Configuring Keystroke with KeyPay

Please read the PA-DSS Implementation Guide for Keystroke POS from our website before proceeding. It is also installed in the \KEYSTROK\DOC subdirectory on your computer.

Choose a Secure Computer to Host the KeyPay Program

The Keystroke Payment Module (KeyPay) can be installed either as a conventional Windows program (KeyPay.exe) or as a Windows Service (KPsvc.exe). SBS recommends the Service method for most users. Whichever method is used, the KeyPay module should be installed on a single computer to handle payment requests for all workstations.

It is important to select a computer physically located in a secure location with access limited to authorized personnel only. This computer, the primary file server, and all POS workstations should also be protected by a secure firewall. Whether the computer hosting KeyPay is a file server itself or an office workstation, it must always be started/running before other POS workstations in order to ensure payments can be reliably processed.

Notes:

- *In this document, unless otherwise designated, the term KeyPay may refer to either installation method (conventional program or Windows Service).*
- *The KeyPay program can support multiple merchant accounts (Credit, Gift Cards, etc.)*
- *KeyPay and Keystroke POS are designed to run on Windows 7 and later and require Microsoft .NET Framework 4.5.*

PCI Settings in Keystroke POS

The official PCI website at www.PCISecurityStandards.org provide detailed information to help your business protect payment card data and operate in a PCI-DSS compliant environment. Also refer to the Keystroke POS document: PA-DSS Implementation Guide for Keystroke POS.

Following is a partial list of PCI-DSS related concerns and software settings, most of which may be automatically enabled the first time Keystroke Version 8.00 or later is run.

1. **Purge all previously processed payment data.**
   When using KeyPay, payment data is not stored in Keystroke data files, so purging is not necessary. If converting from an earlier version to v8.00, you may be prompted to purge all previously processed payment data. If you use an Authorization Method other than KeyPay, the Keystroke system should be configured to automatically purge payment data on a regular basis.
   Relevant settings: Closeout function, Closeout menu, Parameters – Purge Payments: On Save - Automatic, Minimum Interval 1 Day, Payments Over 3 Days. Closeout function, Closeout menu, Purge Payments. Configuration Manager, Tables menu, Sales Payment Types – Purge Ref/ExpDate Immediately.

2. **Require re-entry of the Clerk and Password on idle workstations.**
   The Keystroke system is configured to automatically prompt for a Clerk and Password after no greater than 15 minutes of inactivity.
   Relevant settings: Configuration Manager, Settings menu, Parameters – Auto Logout Time (15 minutes maximum). Sales/Purchase Manager, Transaction menu, Parameters, Display – Auto Logout Time (15 minutes maximum, typically the same or less than the Global Parameter Screen Saver Time).

3. **Maintain strong passwords.**
   The passwords of Clerks with manager level access (typically those with Security Level 0-5, although recommended for all Clerks) must be a minimum of seven characters in length and include both numeric and alphabetic characters. Passwords must also be changed every 90 days and new passwords cannot be the same as the last four passwords used.
   Relevant settings: Clerk Database records – Last Changed and Expires dates.
   Configuration Manager, Settings menu, Parameters – Passwords setting box.
   This is based on the "lowest" Security Level for Edit Clerks, Add Clerks, Change Parameters, File Maintenance, and Edit Security Levels.

Installing KeyPay

Installing the KeyPay Program (vs. Windows Service)

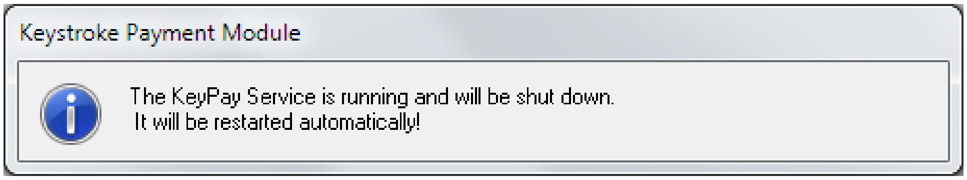
The conventional Windows program (KeyPay.exe) is fully installed (but not launched) as part of the Keystroke program installation. The KeyPay.exe program file can be found in the main \KEYSTROK program directory. If you intend to use this program and not the recommended KeyPay Windows Service, the KeyPay.exe program should be added to the Windows Startup folder (or an automated Batch program) on a single designated computer only.

Installing KeyPay as a Windows Service (Recommended)

The Windows Service version of KeyPay (KPSvc.exe) is also copied to the \KEYSTROK program directory, but must be properly installed before it can be accessed. Run the Keystroke Update Installer (from the Start Menu, Keystroke POS folder). Then click on the Keystroke Extensions icon to download and install the *Keystroke Payment Module as a Windows Service*.

After the Welcome and License Agreement screens, you will be prompted to enter the location where KeyPay Service will be installed. If Keystroke POS is found, and installed on your local C: drive, the installation will default to that directory (usually C:\KEYSTROK). If Keystroke POS is not installed locally, then the installation will default to C:\ KEYSTROK. You can change these settings during the installation, but it is recommended to use the default location so the KeyPay Service program will be updated automatically when Keystroke POS is updated.

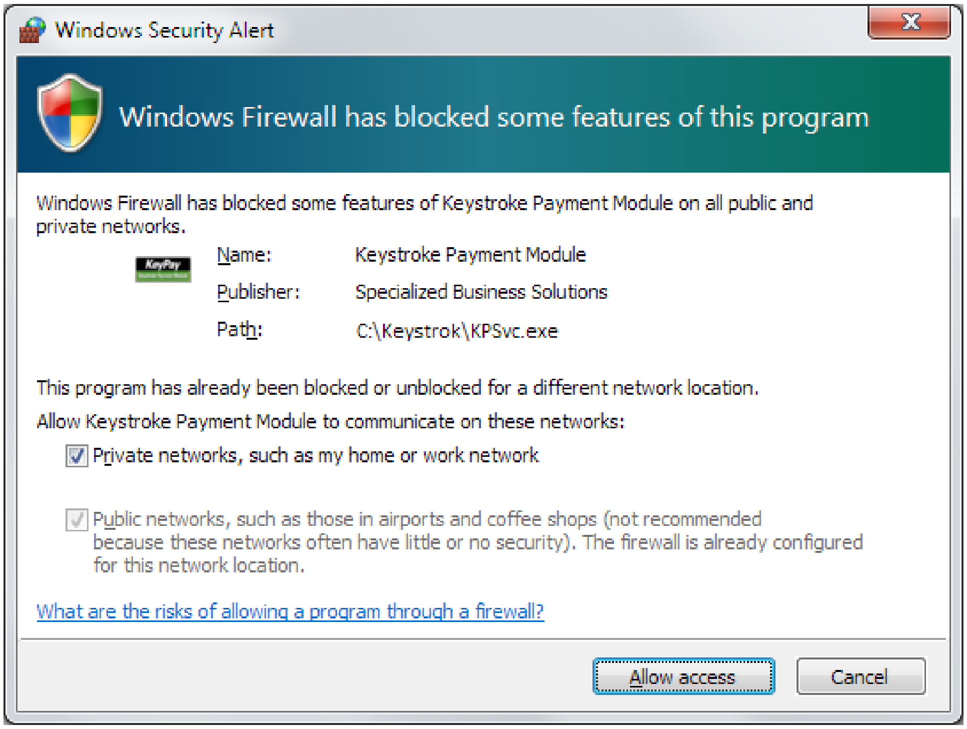
After you begin the installation, you may be notified if the KeyPay Service was already running. Following the prompt shown below, the Service will be stopped automatically, and for the remainder of the installation you will not be able to process payments until the setup is complete.



Keystroke Payment Module

The KeyPay Service is running and will be shut down.
It will be restarted automatically!

On machines with a firewall, such as Microsoft Windows Firewall, you may see a similar screen shown below regarding KPSvc.exe. You will need to click on the Allow Access (or Unblock) option to allow the KeyPay Service to access the internet.



Windows Security Alert

Windows Firewall has blocked some features of this program

Windows Firewall has blocked some features of Keystroke Payment Module on all public and private networks.

Name: Keystroke Payment Module
Publisher: Specialized Business Solutions
Path: C:\Keystrok\KPSvc.exe

This program has already been blocked or unblocked for a different network location.

Allow Keystroke Payment Module to communicate on these networks:

☑ Private networks, such as my home or work network

☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security). The firewall is already configured for this network location.

What are the risks of allowing a program through a firewall?

The KeyPay Service setup will automatically allow both KeyPay.exe and KPSvc.exe into both the Public and Home/Work (Private) networks. If other Firewall Software is installed (McAfee, Norton, etc.), you will have to make exceptions in that software manually. During the installation, you will be automatically prompted to configure KeyPay settings such as Merchant Number, Data Directory, and Password (see next page).

Un-Install Other Payment Programs

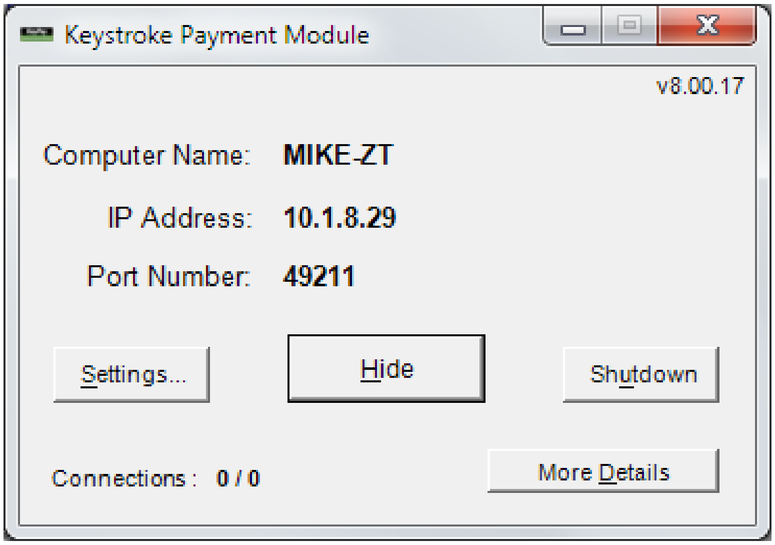
If your business was using a different integrated payment processing program with Keystroke (e.g., PCCharge or ICVerify), be sure to terminate and completely un-install all instances of such programs or Windows Services after KeyPay is completely installed, configured and tested. Review the Windows Startup folder and any other means of automatically launching programs on all computers, file servers, and workstations.
Note: If you are using another payment processing software, please make sure you close your current payment batch before uninstalling their software.

Configuring KeyPay

Upon initial installation of the KeyPay Service, you will be automatically placed in the Keystroke Payment Module - Settings dialog box shown at the top of the following page. After initial installation of the KeyPay Service, you can access these Settings by selecting the KeyPay Settings icon from your Keystroke POS folder on the Windows Start menu.

If running KeyPay as a conventional Windows program, the application should appear on your Windows Notification Area where you can double click the KeyPay icon to access the main Keystroke Payment Module status screen shown immediately below. Click Settings to access the KeyPay Settings, or click Hide to return KeyPay to the Taskbar and leave the program operational. If you click Shutdown (or the Red X), the program will be terminated and unable to process payments until it is restarted.

If running the service, to access the settings, there is a shortcut to KeyPay Settings in your Program Menu, under Keystroke POS.



v8.00.17

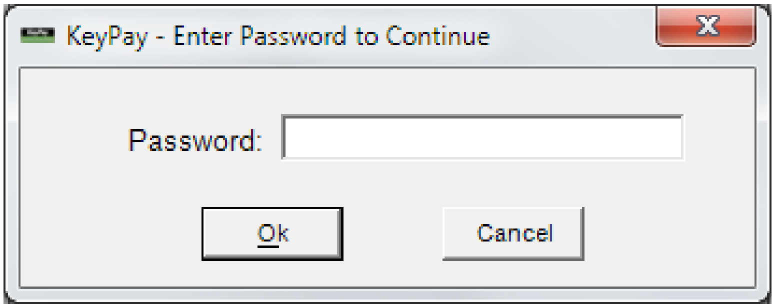
Computer Name: MIKE-ZT

IP Address: 10.1.8.29

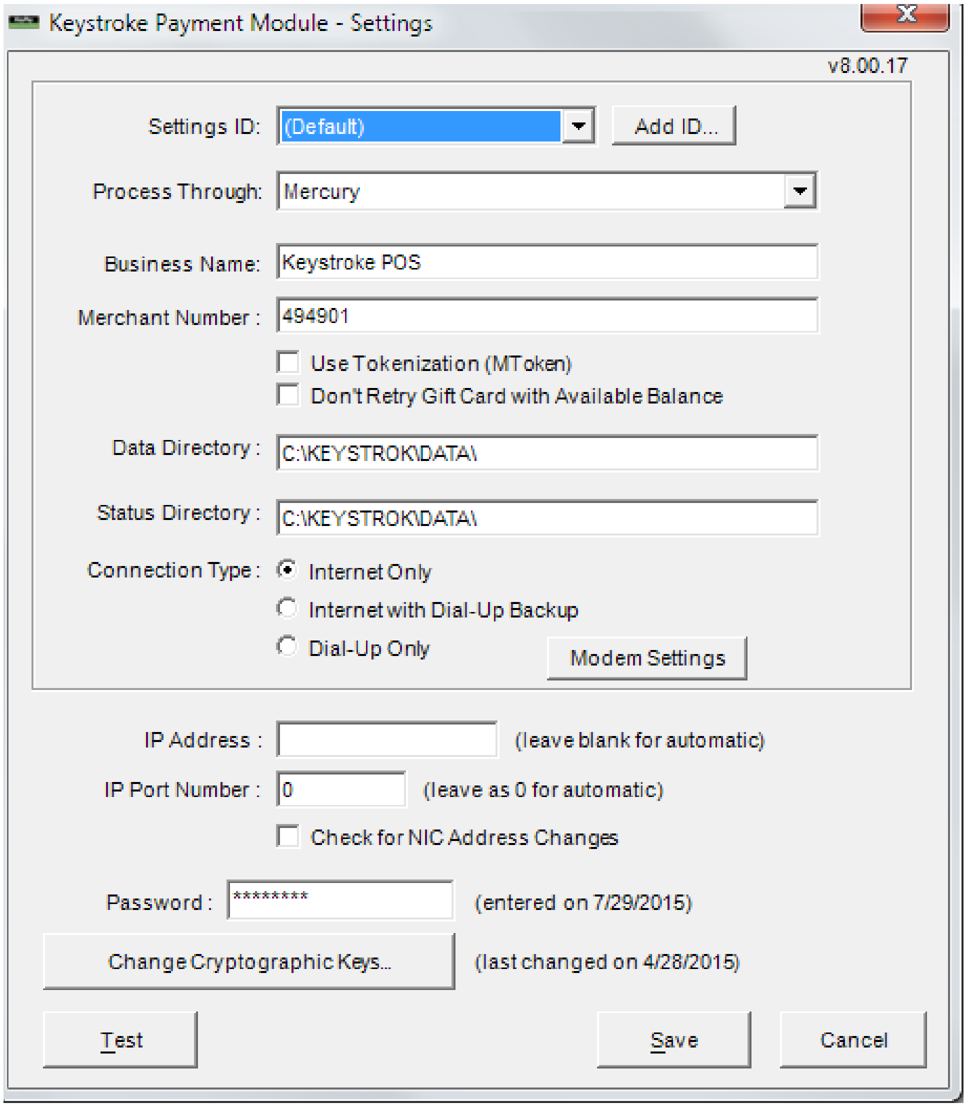
Port Number: 49211

Connections : 0 / 0

If KeyPay has been previously configured, you will be prompted to enter your existing Password. If you have not configured KeyPay, you will be taken to the Settings page (see next page) where you will be required to enter a password.



KeyPay Settings



Keystroke Payment Module - Settings

v8.00.17

Settings ID: (Default)

Process Through: Mercury

Business Name: Keystroke POS

Merchant Number : 494901

□ Use Tokenization (MToken)

□ Don't Retry Gift Card with Available Balance

Data Directory : C:\KEYSTROK\DATA\

Status Directory : C:\KEYSTROK\DATA\

Connection Type : ● Internet Only ○ Internet with Dial-Up Backup ○ Dial-Up Only

IP Address : (leave blank for automatic)

IP Port Number : 0 (leave as 0 for automatic)

□ Check for NIC Address Changes

Password : ******** (entered on 7/29/2015)

(last changed on 4/28/2015)

For most installations with a single merchant account, the Settings ID should remain set to '(Default)', and Process Through set to 'Mercury'. The Business Name is provided by your merchant service provider (if necessary).

If you have more than one Mercury Merchant Account such as for multiple business locations or an e-commerce site, you may wish to create a separate Settings ID for each account using the Add ID button. If using multiple Settings IDs, you must also specify corresponding Settings IDs in the Authorization Methods in the Keystroke POS program.

Enter your Mercury Merchant Number and verify that the Data Directory and Status Directory are both set to correspond with the location of your Keystroke Data Directory. Select the appropriate Connection Type, and if a Dialup modem is available, select Modem Settings to complete and test the modem settings.

In most cases, IP Port Number can be left at 0 which will allow the computer to automatically assign an available number each time. A number can be entered here if the port needs to be fixed in order to allow communications to pass through a firewall.

If Check for NIC Address Changes is On, the program will check the IP Address and Port Number every 20 seconds and then update the KPSTATUS.TMP file if anything has changed. Leave this parameter **OFF** unless the IP address changes while the system is running.

Enter a secure Password (7 characters and at least 1 number and 1 letter – case sensitive). Change Cryptographic Keys resets the keys used by KeyPay to securely encrypted cardholder data. They should be changed at least annually.

The Test button can be used to communicate with the processor (if processing with Mercury). It will establish a connection w/ Mercury and confirm that KeyPay and Mercury are communicating.

Click Save to continue. You will be asked to confirm your Password (if changed or a new one entered). Re-enter your password and click Ok to save the settings.

Additional Network Settings (for KeyPay Service Only)

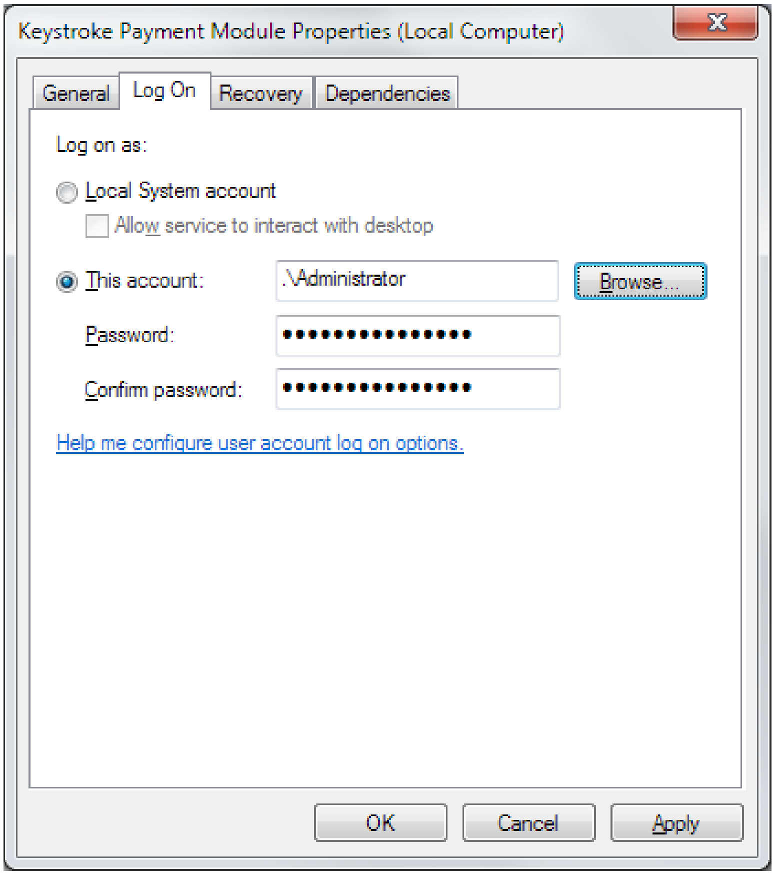
If the KeyPay Service is installed on a different computer than where the Keystroke data files are located (such as a communications server), the Windows Service must be enabled to access the Data and Status Directories over the network.

To enable access for the KeyPay Service:

1. The Data Directory and Status Directory in the KeyPay Settings need to be entered using Universal Naming Convention (UNC) names (e.g., \\server\c\keystrok\data).

2. You may need to edit the Service in Windows and modify the Log On tab to specify a Login User with a Password. Users without Passwords are not allowed to run a Service over a network. Follow the steps below:

   a. From the Windows Start menu, select Administrative Tools, and Services.
   b. Find the Keystroke Payment Module Service, and double-click to open its properties.
   c. Under the Log On tab, change the settings from “Local System account” to “This account:” and type in the User as .\Username (typing in the “.\” before the username - e.g., “.\Administrator”).
   Note: You can use the Browse Button, then click Advanced, then Find Now to see a listing of the valid Users for this computer.
   d. Enter your Password (required).
   e. Click Apply, and Ok to save the settings.
   f. Lastly, you must Stop and Start (or Restart) the service for changes to take effect.



Keystroke Payment Module Properties (Local Computer)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: .\Administrator

Password: •••••••••••••••

Confirm password: •••••••••••••••

Help me configure user account log on options.

Configuring Keystroke POS for Processing with KeyPay

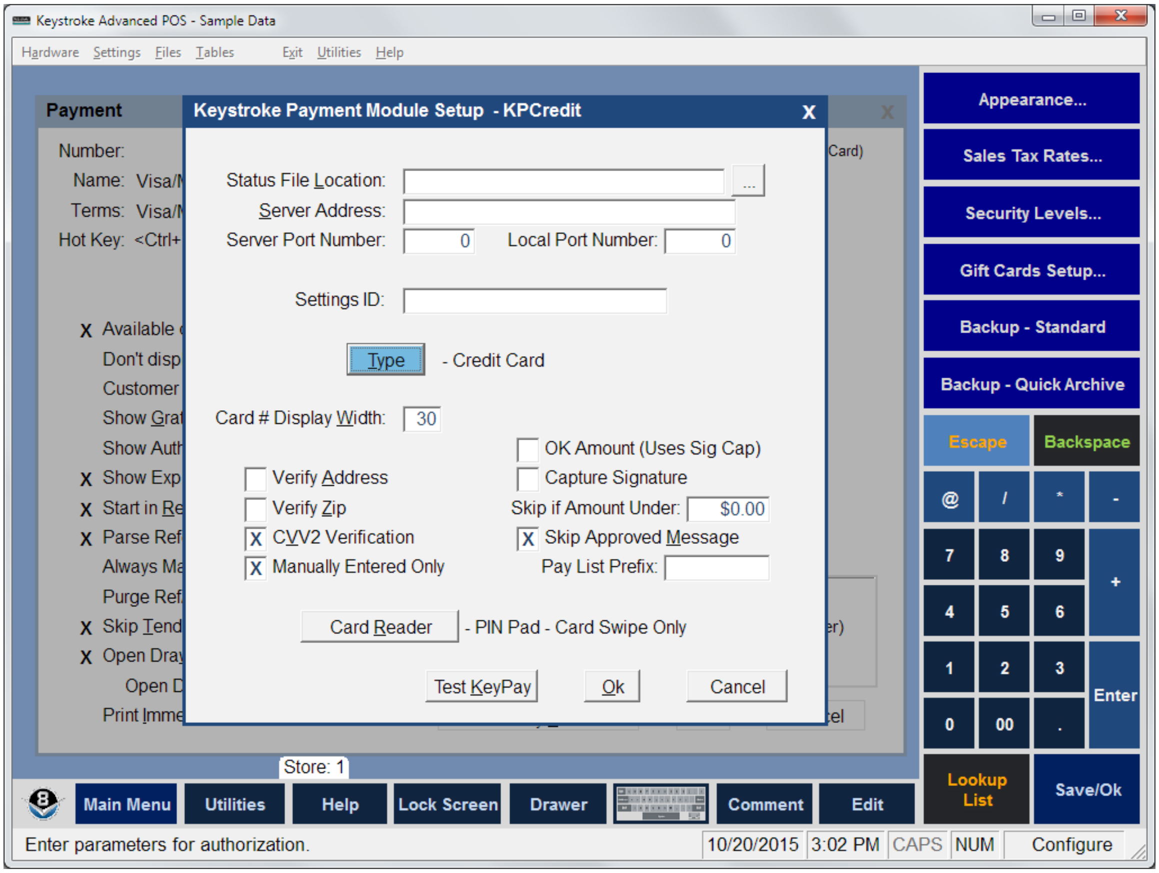
You are now ready to configure Payment Types in Keystroke POS.

In the Configuration Manager, select Tables, Sales Payment Types and an appropriate Payment Type like Visa/MC/Disc. Select the Auth Method button, and either select an available Authorization Method such as KPCredit (for typical credit cards) or press INS or F2 to create a new Authorization Method. If adding a new Auth Method, assign a unique name and select Keystroke Payment Module as the type. To view/edit the current settings for an Authorization Method, press F3 from the list of Auth Methods (i.e. when KPCredit is highlighted).

Repeat the process above for each electronically processed Payment Type. You will need a unique Authorization Method for each different class of payment (Credit, Debit, Gift, EBT, etc.).

Authorization File Setup

The Keystroke POS program ships with a default authorization file "KPCredit.aut" (shown below). While the settings can be changed, in most cases it will work with its default settings.



Keystroke Payment Module Setup - KPCredit

Status File Location:

Server Address:

Server Port Number: 0 Local Port Number: 0

Settings ID:

Type - Credit Card

Card # Display Width: 30

☐ OK Amount (Uses Sig Cap)
☐ Verify Address
☐ Capture Signature
☐ Verify Zip
Skip if Amount Under: $0.00
☒ CVV2 Verification
☒ Skip Approved Message
☒ Manually Entered Only
Pay List Prefix:

Card Reader - PIN Pad - Card Swipe Only

Test KeyPay Ok Cancel

Note that the Merchant ID is not entered here, but rather is entered in the KeyPay program itself.

Status File Location
This identifies the location of the file KPSTATUS.TMP, used by Keystroke to identify how to process payments. If left blank, the program will use the current data directory.
It is recommended to leave this field blank.

Server Address
This is the TCP/IP address of the machine where KeyPay is running. Keystroke typically gets this information from the Status file. It is recommended to leave this field blank. If your firewall blocks most addresses or you have two network adaptors in use, it may be necessary to specify the server address.

Server and Local Port Numbers
This is the TCP/IP port used for processing payments on the machine where KeyPay is running and the local machine running Keystroke. It is recommended to leave these fields blank (0). If your firewall blocks ports it may be necessary to specify the port number.

Note: As long as the KeyPay Status File (KPSTATUS.TMP) is in the Keystroke Data Directory, you can leave the fields above blank (0 for Port Numbers) and the program will get the information from the KPSTATUS.TMP file as it needs it.

Settings ID
The "Settings ID" field is used to identify which settings in KeyPay are to be used to process the request. Leaving this blank will use the default settings in KeyPay (which will work for most installations). Multiple settings are only needed if processing using multiple Merchant ID installations.

Type
The type of payment to be processed (Credit, Debit, Gift, EBT, etc.).

Various Other Checkboxes
Turn On/Off the appropriate check boxes for each type of authorization Method (optional).

Test KeyPay
The "Test KeyPay" button will locate the KPSTATUS.TMP file, ping the server and run a series of test transactions. It can be run from any workstation to ensure that it is properly communicating with KeyPay. If this test fails, check your Firewall settings and be sure KEYPAY.EXE, KPSVC.EXE and KEYSTROK.EXE are all allowed as exceptions.

Processing Payments using Keystroke POS with KeyPay

With Keystroke POS and KeyPay properly installed and configured, processing payments is a snap. For example, in the Sales Manager, after entering a sale and swiping a payment card in the appropriate Payment Authorization Reference field (or manually typing the card number, etc.), select Ok to begin the payment authorization.

In a matter of just a few seconds, Keystroke passes the payment information to KeyPay using a high level encryption method. KeyPay then requests authorization to complete the payment, and returns a response to Keystroke along with a 'tokenized' form of the original payment card number. The tokenized number is a masked number where only the first 2 and last 4 digits are the same as the original card number. This helps to ensure sensitive card data is not exposed any more than is necessary.

Some payment card data is temporarily retained by KeyPay in a secure format to enable tasks such as voiding transactions shortly after completion. However, no unnecessary functionality is provided for reporting, displaying, or in any way exposing sensitive payment card data. Your merchant service provider can assist you if it is necessary to obtain a complete payment card number after a payment has been processed.

Processing Recurring Charges

Keystroke and KeyPay can be used to automatically process regularly recurring transactions such as for monthly fees, including credit card payments if needed. This function emulates the same procedure a Clerk would perform manually to copy existing transactions such as from the alternate Sales Transaction Type "Recurring Charges" and save them as normal "Sales Invoices".

In Keystroke Advanced POS, you process transactions in Sales Manager, under the Special menu, Process Recurring Transactions. In Keystroke POS, the program RECCHRG.EXE can be used to automate this process (but less functionality exists). As transactions are copied, the payments are also copied and processed through KeyPay (if configured with an appropriate Authorization Method). Any payment that fails to be processed will be copied to an alternate Transaction Type (such as On Hold) so that the reason for failure such as an expired credit card can be reviewed and corrected.

RECCHRG.EXE supports all the standard Keystroke command line switches and some special switches, and can easily be run from a batch file. A typical command line would look like:

```
C:\KEYSTROK\RECCHRG.EXE FROM=REC TO=NVC ALT=HOLD
```

This command would copy all sales transactions identified with the Recurring Charges (REC) Transaction Type to Sales Invoices (NVC), and save any problem transactions as On Hold transactions for later review. For additional instructions, please see RECCHRG.DOC in the \KEYSTROK\DOC directory or contact your Authorized Keystroke Dealer for personal assistance.

Emergency Stand-Alone Workstation Setup (Optional)

Keystroke and KeyPay can be pre-configured to run in a stand-alone workstation mode as a temporary measure in the event of an unexpected computer network failure (where workstations cannot communicate with the file server). When operating in this mode, normal sales transactions can be completed and saved on the local hard drive of each independent workstation. Once the cause of the network failure is identified and corrected, the transactions recorded on each independent workstation may be merged into the primary database on the network server.

Note: Generally, a network failure, as is relevant to this section should not be confused with a loss of an internet connection, in which case KeyPay's Dial-Up Backup feature would automatically take over (if enabled). However, if your business relies on some form of wide area network where normal access to primary data files requires the internet, some aspects of this configuration may be utilized with the guidance of an experienced dealer.

How it works:

1. The Keystroke program must be fully installed on the local hard drive of each computer (as opposed to a Client installation), and configured to normally access data files located on the network server (using Startup Switches or .INI file settings). The KeyPay service should be setup on one machine with internet access to process normal transaction requests made to the server data directory.
2. Using an automated batch process that runs on a daily basis (perhaps as part of a regular backup routine), data files from the file server must be copied to each local machine in advance (prior to an unexpected network outage). Typically, transaction data files should be excluded from this copy procedure (or they may be deleted from the local data directory) in order to simplify the recovery procedure (step 4. below).
3. The KeyPay.exe program should be setup on the local machine to look for transaction requests in the local data directory prepared in step 2.
4. In the event of a network failure requiring Keystroke to be operated in this stand-alone mode, Keystroke and KeyPay may be started on each workstation using Startup Switches or .INI file settings that direct the programs to access local data files (from step 2. and 3. above). A batch file or program shortcut should be pre-configured on each workstation for this purpose, with precautions taken to prevent this mode from being utilized unnecessarily.
   Note: Each stand-alone workstation will need either an internet connection or modem and phone line to process payments in this mode.
5. When the network is restored, transactions from each workstation can be merged back into the primary database using the RECMRG.EXE program. For additional instructions on using this special utility program, please see RECMRG.DOC in the \KEYSTROK\DOC directory or contact your Authorized Keystroke Dealer for assistance.

This procedure is intended for the temporary operations during normal system failures only. When running in stand-alone workstation mode as described above, it may be necessary to limit the use of some system operations such as editing database records, accessing alternate Sales Transaction Types, and making system configuration changes. Please consult with your Authorized Keystroke Dealer for further guidance.