44 PM	Configuration settings	22 KB
instmsiw.exe	11/28/2004 8:53 AM	Application	1,780 KB
IP Dial Bridge XML for Mercury 5.04.msi	2/25/2013 10:32 AM	Windows Installer Package	2,872 KB
setup.exe	2/25/2013 10:32 AM	Application	1,187 KB
Setup.ini	2/25/2013 10:32 AM	Configuration settings	6 KB
WindowsInstaller-KB893803-x86.exe	5/16/2005 4:42 PM	Application	2,525 KB

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

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.*

CHAPTER 4

IP/Dial Bridge CONFIGURATION & TESTING

Introduction

This chapter explains how to activate and configure *IP/Dial Bridge for Mercury Payment Systems*.

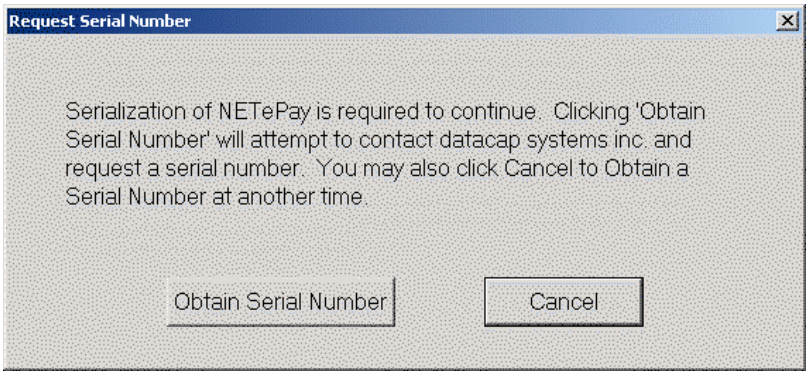
IP/Dial Bridge is activated and programmed over the Internet so a working Internet connection is required for the process.

Note
Firewalls, routers or other systems that can block IP network traffic must allow IP/Dial Bridge to accept traffic on port 9000.

IP/Dial Bridge must complete two actions on the Internet before it is ready to process transactions. The first is to obtain a license file from Datacap's PSCS (Payment Systems Configuration Server) system. The second is to retrieve merchant parameters from Datacap's PSCS server.

Activation and Parameter Download

1. On the first program launch after installation, *IP/Dial Bridge* must obtain a license file over the Internet from Datacap's PSCS (Payment Systems Configuration Server) system. When IP/Dial Bridge detects that a serial number is required, it presents the following dialog:

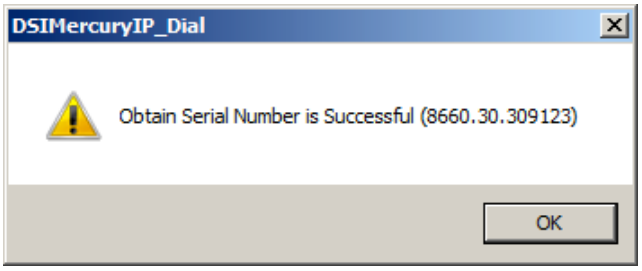


   Click 'Obtain Serial Number' to enable IP/Dial Bridge to contact PSCS for a serial number.

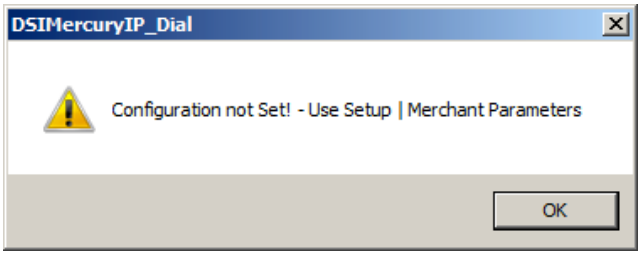
2. If IP/Dial Bridge is unsuccessful in obtaining a serial number, it will present the following dialog:

Click 'OK' and IP/Dial Bridge will close. Failure to successfully obtain a serial number means that IP/Dial Bridge was not able to contact Datacap's PSCS server over the Internet to obtain a serial number. Assure that the Internet connection is operating properly by using the default web browser on the machine where IP/Dial Bridge is installed to contact www.datacapsystems.com. If you are successful in contacting Datacap's website, close the browser, restart IP/Dial Bridge and click 'Obtain Serial Number' again. If you continue to experience difficulties in obtaining a serial number, contact your network administrator to assure that there are no firewall or DNS issues.

3. At this point, IP/Dial Bridge could present two possible responses. If *IP/Dial Bridge is successful in obtaining a serial number but is unable to locate merchant parameters for the assigned serial number*, you will see the following dialog:

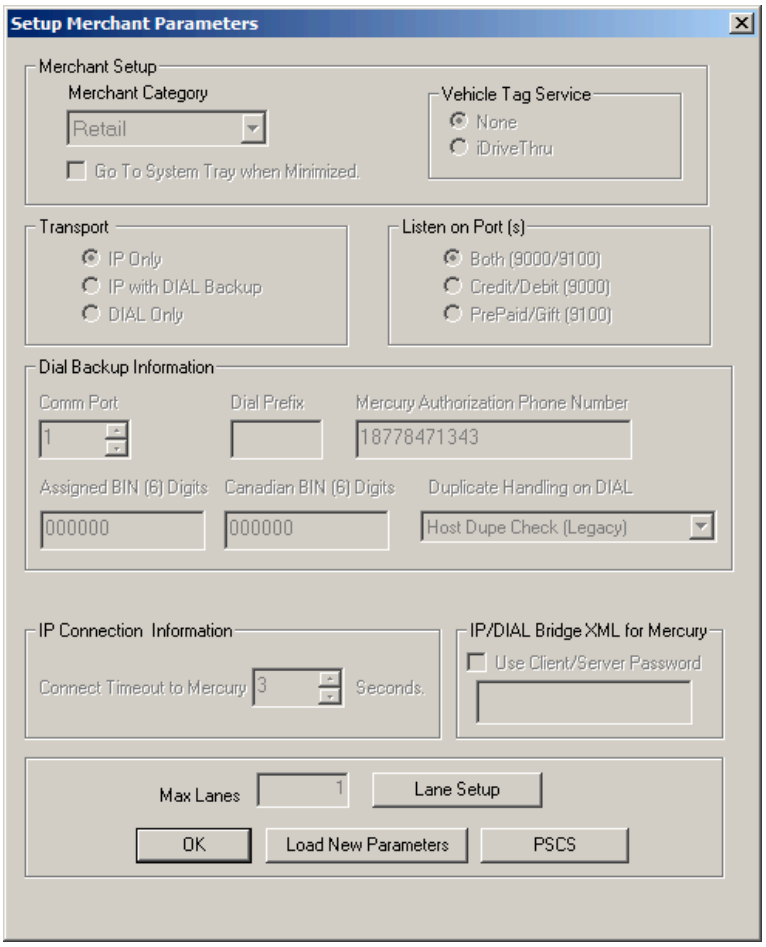


The dialog contains the 10-digit serial number that was automatically assigned to IP/Dial Bridge. Click 'OK' to continue and then you will see the following dialog:

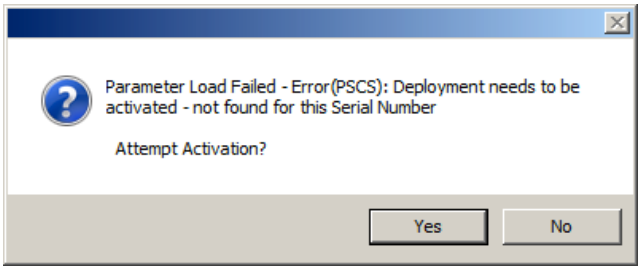


This dialog indicates that IP/Dial Bridge has not yet retrieved merchant parameters from Datacap's PSCS server and cannot operate until parameters are downloaded.

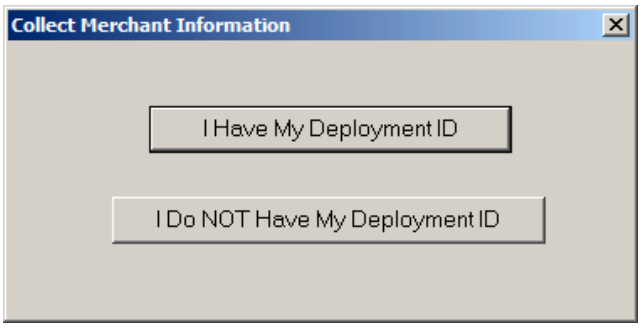
If a parameter file has been created on Datacap's PSCS server for the merchant account, then select 'Merchant Parameters' from the 'Setup' drop down menu. You will then see the following screen:



This setup screen displays the current values for the merchant parameters which are all 0's indicating that merchant parameters have not yet been loaded from Datacap's PSCS server. Click 'Load New Parameters' and you will see the following screen:

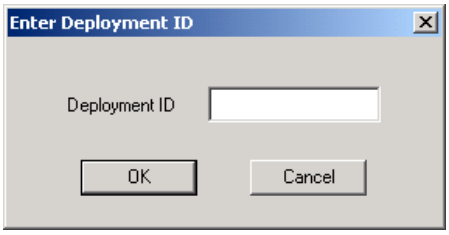


Click 'Yes' to attempt activation and you will see the following screen:



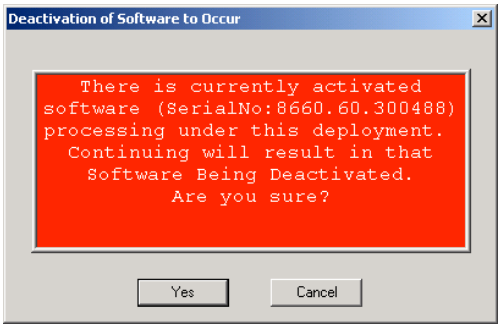
To continue, you must verify that you or someone else has created a Merchant Deployment on Datacap's PSCS server. If a deployment was created you may have been given a Deployment ID, which is typically an eight-character code that has been assigned to the merchant's parameters. If you have a Deployment ID for the merchant, click 'I Have My Deployment ID'. If the merchant's parameters were created on PSCS but you do not have the Deployment ID, proceed to step 4.

When you click 'I Have My Deployment ID', you will see the following dialog:



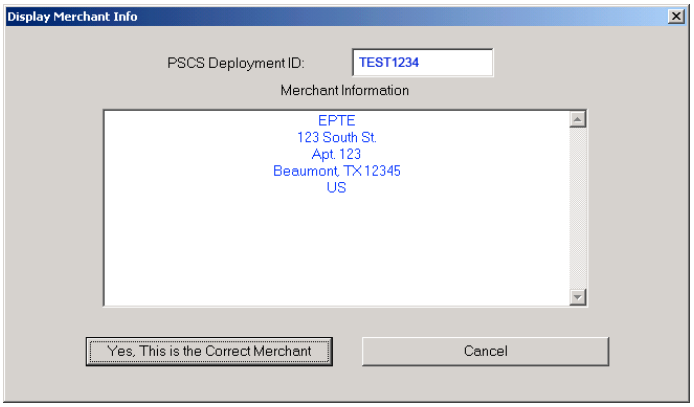
Enter the Deployment ID for the merchant parameter file and click 'OK'.

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



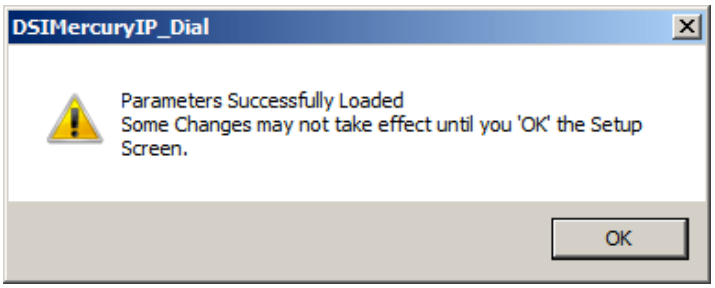
If you see this Deactivation Warning dialog, proceed to step 5.

IP/Dial Bridge will display a screen with merchant demographic data for you to verify as follows:

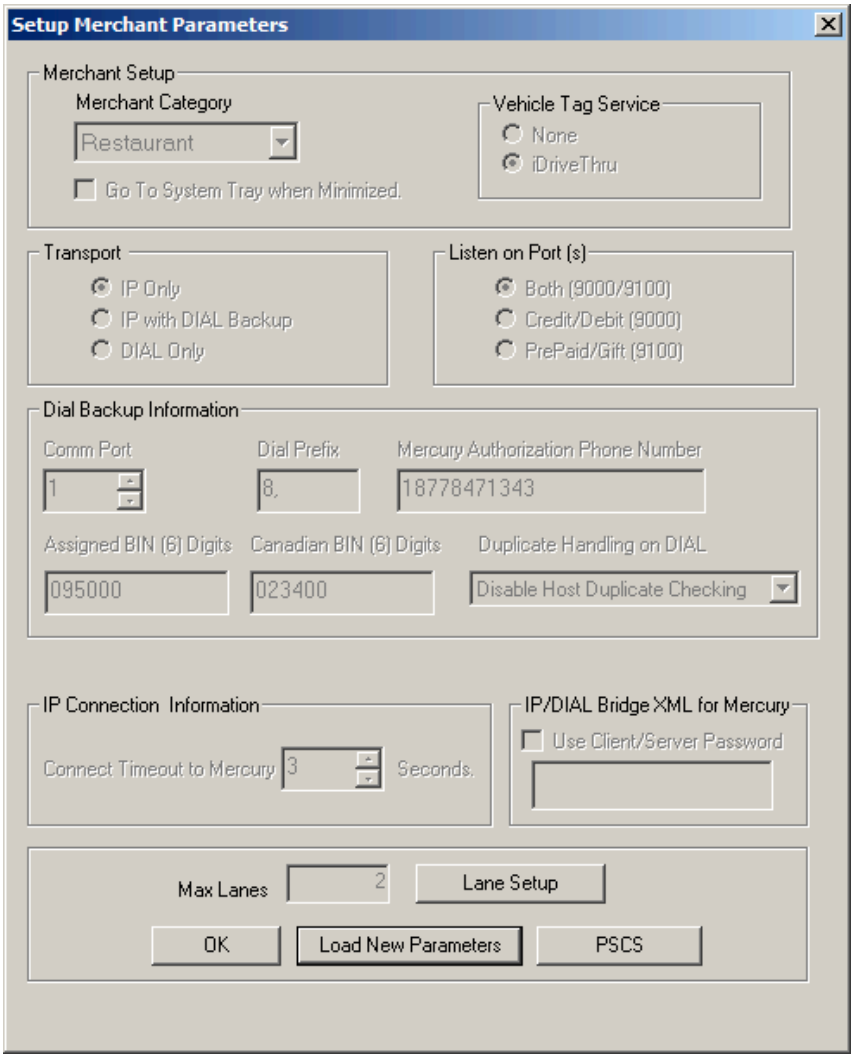


If the displayed information is not correct for the merchant site, click 'Cancel' and retry entry from the beginning of step 4. If the displayed information correctly identifies the merchant site, click 'Yes, This is the Correct Merchant'.

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

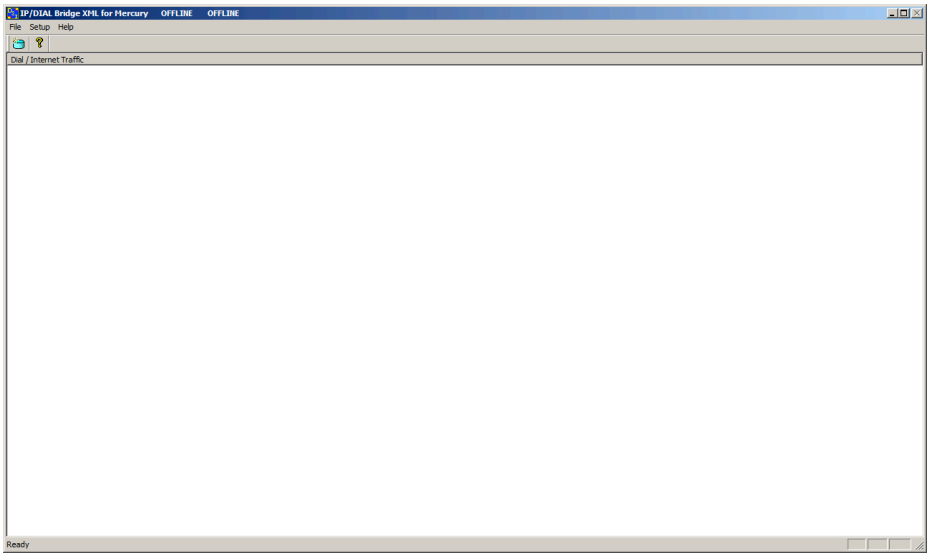


Click ‘OK’ and will then again see the setup screen as follows:



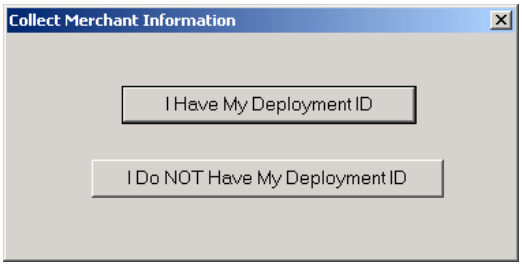
Lane Setup allows you to optionally change the description associated with each lane that was authorized in the PSCS parameter file. You cannot alter the number of lanes in IP/Dial Bridge; changes to the number of lanes must be done by editing the deployment file in PSCS.

The setup screen now contains non-zero values in the text boxes throughout the screen indicating the values retrieved from Datacap’s PSCS server. You should verify that the parameters are correct and then click ‘OK’ to complete the setup process. You will then see the IP/Dial Bridge main status window indicating that IP/Dial Bridge is now programmed and ready to process transactions.

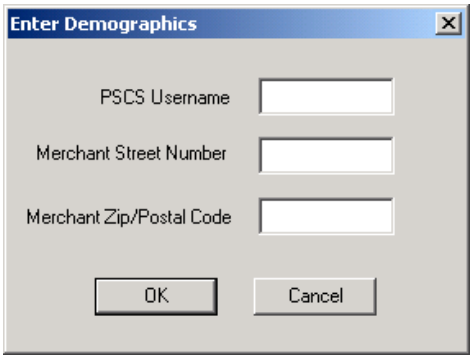


IP/Dial Bridge setup is complete.

4. If you don't have the PSCS Deployment ID for the merchant, click 'I Do NOT Have My Deployment ID' in the following dialog:



You will then see a dialog that will allow you to retrieve the PSCS merchant parameters from Datacap's PSCS server using merchant demographic information as follows:

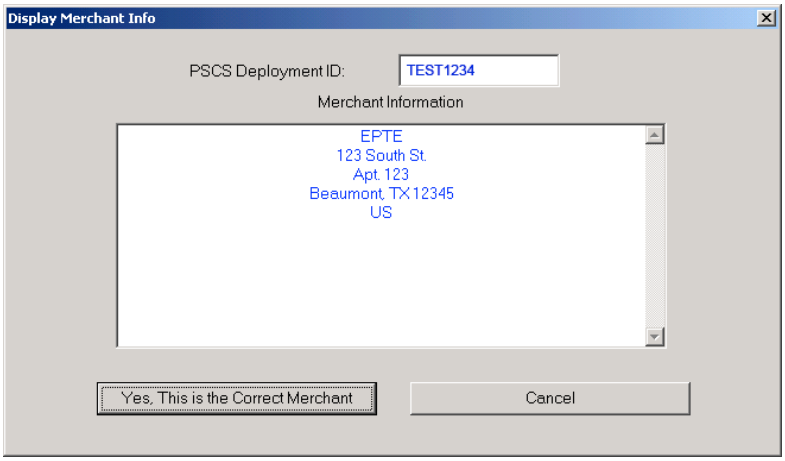


You need the following information to complete the demographics dialog entries:

- The PSCS user under which the merchant parameter file was created on the PSCS server
- The merchant location street number (e.g. enter '123' for 123 Main St.)
- The merchant location 5 digit zip code or 6 character Canadian postal code

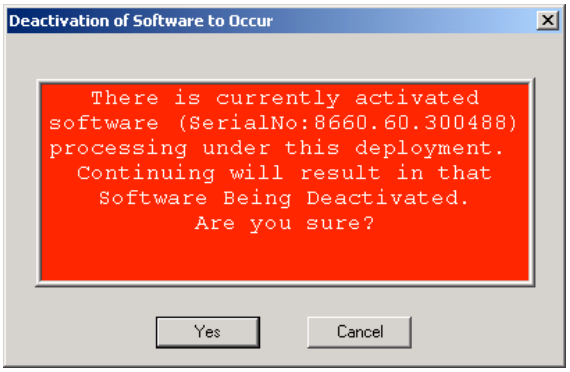
After entering this information, click 'OK'.

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



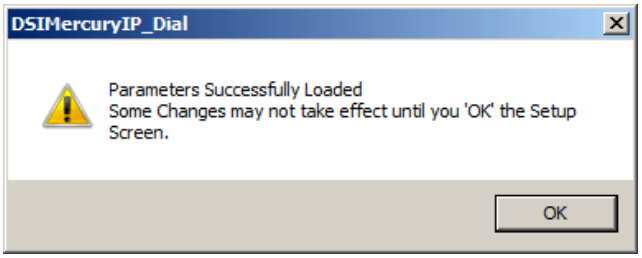
If the displayed information is not correct for the merchant site, click 'Cancel' and retry entry from the beginning of step 4. If the displayed information correctly identifies the merchant site, click 'Yes, This is the Correct Merchant'.

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

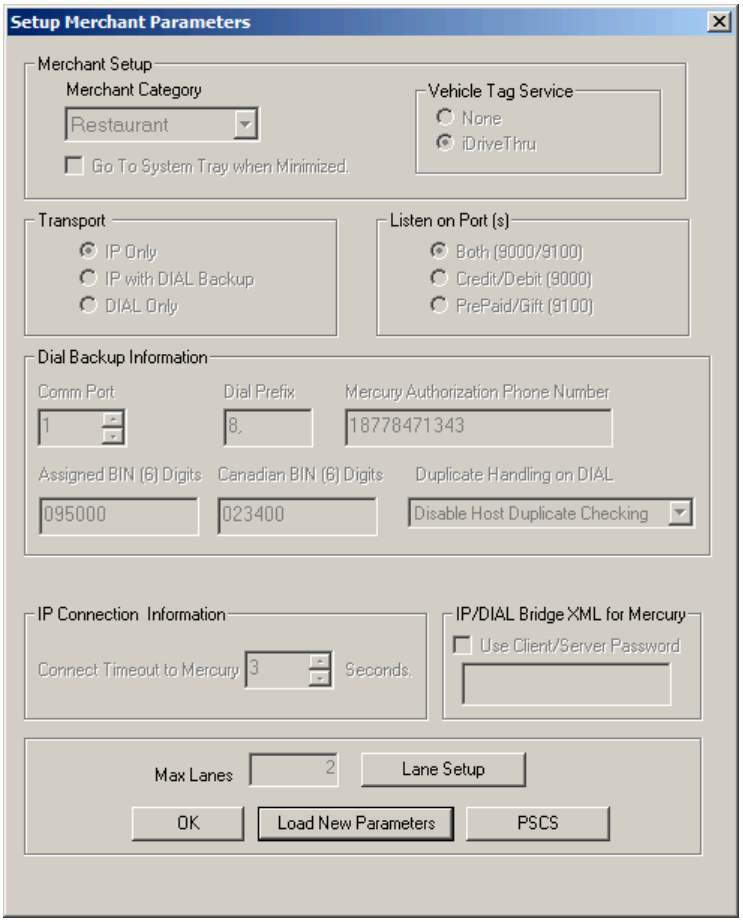


If you see this Deactivation Warning dialog, proceed to step 5.

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



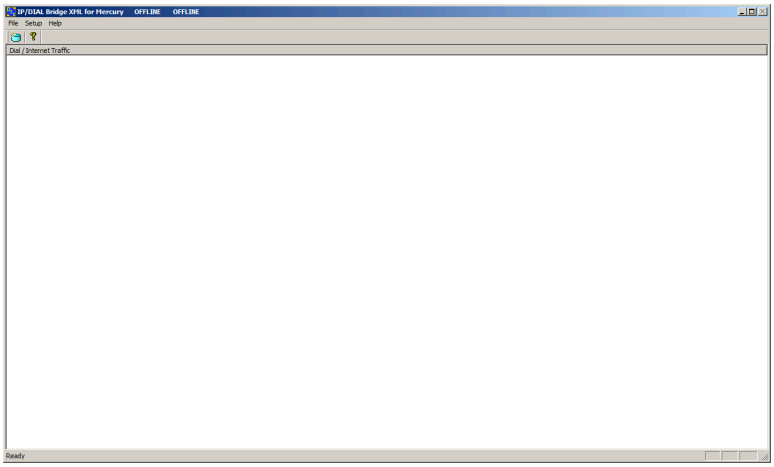
Click 'OK' and you will then see the setup screen as follows:



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

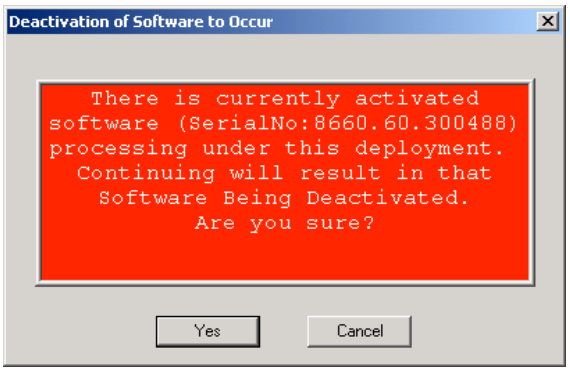
Lane Setup allows you to optionally change the description associated with each lane that was authorized in the PSCS parameter file. You cannot alter the number of lanes in IP/Dial Bridge; changes to the number of lanes must be done by editing the deployment file in PSCS.

You will then see the IP/Dial Bridge main status window indicating that IP/Dial Bridge is now programmed and ready to process transactions.



IP/Dial Bridge setup is complete.

5. If you receive the following Deactivation Warning dialog when entering a Deployment ID or Merchant Demographic Information that means another installation of IP/Dial Bridge is already using the merchant parameters associated with the Deployment ID or demographic information.



Verify that the Deployment ID or demographic information entered is correct; if not click 'Cancel' and retry the entry.

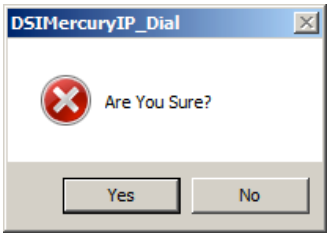
If the Deployment ID or merchant demographic information is correct and you want to force the parameters to load into IP/Dial Bridge, you should be aware that the IP/Dial Bridge with the serial number listed in the dialog box will be deactivated and will no longer be able to process transactions.

This dialog is typically encountered when the current IP/Dial Bridge is a replacement for an IP/Dial Bridge already activated for the same merchant who may have had a computer problem or hard disk failure that no longer allows them to use that earlier IP/Dial Bridge installation. This process will allow the new IP/Dial Bridge installation to use the existing merchant parameters associated with the entered Deployment ID without the need to create a new parameter file on Datacap's PSCS server.

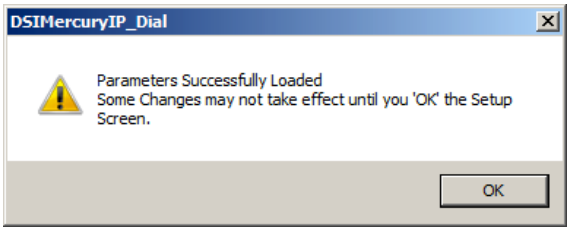
WARNING:

Do not select 'Yes' unless you are certain that the IP/Dial Bridge with the serial number listed in the dialog box should be deactivated.

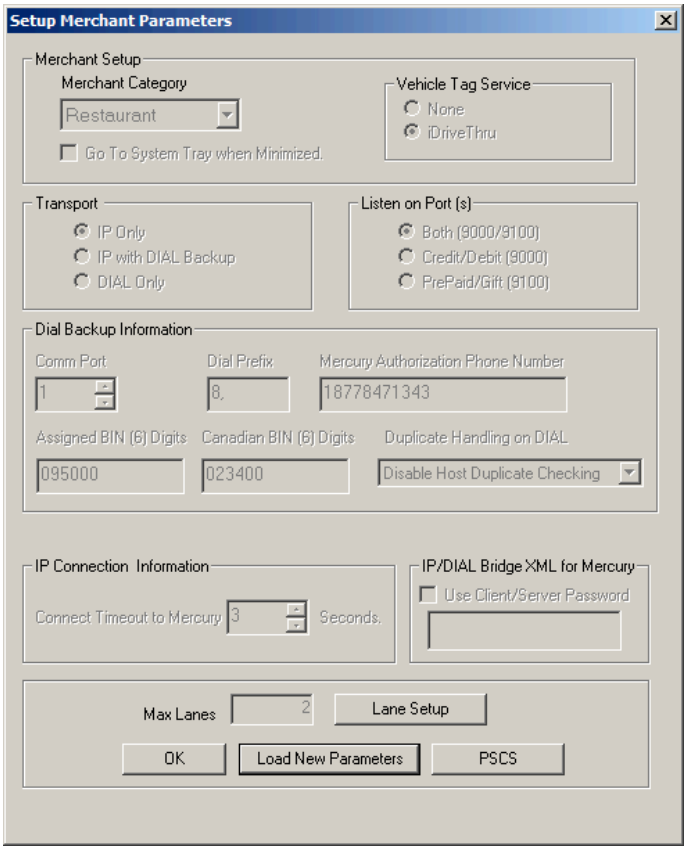
If you are certain that you want to deactivate the IP/Dial Bridge serial number listed in the Deactivation Warning dialog and use it with the new IP/Dial Bridge, then click 'OK'. You will see the following dialog that verifies your choice:



Click 'Yes' to if you are certain that you want to deactivate the IP/Dial Bridge serial number listed in the Deactivation Warning dialog and use it with the new IP/Dial Bridge. You will then see the following screen if the parameter download from Datacap's PSCS server is successful:



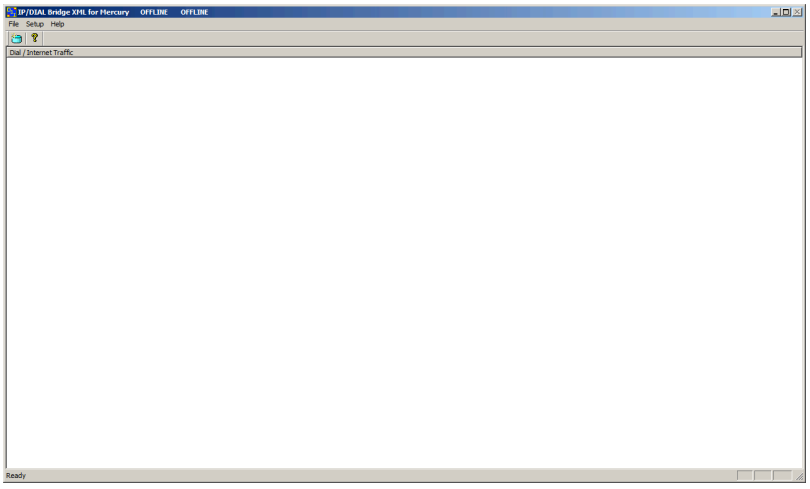
Click ‘OK’ and will then again see the setup screen as follows:



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

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

You will then see the IP/Dial Bridge main status window indicating that IP/Dial Bridge is now programmed and ready to process transactions.



IP/Dial Bridge setup is complete.

Verifying Your Serial Number and Activation

You can verify the serial number assigned to your copy of IP/Dial Bridge by selecting **About** from the **Help** menu item in the main status window. You will see a dialog bog containing the serial number and some additional information of the activation that you may need to supply in certain support situations. An example of the dialog box information is as follows:

Testing

Important! - Before You Start

You should arrange with your bank and payment processor for testing *IP/Dial Bridge* 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 IP/Dial Bridge 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!

IP/Dial Bridge relies on numerous services provided by Windows and other Microsoft software. **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.