

## Introduction

### Purpose

This manual provides network-specific information for Passport® systems at stores that use the WorldPay® network that are:

- Upgrading from Passport V10 with Service Pack Q or later
- Upgrading from Passport V11.02 with Service Pack G, Service Pack J with JMP2 or later or later
- Installing Passport V11.04 for the first time

### IMPORTANT INFORMATION

**Passport V11.04 software requires PX60 hardware platform. Do not upgrade to V11.04 if the store is not already running on PX60 hardware.**

**Upgrading to Passport V11.04 requires advance notice to the WorldPay network that the site is implementing EMV® functionality on Passport.** In this version, EMV functionality affects inside transactions. At least two full days before the scheduled upgrade, advise the merchant to contact the WorldPay network and explain that the site is implementing an upgrade to Passport to enable EMV. The merchant should advise the network representative of the date the upgrade is to take place, and request that the network prepare to enable EMV with appropriate parameter downloads on that date. Ask the merchant to let you know if the network is unable or unwilling to make the necessary preparations for enabling EMV for the store.

**For ALON branded stores, advise the merchant or store manager to contact ALON at 1-877-256-6729 a week before the scheduled upgrade. ALON will provide the merchant or store manager with instructions for preparing for the upgrade.**

On the day of the scheduled upgrade, ask the merchant or store manager if he notified the WorldPay network of the need to prepare to enable EMV network communication. If the merchant or store manager has not notified the WorldPay network of the need to enable EMV network communication, call the network on behalf of the merchant or store manager. Ask the network representative if he can expedite enabling EMV functionality for the store within four hours. If the network representative indicates he can prepare for enabling EMV on the network within the next four hours, continue with the upgrade. Otherwise, consult the merchant or store manager regarding your options, which are:

- Upgrade without enabling EMV and return later for the PDL Download to enable EMV.
- Arrange a later date for the upgrade, after the network has sufficient time to enable EMV.

### Intended Audience

This manual is intended for merchants, cashiers, store managers, and Passport-certified Gilbarco® Authorized Service Contractors (ASC).

*Note: Leave this manual, excluding “Appendix B: Upgrading to Passport V11.04” on page 47 at the site for the manager’s reference. This manual is available for download by Passport-certified ASCs on Gilbarco Online Documentation (GOLD<sup>SM</sup>).*

**REVIEW AND FULLY UNDERSTAND THIS MANUAL BEFORE BEGINNING THE UPGRADE OR INSTALLATION OF PASSPORT V11.04 FOR WORLDPAY.**

## Table of Contents

Topic	Page
<a href="#">Introduction</a>	1
<a href="#">What's New in Passport V11 at WorldPay Stores</a>	5
<a href="#">First Time Installation Instructions</a>	9
<a href="#">Network Site Configuration Programming</a>	10
<a href="#">Network Card Configuration</a>	24
<a href="#">Accepting Magnetic Stripe Contactless Inside</a>	27
<a href="#">Network Journal Report</a>	28
<a href="#">Network Reports</a>	29
<a href="#">CWS Network Functions</a>	38
<a href="#">Third-party Licenses</a>	41
<a href="#">Appendix A: Stores with TCP/IP SSL Connections and Programming for Gilbarco RV042 Firewall Router</a>	43
<a href="#">Appendix B: Upgrading to Passport V11.04</a>	47
<a href="#">Appendix C: WorldPay Egress Rules for the SZR</a>	49

## Related Documents

Document Number	Title	GOLD Library
MDE-3816	Passport Hardware Start-up and Service Manual	<ul style="list-style-type: none"> <li>• Passport</li> <li>• Service Manual</li> </ul>
MDE-4696	Ingenico® PIN Pad Kits (PA0379XXXXX and PA0383XXXXX) Installation Instructions	POS Peripheral Devices
MDE-4826	Passport Card and Face-based Local Accounts Setup and Operations Manual	Passport
MDE-4834	Passport System Recovery Guide for Passport V8.02+	Passport
MDE-4866	Passport Firewall Router Start-up and Service Manual	Passport
MDE-4954	Passport Start-up and Service Manual for the Cisco® Firewall Router (Q13708-08)	Passport
MDE-5025	Passport Point of Sale System Passport V9+ System Reference Manual	Passport
MDE-5026	What's New in Passport Versions 9 and 10	Passport
MDE-5083	Passport Hardware Start-up and Service Manual for PX60 Platform	<ul style="list-style-type: none"> <li>• Passport</li> <li>• Service Manual</li> </ul>
MDE-5167	Gilbarco Deployment Service (GDS) Start-up and Service Manual	Passport
MDE-5213	VeriFone® MX915 PIN Pad Kit Installation Instructions	Passport
MDE-5218	MX915 PIN Pad to Passport Configuration Poster	Passport
MDE-5266	What's New in Passport Version 11	Passport
MDE-5382	Secure Zone Router (Acumera) Installation Instructions	Passport
SP-3803	Wiring Quick Reference for Applause and EMV Connectivity	Passport

## Abbreviations and Acronyms

<b>Term</b>	<b>Description</b>
AID	Application Identifier
ASC	Authorized Service Contractor
BOS	Back Office System
CD	Compact Disc
COM	Communication
CRIND®	Card Reader in Dispenser
CVM	Cardholder Verification Method
CVV	Cardholder Verification Value
CWS	Cashier Workstation
DNS	Domain Name System
EBT	Electronic Benefits Transfer
EDH	Enhanced Dispenser Hub
EMV®	Europay®, MasterCard®, and Visa®
GOLD	Gilbarco Online Documentation
ISP	Internet Service Provider
LAN	Local Area Network
MWS	Manager Workstation
PA-DSS	Payment Application Data Security Standard
PPU	Price per Unit
RAS	Remote Access Service
SSL	Secure Sockets Layer
SVS	Stored Value Solutions
SZR	Secure Zone Router
TCP/IP	Transmission Control Protocol/Internet Protocol
TID	Terminal ID
VEPS	VISA Easy Payment Services
WAN	Wide Area Network

## Technical Support

If you are a store manager or merchant and you need assistance with your Passport system, call Gilbarco at 1-800-800-7498.

If you are an ASC and need to verify RAS connection or activate a Passport feature, call Gilbarco at 1-800-800-7498. If you need assistance with an upgrade or installation issue, call Gilbarco at 1-800-743-7501. Be prepared to provide your ASC ID.

To contact the WorldPay Help Desk, call 1-800-200-5965.

## Network Data Retention

The Passport system's network database saves all transaction details for 35 days, which means Passport purges network transaction details older than 35 days. This network setting is not editable.

Besides meeting Payment Application Data Security Standard (PA-DSS) compliance requirements, it also allows retailers to use the Backup Journals/Reports utility to save up to one full month of Passport system data on a single CD. For additional information on saving journals and reports to CD, refer to *MDE-5025 Passport V9+ Reference Manual*, found on user documentation CD that accompanies the Passport software.

---

# What's New in Passport V11 at WorldPay Stores

The following features have been updated or are new for the WorldPay stores:

## Network Site Parameters

Beginning with V11.02, the **Network Site Parameters** section includes the new **EMV Parameters** tab for configuring how Passport is to behave for EMV transactions inside. For more information about **Network Site Parameters**, refer to [“Network Site Configuration Programming”](#) on [page 10](#).

## Passport V11 Core Feature Enhancements

For more information on any of the new features, refer to *MDE-5266 What's New in Passport Version 11*.

### EMV Support on Inside Transactions

Beginning with V11.01, Passport supports EMV for inside transactions in the U.S. Passport V11.02 for WorldPay provides inside EMV support for WorldPay customers. Customers using a credit or debit card with an embedded microchip must insert the card into the chip reader on the inside PIN pad and leave it until the chip reader displays instructions to remove the card. Cashiers at the Cashier Workstation (CWS), as well as customers inside, will notice new prompting related to EMV functions.

Enabling EMV inside may require new PIN pads or new PIN pad software. EMV-capable PIN pads are VeriFone MX915, Ingenico iSC250, and Ingenico iPP320. In addition, the ASC can change PIN pad configurations in **MWS > Set Up > Register > Register Set Up**. The ASC must update network configuration parameters in **MWS > Set Up > Network > WorldPay** for EMV inside transactions.

### WorldPay does not support refund transactions for EMV Debit cards.

For more information and Passport behavior, refer to [“CWS Network Functions”](#) section on [page 38](#).

### Tender Keys in CWS

The CWS reflects a basic change beginning with V11.01. A new tender key, labeled **Card**, replaces the **Credit** and **Debit** tender keys. The cashier selects the **Card** tender key when the customer presents a credit, debit, or prepaid card for payment. This change is made because EMV chip cards can contain multiple EMV applications that support credit and debit payment. Passport does not know the specific payment application to use for the transaction until after the cashier begins tendering the transaction, the customer inserts an EMV chip card, and the PIN pad communicates with the chip on the card. Passport determines the card type and Passport logs the transaction based on this determination. Credit and Debit tenders continue to appear on Accounting reports as before.

### **EBT Food (Non-integrated) and EBT Cash (Non-integrated) Tenders**

Passport provides new Tender Group selections that allow the merchant to program EBT Food and EBT Cash tenders for stores that use an external EBT terminal to authorize EBT Cash and EBT Food transactions when the primary payment network does not support EBT Cash and EBT Food card types. These new EBT tenders are available for inside transactions only. The EBT Food tender applies food stamp restrictions to the items in the transaction as well as exempts tax for the items that qualify for food stamps.

*Note: These are the default EBT Tender settings and do not need to be changed.*

### **New Passport Point of Integration with Impulse™**

Passport can display on the CWS the content that usually displays on the Impulse cashier facing tablet for certain implementations of the Impulse service.

### **Signature Capture**

Beginning with V11.02 Service Pack D, Passport supports electronic signature capture at the Ingenico iSC250 and VeriFone MX915 PIN pads. Passport stores the electronic signature with the merchant receipt and uploads it to Insite360 receipts. Reprints of electronic signature capture receipts automatically print the captured signature. Receipt searches performed at the CWS do not display the captured signature; instead, an indication that the signature was electronically captured is displayed.

In addition, the merchant can configure settings for printing customer and merchant receipts, through **Set Up > Network Menu > WorldPay > Network Site Configuration**. For more information, see [“Network Site Configuration Programming”](#) on [page 10](#).

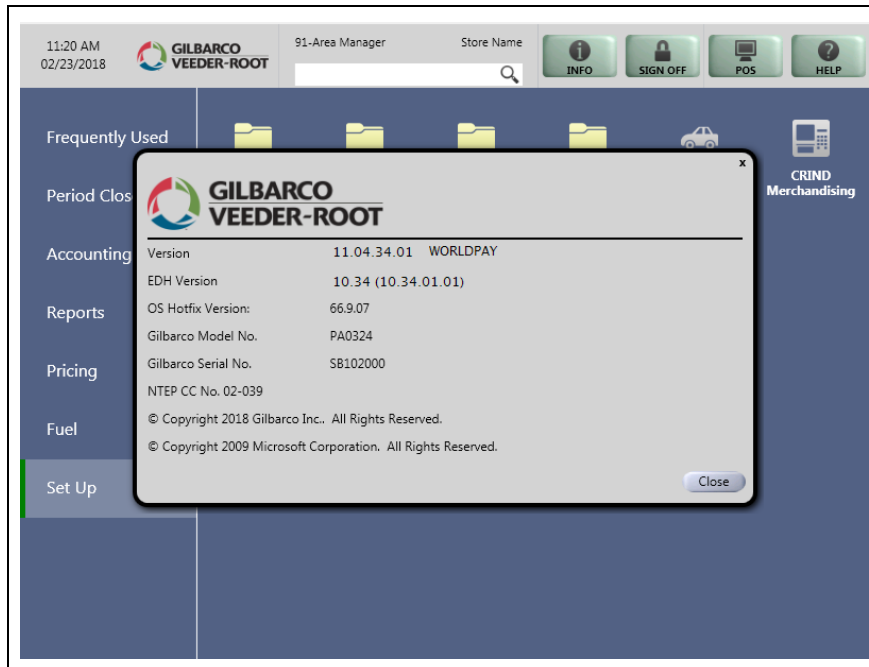
### **Receipt Printer Settings for Faster Printing**

To increase the receipt printer speed, your ASC can change the settings on the Epson® receipt printer, which increases the baud rate of the printers.

## New Graphical User Interface

Beginning with V11.04, Passport supports a selection of updated user interfaces, along with the classic interface. At upgrade or install, Passport defaults to the new interface.

**Figure 1: Manager Workstation (MWS) Main Screen After Sign On**



The user cannot configure the MWS to return to the classic view; however, the CWS can be configured based on the user's preference. The merchant can configure the default interface for use in CWS and each user may configure a preference for use with the CWS in the **MWS > Set Up > Employee > Preferences** tab. Theme options for the CWS are Classic, Modern, and Retro.

**Figure 2: CWS Classic Theme**



Figure 3: CWS Modern Theme

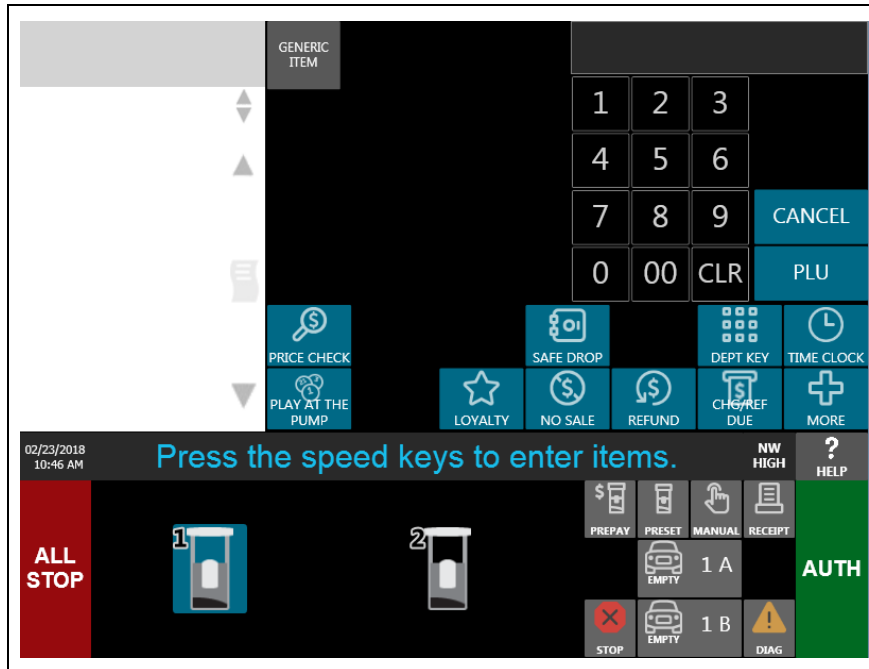
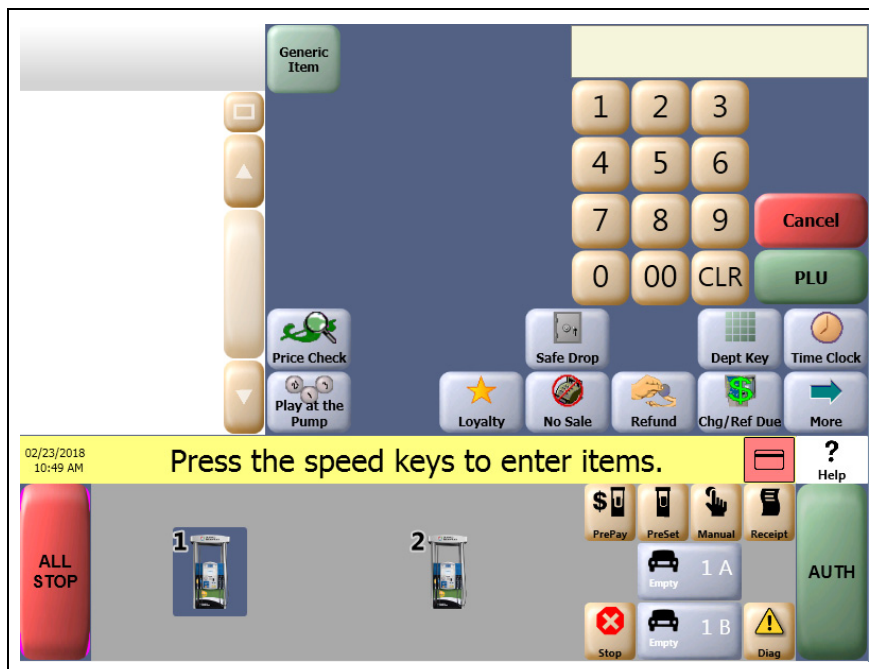


Figure 4: CWS Retro Theme



### Network Batch Totals for BOS Processing

The Passport Back Office Interface allows the merchant to send information about each network batch close that occurs during the business day to the BOS. Passport generates a network batch file at the close of each batch. The information included in batch totals XMLGateway files varies by network.



# First Time Installation Instructions

This section describes the WorldPay-specific installation procedure. Read the entire section before starting the setup process. The Passport V11.04 system supports two types of connection to the WorldPay network:

- Dial Up network connection.
- TCP/IP network connection using native Secure Sockets Layer (SSL) encryption.

## IMPORTANT INFORMATION

Sites with a serial connection between the Passport system and Systech box must be configured as Dial Up using a serial connection with a standard Passport system modem.

“[Sites with TCP/IP SSL Connection](#)” on [page 9](#) applies only to sites with TCP/IP (Ethernet®) connection between the Passport Firewall Router and WorldPay network.

## WorldPay Terminal ID

The site identification code on the WorldPay network is usually referred to as the Terminal ID [(TID) 24-digit], but is actually comprised of three codes, in the following order:

- 15-digit Merchant ID
- 8-digit TID
- 1 check digit

**For ALON branded stores, advise the merchant or store manager to contact ALON at 1-877-256-6729 a week before the scheduled installation. ALON will provide the merchant or store manager with instructions for preparing for the installation.**

For all other stores, obtain the full Terminal ID in advance of the installation, as the information must be configured properly for the site to communicate with the WorldPay network. **The merchant or manager should have received the eight-digit TID beforehand.** Call the WorldPay Help Desk at 1-800-200-5965 with the eight-digit TID to obtain the **Check Digit** and **Merchant ID** for completing the Terminal ID field in Site Configuration Programming.

### Sites with TCP/IP SSL Connection

In this configuration, the Passport system encrypts network transactions over a TCP/IP link using SSL.

## IMPORTANT INFORMATION

The following procedures are dependent on obtaining specific information, such as **Domain Name System (DNS) addresses, Default Gateway IP address, and Static WAN IP address** from the site's Internet Service Provider (ISP) and IT staff. Gilbarco Technical Support does not provide this site-specific information.

The following must be performed before configuring the Passport system's WorldPay Network Site Parameters.

Beginning with V10, Passport for WorldPay supports a native SSL link to the WorldPay network. This configuration eliminates installing a Systech device at the store and allows high-speed connectivity to the WorldPay network. Before the installation date, determine whether the site will be using an RV042 or a Secure Zone Router (SZR).

If using a SZR, follow *MDE-5382 Secure Zone Router (Acumera) Installation Instructions* and *MDE-5396 Secure Zone Router Site Survey Manual* for configuration and installation. The WorldPay egress rules contained in Appendix C should be provided to the store's IT network representative to be added to the site perimeter firewall.

If using an RV042 router, follow “[Appendix A: Stores with TCP/IP SSL Connections and Programming for Gilbarco RV042 Firewall Router](#)” on [page 43](#) for configuration and installation.

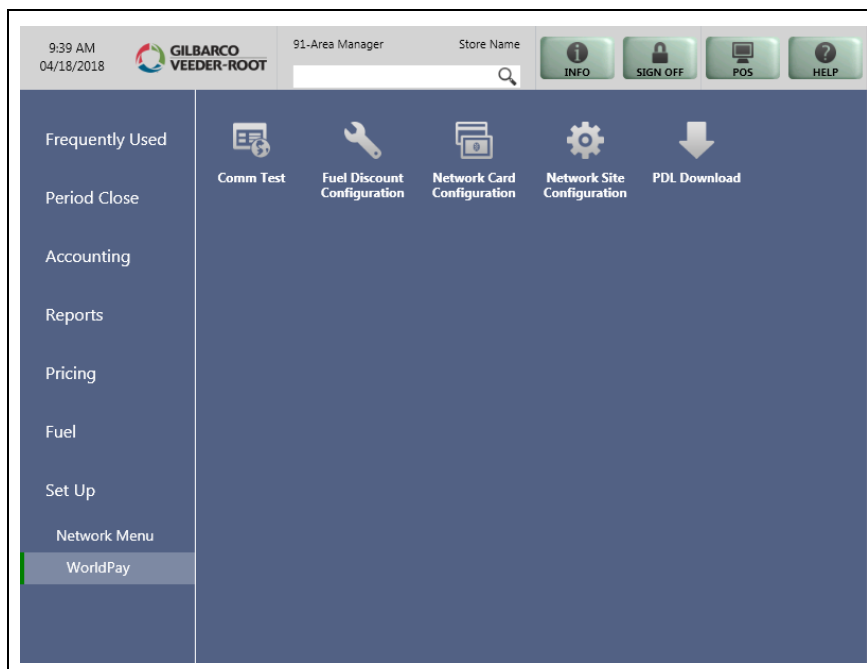
## Network Site Configuration Programming

*Note: Install and run the Enhanced Dispenser Hub (EDH) before you start the network configuration.*

To establish communication with the WorldPay network and process credit and debit card transactions, proceed as follows:

- 1 From the MWS main menu, select **Set Up > Network Menu > WorldPay**.

**Figure 5: WorldPay Network Configuration Menu**



The following option buttons display in WorldPay Network Configuration screen:

- Comm Test
- Fuel Discount Configuration
- Network Card Configuration
- Network Site Configuration
- PDL Download

- 2 Select **Network Site Configuration**. The WorldPay Network Site Parameters screen opens.

**Figure 6: WorldPay Network Site Parameters Screen**

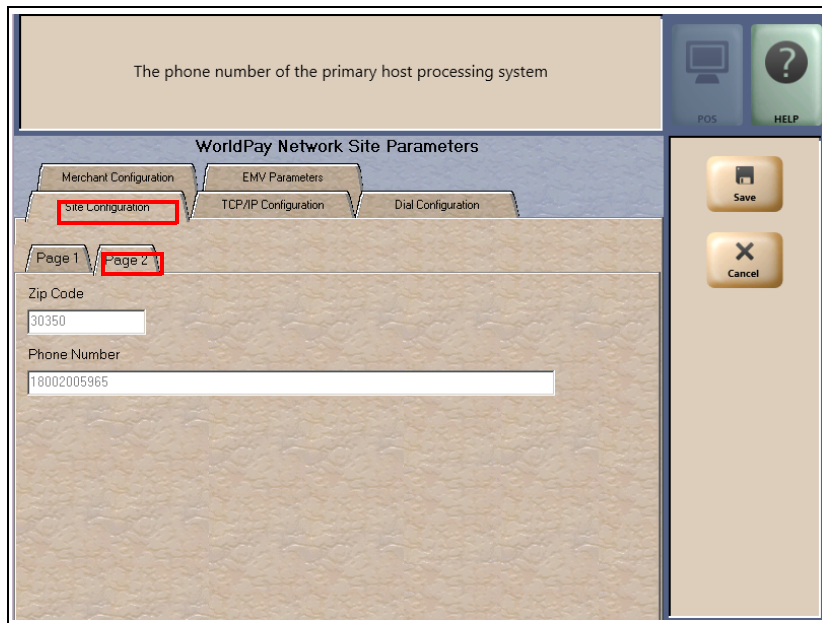
- 3 Select the **Site Configuration - Page 1** tab. This tab reflects basic site configuration information. All the fields, except Terminal ID, are updated through a PDL from the WorldPay network and are not editable on the Passport system. On a fresh installation, all fields appear blank until the Passport system receives a PDL from the WorldPay network. Program the 24-digit Terminal ID obtained from the WorldPay Help Desk into the Terminal ID field on this tab. If any information on the **Site configuration - Page 1** tab is incorrect after Passport receives the PDL from WorldPay, call the WorldPay Help Desk to resolve.

The following table lists the fields on the Site Configuration - Page 1 tab:

Field	Description
Terminal ID	The WorldPay network unique site identifier. WorldPay assigns this identifier. Refer to <a href="#">"WorldPay Terminal ID"</a> on page 9 for instructions on completing this field.
Site Name	The store name as known by the WorldPay network. Not editable.
Street Address	The store street address as known by the WorldPay network. Not editable.
City	The city in which the store is located. Not editable.
State	The state in which the store is located. Not editable.

- 4 Select the **Page 2 tab** and confirm that the Phone Number field is displayed correctly for the site.

**Figure 7: Site Configuration - Page 2 Tab**

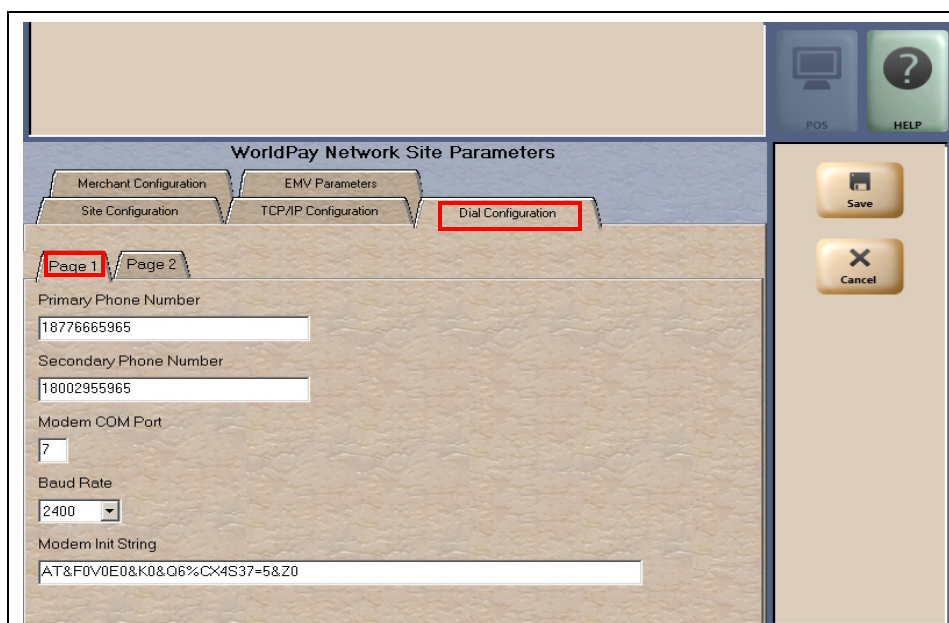


The following table lists the fields on the Site Configuration - Page 2 tab:

Field	Description
ZIP Code	The ZIP Code in which the store is located. Not editable.
Phone Number	The store phone number as known by the WorldPay network. Not editable.

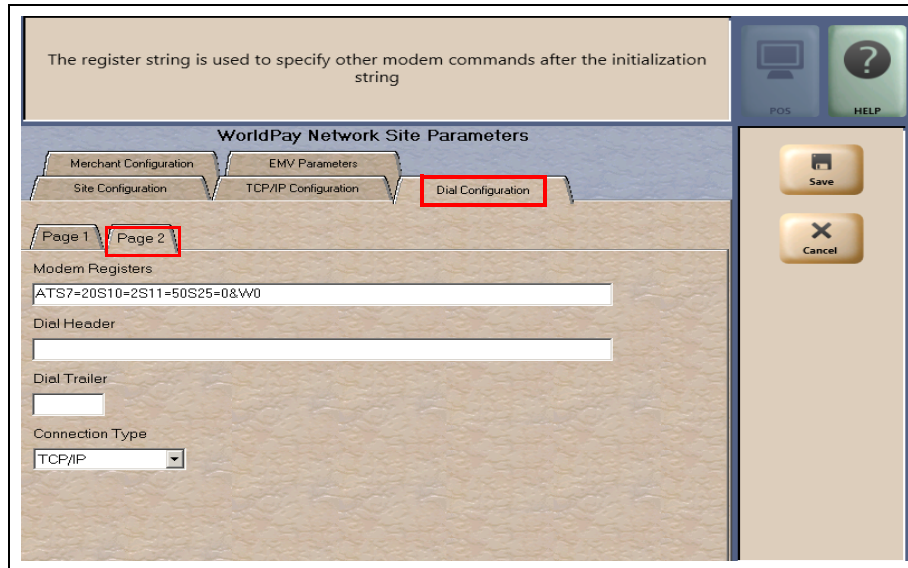
- 5 After completing the **Site Configuration** tab, select the **Dial Configuration** tab. The Dial Configuration tab opens.

**Figure 8: Dial Configuration Tab**



- 6 Select the **Page 2** tab.

**Figure 9: Dial Configuration - Page 2 Tab**



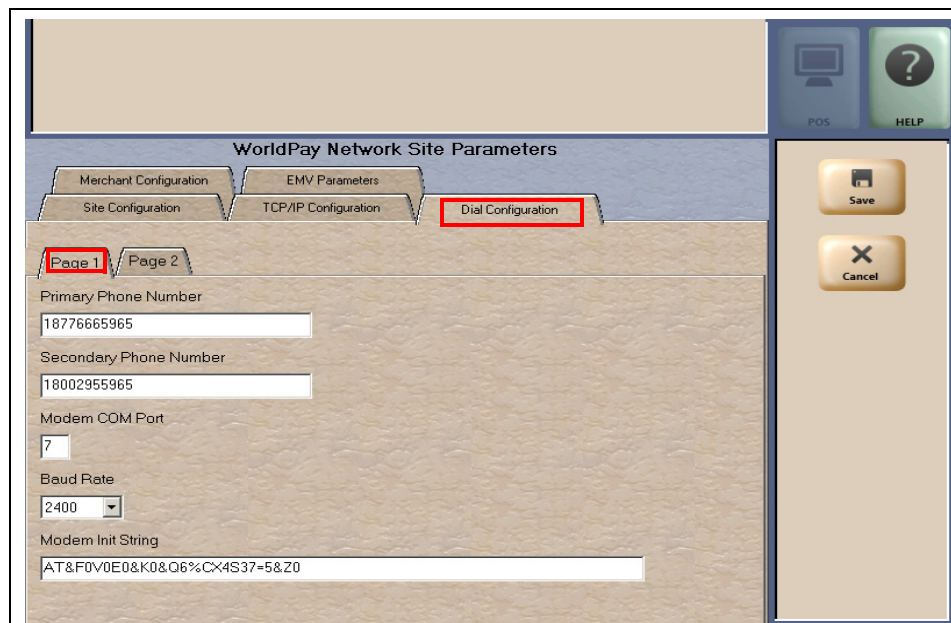
- 7 Select the **Connection Type** field drop-down menu (see [Figure 9](#)). The available options are **Dial Up** and **TCP/IP** (defaults to TCP/IP).
  - If the site is using a modem to connect with the WorldPay network, select **Dial Up**.
  - If the site is using a secure Internet connection to connect with the WorldPay network, select **TCP/IP**.
- 8 The next configuration step depends upon the **Connection Type** selected. If the Connection Type is set to **TCP/IP**, go to step 10 on [page 15](#). Otherwise, if the Connection Type is set to Dial Up, complete configuring the **Page 2** parameters.

The following table lists the fields on the Site Configuration - Page 2 tab:

Field	Description
Modem Registers	Additional required modem settings. The following are values for specific modem models: <ul style="list-style-type: none"> <li>• MultiTech 007: no change required</li> <li>• MultiTech 009: ATS7=15S10=2S11=50S25=0&amp;W0</li> </ul>
Dial Header	Number the modem dials before the phone number. Configure this field only if it is needed to access an outside line. Default is blank.
Dial Trailer	Number the modem dials after the phone number. Default is blank.

- 9 Select the **Page 1** tab. The parameters on this page provide further configuration data for sites using a dial connection to the WorldPay network.

**Figure 10: Dial Configuration - Page 1 Tab**



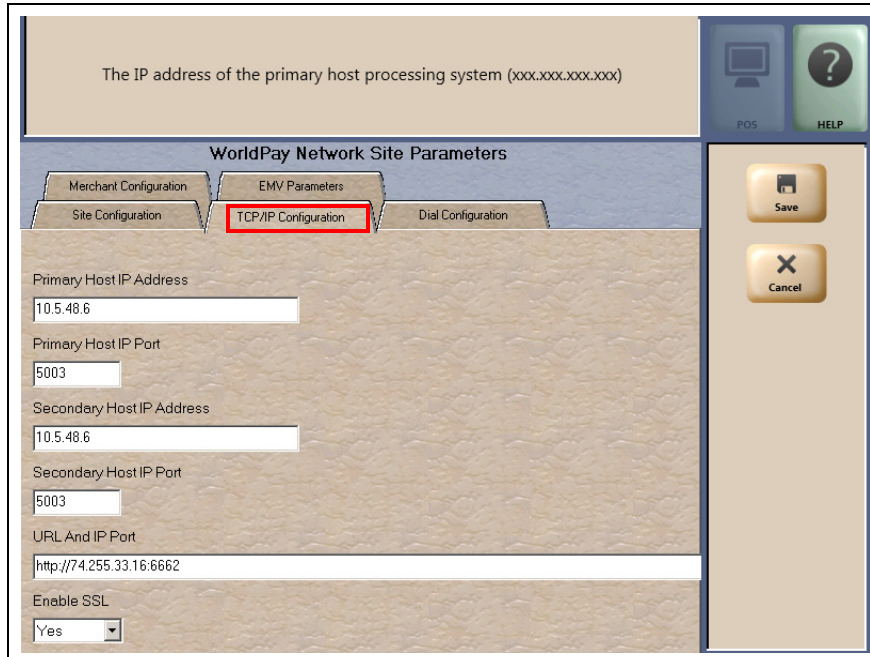
The following table lists the fields on the Dial Configuration - Page 1 tab:

Field	Description
Primary Phone Number	The primary phone number the modem dials to connect to the WorldPay network. 14-character string consisting of letters, numbers, and space character.
Secondary Phone Number	The backup phone number the modem dials to connect to the WorldPay network if the first phone number is unsuccessful. 14-character string consisting of letters, numbers, and space character.
Modem COM Port	COM port on the EDH where the modem is connected. 1-digit field. Defaults to blank.
Baud Rate	Modem connection speed. Drop-down menu field with available selections of: <ul style="list-style-type: none"> <li>• 1200</li> <li>• 2400</li> </ul>
Modem Init String	Modem initialization commands. The following are values for specific modem models: <ul style="list-style-type: none"> <li>• MultiTech 007: AT&amp;F+A8E=,,,0VE&amp;K&amp;Q6%CX4+MS=1</li> <li>• MultiTech 009: AT&amp;F0V0E0&amp;K0&amp;Q6%CX4S37=5&amp;Z0</li> </ul>

After completing the fields on the Page 1 tab, go to step 11 on page 16.

- If the selection in step 7 on page 13 was TCP/IP, select the **TCP/IP Configuration** tab. This tab provides the configuration parameters for TCP/IP communication with the WorldPay network.

**Figure 11: TCP/IP Configuration Tab**



The following table lists the fields on the TCP/IP Configuration tab:

Field	Description
Primary Host IP Address	Primary IP address used for TCP/IP communication. 15 characters comprised of digits and period punctuation character. Format is XXX.XXX.XXX.XXX. Defaults to blank.
Primary Host IP Port	Primary communication port for the WorldPay network. 4-digit string. Defaults to blank.
Secondary Host IP Address	Backup IP address used for TCP/IP communication if the primary IP address is not successful. 15 characters comprised of digits and period punctuation character. Format is XXX.XXX.XXX.XXX. Defaults to blank.
Secondary Host IP Port	Backup communication port for the WorldPay network. 4-digit string. Defaults to blank.
URL and IP Port	Alternate WorldPay network URL. This field must contain the following value: <a href="http://tptrans.lynksystems.com:6662">http://tptrans.lynksystems.com:6662</a>
Enable SSL	Yes/No drop-down menu. If set to Yes, Passport uses SSL encryption.

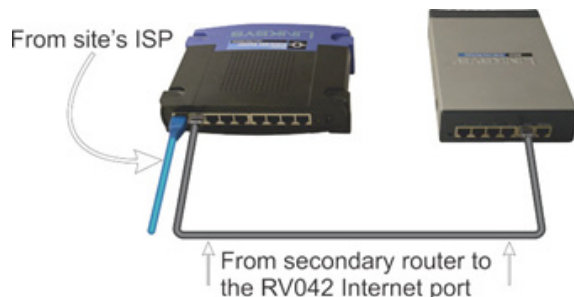
## IMPORTANT INFORMATION

Passport ensures **secure connection through SSL** allowing a merchant to come directly into the WorldPay SSL gateway. For more information, refer to [“Appendix A: Stores with TCP/IP SSL Connections and Programming for Gilbarco RV042 Firewall Router”](#) on page 43.

Ensure that the SSL selection is correct for your system, otherwise Passport will display “Communication Error” on the yellow bar when sending the first transaction.

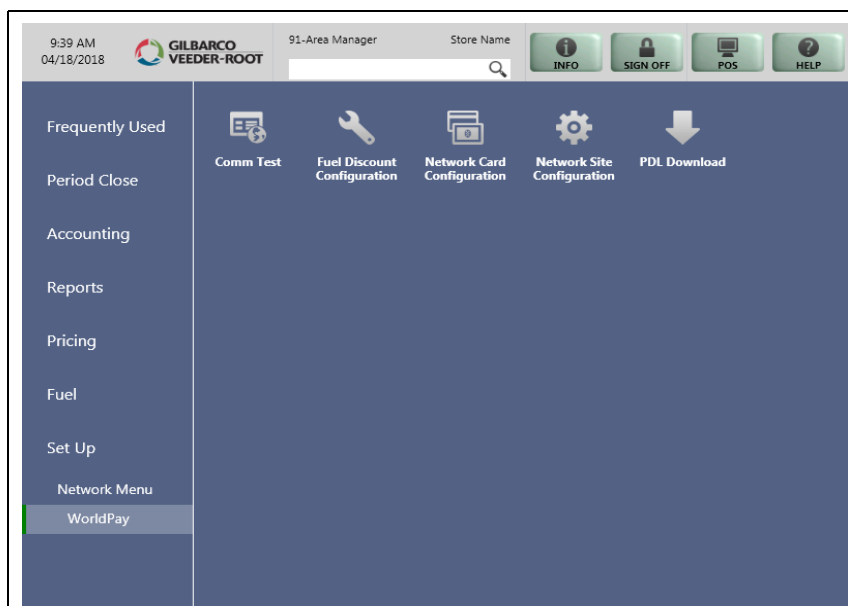
If the ASC sets “Enable SSL” but the configuration is not correct, the CWS yellow bar displays **Communication Error** and the Network Status screen displays the message **“Network Offline. SSL Certificate Validation Failed. Please contact Help Desk.”**

Example of Router Setup



- 11 After programming the parameters on the TCP/IP Configuration or Dial Configuration tab, select **Save** to save the data and exit from the WorldPay Network Site Parameters screen. The Passport system is ready to request a PDL from the WorldPay network. Select **PDL Download** on the WorldPay network menu.

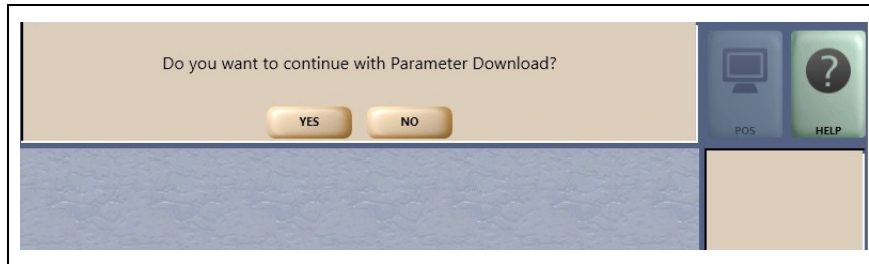
**Figure 12: WorldPay Network Menu - PDL Download**





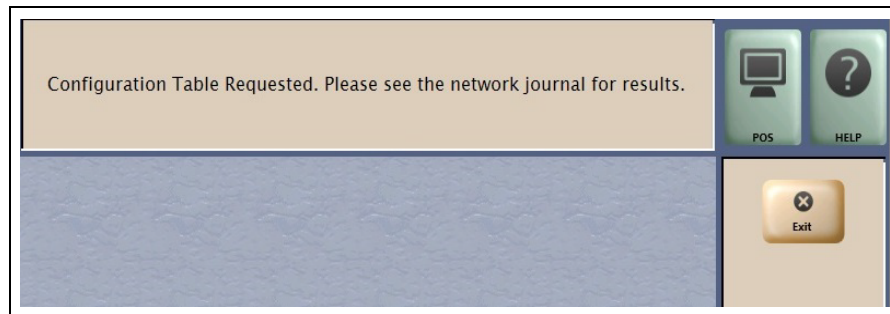
The PDL prompt opens.

**Figure 13: PDL Prompt**



- 12 Select **Yes** to begin the PDL with the WorldPay network. When the PDL request is complete, the Passport system displays the results.

**Figure 14: PDL Complete**



- 13 Select **Exit** to exit from the PDL Download screen and return to the WorldPay Network Menu screen. Exit from the Network Menu screen.
- 14 Ensure that the Passport system is communicating with the WorldPay network and successfully received a PDL by navigating to **MWS > Reports > Journal Reports > Network Journal Report**.

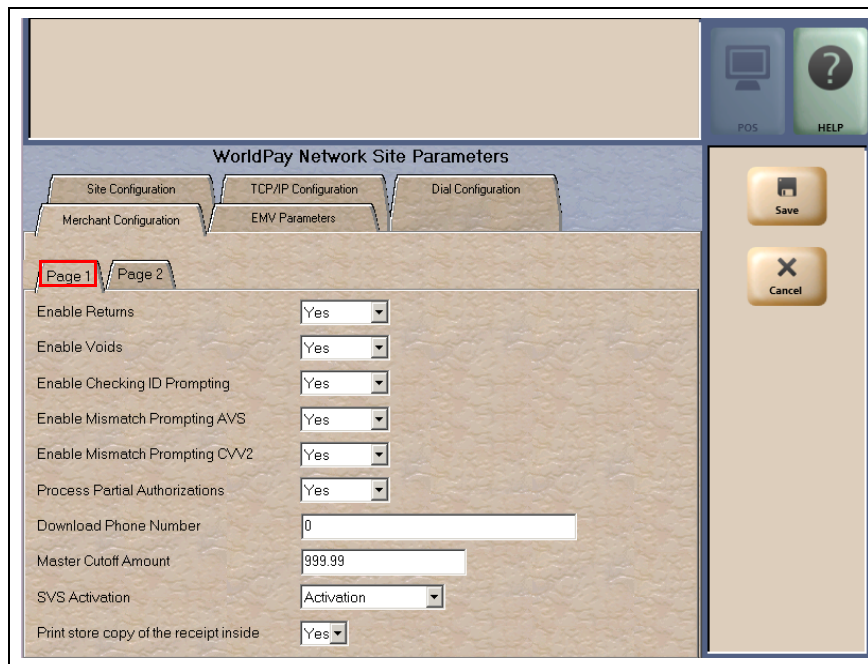
Press **Select > Print Preview**. Review the Network Journal Report to determine if the PDL was successful.

If the PDL was not successful, go to **MWS > Set Up > Network Menu > WorldPay > Network Site Configuration** to review the WorldPay Network Site Parameters.

- 15 After the Passport system receives a successful PDL from the WorldPay network, return to **MWS > Set Up > Network Menu > WorldPay > Network Site Configuration** to review the parameters that opens on the **Site Configuration Page 1** and **Page 2** tabs. With the exception of the Terminal ID, this information was received as part of the PDL. If any of these fields do not appear correct or the store manager indicates they are incorrect, call the WorldPay Help Desk for assistance.

- 16 Select the **Merchant Configuration - Page 1** tab.

**Figure 15: Merchant Configuration Tab - Page 1**



This information was also received as part of the PDL, but the fields are editable. Review the parameters with the store manager and make adjustments as required.

### IMPORTANT INFORMATION

EMV Refunds are not allowed for EMV Credit or Debit transactions.

**WorldPay does not support returns and voids for EMV debit cards**, regardless of the settings for the "Enable Returns" and "Enable Voids" fields. If the cashier attempts to perform a refund and the customer swipes or inserts a debit card at the PIN pad, **Passport declines the refund transaction.**

The cashier must, instead, refund to cash any sale transaction completed using a debit card.

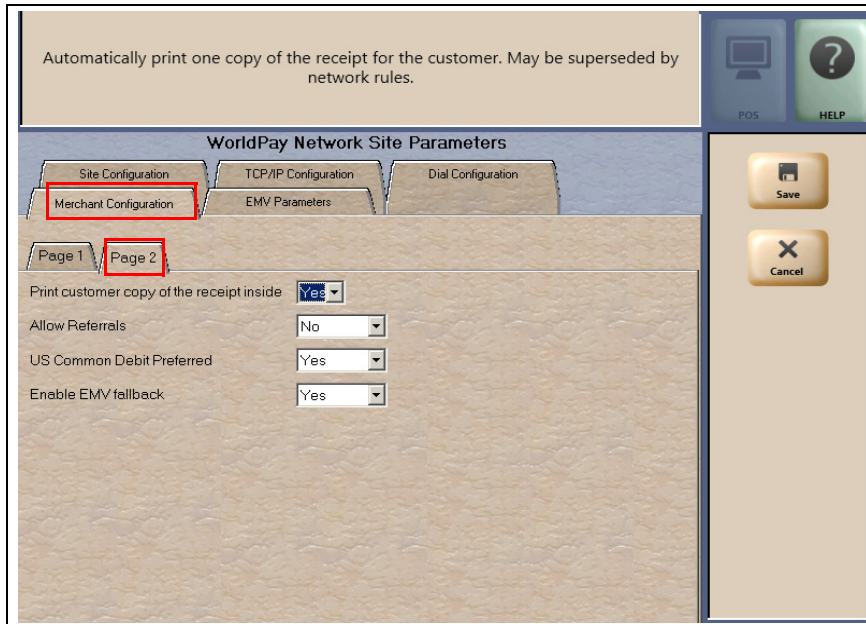
For more information and Passport behavior, refer to "[CWS Network Functions](#)" section on [page 38](#).

The following table lists the fields on the Merchant Configuration - Page 1 tab:

Field	Description
Enable Returns	<ul style="list-style-type: none"> <li>If set to Yes, allows the site to process a refund through the WorldPay network when the original sale transaction occurred in a previous batch.</li> <li>If set to No, the Passport system declines a refund in which the original sale occurred in a previous batch.</li> </ul>
Enable Voids	<ul style="list-style-type: none"> <li>If set to Yes, allows the site to process a refund through the WorldPay network when the original transaction occurred in the current batch.</li> <li>If set to No, the Passport system declines a refund in which the original sale occurred in the current batch.</li> </ul>
Enable Checking ID Prompting	<ul style="list-style-type: none"> <li>If set to Yes, the Passport system prompts the cashier to check the customer's identification when the WorldPay network requests it.</li> <li>If set to No, the Passport system declines the transaction if the WorldPay network requests cardholder identification.</li> </ul>
Enable Mismatch Prompting AVS	<ul style="list-style-type: none"> <li>If set to Yes, if the WorldPay network indicates the ZIP Code the customer entered does not match the ZIP Code on file, the Passport system prompts the cashier to accept or decline the payment.</li> <li>If set to No, the Passport system declines the transaction if the WorldPay network indicates the ZIP Code the customer entered does not match the ZIP Code on file.</li> </ul>
Enable Mismatch Prompting CVV2	<ul style="list-style-type: none"> <li>If set to Yes, if the WorldPay network indicates the Cardholder Verification Value (CVV) the customer entered does not match the Cardholder Verification code on file, the Passport system prompts the cashier to accept or decline the payment.</li> <li>If set to No, the Passport system declines the transaction if the WorldPay network indicates the Cardholder Verification code the customer entered does not match the Cardholder Verification code on file.</li> </ul>
Process Partial Authorizations	<ul style="list-style-type: none"> <li>If set to Yes, allows the site to accept partial approval of post pay transactions.</li> <li>If set to No, the Passport system declines payment on a post pay transaction if the WorldPay network approves for less than the full sale transaction amount.</li> </ul>
Download Phone Number	Provides an alternative phone number for requesting and receiving PDL.
Master Cutoff Amount	Provides the absolute maximum amount for WorldPay network transactions.
SVS Activation	<p>Controls the transaction message type that the Passport system uses to activate SVS cards. The transaction type depends upon the SVS program to which the site is subscribed. This field does not come from the WorldPay network PDL. Available values are:</p> <ul style="list-style-type: none"> <li>Activation: the Passport system sends transaction code 07 for SVS card activations.</li> <li>Issue Card: the Passport system sends transaction code 18 for SVS card activations.</li> </ul> <p>Defaults to Activation.</p>
Print store copy of the receipt inside	If set to Yes, the merchant copy of the receipt prints automatically for all inside Concord network transactions. This may be especially important for stores that enable electronic signature capture at the PIN pad, as the customer signature prints as part of the receipt.

- After completing programming on the **Merchant Configuration - Page 1** tab, select the **Page 2** tab.

**Figure 16: Merchant Configuration Tab - Page 2**



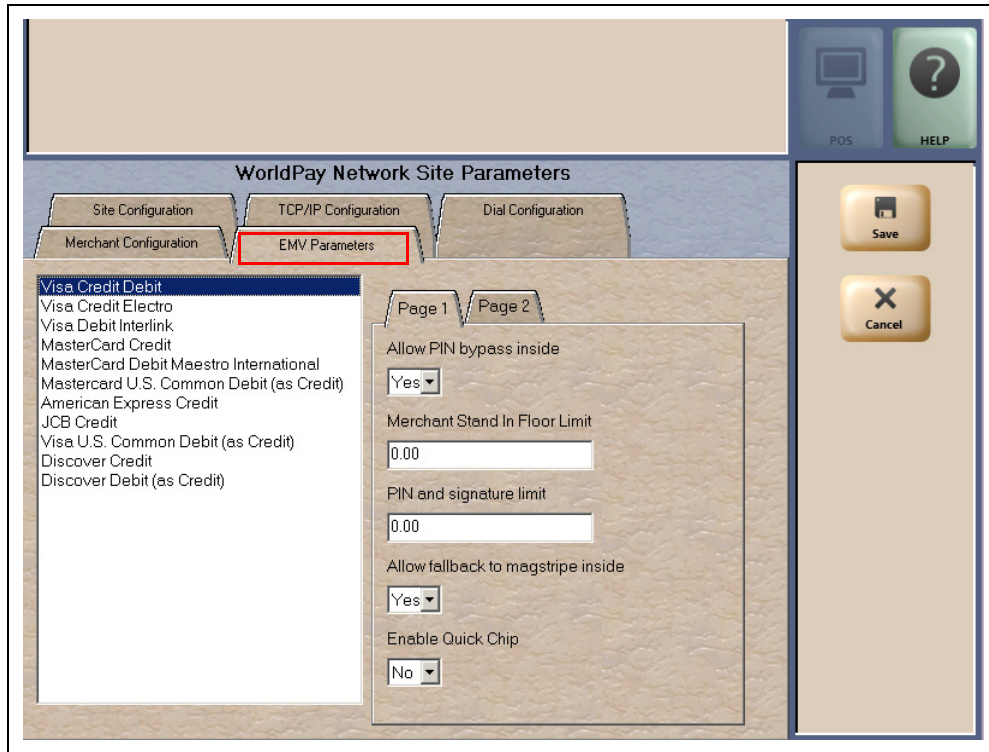
This tab contains additional configuration fields for EMV chip card transactions.

The following table lists the fields on the Merchant Configuration - Page 2 tab.

Field	Description
Print customer copy of the receipt inside	If set to Yes, the customer copy of the receipt prints automatically for all inside Concord network transactions. This may be especially important for stores that enable electronic signature capture at the PIN pad, as the customer signature prints as part of the receipt.
Allow Referrals	Used to allow call for auth operation using the referral number.
US Common Debit Preferred	<p>If set to Yes, when the customer presents an EMV card that contains both US Common and International Debit Application Identifiers (AID), Passport displays or uses the US Common Debit AID.</p> <p>If set to No, when the customer presents an EMV card that contains both US Common and International Debit AID Passport displays or uses the International Debit AID.</p> <p>If the card contains only one debit AID, Passport displays or uses it without regard to the setting for this field</p>
Enable EMV Fallback	<p>If set to Yes, when the customer inserts an EMV chip card into the inside PIN pad chip reader, the PIN pad detects the card AID, but fails to read the chip. Passport uses the Allow Fallback field value for the card AID (found on the EMV Parameters tab) to determine how to handle the card.</p> <p>If set to Yes, when the customer inserts an EMV chip card into the PIN pad chip reader, a chip read error occurs and the PIN pad does not detect the card AID, Passport declines the card.</p> <p>If set to No, when the customer inserts an EMV chip card into the inside PIN pad chip reader and a chip error occurs, Passport declines the card.</p>

- 18 After completing programming on the **Merchant Configuration - Page 2** tab, select the **EMV Parameters** tab. The fields under the EMV Parameters tab control how Passport processes transactions when the customer presents an EMV chip card, based on the AIDs Passport finds on the chip card. Some fields are not editable. Select the Page 1 tab.

Figure 17: EMV Parameters - Page 1 Tab



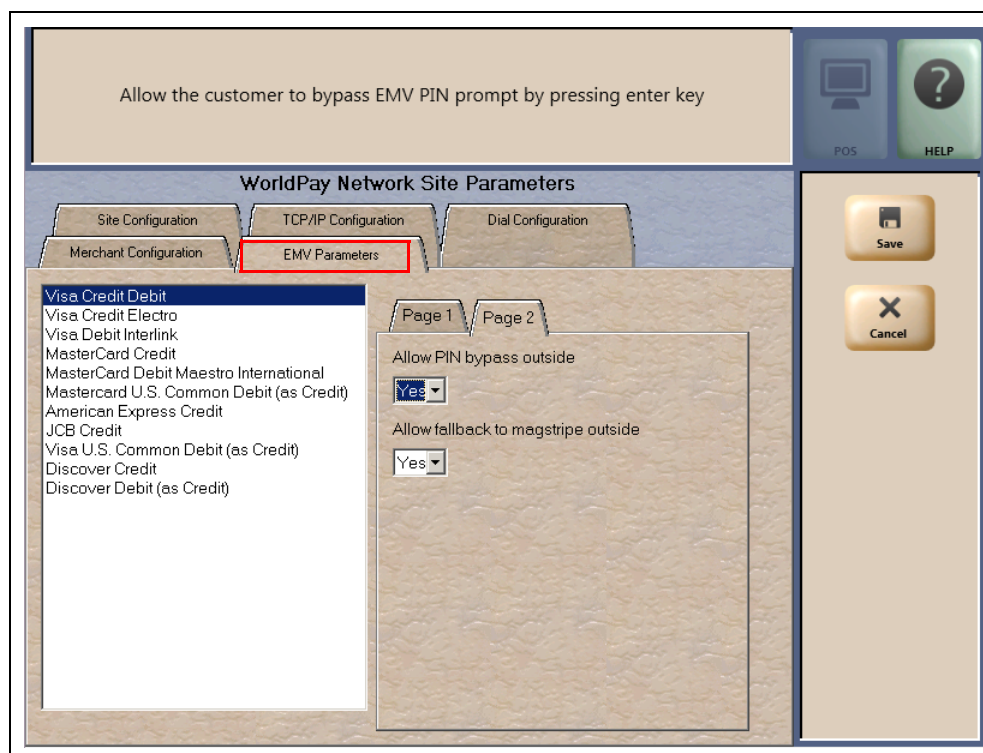
**Fields on the EMV Parameters - Page 1 Tab**

Field	Description
Allow PIN bypass inside	<p>If set to Yes, and the EMV application requires PIN entry, Passport prompts for PIN but allows the customer to press the <b>ENTER</b> key on the PIN pad without first entering digits for a PIN.</p> <p>If set to No, and the EMV application requires PIN entry, Passport prompts for PIN and the customer must enter a PIN to move forward in the transaction.  <i>Note: Some debit applications set this field to Yes by default and the merchant cannot change this setting.</i></p>
Merchant Stand In Floor Limit	<p>For this EMV card AID, maximum transaction dollar amount for this EMV card AID that the merchant will accept locally to store and forward when the network is offline. Defaults to 0.00, which means never allow offline transactions for this EMV card AID. This field is not editable for any debit AID.  <i>Note: Use care in changing this value. This field defaults to \$0.00, which means Passport relies the authorization to EMV chip card if the Passport cannot communicate with the WorldPay payment network. If the merchant configures an amount other than \$0.00 for this field, transactions locally accepted as a result of this configuration may receive a decline from the payment network when communication resumes. Also, the transaction may still get approved locally depending on a number of internal validations. If this occurs, the merchant is responsible for the charge back on the transaction. Advise the store owner or manager to discuss the financial implications of changing the value of this field.</i></p>

Field	Description
PIN and signature limit	<p>For this EMV card AID, minimum transaction dollar amount for this EMV card AID that will verify cardholder data. Defaults to \$0.00</p> <p>If the Cardholder Verification Method (CVM) was "signature", the receipts shall contain a signature line.</p> <p>If the CVM was a PIN-based CVM, the receipts shall contain a mention "Verified by PIN".</p> <p>This field should be configured if the merchant adheres to VISA Easy Payment Services (VEPS) or similar program offered by other card brand to eliminate signatures for low value transactions.</p> <p><i>Note: This is a new field in this version, and ASC should consult the merchant or store manager regarding its setting for the store.</i></p>
Allow fallback to magstripe	<p>If set to Yes, when the customer inserts a chip card into the chip reader on the PIN pad inside at the register and a chip error occurs, Passport uses the fallback to magnetic stripe parameters received from the WorldPay network for the card type to determine whether to prompt the customer to remove the card from the chip reader and swipe it.</p> <p>If set to No, when the customer inserts a chip card into the chip reader on the PIN pad inside at the register and a chip error occurs, Passport declines the card.</p> <p><i>Note: Passport does not allow fallback to magnetic stripe read, regardless of this setting, if the Enable EMV Fallback field on the <b>Merchant Configuration - Page 1</b> tab is set to No.</i></p>
Enable Quick Chip	<p>If set to Yes, Passport obtains all necessary EMV data from the chip card earlier in the transaction by notifying the chip card that the network is not available. As a result, the PIN pad prompts the customer to remove the chip card before the transaction has completed with the chip card issuer, up to a few seconds earlier.</p> <p>If set to No, Passport performs EMV transactions without the shortcut of Quick Chip processing. The PIN pad prompts the customer to remove the chip card after the transaction has completed with the chip card issuer.</p> <p>Defaults to No.</p>

19 After completing the fields on the **EMV Parameters - Page 1** tab, select the **Page 2** tab.

**Figure 18: EMV Parameters - Page 2 Tab**



## Fields on the EMV Parameters - Page 2 Tab

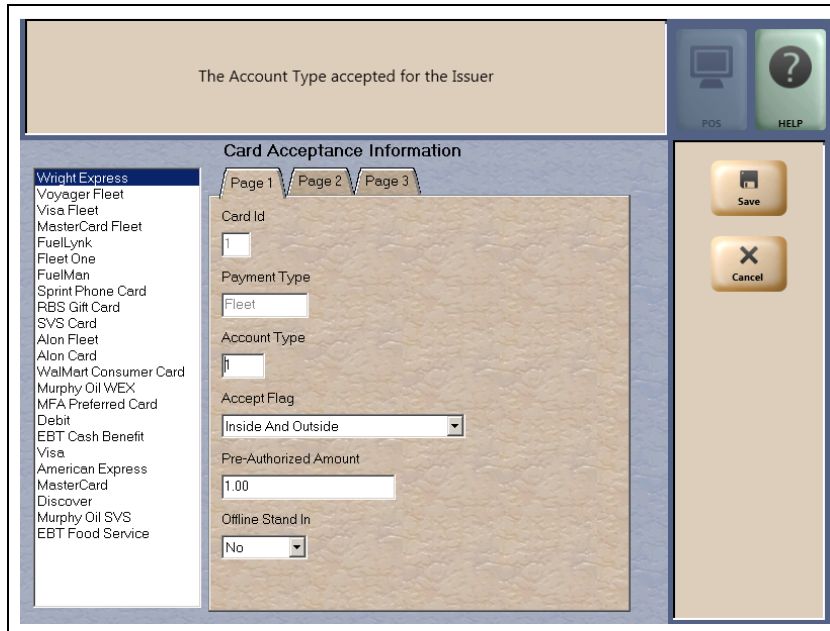
Field	Description
Allow PIN bypass outside	<p>If set to Yes, and the EMV application requires PIN entry, the CRIND prompts for PIN but allows the customer to press the ENTER key on the CRIND keypad without first entering digits for a PIN.</p> <p>If set to No, and the EMV application requires PIN entry, the CRIND prompts for PIN and the customer must enter a PIN to move forward in the transaction.</p> <p><i>Note: Some debit applications set this field to Yes by default and the merchant cannot change this setting.</i></p>
Allow fallback to magstripe inside	<p>If set to Yes, when the customer inserts an EMV chip card into the CRIND card reader and the CRIND detects the chip card AID but a chip error occurs, the CRIND prompts the customer to remove the card to read the magnetic stripe. If the CRIND does not detect the chip card AID and a chip error occurs, the CRIND declines the card.</p> <p>If set to No, when the customer inserts an EMV chip card into the CRIND card reader and a chip error occurs, the CRIND declines the card.</p> <p><i>Note: Passport does not allow fallback to magnetic stripe read, regardless of this setting, if the Enable EMV Fallback field on the <b>Merchant Configuration - Page 1</b> tab is set to No.</i></p>

- 20** After completing the field on the EMV Parameters - Page 2 tab, click **Save** to save all programming and return to the **Network** menu screen.

# Network Card Configuration

The Network Card Configuration Card Acceptance Information tabs contain card acceptance parameters. Card types that the WorldPay network accepts are listed in the left pane. The three tabs provide the configuration parameters for each selected card. Multiple cards may be programmed before selecting Save.

**Figure 19: Card Acceptance Information - Page 1 Tab**



**Figure 20: Card Acceptance Information - Page 2 Tab**

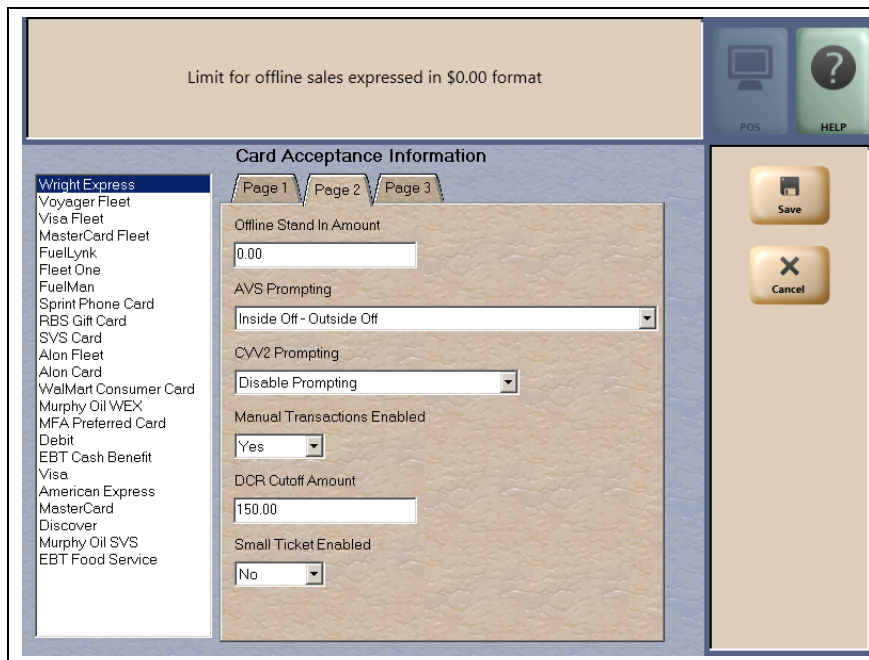




Figure 21: Card Acceptance Information - Page 3 Tab

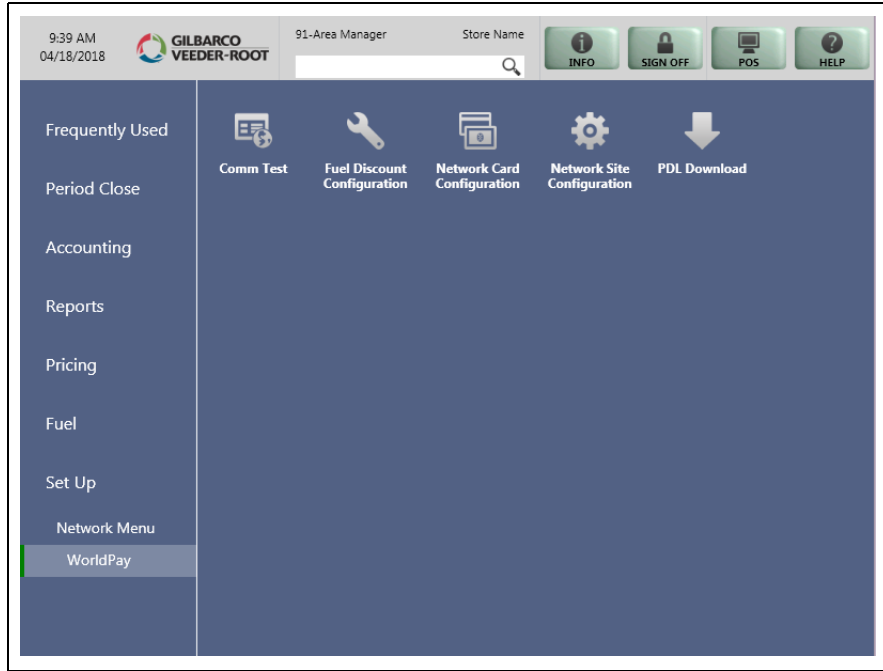
The following table lists the fields on the Card Acceptance Information tabs:

Field	Description
Card ID	Identifier assigned by the Passport system. This field is not editable.
Payment Type	Card type assigned by the WorldPay network. This field is not editable.
Account Type	Card code assigned by the WorldPay network. This field is not editable.
Accept Flag	Determines where this card type is accepted, Inside, Outside, Inside and Outside. This field is editable.
Pre-authorized Amount	Dollar value used to request pay-at-the-pump authorizations from the WorldPay network.
Offline Stand In	Determines whether this card type can be accepted when the WorldPay network is offline. Does not affect debit, prepaid, and EBT cards.
Offline Stand In amount	If offline Stand In is set to Yes, maximum transaction dollar amount allowed for offline transactions.
AVS Prompting	Determines when Passport prompts for ZIP Code. Available values are: <ul style="list-style-type: none"> <li>• Inside Manual - Outside Off.</li> <li>• Inside Swipe - Outside Off.</li> <li>• Inside Both - Outside Off.</li> <li>• Inside Manual - Outside Swiped.</li> <li>• Inside Swipe - Outside Swiped.</li> <li>• Inside Both - Outside Swiped.</li> <li>• Inside Off - Outside Swiped.</li> <li>• Inside Off - Outside Off.</li> </ul>
CVV2 Prompting	Determines when Passport prompts for CVV. Available values are: <ul style="list-style-type: none"> <li>• Accepted Inside Only (prompt inside only).</li> <li>• Disable Prompting (do not prompt).</li> </ul>
Manual Transactions Enabled	If set to Yes, Passport allows manual entry of the card account number for inside transactions. Does not apply to debit cards.
DCR Cutoff Amount	Maximum transaction dollar amount that can be authorized. The WorldPay network can override this value for FuelMan®, Fleet One <sup>SM</sup> , and FuelLynk cards.
Small Ticket Enabled	If set to Yes, the Passport prints a receipt without the signature line when the transaction amount is less than the amount programmed in the Small Ticket Amount field.
Small Ticket Amount	Maximum transaction dollar amount for Small ticket behavior.
Debit First Prompt Enabled	If set to Yes, the CRIND prompts "Is this a debit card?"
Referral Number	Contact phone number for the selected card.

## Performing Comm Test

The Communication Test sends a special message to the WorldPay network to verify the network connection. A timeout indicates a communication failure, which may be related to a temporary interruption of communications or a configuration error.

**Figure 22: Comm Test**



**Figure 23: Communication Test - Failure Result**



## Accepting Magnetic Stripe Contactless Inside

Passport can be configured to accept tap for mag stripe contactless cards on VeriFone and Ingenico PIN pads. To allow contactless mag stripe taps at the PIN pad, proceed as follows:

- 1 Go to **MWS > Set Up > Register > Register Set Up**.
- 2 Select the register where the PIN pad is located.
- 3 In the **Device Configuration** section, select the **Contactless** checkbox.
- 4 Select **Save** to save the configuration and exit.

**Figure 24: Register Set Up - Device Configuration**

The screenshot shows the 'Register Set Up' window for 'Register 1'. The 'Device Configuration' section is expanded, showing the following settings:

- Line Display: POS Line Display
- PIN Pad Type: Verifone MX 915
- Connection: TCP/IP
- IP Address: 10.28.120.146
- Electronic Signature:
- Forward Outside Trans:
- GVR Mat Reader:
- Contactless:  (highlighted with a red box)
- EMV Capable:

On the right side, there are 'Save' and 'Cancel' buttons. The bottom right corner shows 'Operator 91' and 'Store Store Name'.

### IMPORTANT INFORMATION

The WorldPay network does not yet support Contactless EMV cards. The Contactless field only affects mag stripe contactless tap.

If the customer attempts to present a contactless EMV card, Passport declines the transaction with the error message, "**Contactless not allowed**" on the CWS yellow bar and a "**Declined**" message in the PIN Pad.

## Network Journal Report

This report shows network journal entries for regular network transactions, as well as settlement and communication issues. The Network Journal Report configuration screen allows you to filter by various criteria, such as Date and Time, Exceptions, Source, Journal Type, and Specific Journal Text. The store manager can use the Network Journal Report as an aid in searching for disputed transactions.

**Figure 25: Network Journal Report Screen**

The screenshot displays the 'Network Journal Report' configuration interface. It includes the following elements:

- Date/Time:** A section with a radio button for 'Current Date' (selected) and a text field containing '06/23/2018'. Below this are two 'Select' buttons, each with a date field (06/23/2018) and a time field (01:30:06).
- Exception Flag:** Radio buttons for 'Exception', 'Transaction', and 'All' (selected).
- Journal Text:** A text input field with a 'Clear' button.
- Source ID (Register \ CRIND \ Other):** Radio buttons for 'All' (selected) and 'Select', and a text input field containing 'OtherSource'.
- Journal Type:** Radio buttons for 'All' (selected) and 'Select', and a text input field.
- Sort By:** A dropdown menu set to 'Timestamp' and radio buttons for 'Ascending' (selected) and 'Descending'.
- Right Panel:** Three buttons: 'Print Preview', 'Print', and 'Exit'.
- Top Right:** 'POS' and 'HELP' icons.

Beginning with V11.02, Passport includes EMV Transaction Details as a transaction type for EMV chip card transactions. To filter for only EMV chip card transactions, enter “EMV Transaction” in the Journal Text field.

## Network Reports

Network reports show data on Credit and Debit card transactions transmitted to the WorldPay network. Some network reports provide information on the status of transactions while others list the total amounts for transmitted transactions. By default, none of the network reports are configured to print at Shift or Store Close.

The following table lists the WorldPay network reports and the period for which they can be programmed to print automatically:

Report Name	Shift Close	Store Close	Configuration – On Demand Only
WorldPay Card Configuration	-	-	X
WorldPay EMV Configuration	-	-	X
WorldPay EMV Transaction Statistics	-	X	X
WorldPay EMV Transaction Statistics (Current)	-	-	X
WorldPay Exceptions	-	X	-
WorldPay Network Sales Report by Day	-	X	-
WorldPay Network Sales Report by Shift	X	X	-
WorldPay Settlement	-	X	-
WorldPay Network Site Configuration	-	-	X

### IMPORTANT INFORMATION

WorldPay network reports do not contain secure data, such as card account data. Therefore, there is no secure version of any report. For more information on secure reports, refer to *MDE-XXXX Passport EDH (WorldPay) V09.34 Implementation Guide for PA-DSS V3.2*.

To view network reports on demand, go to **MWS > Reports > Network Reports**.

## WorldPay Network Card Configuration Report

This Report contains the current configured card type parameters. [Figure 26](#) shows the portions of the report:

**Figure 26: WorldPay Network Card Configuration Report**

WorldPay Card Configuration Report	
WorldPay 600 Morgan Falls Rd Atlanta, GA, 30350 1800 200 5965 TID: 542929803122506000085477	
Configuration ID: 0	REPORT PRINTED: Oct 24,2016 15:31
<hr/>	
CARD:	Wright Express
Type:	Fleet
Account Type:	1
Accepted Flag:	2=Inside and Outside
Preauth Amount:	\$1.00
Offline Stand-In:	2=Disabled
Offline Stand-In Amount:	\$0.00
Address Verification (AVS) Prompting:	8=Inside Off/Outside Off
Cardholder Verification (CVV) Prompting:	2=Disable Prompting
Manual Transactions Enabled:	1=Enabled
DCR Cutoff Amount:	\$150.00
Small Ticket Enabled:	2=Disabled
Small Ticket Amount:	\$0.00
Debit First Prompt Enabled:	1=Enabled
Referral Number:	
PAN Ranges:	
	690046000000000000 - 69004606999999999999
	69004604770000000000 - 69004606999999999999
	69004608000000000000 - 69004699999999999999

## WorldPay EMV Configuration Report

This report provides information regarding EMV processing parameters for each EMV card AID Passport supports, along with the fields programmed in the **MWS > Set Up > Network Menu > WorldPay > Network Site Parameters > EMV Parameters**. [Figure 27](#) shows a sample excerpt of the American Express® Credit AID.

**Figure 27: WorldPay EMV Configuration Report**

EMV Configuration Report			
Report created: 10/26/2016 04:33:00 PM			
Network Configuration Values			
US Common Debit Preferred:		True	
Pinpad Configuration Values			
PinPad Id:	1	EMV Enabled:	True
PinPad Id:	2	EMV Enabled:	True
Configuration Values			
American Express Credit (AID: A00000002501)			
AID Activated:	4	Term	E0B8C8
Addl	F000F0A001	Capability:	
Capability:		Merch Cat	5311
Term Country:	840	Code:	
TAC Default:	C800000000	Term Currency:	840
TAC Online:	C800000000	TAC Denial:	0000000000
Trans Cur Exp:	2	Partial Select:	True
App Ver Num		Trans Cat	R
Pri:		Code:	
Term Floor Lim:	0	PSPId:	
Rand Sel	99	Rand Sel	0
Max%:		Thresh:	
Fallback expiry:	2099-12-31	Rand Sel	99
Default DDOL:	9F3704	Target%:	
No CVM limit:	0	Acquirer ID:	
Application	False	Default TDOL:	
Account		Is debit Card:	False
Selection:		Trans Refer	61000000
Terminal Risk		Currency Conv:	
Management		Transaction	
TTO:		Types:	
Application	True	Card Type:	
Selection:			

## WorldPay EMV Transaction Statistics Report

This report breaks down the transactions by Entry Mode and are filtered by batch and inside register. Card errors are counted per register.

**Figure 28: EMV Transaction Statistics**

<u>EMV Transaction Statistics</u>										
Network Batch Number:		6								
Open:		10/19/2016 12:47:45PM								
Close:		10/25/2016 4:03:18PM								
TOTAL TRANSACTIONS:										
ENTRY MODE	TRANSACTIONS					% OF TRANSACTIONS				
Manual	3					7.69				
Swiped	9					23.08				
Transponder	0					0				
EMV contact	17					43.59				
Swiped fallback	8					20.51				
Voice fallback	2					5.13				
EMV contactless	0					0				
EMV TRANSACTION COUNTERS PER TERMINAL										
Terminal Number	Chip Error	Card Removed	Unsupported APP	MSD Fallback	Offline Approved	Offline Declined	Approved	Declined	Approved Host Disconnected	Decline After Host Approved
	22	0	0	17	1	3	8	6	0	0

## WorldPay EMV Transaction Statistics Report (Current)

This report is similar to the **WorldPay EMV Transaction Statistics Report**, except for the current open batch.

## WorldPay Exceptions Report

This report provides summary information on refund and offline transactions as well as batch settlement status.

The value in the Amount column represents the transaction total, less any surcharge (debit or EBT Cash card) fees. Starting with 11.02, EMV transactions entry methods are differentiated as “Chip” or “Insert”.

### IMPORTANT INFORMATION

The COMPLETIONS NOT INCLUDED IN BATCHES section lists all dispenser transactions that were rejected by the WorldPay network after approving the preauthorization. The store manager must call the WorldPay Help Desk regarding payment of these transactions.



Figure 29: WorldPay Exceptions Report

WorldPay Exceptions Report									
Friendly Store 7300 W Friendly Ave Greensboro, NC, 27410 1-555-555-5555 TID: 5429290080431276304473				REPORT PRINTED: May 21, 2015 10:20:02 LAST EOD: 5/21/2015 4:29:10 AM					
Configuration ID: 1									
FROM: 5/20/2015 4:31:01 AM									
TO: 5/21/2015 4:20:10 AM									
Starting Batch Number: 2015-05-20-001									
Closing Batch Number: 2015-05-21-001									
Number of Shift Closes: 0									
Number of Automatic Batches: 0									
Total Number of Batches: 1									
BATCH STATUS									
2015-05-20-001				Balanced					
EXCEPTIONS	Credit	Debit	Fleet	EBT	Prepaid	Total	Amount	Fees	
Return	0	0	0	0	0	0	\$ 0.00	\$0.00	
Void	0	0	0	1	0	0	\$10.00	\$0.10 *	
Offline	0	0	0	0	0	0	\$ 0.00	\$0.00	
* Fees are not included in the Void Amount									
ENTRY METHODS									
Inside Swiped							28.37%		
Inside Manual							2.01%		
Pump Swiped							69.62%		
COMPLETIONS NOT INCLUDED IN BATCHES									
Batch	Date/Time	SEQ#	Trx.	Account Number	Total Amount	Action Code			





## WorldPay Settlement Report

This report provides summary network transaction information (count and dollar amount) for each card type.

The value in the Host Total column represents the transaction total, less any surcharge (debit or EBT cash card) fees.

**Figure 32: WorldPay Settlement Report**

WorldPay Settlement Report					
Friendly Store 7300 W Friendly Ave Greensboro, NC 27410 1-555-555-5555 TID: 5429290080431276304473					
Configuration ID: 1			REPROT PRINTED: May 21, 2015 4:31:10 AM		
FROM: 5/21/2015 4:31:01 am					
TO: 5/21/2015 4:20:10 AM					
NETWORK PAYMENTS SUMMARY					
Batch Number: 2015-05-20-001		Pending			
Card	Transaction	Count	Host Total	Fees	Total Amount
Debit		2	\$74.43		\$74.63
	Sales	2	\$74.43	\$ 0.20	\$74.63
MasterCard		1	\$57.21		\$57.21
	Sales	1	\$57.21	\$ 0.00	\$57.21
EBT Cash		3	\$21.00		\$21.10
	Sales	2	\$26.00	\$ 0.20	\$26.20
	Voids	1	-\$5.00	-\$0.10	-\$ 5.10
BATCH TOTALS		6	\$152.74	\$0.30	\$152.74
GRAND TOTALS:		6	\$152.74	\$0.30	\$152.74

## WorldPay Network Site Configuration Report

The WorldPay Network Site Configuration Report contains the site-level network parameters, including site identification, merchant processing rules, and communication parameters.

**Figure 33: WorldPay Network Site Configuration Report**

<b>WorldPay Site Configuration Report</b>	
WorldPay 600 Morgan Falls Rd Atlanta, GA, 30350 1800 200 5965 TID: 542929803122506000085477	
REPORT PRINTED: Jan 18, 2017 08:31	Configuration ID: 0
<b>Site Identification</b>	
Site Name:	WorldPay
Site Address:	600 Morgan Falls Rd
Site City:	Atlanta
Site State:	GA
Site Zip Code:	30350
Site Phone Number:	1800 200 5965
Hardware Version:	PASS
Software Version:	
Firmware Version:	
<b>Processing Parameters</b>	
EOD Host Posting:	3=Close Shift and Batch Limit and Post; includes terminal initiated and auto-close.
CCW EOD Close:	3=Automated EOD close prompting and performance disabled.
Batch Size Limit:	99
Enable Returns:	Enabled
Enable Voids:	Enabled
Enable Merchant And Journal PAN Masking:	Enabled
Enable Mismatch Prompting AVS:	Enabled
Enable Mismatch Prompting CUV2:	Enabled
Enable Check ID Prompting:	Enabled
Enable Process Partial Auth:	Enabled
Master Cutoff Limit:	\$999.99
Inside Debit Sales Fee:	\$0.00
Inside Debit With Cashback Sales Fee:	\$0.00
Outside Debit Sales Fee:	\$0.00
Inside EBT Cash Benefit Sales Fee:	\$0.00
Outside EBT Cash Benefit Sales Fee:	\$0.00
Download Phone Number:	0
<b>Communication Parameters</b>	
Connection Type:	TCP/IP
Primary IP Address:	10.5.48.6
Secondary IP Address:	10.5.48.6
URL And IP Port:	http://74.255.33.16:6662
Enable SSL:	Enabled
Primary Phone Number:	18776665965
Secondary Phone Number:	18002955965
Modem Port:	7
Baud Rate:	2400
Modem Init String:	AT&F0V0E0&K0&Q6%CX4S37=5&Z0
Modem Register:	ATS7=20S10=2S11=50S25=0&W0
Dial Header:	
Dial Trailer:	

# CWS Network Functions

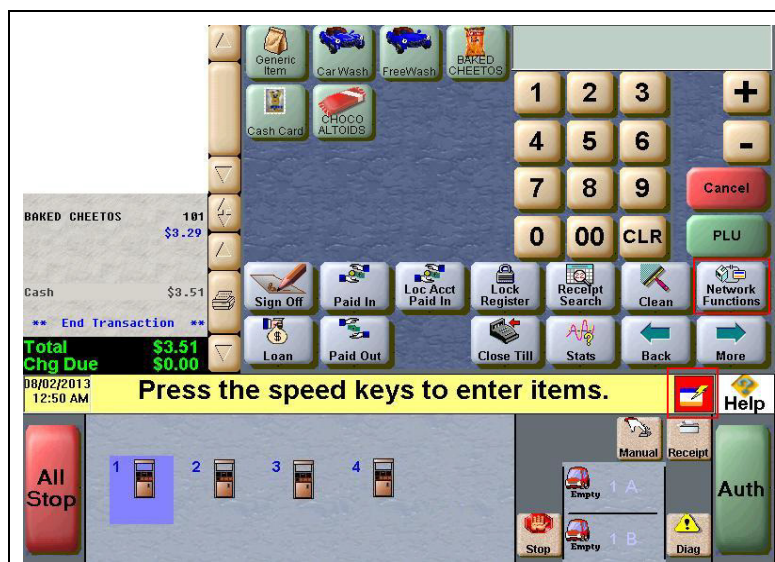
The Network Functions screen contains the Network Status window and Network Functions buttons.

## Accessing Network Functions

You can access the Network Functions screen in one of the following ways:

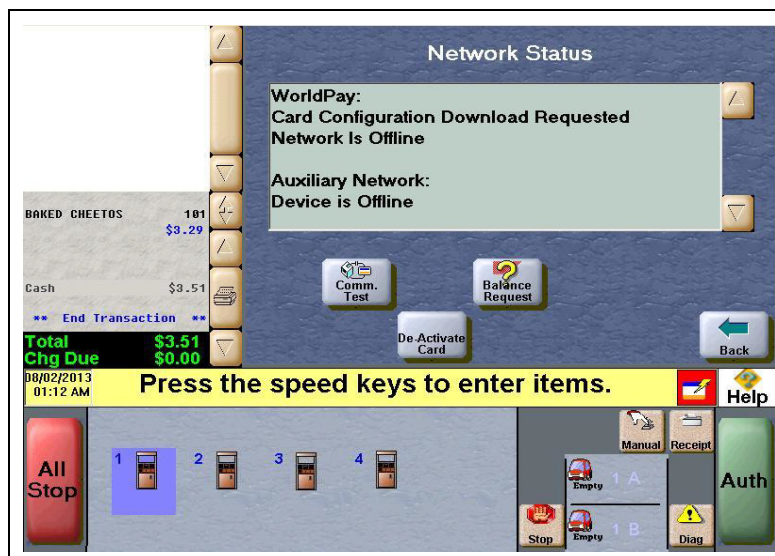
- On the CWS idle screen, select **More > Network Functions**.
- Select the **Network Status** Indicator when it is displayed on the message bar.

**Figure 34: Network Functions and Network Status Buttons**



With either action, the Network Status screen opens.

**Figure 35: Network Status Screen**



The Network Status screen provides information on all networks connected to the Passport system.

## Checking Network Status

The Network Status screen allows you to view a record of network events such as communication errors that occurred. Each network event is assigned a severity rating (low, medium, or high). When a new event occurs and has been added to the list, the Network Status button is also updated. The color of the Network Status button indicates the severity of the rating of the event:

Color	Severity
Green	Low
Yellow	Medium
Red	High

If multiple events occurred, the color of the Network Status button indicates the highest severity rating of the events. The Network Status button color changes when an event is corrected or after a predetermined time.

The following table lists some of the network messages that may display for the WorldPay network:

Message on Network Functions Screen	Network Status Indicator Color	Comments
Network Is Offline	Yellow	The store is not connected to the WorldPay network. This does not always indicate an issue, as the WorldPay network does not require a full-time connection.
Network is Online	Green	The store is connected to the WorldPay network.
Card Configuration Request Successful	Green	PDL completed successfully.
Card Configuration Download Requested	Green	PDL initiated
Card Configuration Request Failure	Yellow	Last PDL failed download or Passport failed to apply the download. If this error occurs frequently, call the WorldPay Help Desk.
About to reach transaction limit. Perform a Store Close	Red	Nearing the transaction limit for the current batch. If a batch close is not automatically triggered, perform a Shift Close.
Settlement with the host succeeded	Green	Last batch close finished successfully.
Settlement with the host failed. Automatically retrying	Yellow	Last batch close attempt failed. If this error repeats, call the WorldPay Help Desk.
Redialing secondary	Red	Cannot connect using the primary line, switching to secondary.
Call for authorization	Red	Cannot connect to the WorldPay network. Call Help Desk immediately.

In addition, the Network Functions screen also provides buttons for specific network requests.

The following table describes the “Network Functions” buttons and their behavior:

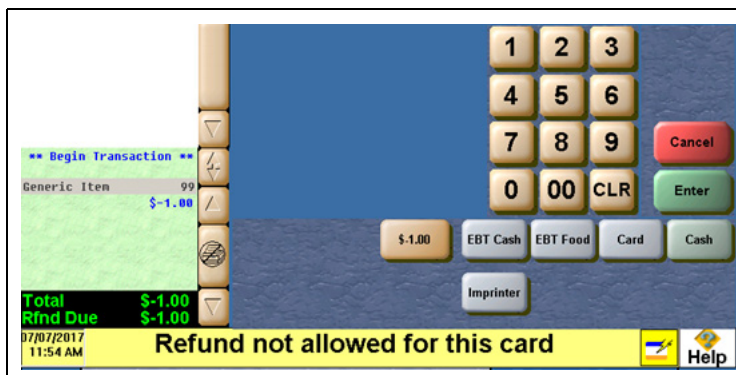
Button	Behavior
Comm. Test	Perform an echo test with the WorldPay network. The message “Successful X-MIT” indicates successful test of WorldPay network communications. The Message, Send timed out” indicates failure of WorldPay network communications.
De-Activate Card	Deactivate an activated gift or cash card through the WorldPay network. The Passport system prompts the cashier to enter the de-activation dollar amount and swipe the customer’s card. After the service runs successfully, the Passport system prints a receipt and displays the message “Deactivation Complete”.
Balance Request	Obtain current balance of a gift or cash card and print a receipt showing the balance for the customer.

## Refunds with EMV

WorldPay does not allow refunds for EMV Credit and Debit cards. WorldPay does not support Returns and Voids for Debit cards.

Also, a EMV transaction could be refunded to cash as in typical magstripe initiated transactions.

**Figure 36: POS Declining an EMV Debit Transaction**





---

# Third-party Licenses

## OpenSSL™ License

Copyright © 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3 All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

- 4 The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
- 5 Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
- 6 Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).  
This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

## SSLeay License

Copyright © 1995-1998 Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)). All rights reserved.

This package is an SSL implementation written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1 Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
- 2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3 All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com))”

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptographic related.

- 4 If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com))”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.].

## Appendix A: Stores with TCP/IP SSL Connections and Programming for Gilbarco RV042 Firewall Router

For stores with TCP/IP SSL connections and Gilbarco RV042 Firewall Router, Passport encrypts network transactions over a TCP/IP link using SSL.

Obtain the following information from the site's Internet Service Provider (for example, Time-Warner Cable® or Comcast®) or the site's IT personnel:

- Primary DNS IP address: \_\_\_\_\_.
- Secondary DNS IP address: \_\_\_\_\_.

*Note: At least one DNS IP address is required. A secondary address is recommended to ensure DNS resolution and connectivity to the WorldPay network.*

After obtaining this information, proceed as follows to configure the Passport RV042 Router for communication with the WorldPay network:

- 1 Ensure that the site has a networking device with firewall capabilities (for example, router or switch) to be placed between the Passport RV042 Router and the site's Internet modem.

### CAUTION

DO NOT connect the Internet directly to the WAN port on the firewall router. This compromises PA-DSS compliance. For additional information, refer to *MDE-XXX Passport EDH (WorldPay) V09.34 Implementation Guide for PA-DSS V3.2*.

- 2 Obtain from the site's IT personnel the IP address and subnet mask of the device used to connect the Passport RV042 Router to the site's Internet modem. Enter the IP address and subnet mask in the Default Gateway Address of the RV042 Router's Setup page.
- 3 Obtain from the site's IT personnel the static IP address used as the WAN IP address for the RV042 Router. Enter this static IP address in the WAN IP address of the RV042 Router's Setup page.

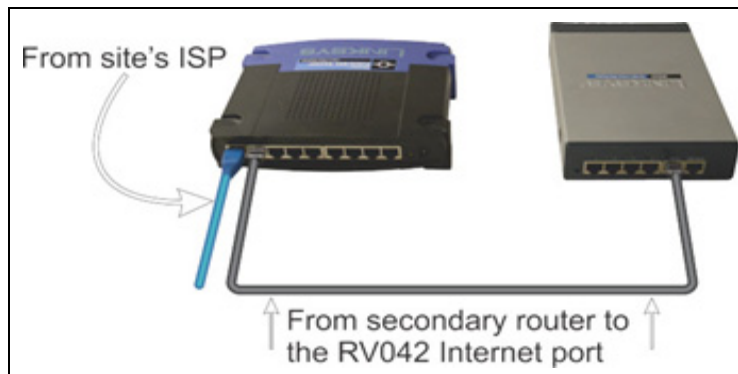
### CAUTION

A static IP address is mandatory. Use of a dynamic IP address results in loss of communication to the WorldPay network.

- 4 To program, ensure that the RV042 Firewall Router WAN/Internet port is enabled. For more information, refer to *MDE-4866 Passport Firewall Router Start-up and Service Manual* or *MDE-4954 Passport Start-up and Service Manual for the Cisco Firewall Router (Q13708-08)*.

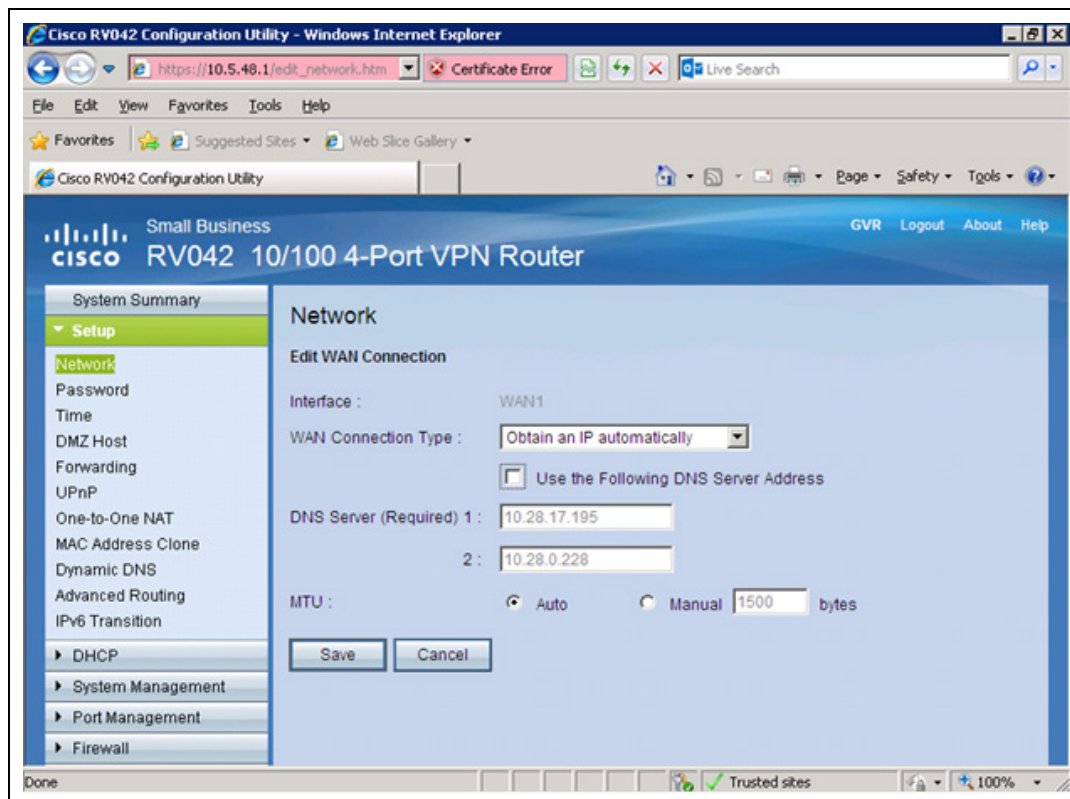
- 5 Connect the RV042 Firewall Router to the customer-provided network device, using a CAT5 cable from the RV042 Firewall Router WAN/Internet port.

Figure 37: Router Setup



- 6 Enter the Primary and Secondary DNS addresses (obtained from the store IT personnel or ISP) into the appropriate fields on the RV042 Router's Setup page.
- 7 Configure the WAN Connection Type section of the RV042 Firewall Router setup page (see Figure 38).

Figure 38: Configuring WAN Connection Type



- 8 Obtain appropriate settings for the “WAN Connection Type” selection from the merchant, either **Static** or **Obtain an IP automatically** for the network.

9 To add the Service Management rule, proceed as follows:

a Select **Firewall > Access Rules**.

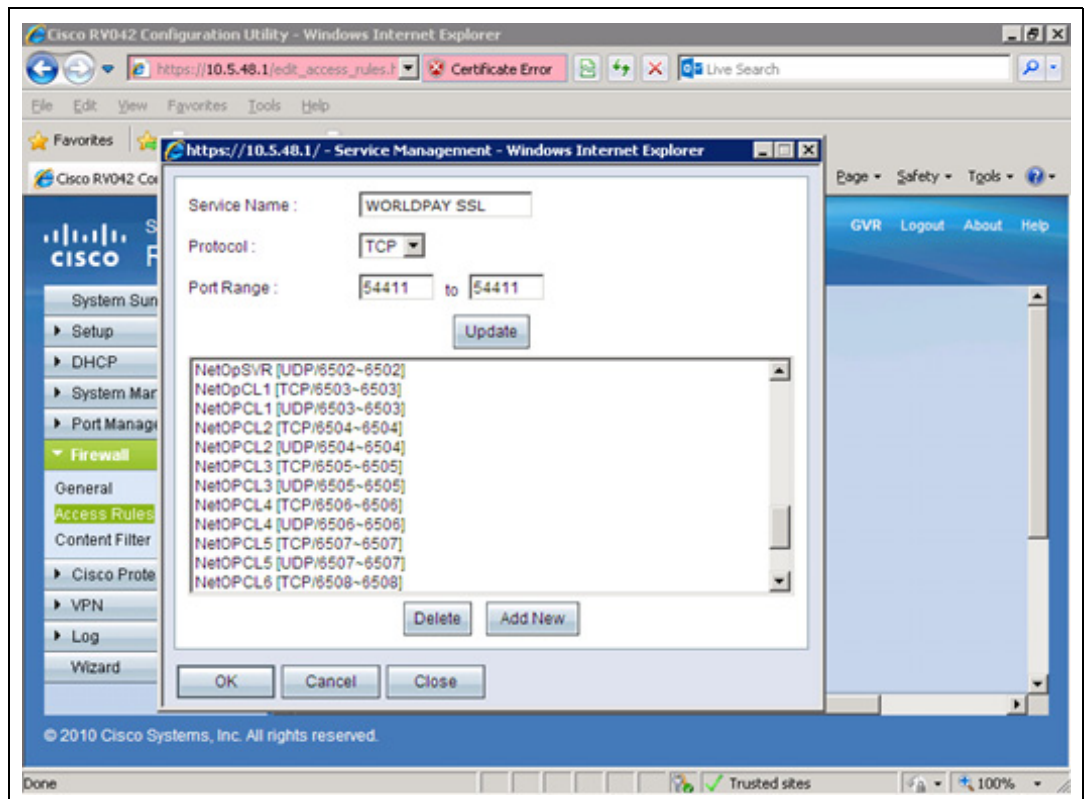
b Click **Add New** to add a new firewall access rule.

c Click **Service Management**.

d Add a new Service Management rule with Service Name of “WORLDPAY SSL”. Select **TCP** as the Protocol. Enter “54411” for both values for Port Range.

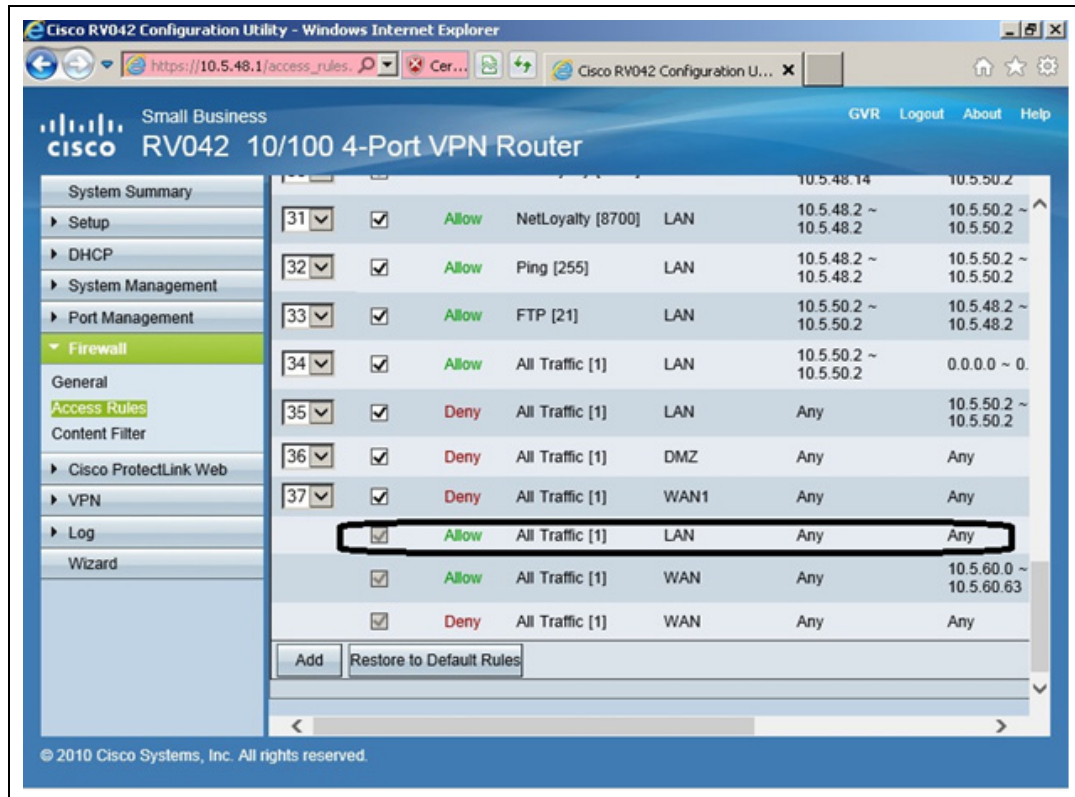
e Click **Update** to add the rule.

**Figure 39: Adding the Service Management Rule**



- At the bottom of the Firewall Access Rules, ensure that the rule shown in [Figure 40](#) is selected and set to “Allow”.

**Figure 40: Selected Rules Setting**



- Configure the WAN2EDH and EDH2WAN firewall access rules using the information obtained in step 2 on [page 43](#). For additional information, refer to either Appendix D of *MDE-4866 Passport Firewall Router Start-up and Service Manual* or *MDE-4954 Passport Start-up and Service Manual for the Cisco Firewall Router (Q13708-08)*.
- After completing all the steps, exit out of all screens.

## Appendix B: Upgrading to Passport V11.04

This section provides WorldPay-specific information the ASC needs for upgrading from Passport V10Q or V11.02G.

### IMPORTANT INFORMATION

**Upgrades to WorldPay V11.04 are supported only for locations running:**

- **WorldPay V10 with Service Pack Q and later**
- ~ OR ~
- **WorldPay V11.02 with Service Pack G or J with Maint PackX.**

If the Passport system is installed with an earlier version or service pack, then you must first upgrade to one of these minimum versions before upgrading to WorldPay V11.04, or perform a clean install.

If you are performing an upgrade, as opposed to a clean installation, and you are swapping out or installing new VeriFone MX915 PIN pads, do not install the PIN pads until the software upgrade has completed.

**Before beginning the upgrade, the ASC must perform the following:**

- Ensure that all dispenser software and firmware meet applicable requirements to support loyalty and other fuel discounting functionality, including support of \$0.000 PPU.
- Print the **Network Configuration Report**. This will be helpful if a clean install is required and to confirm all network settings (including Host Connection Type and other parameters in Global Information).
- Confirm with the WorldPay Help Desk the 24-digit Terminal ID to be used after the upgrade.
- Perform Store Close and ensure that all network transactions have completed by checking the Store and Forward Transactions Report for fallback transaction information. Call WorldPay Help Desk 1-800-200-5965 in order to check the period was closed successfully.
- Print all necessary reports and ensure all file transfers from Passport to BOS have completed.

**After the upgrade, the ASC must perform the following:**

- Update the Terminal ID field in **MWS > Set Up > Network Menu > WorldPay > Network Site Configuration** using the steps in [“WorldPay Terminal ID”](#) on [page 9](#).  
*Note: The PDL will fail unless the Terminal ID is updated after the upgrade.*

### **IMPORTANT INFORMATION**

WorldPay **Terminal ID changed from 22 to 24 digits** in this version. WorldPay instructions are to insert “00” into the proper place within the TID (after the 15th digit)  
For example:

- **Merchant ID:** 542929001000041 (15-digit)
- **TID:** 00117704 (the 6-digit TID padded to 8 digits with two leading zeros)
- **Check digit:** 8 (1 digit)

So, if in previous version the field Terminal ID was the following:

5429290010000411177048  
542929001000041001177048 will be in the new version

After the upgrade, the ASC must add the 00 after the Merchant ID port such that the new Terminal ID is 542929001000041001177048. This breaks down to:

- **Merchant ID:** 542929001000041
- **TID:** 00117704
- **Check digit:** 8

**For ALON branded stores, the merchant or store manager must contact ALON at 1-877-256-6729 a week before the scheduled upgrade. ALON will provide the merchant or store manager with instructions for preparing for the upgrade, including Terminal ID configuration.**

- Request a PDL Download by going to **MWS > Set Up > Network Menu > WorldPay > PDL Download**.
- For upgrades from V10:
  - Enable EMV in Manager Workstation with at least one PIN pad set to “EMV Capable”.
  - Review the parameters on **MWS > Set Up > Network Menu > WorldPay > Site Configuration > EMV Parameters** tab with the store owner or store manager. If applicable, advise the store owner or manager to contact WorldPay Help Desk to discuss the financial implications and suggested settings on this screen.
- If installing a VeriFone MX915 or Ingenico iSC250/iPP320 PIN Pad after the upgrade, ensure that the **EMV Capable field** is selected in **MWS > Set Up > Register > Register Set Up > Device Configuration**.
- Review the settings in **MWS > Set Up > Register > Register Set Up > Device Configuration** with the merchant or store manager. For more information, refer to [“Accepting Magnetic Stripe Contactless Inside”](#) on [page 27](#).
- Review [“What’s New in Passport V11 at WorldPay Stores”](#) on [page 5](#) with the merchant or store manager and answer any questions, especially those regarding inside EMV processing.



## Appendix C: WorldPay Egress Rules for the SZR

As part of a SZR installation using *MDE-5382 Secure Zone Router (Acumera) Installation Instructions*, have the store's IT network representative add the `Tptrans.lynksystems.com` TCP-6662 (Primary Payment Hostname) egress rules to the site's perimeter firewall.

*American Express® is a registered trademark of American Express Company. Cisco® is a registered trademark of Cisco Systems Inc. Comcast® is a registered trademark of Comcast Corporation. CRIND®, Gilbarco®, and Passport® are registered trademarks of Gilbarco Inc. Diners® is a registered trademark of Citicorp Diners Club Inc. Discover<sup>SM</sup> is a service mark of Novus Credit Services Inc. EMV® is a registered trademark of EMVCo LLC. Ethernet® is a registered trademark of Xerox Corporation. Europay® and MasterCard® are registered trademarks of MasterCard International Inc. Epson® is a registered trademark of Seiko Epson Corporation. Fleet One<sup>SM</sup> is a service mark of Fleet Financial Group Inc. FlexPay™ is a trademark of Gilbarco Inc. FuelMan® is a registered trademarks of FleetCor Technologies Operating Company LLC. GOLD<sup>SM</sup> is a service mark of Gilbarco Inc. Impulse™ is a trademark of Odysii. Ingenico® is a registered trademark of Groupe Ingenico. Sprint® is a registered trademark of Sprint Nextel. Time-Warner Cable® is a registered trademark of Time Warner Inc. VeriFone® is a registered trademark of VeriFone Inc. Visa® is a registered trademark of Visa Inc. Voyager® is a registered trademark of U.S. Bancorp Licensing Inc. Walmart® is a registered trademark of Wal-Mart Stores Inc. Wayne® is a registered trademark of Dresser Industries, Inc. WorldPay® is a registered trademark of WorldPay US Inc. Wright Express® is a registered trademark of Wright Express Financial Services Corporation.*

© 2018 Gilbarco Inc.  
7300 West Friendly Avenue · Post Office Box 22087  
Greensboro, North Carolina 27420  
Phone (336) 547-5000 · <http://www.gilbarco.com> · Printed in the U.S.A.  
MDE-5419B Passport® V11.04 Network Addendum for WorldPay® · November 2018

