Restaurant Manager

RM Gateway's Paygistix Integration Guide

6/20/2017

1734 Elton Road, # 219, Silver Spring, MD 20903

Email: support@actionsystems.com

Website: www.rmpos.com

TOC

Overview

Paygistix is a RM Gateway EMV processing option that is available in starting with Restaurant Manager version 19.1. Paygistix is a compelling RM Gateway option because it provides a single solution for MSR, NFC, and EMV. The Paygistix gateway is currently certified with Payment Logistics (preferred vendor) and First Data Omaha.

Paygistix EMV is implemented in a way that cardholder data never enters the POS environment. By employing tokenization technology, the Paygistix EMV interface eliminates the need for Restaurant Manager to store sensitive cardholder information. When configured for normal use, the POS application and terminal are completely out of PCI scope when using a payment terminal with Paygistix EMV. One huge advantage to the Paygistix interface is that most credit card handling changes will be handled through the device and not Restaurant Manager.

Will Credit Card Processing be the Same?

The steps for processing a credit card payment at the POS will be somewhat similar to how restaurants have always processed credit cards in the past. However, there will be some noticeable differences. Here are some of the key differences.

You will no longer be able to just swipe a card from anywhere within an open order to enter a CC payment. Unlike traditional credit card processing with a standard MRS, EMV payment requires the POS to awaken the EMV terminal to establish communications.

To enter an EMV credit card payment, the employee will enter the Settlement screen and chose a CC payment type. At this point, a prompt will appear telling the employee to dip the credit card on the EMV terminal. The EMV terminal will communicate with the processor and seek an approval code. The EMV terminal will pass a long a token to Restaurant Manager when authorization has been obtained, a credit slip (on existing POS printer) will print out, and the employee can add a tip on the POS station or the EMV terminal. CC Tab transaction will be processed significantly different. All CC tabs will now require a pre- authorization and dipping the card into the EMV terminal because the EMV terminal will first contact the processor and then pass a token back to the POS rather than communicating directly to the POS. CC Tabs must be completed with Complete Auth and will require the card to be present when completing the transaction to remain EMV compliant.

Please note an EMV terminal is not simply a standard MSR and EMV credit card processing will not be exactly the same as before because of the change in communication flow. The EMV terminal will complete at least twelve functions before passing tokens to the POS. Some of the functions an EMV terminal will perform is determining card type (i.e. credit card vs debit card), the restrictions of the card, if a PIN required, plus many more functions. At this point the EMV terminal will go out to the processor to check if the card is valid and then pass a token back to the POS. In other words, there is no longer just simply swiping a card. This translates into slightly longer processing times and change in functionality. There is definitely a trade off in functionality for enhanced security. However, security should be of the utmost importance as this demonstrates the restaurant has a strong commitment to protecting the customers data. In addition, EMV shifts liability back up to the processors leading to a reduction in charge backs. Another benefit is that EMV terminal will now process NFC transaction. Please visit the FAQ's section of the document to see what functionality has changed.

Will EMV Make You PCI Compliant?

Simply put: No ! In reality, you don't need to implement EMV in order to be PCI compliant. Whats the between difference EMV and PCI-DSS ? EMV uses technology that authenticates that a card is valid and belongs to the person using it, but PCI -DSS involves a broader set of data security controls that protect cardholder data through the payment transaction process. In fact, EMV and PCI Compliance are managed by two separate entities with completely different set of governing rules. This article published by the PCI -SSC helps explain the difference between the two organizations. So do you need EMV ? EMV should be considered one component to building an overarching, cohesive data security strategy that helps you reduce your liability risk. Will you still need to follow PCI-DSS best practices? Yes you will. ASI has published a set of general guidelines that you can view here: RM PCI Implementation Guide.

What Does Out of Scope Mean?

As discussed above, if EMV does not apply to PCI-DSS compliance, than what does out of scope mean? In a traditional Credit Card processing environment, an MSR is connected directly to the POS. Keep in mind that a standard MSR is nothing more than a keyboard substitute. A card is swiped and passes the payment information through the POS software for authorization. The POS software then receives authorization from the processors where the transaction can be finalized. This is considered in scope because all cardholder data is present throughout the POS software and OS software (swipes are recorded within virtual memory unless correctly configured differently.

In an out of scope environment, the EMV device is awaken by the POS to start the payment process. Here is the difference: instead of first sending the information through the POS software, the EMV device sends transaction data directly to the processor for approval. The EMV terminal will receive the authorization from the processor and pass it back to the POS via a token. This arrangement takes

the POS system out of the authorization process because no card holder data is sent to the POS, thus taking the POS system out of PA-DSS scope. Once again, just because EMV processing is considered out of scope does not mean you are relieved from PCI compliance.

What Processors are Supported?

Paygistix EMV Certified Support

- Payment Logistics (as a preferred vendor)

Other Processors Platforms Pending (non-preferred)

- FD Omaha platform

What Card Types Are Accept?

Restaurant Manager only supports the following card types:

- Visa
- MasterCard
- AMEX
- Discover
- Debit

Note: 3rd party, gift cards, 3rd party loyalty, & EBT Cards are not currently supported by Restaurant Manager using an EMV terminal.

Does Paygistix Support NFC Payments?

Paygistix supports the following Digital Wallet & NFC payment methods:

- Android Pay
- Apple Pay
- Mastercard Pay Pass
- Samsung Pay
- Visa payWave

What Restaurant Manager Credit Card functions are Supported with Paygistix?

- Basic Sale
- Adding a Tip
- Tip Adjustments
- Auto Finalize
- Bypass Order Entry for Authorized Credit Cards
- Display tabs with authorized credit cards
- CC Tab - CC Tabs now require pre-authorization and will no longer just record customer name and card data without Pre-Auth. When doing a CC Tab, RM is sending PreAuthByRecordNo which is a “manual transaction” (not “card present”). This means that users will have a higher CC fee when using CC Tab. Considered Non-EMV Compliant
- Exit order after auth and complete pre-auth
- Require Confirm
- Save/Restore loyalty module credit card info. Considered Non-EMV Compliant
- Warn if no tip adjust
- Repeat Sale (using the Copy&Paste)
- PreAuth (i.e., using CCTab)
- RepeatAuth (using the Copy&Paste)
- Complete Auth - A CC Tab transaction is not EMV-compliant unless the user re-inserts the card during [Complete Pre-Auth]. Considered Non-EMV Compliant if card not present.

- Debit
- Void
- Reversal
- Refund

What are the Known Limitations ?

- Gift Cards, Loyalty, and EBT are not supported using an EMV terminal
- Debit is not applicable with: pre-authorizations, manual entries, or pop-up mode
- Offline processing is not supported. Please see section on Router for alternative method to Offline processing.
- Some settings are misleading (i.e., because they say that it's "mercury only" but actually supports Paygistix):
    - Enable credit card pre-auth (NETePay only)
    - Always print Void slip (Mercury only)
- Some settings are not followed by Paygistix:
    - Maximum tip multiplier
    - Security level to override max tip multiplier
    - Prompt for excess handling
    - Security level to apply excess to pre-authorization
    - Allow multiple tip revisions
    - All settings regarding CC Retrieve info:
        - Audit button presses
        - Transaction directory
        - Security level to enter credit card information manually
        - Allow duplicate charges
- RMHH, RMTablet, and RMKiosk do not support Paygistix
- When set up for "Time Initiated Batch Close", Payment Logistics will automatically send a Batch Close email to merchant. On the email confirmation, the time stamp does not specify the time zone and may confuse users.
- Unlike the old CC implementation, Paygistix will not process additional payments when the check total is already full paid
- Credit Card Demo Mode in not supported

Do I still need an Internet Connection?

Yes. In fact, every PAX unit needs a direct internet connection for authorizations. Please see section on Router.

What transactions are not considered EMV-compliant?

- CC Tab functionality if not re-inserting card during CompleteAuth
- Copy & Paste
- Frequent Diner using saved card
- Changing the Base Amount

Requirements

The following topics are the requirements for running the Paygistics interface in a Restaurant Manager environment.

Restaurant Manager Requirements

- Restaurant Manager v19.1 or greater
- Upgrade code if upgrading from previous versions prior to v19.
- Credit Card Authorization must be enabled
- MSR - old MSR should be retained to process gift cards and employee badges, etc.
- WOPKG19.1.2016.01250 or later if using OO, RMTablet, RM Handheld (note EMV not supported on RM Tablet, RM Handheld, RDP).

Payment Logistics

- Credit Card processing account
- Paygistix Client Software - provided by Payment Logistics.

Software

- Microsoft .NET Framework 3.5 Service Pack 1 - installed on all stations with PAX unit attached. Down load here..

Operating Systems

- Windows 7 Pro
- Windows 8 Pro
- Windows 10 Pro
- Windows Server 2008 and 2012

Note: Windows XP and Windows 2003 Server are not supported by ASI and are PCI Non Compliant.

Internet Connection

Each PAX unit requires an internet connection to seek authorizations. It is essential for a hard wired PAX device to have a connection near the POS station or through the POS station (see Wiring Hardware below). Please contact the local network administrator in advance to allow internet access. It is also essential that your POS system be setup on a network static IP scheme so the PAX units be able to communicate with the POS station.

Important: all stations and the rmserver must be configured with an static IP scheme. Example: rmserver 192.168.1.100, POS Station 1 192.168.1.101. , POS Station 2 192.168.1.102. , etc. In addition, there must be room on the network IP range to accommodate the PAX devices.

Hardware

The following is a list of the PAX terminals that Paygistics offers:

- **S80** :Traditional restaurant credit card service (Not pay at table) , tethered IP connection , EMV Level 1 & 2 Certified, NFC Ready, Pin Debit Ready, built in printer (not needed with RM)
- **S300**: Pay at the counter (customer facing), tethered IP connection, EMV Level 1 & 2 Certified, NFC Ready (paired with R50), Pin Debit Ready, signature capture with online archival
- **D210**: Supports traditional restaurant credit card processing, tethered, or wireless IP connection, EMV Level 1 & 2 Certified, NFC Ready, Pin Debit Ready(wireless; reads NFC). this device can also be used for Pay-At-Table. Note Restaurant Manager and Paygistics do not support pay at the table at this time.

Note: The S80 unit has a built in printer which is not needed with Restaurant Manager. CC receipts will still print to local guest check printer.

Wiring Hardware

All PAX units are tethered to the POS network via a Cat5 cable with a standard RJ45 connector. Below are the options you can consider prior to installation:

- Run a dedicated Cat5 cable going directly from the router to the wall near the PAX unit.
- Use a USB Ethernet adapter on the POS computer and bridge the two connections

- Some newer model POS units come with a second Ethernet post. Plug the PAX unit into the second port and bridge the connections.
- Use a small network switch or hub. This is ideal if you have a bank of computers near each other. For security reasons, you will have to terminate any open/unused ports.

Router

Because transactions are processed from the Verifone units (via NETePay) to the internet, it is important that a constant internet connection be maintained. The benefit to processing with an EMV terminal is that cardholder data is kept out of scope. To keep out of scope it is important that cardholder data is not stored within Restaurant Manager software, the same data needed for off-line processing. Therefore, ASI recommends use of the Cradlepoint ARC MBR1400 with integrated 3G/4G wireless modem. There are three specific models with 3G/4G rollover you will want to consider:

- ARC MBR1400LPE-VZ – 3G/4G Verizon with multi-band LTE
- ARC MBR1400LPE-AT – 3G/4G AT&T with multi-band LTE
- ARC MBR1400LPE-SP – 3G/4G Sprint with multi-band LTE

Cradlepoint routers are designed to roll over to wireless connection when a wired internet connection fails. This helps ensure continuous credit card processing. This router can be used as a primary or secondary router. More information on the cradle point Router can be found here: https://cradlepoint.com/products/arc-mbr1400.

Procedures

You will find the installation of Paygistics software and hardware to be an easily process. Payment Logistics makes the installation of hardware effortless since the PAX devices will come pre-programmed. Prior to installation, Payment Logistics will send the reseller information needed to download and initialize the Paygistix server client software needed at the stations. In addition, Payment Logistics will send information needed for station configuration setting. This section of the document will outline the following:

- Requirements
- Paygistics Setup
- Restaurant Manager Setup
- CC Batch Close Options
- Windows Settings for PCI
- Bridging Connections

Please read all sections carefully to insure proper installation.

Paygistix Setup

The following are the steps for ordering from Payment Logistics and the setup process:

- Reseller will contact Payment Logistics to submit a merchant application for a new merchant.
- Debit card processing must be requested in advance. Upon request and prior to shipping, Payment Logistics will pre-configure your PAX device to accept debit cards. Debit card processing does require the customer to enter a choice of Debit or Credit followed by a pin number. Therefore you should request on of the customer facing PAX devices.
- Payment Logistics prepares the PAX terminals and ships them out. Simultaneously, Payment Logistics also creates an activation code for each Paygistix Client and sends it to the dealer via email.
- Payment Logistics will provide usernames, passwords, and vendor number for server mode app. It is important that you have this information at hand the day of installation. This information will be used in Restaurant Manager's Station Configuration so each station can communicate with the attached PAX Device.
- On the install day, the dealer installs Paygistix Client and enters an activation code into the software.
- The activation occurs and Paygistix server client automatically picks up its settings.
- The dealer plugs in the PAX terminals into the network and the terminals pick up an IP address via DHCP.
- The terminals report the IP Address to Paygistix Server Client

Payment Logistics uses a template to pre-configured PAX unit settings for integration with Restaurant Manager software. This means resellers simply have to plug the device into network. This also means you must make sure you order the correct equipment and let Payment Logistics know if you will be using NFC and/or debit card processing. Paygistix will pick up an IP via DHCP for the PAX device and then report the device to Payment Logistics automatically.

Installing Paygistix Software

Reseller will receive a link to download the Paygistix Server Client software which is similar to Mercury's DSI Client. Along with a the software download, you will receive an activation code for each terminal. Make sure you request an activation code for any computer where you plan to run Session Open/Close when Close CC Batch is enabled. It is important that you have these codes at the time of installation.

Paygistix Server Client must be installed on the RMSERVER. It is recommended that you install the Paygistix software as an administrator, especially on Windows 10. Again, it is critical that all POS terminals and rmserver be setup up with an IP scheme (i.e. 192.168.x.xxx), the PAX devices have access to the internet. and firewall, router allow communication for port . You should also make sure the port 8080 is allowed on the server computer's Windows firewall if enabled. After installation, you must enter the activation code. It is mandatory the Paygistix Server Client be running for credit cards to be processed thru Restaurant Manager. Therefore, it should be considered mandatory the client software be added to the Window's Start folder or added to Restaurant Manager's RMStart program. Note: in most circumstances, PaygistixClient.exe will be installed in Window's Program Files\ Payment Logistics \ Paygistix Client.

Note: The Paygistix Client Software should be running as an "administrator for all users".

Installing PAX Hardware

Payment Logistics uses a template for pre-configured PAX unit settings created for integration with Restaurant Manager software. This means resellers simply have to plug the device into network. After being connected to the network, Paygistix will pick up an IP via DHCP for the PAX device and then report the device to Payment Logistics automatically.

Note: A "clear batch" is required before a device can be downloaded with new settings. When a clear batch (RMPOS > Misc . CC Options) is performed on a device it does not clear the batch at the gateway, just on the pinpad device. It is required because the terminal will not download new settings if it has any transactions in it.

Payment Logistics Contact Info

Orders for Paygistix are placed through the Payment Logistics Partner Support Team. They can be contacted at 1-888-472-9564. The support team will place the order and then pass the order to the Technical Support Team. The Technical Support team will reach out to your dealership to outline the details for installation.

Restaurant Manager Paygistix Setup

Paygistix EMV setup for Restaurant Manager is a relatively easy process that should take no more than 30 minutes for an experienced user. Paygistx EMV setup for Restaurant Manager will involve the following:

- Configure RMCCWin- disable credit card processing
- Setup new EMV payment(s) - use EMV/NFC payment setting in Method of Payment Setup Form
- Configure Paygistix EMV using options in RM Gateway / Payment Processing Interface in Station Configuration.
- Configure Pre-Auth Options for CC Tabs
- Configure POS Function Buttons

Installing Restaurant Manager Software

All upgrade/update procedures should be followed. This includes closing all Restaurant Manager programs at the POS, RM Server computer, and doing a complete back up. This will require that the session be closed and all employees logged out. You should have the upgrade in advance of installation. When running the installation package, and if you are currently on v19.0, choose one of the two "Update current version" options when prompted. Choose on of the two Upgrade options if upgrading on any version prior to 19.

Paygistix setup for Restaurant Manager is a relatively easy process that should take no more than 15 minutes for an experienced user. It is important that you have all the information Payment Logistics has provided at the time of setup. Specifically, you will need the following:

- **User name and password for each terminal**- both user name and password are unique for each station
- **Vendor ID**- this will typically be a four digit number
- **URL**- in most cases this will be the IP of the server computer (i.e. http://192.168.1.10/8080/). If running a terminal on a server/POS computer use the IP loopback (i.e. http://127.0.0.1/8080/)

This information is critical for the Station Configuration Setup.

Paygistix setup for Restaurant Manager will involve the following:

1. Configure RM Gateway Supplemental Setup (RMCCWIN)- disable credit card processing
2. Setup new EMV payment - use new EMV/NFC payment setting in Method of Payment Setup Form
3. Configure Paygistix using options in RM Gateway / Payment Processing Interface.
4. Configure Pre-Auth Options for CC Tabs
5. Configure POS Function Buttons

RM Gateway Supplemental Setup (RMCCWIN)

RM Gateway Supplemental Setup (RMCCWIN) is not needed in for processing credit cards with Paygistix. Because of this, you will want to configure your system as follows:

- Disable credit card processing- open RM Gateway Supplemental Setup (RMCCWIN) and set the Credit Card Option's field "Credit Card Interface Type" to "disabled". The process will require an administrator password.
- Remove RM Gateway Supplemental Setup (RMCCWIN) from RMStart or similar command files used during Windows start up. RMCCWin is still needed to process 3rd party gift cards. Do not remove RMCCWin from RMStart if using 3rd party gift cards.
- Remove any client software used by other credit card processing systems at Windows start up.

It is important that these steps are performed prior to installing a new Restaurant Manager build when replacing another credit card processing system with Paygistix.

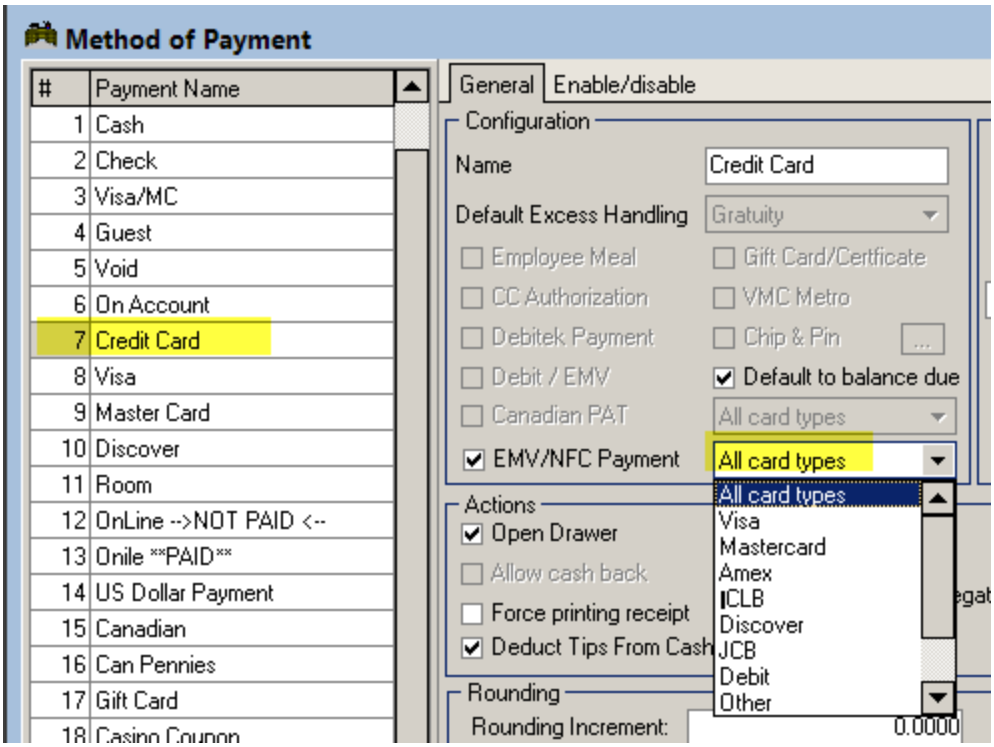
Forms of Payment Setup

Forms of Payment setup for Vantiv EMV in similar to any other credit processing with two exceptions. The first exception is rather than using the CC Authorization option in the Method of Payment form, you will use the EMV/NFC Payment option. The second difference is you will want to use the drop down menu to the right of this option to define a card type rather than using Automatic Credit Card Detection.. Note: Payment type # 3, Credit Card, will not work with EMV. You should disable this method on all stations.

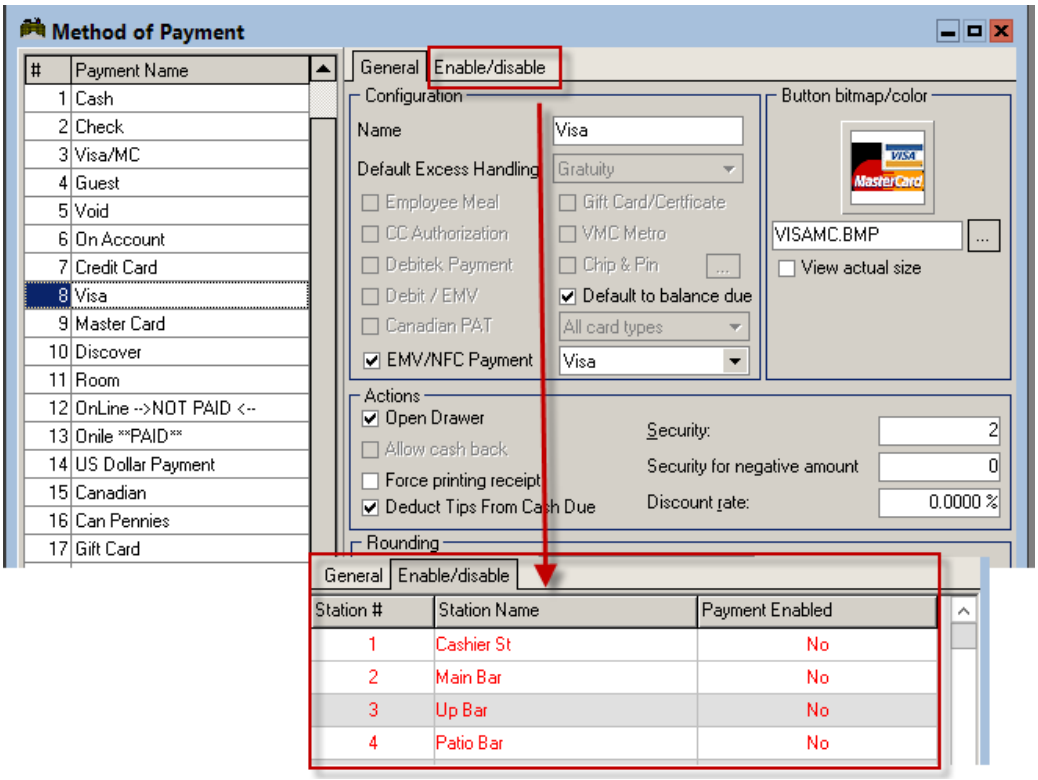
Naming Payments - Note Mastercard must be spelled as one word as well as Dinersclub.

Single Catch All CC Payment

You can setup a form of payment (Payment #3 Credit Card cannot be used for this) as a catch all if need. In this circumstance, you will use "All Card Types" option in the drop down menu.

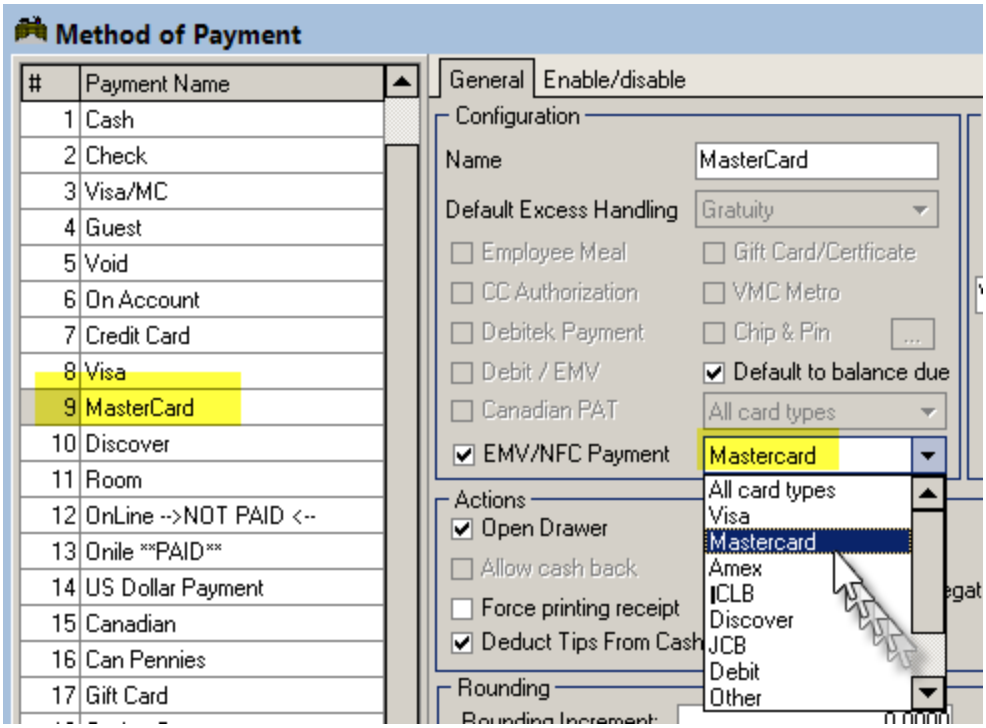


You will also want to setup a CC EMV payment type for each type of credit card (Visa, Mastercard, Amex, etc), enable the EMV / NFC Payment option, and select a card type using the drop down menu. You will then want to take each individual payment type and disable it with the exception of the catch all payment. This arrangement will make for a clean settlement screen while providing accurate settlement reporting.



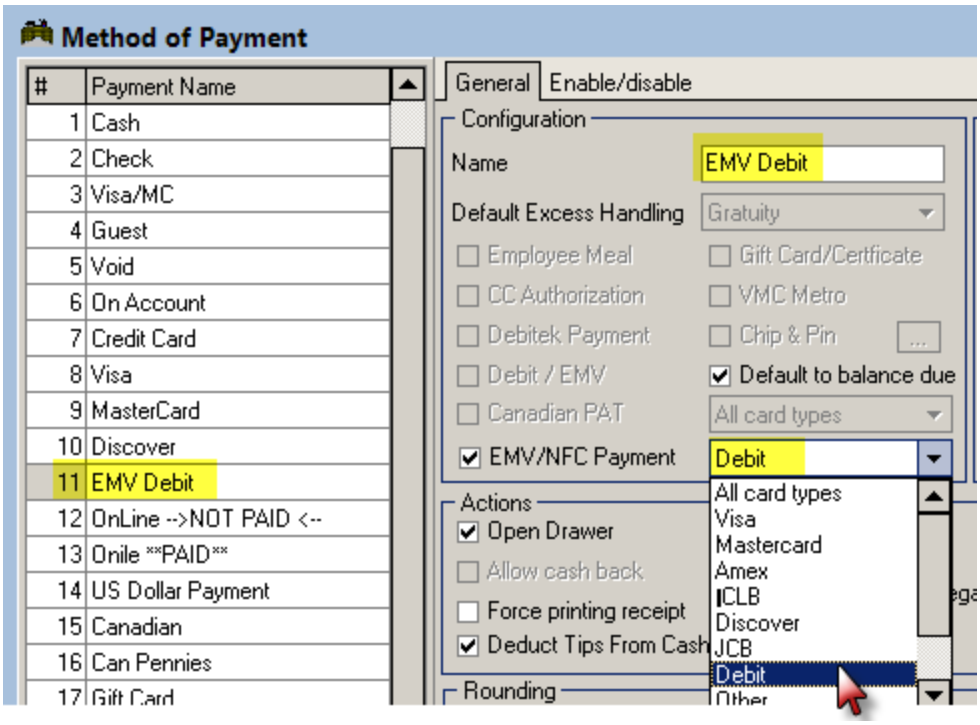
Individual EMV CC Payments

If you do not want to set up a catch all payment method, you can create an individual payment method for each credit card type accepted. For each form of payment you must enable the EMV / NFC Payment option and select a card type using the drop down menu.



Debit Card Payment

Chances are you never use this form of payment. We are creating this form of payment to prevent certain errors from happening. Create your form of payment , enable the EMV / NFC Payment option, and select the "Debit" option using the drop down menu.



Note: Debit card processing must be specifically requested at the time of ordering Payment Logistics. When ordered, Payment Logistics will configure the PAX devices to prompt for Debit or Credit.

Station Configuration Setup

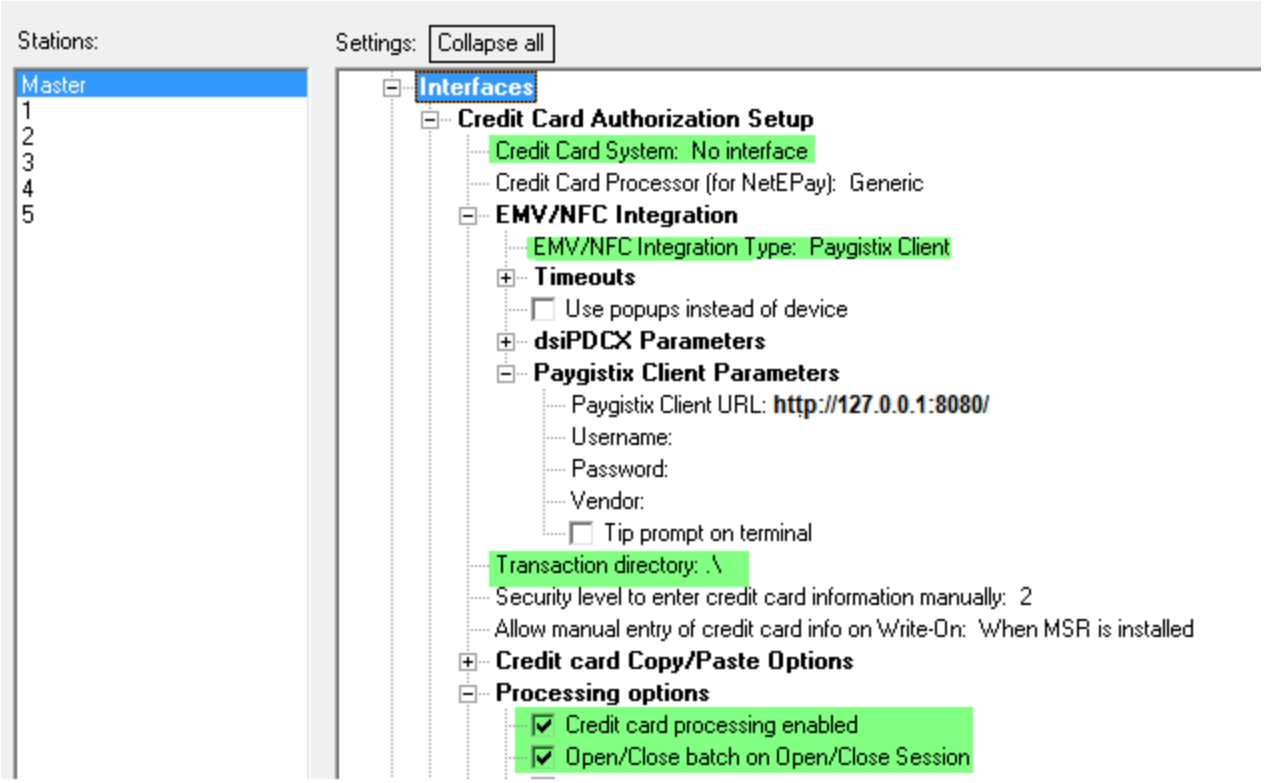
Each station will have to be configured differently under the Paygistix Client Parameters under Credit Card Authorization because each PAX device associated with a station will have its own user name and password. In addition, settings for the Master Station Configuration will be different than the stations.

Master Station Configuration Settings

Use the following steps for the Master Station Configuration only:

1. Click "Admin Settings" and enter Administrator Password
2. Use Search button and use "NFC" in search field. Paygistix settings are under Interfaces > RM Gateway / Payment Processing Interface)
3. Use the drop down menu on Credit Card System (under RM Gateway / Payment Processing Interface) and select "No Interface"
4. Click on the plus next to "EMV/NFC" Integration to expand the menu tree and configure the following options:
    - **EMV/NFC Integration Type** = Paygistix Client (this can be copied to all stations)
    - **Timeouts** = Set the Timeouts as high as possibly convenient. For example, during CCTab, a setting of 10 could causes POS to timeout after ten seconds even when the device transaction succeeded. This means that the amount was actually charged to the card but is not reflected in the POS and will result in an unbalance batch.
    - **Use popups instead of device** = This option is not used with PL's Server Client App
5. **Paygistix Client Parameters:** - The settings under this heading should be left to their default settings. These options are only for stations with a PAX unit attached.

6. **Processing Options**- configure the following options:
    - Credit Card Processing - enabled (this can be copied to all stations)
    - Open Close Batch on Open Close Session- enable if using Merchant Initiated Batch. Disable if using Payment Logistics Time Initiated Batch Close (this can be copied to all stations)



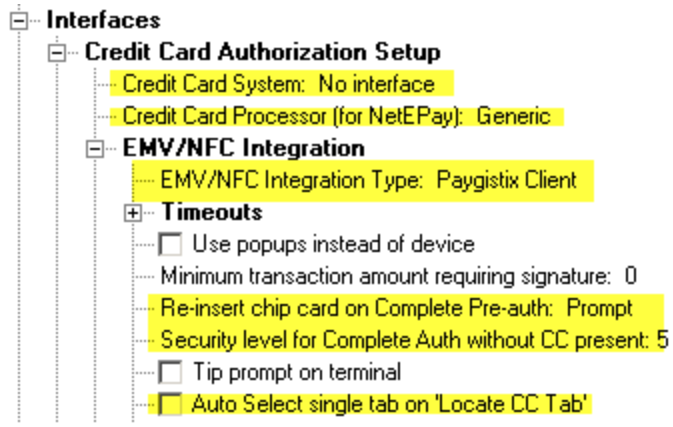
Station Configuration Settings

Use the following steps to configure all station configuration settings except for the Master Station.

1. Click "Admin Settings" and enter Administrator Password
2. Use Search button and use "NFC" in search field. Paygistix settings are under Interfaces > RM Gateway / Payment Processing Interface)
3. Click on the plus next to "EMV/NFC" Integration to expand the menu tree and configure the following options:
    - **EMV/NFC Integration Type** = Paygistix Client (this can be copied to all stations)
    - **Timeouts** =Use default settings
    - **Use popups instead of device** = This option is not used with PL's Server Client App
    - **Minimum transaction amount requiring signature** = This amount is the limit for requiring to print a credit card transaction or require a signature. For example, if sets to $15, then for any transaction under $15, RMPOS would not print a credit card slip or require a signature.
    - **Re-insert chip card on Complete Pre-Auth** = Use default setting "Prompt". If using the CC Tab feature to pre-authorize credit cards, chip cards must be re-inserted into the chip reader on Complete Pre-auth in order to be EMV compliant. If the card it is NOT re-inserted into the reader, Restaurant Manager can still process the transaction using a token; however it will not be EMV compliant and the merchant assumes the liability in the event of a charge back. It is preferable to re-insert the card if possible, but that requires the customer to be on premise to present their card to the bartender or server. Setting this option to "Prompt" will provide the option to re-insert card for added liability protection, however the customer

must present their card to the bartender or server again in order to complete the settlement process. This option only applies to all cards with a smart chip.

- **Security Level for Complete Auth without CC present** = The default setting is 9. Enter the security level to permit closing a pre-auth EMV transaction with Complete Pre-Auth when a card is not present. Closing a transaction without a card present is considered to be non EMV compliant and the merchant will assume all charge back costs.
- **Tip Prompt on Terminal** = Optional. This option determines if the terminal will display a tip prompt when processing a sale. This may be preferred for customer facing devices but is not ideal for establishments were the EMV device is not present.
- **Auto Select single tab on "Locate CC"** = When doing 'Locate CC Tab' (for tabs opened with EMV devices), RMPOS might wrongly open a Tab having the same last 4-digits belonging to a different customer. To prevent this, disable this option so that the user will need to touch to confirm the correct tab. This option affects NFC/EMV users only.



4. **Paygistix Client Parameters**: configure the following options as follows:
   - **Paygistix URL** = enter the IP of the server computer along with port 8080 followed by a forward slash. Example:http://192.168.1.100:8080/. (this can be copied to all stations). If running a POS station on the server computer use the IP loopback (http://127.0.0.1:8080/). Make sure that the firewall of the target machine is not blocking port 8080.
   - **UserName** = provided by Payment Logistics. The user name will differ for each station.
   - **Password** = provided by Payment Logistics. The password will differ for each station.
   - **Vendor** = given by Payment Logistics (this can be copied to all stations)
   - **Tip prompt on terminal** = default setting is disable. When disabled, you will enter tips at the POS station using the "Tip" button on the Settlement Screen at the POS. If enabled, the tip prompt will appear on the PAX unit directly after the card swipe. This setting is intended for customer facing units.
   - **Transaction Directory** = use the default ".\" which causes Restaurant Manager to use the Restaurant Manager working directory. If you enter a different directory name, make sure to specify the drive letter and full path (this can be copied to all stations)
5. **Processing Options**- configure the following options:
   - **Credit Card Processing** - enabled (this can be copied to all stations where processing is allowed and a PAX device is present)
   - **Open Close Batch on Open Close Session**- enable if using Merchant Initiated Batch. Disable if using Payment Logistics Time Initiated Batch Close. (this can be copied to all stations)
6. **Credit Card Receipt Options** - configure the following option:

   Always Print EMV Void Slip = Sites using signature capture unit (i.e. MT30) will want to enable this function if they have opt to not print CC Receipts.
7. Add Tip Options - Enable "Wait for add-tip approval"

Configure Pre-Auth for CC Tabs

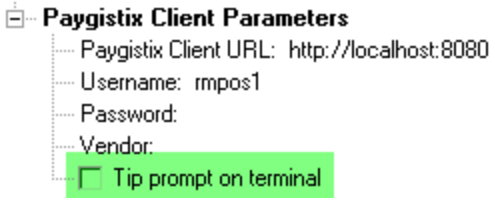
As stated in the Introduction and FAQ's sections, CC Tabs require PreAuths to be enabled. You will want to go into Station Configuration > Interface > RM Gateway / Payment Processing Interface > Credit Card Pre-Authorization.Configue the option under the menu branch as needed. At a minimum you will need to enable Credit Card Per-Auth, and set a default amount (i.e. $1.00) Prompts and repeat pre-auth can be disabled if needed. Note - Discard initial pre-auth does not apply to EMV.

Configuring Tips at the POS

The handling of tips will differ slightly when using the Paygistix interface. In most circumstances, tips are added when submitting an authorization, after submitting an authorization, and after finalizing a guest check. The three sections below will tell you how to configure the POS system to handle each scenario mention above.

Configuring Tips at Time of Authorization

In most cases, adding a tip at the time of authorization is performed in a quick service environment when the customer is present. The process outlined in this section does not include the circumstances where an automatic gratuity is being added. Since we are adding a constant tip amount prompt to the PAX device, this section applies to when the customer is entering a tip whether it be a counter service or pay at the table. In this circumstance, all you will need to do is enable the "Tip prompt on Terminal" under Paygistix Client Parameters in Station Configuration > RM Gateway / Payment Processing Interface. This option requires the use of an Administrator password.



Configuring Tips After Authorization

Adding a tip after authorization but before finalizing a transaction is common place for most full service restaurants and bars. In this circumstance you will want to enable the following settings:

1. Require Confirm (Revenue Center setting)
2. Warn if no tip adjustment (Station Configuration setting)

Configuring Tips After Finalization

Many establishments choose to submit credit cards, finalize for the base amount, and then return at a later time to enter a tip (i.e. after a restaurant has closed). This process will require disabling the "Require CONFIRM" in the Revenue Center Setup Form. Disabling this prompt will have the effect of automatically finalize the transaction when the bill has been paid in full. You will also want to enable the Revenue Center setting "Auto Finalize". You should consider adding the Adjust Tip function button to all POS Modes Status screens if the restaurant chooses to add tips after credit card finalization (see section below).

Configuring POS Function Buttons

There are two function buttons you may want to add to the POS

- **Locate CC Tab** - this function button will awaken the PAX unit. Once awakened, the employee can swipe the credit card in the PAX, which in turn, will communicate with the POS and open any tab associated with the swiped card.
- **Adjust Tip** - this function button will allow employees to adjust tips after a credit card payment has been finalized. The behavior of this function is controlled in station configuration under Revise by Employee and Tip Adjust options.
- **Complete Pre-Auth** - you will want to add this function button to the Tab Settlement screen. All CC Tabs will require Pre-Auths to be processed. Therefore it will be necessary to add the Complete Pre-Auth to the Tab Settlement screen.

The function buttons above are added in the RM Back office Module under Setup > Screen Layouts > POS Function Button Layouts. The Adjust Tips function button can be added to all POS Mode Status screens. The Locate CC Tab function button can only be added to the tab Status screen.

Delivery Considerations

You might want to consider some of the following options if your restaurant does delivery or call in orders where you take card numbers over the phone.

Add Pre-Auth functionality to delivery- adding this option will help if it is common for customers to call back to add or adjust items after the initial call. The Pre-Auth will capture a predetermined dollar amount and the Complete Auth will finish the order when the driver is ready to go out the door. This will help prevent the order taker asking for a card a second time.

Enable Save/Restore loyalty module credit card info - this option will save a credit card number to a specific telephone number. Once the CC number has been recorded, it will save the employee time by not having to manually re-enter the number.

Note: all credit card transactions performed without a card is not present is considered to be non-emv compliant and liability remains with the merchant.

Closing a CC Batch

A restaurant with multiple stations is registered at Payment Logistics as one account (i.e., one Merchant ID) with MULTIPLE users. This is because each station will have separate user names per each device. Note that each station should be installed with a Paygistix client. Closing a CC batch can be performed through the Restaurant Manager POS System (Merchant Initiated) or through Payment Logistics (Time Initiated) . The later method will have to be arranged with Payment Logistics. Please read the section below to see which method will benefit the restaurant the best.

Merchant Initiated Batch Closing

Merchant initiated batch closing is the process where a CC batch is closed at a predetermined time through the restaurant Manager POS system. When the batch is closed, all transactions from all stations merge into one batch. Note that batch reports are not available when doing Merchant Initiated batch closing.

When "Open/Close batch on Open/Close Session" is enabled, the batch is closed when the session is closed. When this happens, the following is seen in the SessOpen screen:

Time Initiated Batch

Time initiated batch closing is when a CC batch is closed at a predetermined time and is initiated by Payment Logistics. You must contact Payment Logistics to have them set up the account to automatically close at the desired time. The benefit to Time Initiated batch closing is Payment Logistics will send an email to a predetermined restaurant email address that confirms the batch has been closed along with a credit card batch summary. This email will not go out if the time initiated batch fails or if the site uses the Merchant Initiated batch option.

To set-up for Time-Initiated Batch Close all station Restaurant Manager "Open Close Batch on Open Close Session" options should be disabled.

There may be time when the merchant needs to clear the batch (e.g., when the batch is not balanced). The following should be done:

- Log in to the Payment Logistics Merchant Portal
- Select “End of Day” then “Credit”
- Force to close the batch

Windows Settings for PCI

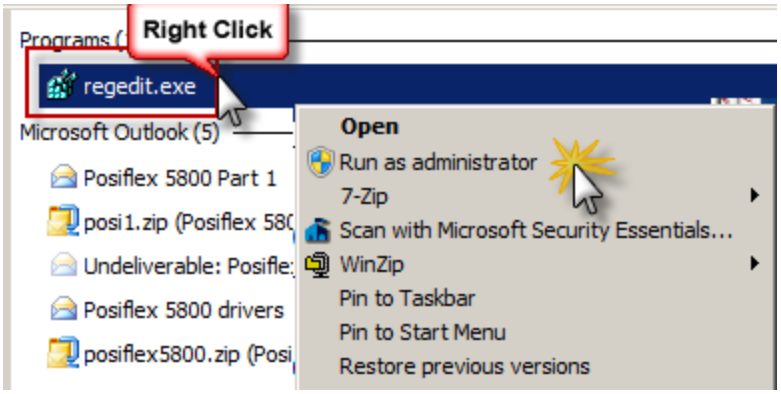
There are several Windows settings that must be configured to prevent the system from inadvertently capturing credit card (PAN) information. The main objective is to reduce the threat of the possibility of malware stealing PAN information in virtual memory. In most circumstances, credit card data is not contained within the rmwin folder when using Paygistix. However, if the Pop Up Mode is enabled in Station Configuration, there will be the possibility that credit card data is captured in the POS computers virtual memory via a keyboard entry or standard MSR swipe. It is imperative you use the following steps to eliminate this possibility. This is done by clearing the system pagefile. sys at shutdown, disabling System Management of PageFile.sys, and disabling system restore. These settings only need be configured on all computers with an MSR attached or where credit data is entered manually. The following instructions are for Windows 7.

Clearing the System Pagefile.sys on Shutdown

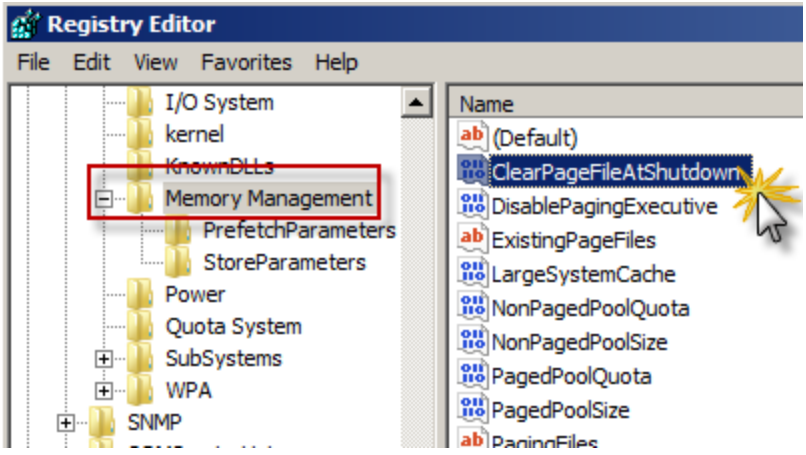
Windows has the ability to clear the Pagefile.sys upon system shutdown. Doing so will purge all temporary data from the pagefile.sys (temporary data may include system and application passwords, cardholder data (PAN/Track), etc.).

NOTE: Enabling this feature may increase windows shutdown time.

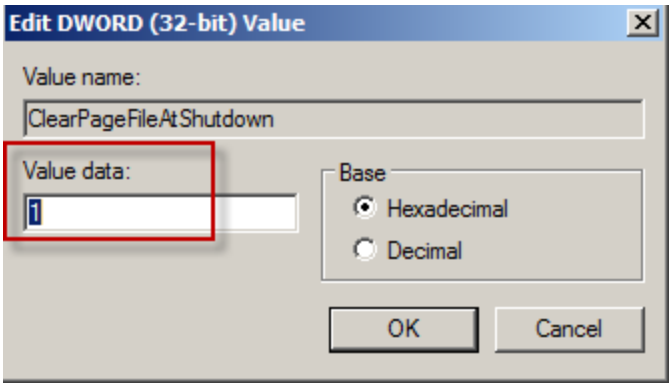
1. Click on the Windows "Start" and in the search box type in "regedit".
2. On the program list, right click on regedit.exe and select "Run as Administrator"



3. Navigate to HKEY_Local_Machine\System\CurrentControlSet\Control\Session Manager\Memory Management. Double click "ClearPageFileAtShutdown".



4. Change Value data from 0 to 1



5. Click OK and close Regedit

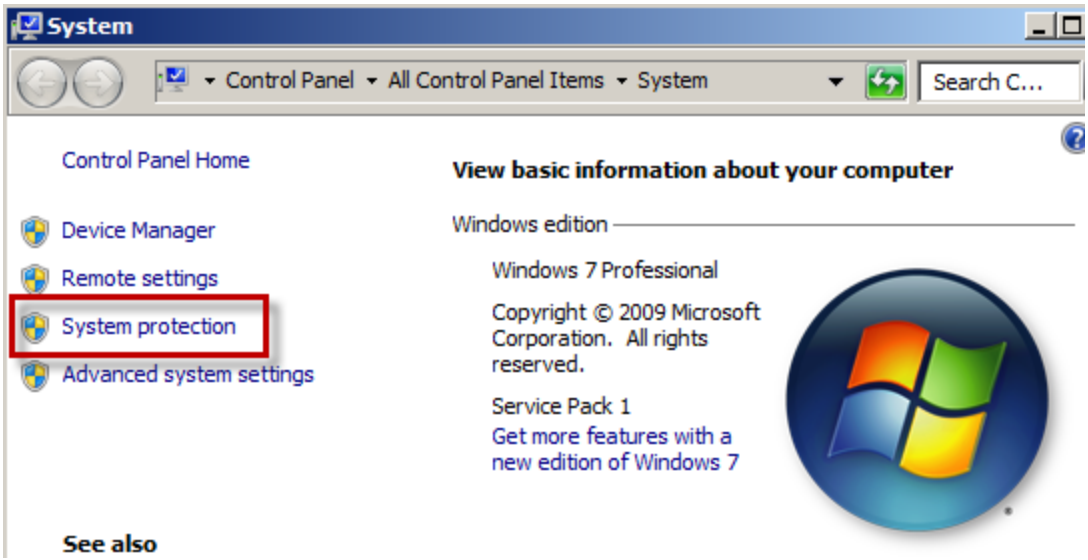
NOTE: If the value does not exist, right click on the Memory Management folder, select "New" on the drop down menu select "DWORD (32-bit or 64 bit depending on OS) Value" and add the following:

- Value Name: ClearPageFileAtShutdown
- Value Type: REG_DWORD
- Value: 1

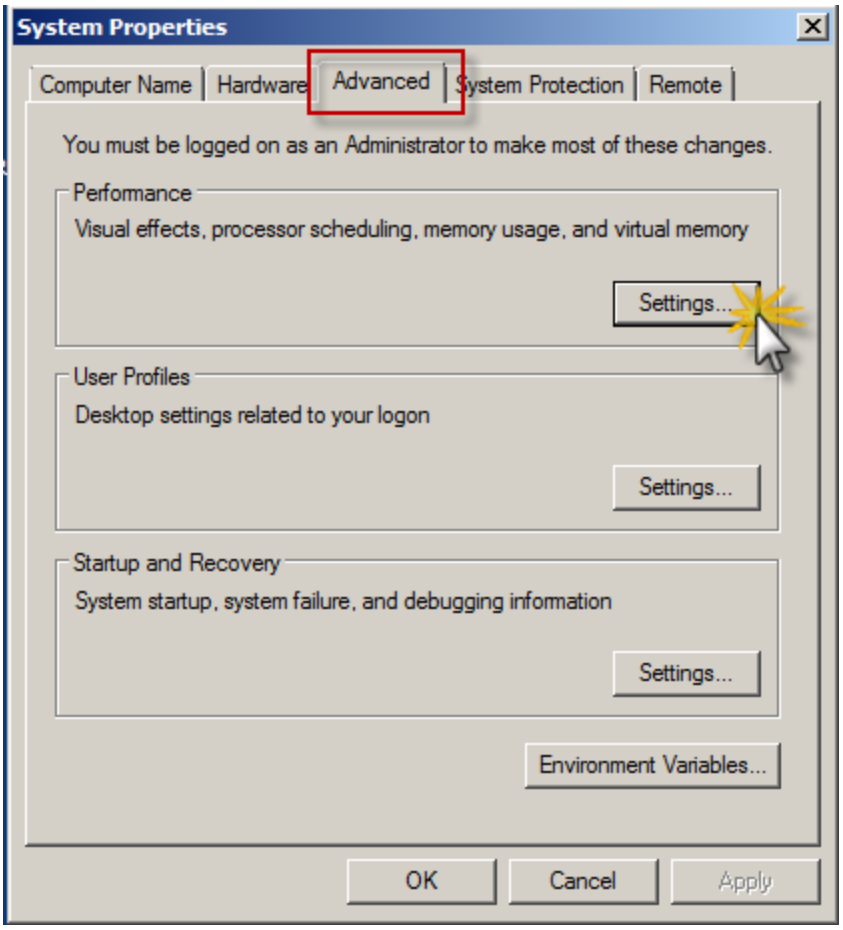
Disabling System Management of PageFile.sys

You will want to disable memory page swapping to the hard drive. The following steps will show you how to tweak virtual memory settings in Windows by disabling (pagefile.sys).

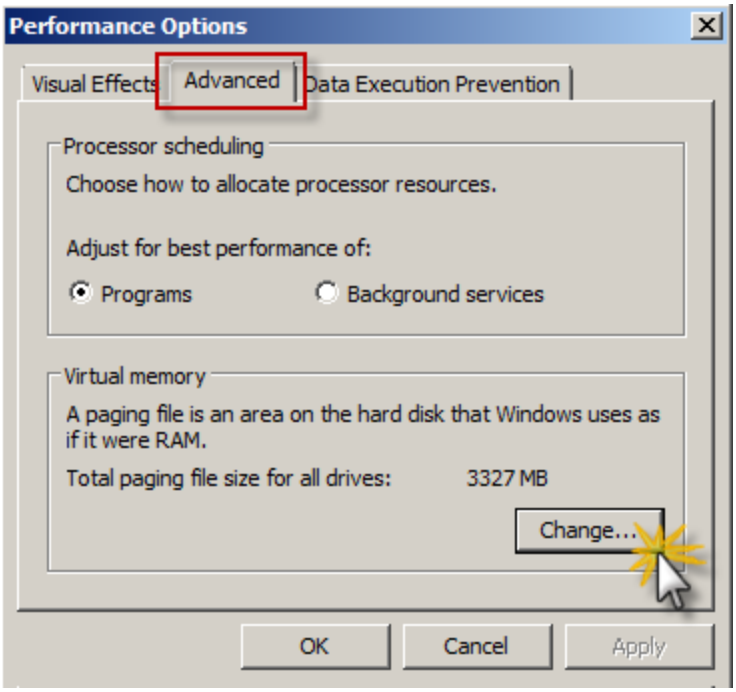
1. Right Click on Computer > Select "Properties"
2. Select "System Protection" on the top left list



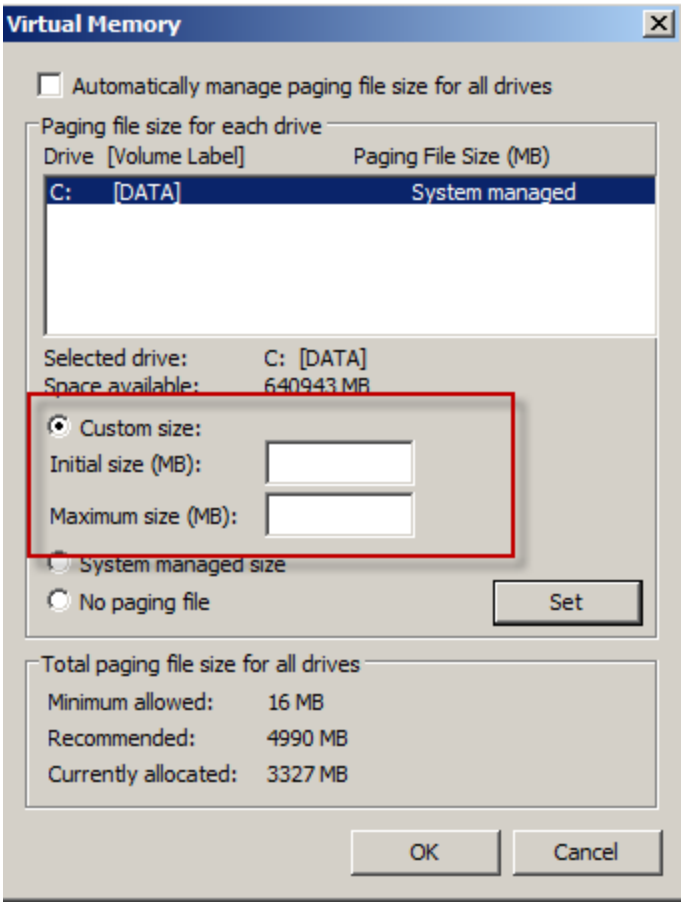
3. Select the "Advanced" tab and click "Settings" under Performance section



4. Click the "Advanced" tab in the Performance Options window and click "Change" under Virtual Memory



5. In the Virtual Memory window:
    - Uncheck "Automatically manage page file size for all drives"
    - Select "Custom Size"
    - Enter the following for the size selections:
        - **Initial Size** - as a good rule of thumb, the size should be equivalent to the amount of memory in the system.
        - **Maximum Size** - as a good rule of thumb, the size should be equivalent to 2x the amount of memory in the system.
    - Click "Set"



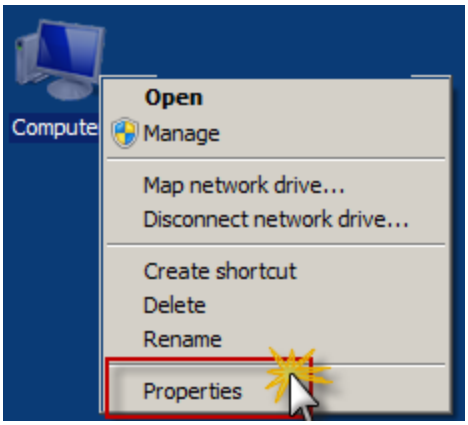
6. Return to default windows screen by clicking "OK" three times
7. Reboot the computer

Note: you may want to increase the size of your RAM to counter the effects of disabling pagefile.sys

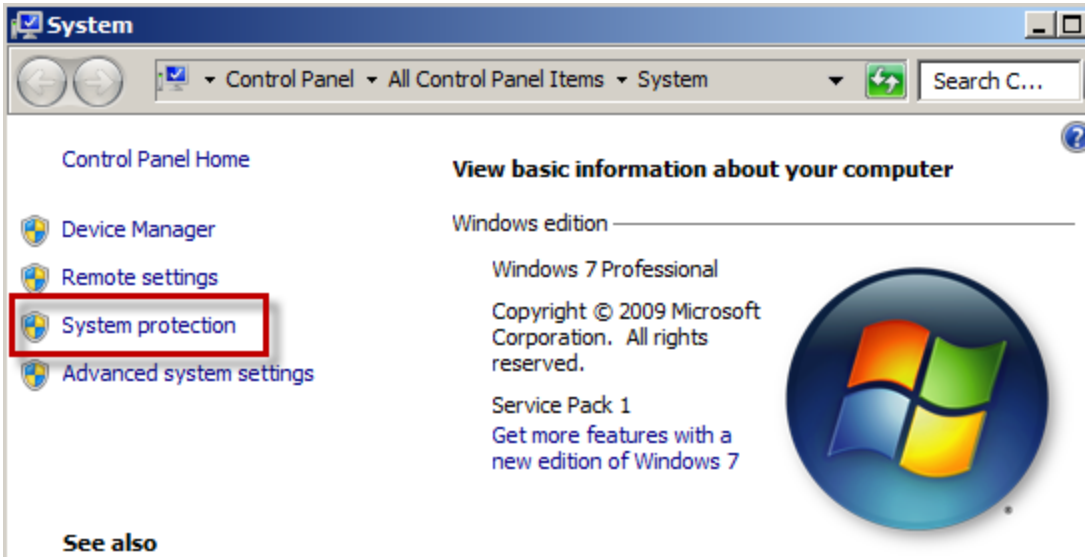
Disabling System Restore

The following steps describe how to disable system restore points. This is critical as a system restore point may inadvertently capture cardholder data if it is not disabled and compromise your PCI DSS compliance.

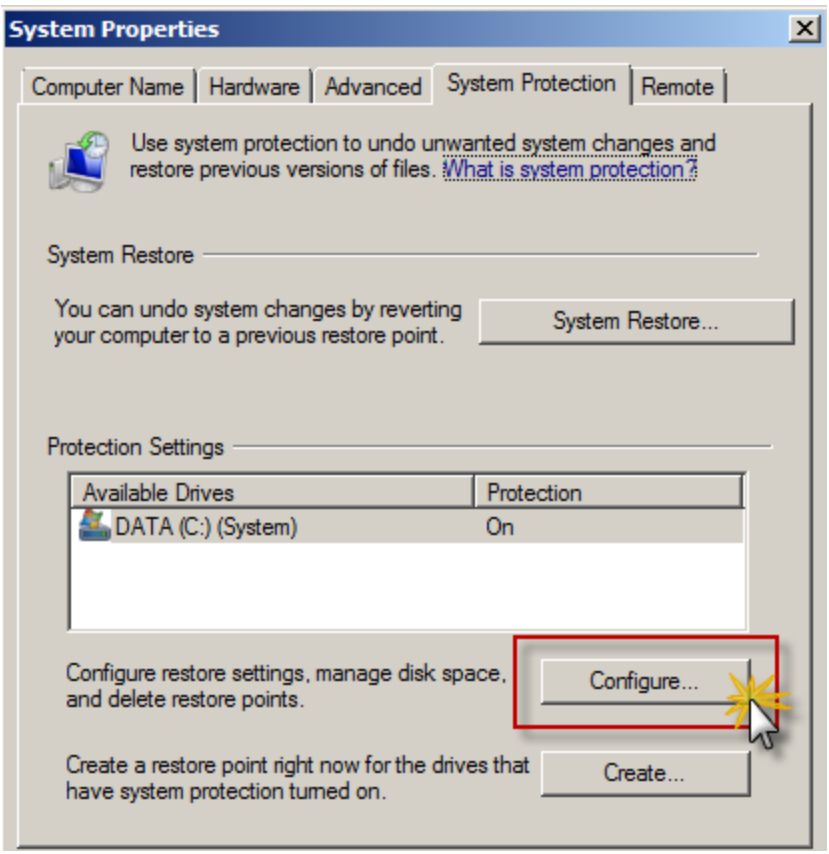
1. Right Click on Computer and Select "Properties" on the pop up menu pop up.



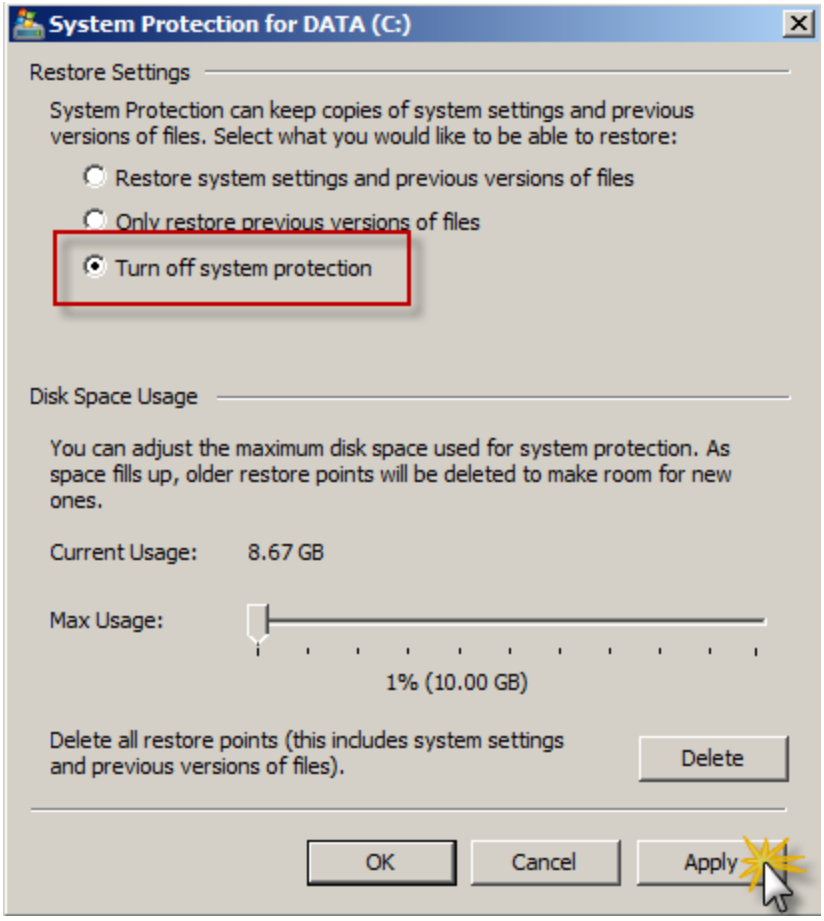
2. Select "System Protection" on the top left list.



3. Click "Configure" under the System Protection tab.



4. Click to enable "Turn off system protection", click "Apply", and then click "OK" to close System Protection window.

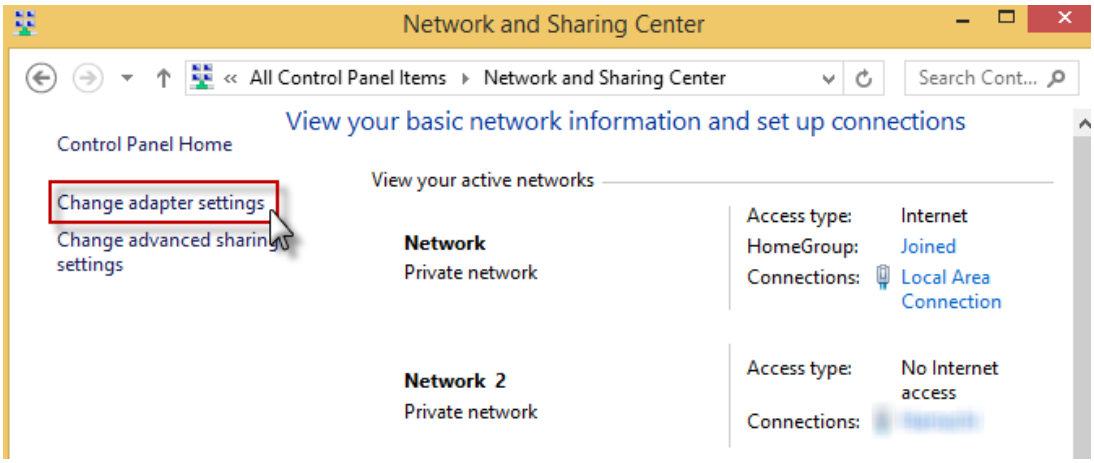


5. Click "OK" to close System Proprieties window.
6. Reboot computer.

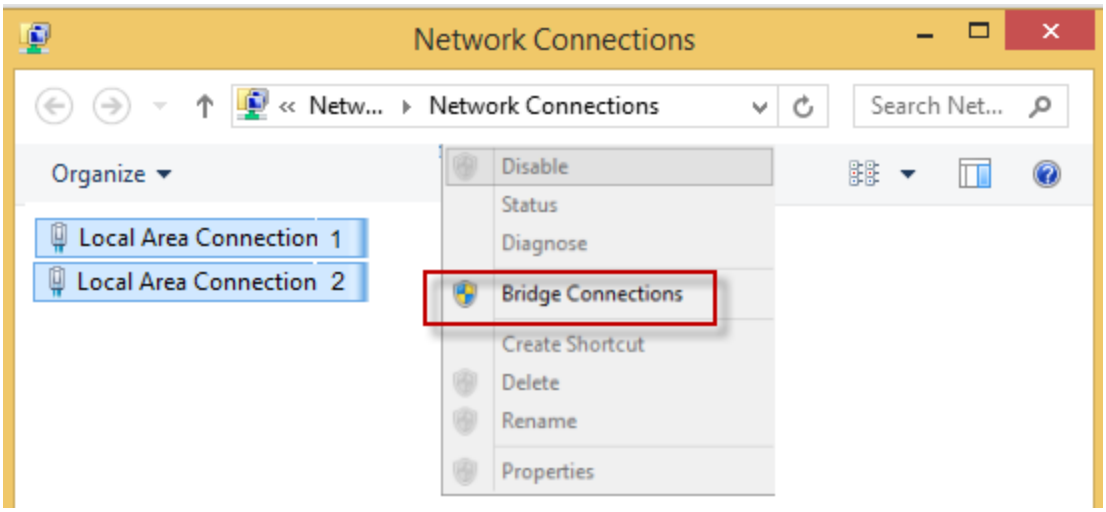
Bridging Internet Connections

Windows provides the capability to connect or bridge two different network types through software. This can eliminate the need to buy a hardware device to connect two disparate networks. To bridge multiple network connections:

1. Open Window's Control Panel, click Network and Sharing Center and click Change adapter settings:



2. Select the adapters that you want to bridge using one of two methods:
    i. Left click and and circle the two network connections
    ii. Hold the "Ctrl" key on keyboard and click on both network connections



3. Right click on one of the highlighted network connections, select the "Bridge connections" option.

Related Documents

The following documents detail the both the Paygistix use at the POS and common PCI Guidelines for safe installations.

Paygistix Installation Guide (PDF Format)

Paygistix at the POS for Full Service Restaurants (PDF Format)

Paygistix at the POS for Counter Service Restaurants - QSR (PDF Format)

Paygistix at the POS for Cashier Environments (PDF Format)

Paygistix at the POS for Pre-Auths (PDF Format)

RM PCI Compliance Guide (HTML Format)