# Introduction

## Purpose

This manual provides network-specific information for Passport™ systems at Marathon® stores that use the HPS-Dallas network.

**Upgrading to Passport V21 requires the use of a Gilbarco® certified Managed Network Service Provider (MNSP). The Marathon Managed Firewall solution provided by Cybera® is the preferred option. The MNSP allows a simpler configuration and footprint of your Passport POS. The MNSP allows for removal of high-speed device MicroNode and removal of RV042 (store router). The MNSP combines these functions along with network communications, PCI/Card Brand Compliance and 4G cellular backup.**

### IMPORTANT INFORMATION

**Upgrading to Passport V21 requires advance notice to the HPS-Dallas network (1-800-378-1204) if the site is implementing EMV® or installing an MNSP device**.

**EMV**
EMV functionality affects inside and outside transactions. At least two full days before the scheduled upgrade, advise the merchant that he must contact the HPS-Dallas network (1-800-378-1204) 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.

On the day of the scheduled upgrade, ask the merchant or store manager if he notified the HPS-Dallas network of the need to prepare to enable EMV network communication. If the merchant or store manager has not notified the HPS-Dallas 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 Parameter Download (PDL) to enable EMV.
- Arrange a later date for the upgrade, after the network has sufficient time to enable EMV.

**MNSP**
Network communications/protocols need to be updated in real time when replacing the high-speed device MicroNode with the MNSP device. On the day of the scheduled upgrade, after batch close, contact the HPS-Dallas network (1-800-378-1204), inform them which MNSP is being installed and request IP addresses be modified (This could take 4 hours so plan to make the call as soon as the site is down). The HPS-Dallas network will provide new communication/protocols (IP addresses) depending on which MNSP device is being installed. They will also provide Transport Layer Security (TLS) Encryption certificate URLs if needed.

*Note: Validate with MNSP that the site's router/firewall is configured to send messages to loyalty and mobile hosts. Locations using Marathon's preferred MNSP provider (PDI Security Solutions, Cybera) with standard template have been configured to connect to the hosts. If you are using a custom template, please contact Cybera prior to installation. Any other firewall device(s) at the site might need updating.*

**Loyalty App Host Information**

- Production IP: 15.197.220.17
- Production TLS: prod.mpc.oc.ai
- TCP Ports: 4110

**Mobile Payment Host Information**

- Production IP: 3.33.215.201
- Production TLS: prod.mpc.oc.ai
- TCP Ports: 4010

**IMPORTANT INFORMATION**

Due to the End of Life of the Ingenico® PIN Pads (iSC250 & iPP320), these devices were not certified with the HPS-Dallas network for Passport V21. When upgrading to V21.02, Passport will check to see if an Ingenico PIN Pad is connected. If one is detected, an error message will be displayed and the upgrade will be aborted. For a clean install of V21.02 Ingenico will not be an option on the Register Set Up screen. Although the iSC-250 and iPP-320 will still process EMV transactions on V20.02, it is recommended that a site upgrade their PIN Pads to Verifone® MX915 to remain in compliance with the approved HPS-Dallas network EMV configuration. Sites that continue using iSC-250 or iPP-320 after upgrading to Passport V20.02 will do so at their own risk of receiving fraud liability charge backs due to using a non-EMV certified solution.

## Intended Audience

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

*Note: Leave this manual at the site for the manager's reference. This manual is available for download by Passport-certified ASCs on Gilbarco's Extranet Document Library (GOLD℠).*

***REVIEW AND FULLY UNDERSTAND THIS ENTIRE MANUAL, BEFORE BEGINNING UPGRADE TO OR INSTALLATION OF PASSPORT V21 FOR MARATHON.***

# Table of Contents


| Topic | Page |
|---|---|
| Introduction | 1 |
| What's New in Passport V21 at Marathon Stores | 5 |
| What's New in Passport V20 for Marathon Stores | 7 |
| What's New in Passport V12 for Marathon Stores | 9 |
| What's New in Passport V11.04 for Marathon Stores | 9 |
| Assigning Product Codes | 10 |
| Programming Network Site Configuration | 11 |
| Programming Network Card Configuration | 21 |
| Requesting a PDL Download | 22 |
| Requesting Email | 23 |
| Fuel Discount Configuration | 24 |
| Comm Test | 25 |
| Network Journal Report | 26 |
| Network Reports | 28 |
| CWS Network Functions | 40 |
| EBT Food and EBT Cash Tenders | 42 |
| Appendix A: Network Events Messages | 44 |
| Appendix B: Mobile Payment Configuration | 45 |
| Appendix C: Loyalty Configuration Access | 49 |
| Appendix D: Upgrading to Passport V21 | 56 |


# Related Documents

| Document Number | Title | GOLD Library |
|---|---|---|
| MDE-5025 | Passport V9+ System Reference Manual | Passport |
| MDE-5266 | What's New in Passport Version 11 | Passport |
| MDE-5382 | Secure Zone Router (Acumera) Installation Instructions | Passport |
| MDE-5470 | What's New in Passport Version 12 | Passport |
| MDE-5519 | What's New in Passport Version 20 | Passport |
| MDE-5545 | Passport EDH (Heartland-Dallas) V11.24.01* Implementation Guide for PA-DSS V3.2 | Passport |
| MDE-5574 | What's New in Passport Version 21 | Passport |

## Abbreviations and Acronyms

| Term | Description |
|---|---|
| AFD | Automated Fuel Dispensers |
| AID | Application Identifier |
| ASC | Authorized Service Contractor |
| BOS | Back Office System |
| CRIND® | Card Reader in Dispenser |
| CWS | Cashier Workstation |
| EDH | Enhanced Dispenser Hub |
| EMV | Europay®, MasterCard®, and Visa® |
| GOLD | Gilbarco Online Documentation |
| HPS-D | Heartland Payment Systems-Dallas |
| ISP | Internet Service Provider |
| MNSP | Managed Network Service Provider |
| MWS | Manager Workstation |
| OPT | Outdoor Payment Terminal |
| PA-DSS | Payment Application Data Security Standard |
| PCATS | Petroleum Convenience Alliance for Technology Standards |
| PDL | Parameter Data Load or Parameter Download |
| POS | Point of Sale |
| PPU | Price per Unit |
| RAS | Remote Access Service |
| SZR | Secure Zone Router |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TLS | Transport Layer Security |

## Technical Support

If you are a store manager or a 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 an installation, call Gilbarco at 1-800-743-7501.
*Note: Be prepared to provide your ASC ID.*

To contact the Marathon Help Desk, call 1-800-378-1204.

## Network Data Retention

The Passport system's network database saves transaction details for 35 days. This network setting is not editable. In addition to meeting Payment Application Data Security Standard (PA-DSS) compliance requirements, it allows retailers to use the Backup Journals/Reports utility to save one full month of Passport system data on a single CD. For more information on saving journals and reports to CD, refer to *MDE-5025 Passport V9+ System Reference Manual*.

# What's New in Passport V21 at Marathon Stores

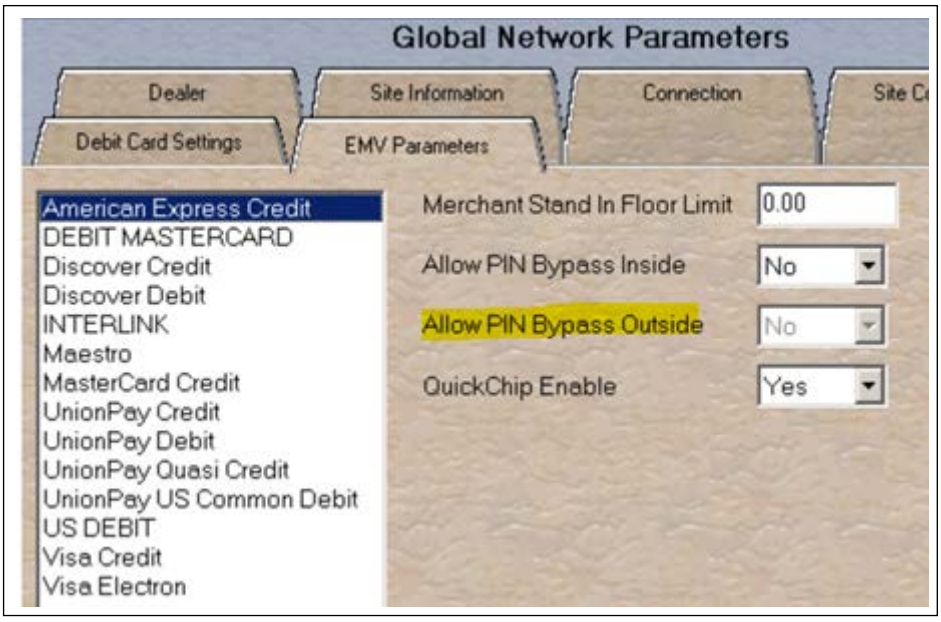
## Allow PIN Bypass for American Express® Cards

Beginning with Passport V21.03, support for PIN bypass has been added at Automated Fuel Dispensers (AFD) for American Express. The "Allow PIN Bypass Inside" and "Allow PIN Bypass Outside" option has been defaulted to "Yes" for American Express cards on the **EMV Parameters** tab in Global Network Parameters. When the value of the option is set to "Yes" the customer is allowed to bypass PIN entry inside the PIN Pad and outside at the CRIND.

To view or edit the configuration for PIN Bypass for American Express cards, proceed as follows:

1. Go to **MWS > Set Up > Network Menu > HPS > Global Info Editor.**
2. On the EMV Parameters tab, select **American Express Credit** card, select the **Allow PIN Bypass Inside** drop-down option or the **Allow PIN Bypass Outside** drop-down option, and select "**Yes**" or "**No**" to enable or disable PIN Bypass for American Express Cards.
3. Click **Save** to save any changes made.

**Figure 1: Global Info Editor - EMV Parameters Tab**




## New PIN Bypass Functionality

Beginning with Passport V21.03, the "credit or debit" prompt inside the POS and outside the Outdoor Payment Terminal (OPT) has been replaced by a new PIN bypass flow. When a customer presents their Debit/ATM card for payment, they will be presented with a PIN prompt, the customer can press ENTER, ***without*** entering a PIN and process the transaction as credit. If a PIN is entered, the transaction will be processed as a normal debit transaction. This change will provide the merchant with further liability protection against lost and stolen cards. The new prompt flow for PIN entry is not configurable.

## EMV Contactless Outside

Beginning with Passport V21.03, EMV Contactless is available for outdoor transactions on Flexpay™ IV dispensers (M7), Flexpay II dispensers (M5), and Wayne iXPay I. Customers may use their EMV contactless enabled credit or debit card to pay for transactions. The customer may tap the card or must bring the card within proximity of the EMV-capable reader.

Dispensers need to be updated with the following firmware:

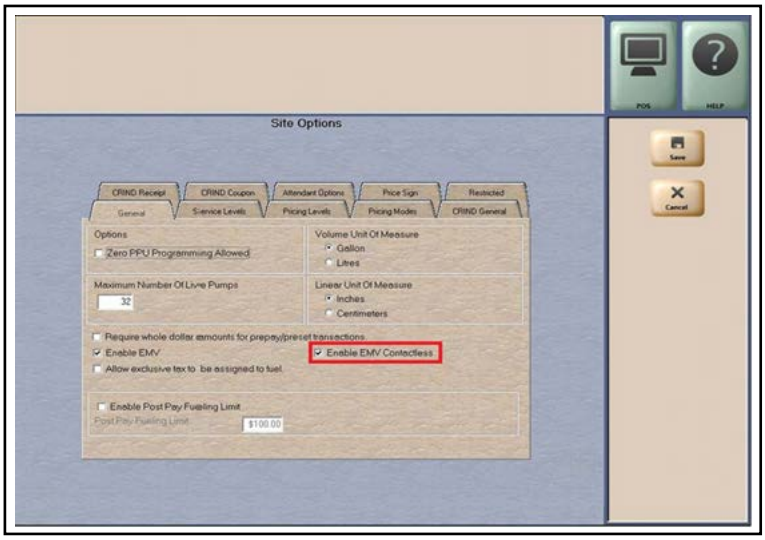
- M7 and M5 Vipa 6.8
- iXPay 6.8.2.XX

To prepare for EMV Contactless outside, contact the HPS-Dallas network at least two business days before the upgrade and tell them when EMV Contactless outside will be enabled.

To configure Passport for EMV Contactless for outdoor transactions, proceed as follows:

1. Go to **MWS > Fuel > Site Options**.
2. On the **General** tab, select the **Enable EMV Contactless** check box to enable EMV Contactless outside.
3. Click **Save** to save the changes.

**Figure 2: Store Options - General Tab**




## Passport V21 Core Feature Enhancements

For information on any of the new core features, refer to *MDE-5574 What's New in Passport* Version 21.

# What’s New in Passport V20 for Marathon Stores

The following features have been updated or are new for Marathon stores.

## WEX EMV Cards

Starting in Passport V20.04, WEX EMV chip cards are accepted for both inside and outside payments. After the upgrade, a new PDL must be requested (**MWS > Set Up > Network > Marathon > PDL Download**), which will be applied after the next store close. WEX EMV card details will appear in the EMV Configuration Report and can be checked to confirm that the PDL was received and processed.

## Allow Unsupported Chip Card Outside

Until the HPS-Dallas payment network is prepared to process Voyager chip cards as EMV, starting in Passport V20.04 the merchant can configure Passport to control whether these cards are processed as magstripe at outdoor terminals.

A new option called “Allow Unsupported Chip Card As Magstripe Outside” has been added to the Site Configuration tab on the Site Configuration screen (**MWS > Set Up > Network > Marathon > Global Info Editor > Site Configuration tab**). When set to **Yes** and an EMV card which has an unsupported Application Identifier (AID) is inserted at the CRIND, the customer will be prompted to remove the card. The magstripe will be read as the card is being removed, and the sale will be processed as a magstripe transaction. When set to **No**, an error message will display at the CRIND and on the cashier workstation when the unsupported chip card is inserted at the CRIND. The default setting is **Yes**. This enhancement applies to any unsupported chip card that is inserted at the dispenser.

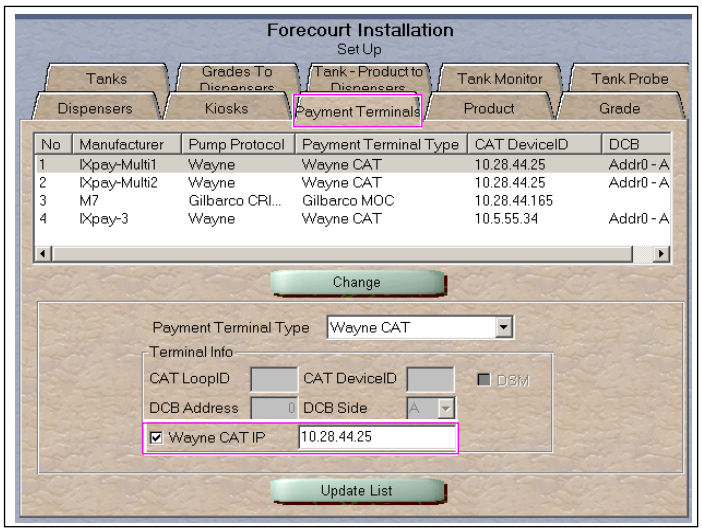
## Wayne iX Pay™ Terminal

Passport V20.02 is the first release to support Wayne iX Pay payment terminal for EMV with communication via IP.

To configure Passport to communicate with a Wayne iX Pay payment terminal, proceed as follows:

1. Navigate to **Set Up > Forecourt > Forecourt Installation**.
2. Select the **Payment Terminals** tab.
3. Select **Wayne CAT** from **Payment Terminal Type** drop-down list.
4. Select the **Wayne CAT IP** check box to enable the text box for the IP address
5. Enter the IP address of the payment terminal. If Wayne CAT IP is not selected, the payment terminal can be configured via the serial protocol.
   *Note: If a single Wayne iX Pay board controls both sides of the dispenser, enter the same IP address for both sides.*

**Figure 3: Forecourt Installation**




## Passport V20 Core Feature Enhancements

For information on any of the new core features, refer to *MDE-5519 What's New in Passport Version 20.*

# What's New in Passport V12 for Marathon Stores

The following features have been updated or are new for Marathon stores.

## WEX Bulletin

Starting with V12.02, Passport enables support of the Technical Specification Compliance Policy, effective January 1, 2019. The year 2020 compliance requirements of this notice will be part of a future release. Sites that are not compliant will face penalties via an increase in interchange rates. For more information on merchant requirements and penalties, contact WEX at MerchantInquiry@wexinc.com.

## Passport V12 Core Feature Enhancements

For information on any of the new core features, refer to *MDE-5470 What's New in Passport Version 12*.

# What's New in Passport V11.04 for Marathon Stores

The following features have been updated or are new for Marathon stores.

## EBT Food and EBT Cash Tenders

Passport provides new Tender Group selections that allow the merchant to program EBT Food and EBT Cash tenders for stores that want to process EBT with Passport on the HPS-Dallas Network. The site would need to provide FNS number and a copy of certificate to the Territory Manager for EBT to be enabled on the PDL. The EBT Tenders may need to be activated/deactivated in Manager Workstation (MWS) Tender Maintenance. If the site wants to utilize an external EBT terminal, set the EBT Food/CASH to the EBT Food (Non-integrated) and EBT Cash (Non-integrated) Tender Group.

## Network Connection Type

Stores upgrading to V11.04 or later now have a new option of using TLS with their TCP/IP connection. TLS allows the merchant to use a direct secure network communication path over their store's Internet Service Provider (ISP). On the day of the scheduled upgrade, ask the merchant or store manager if he notified the HPS-Dallas network of the wish to enable TLS network communication. Marathon requires that stores running V11.04 and higher use a MNSP solution and program Passport to use TLS. If the merchant or store manager has not notified the HPS-Dallas network, call the network on behalf of the merchant or store manager. Ask the network representative if he can expedite enabling the merchant for TLS communication.

## Comm Test Network Application in MWS and POS

This feature allows a site to validate that the HPS Dallas Network TCP/IP with TLS is online and working.

## 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*.

# Assigning Product Codes

After configuring products or grades, exercise care in assigning network codes to fuel products or grades. Assigning an incorrect product code to a fuel product or grade may cause the HPS-Dallas network to decline transactions, especially for those tendered with a fleet card, as fleet cards often apply fuel restrictions to the transaction.

To assign network product codes, proceed as follows:

1. Go to **MWS > Setup > Forecourt > Forecourt Installation** and click **Assign Network Codes**.

2. Ensure that the Fuel Grade Descriptions are accurate.

3. Confirm that each fuel grade is using the correct NACS product code. Marathon suggests using the following standard NACS product codes.

   **Product Description Product Code:**
   - Regular Unleaded 001
   - Mid-Grade Unleaded 002
   - Premium Unleaded 003
   - Diesel #2 019
   - Diesel #1 021
   - E-85 026
   - Diesel Off-Road (#1 & #2 Non-Taxable) 032
   - Kerosene 300

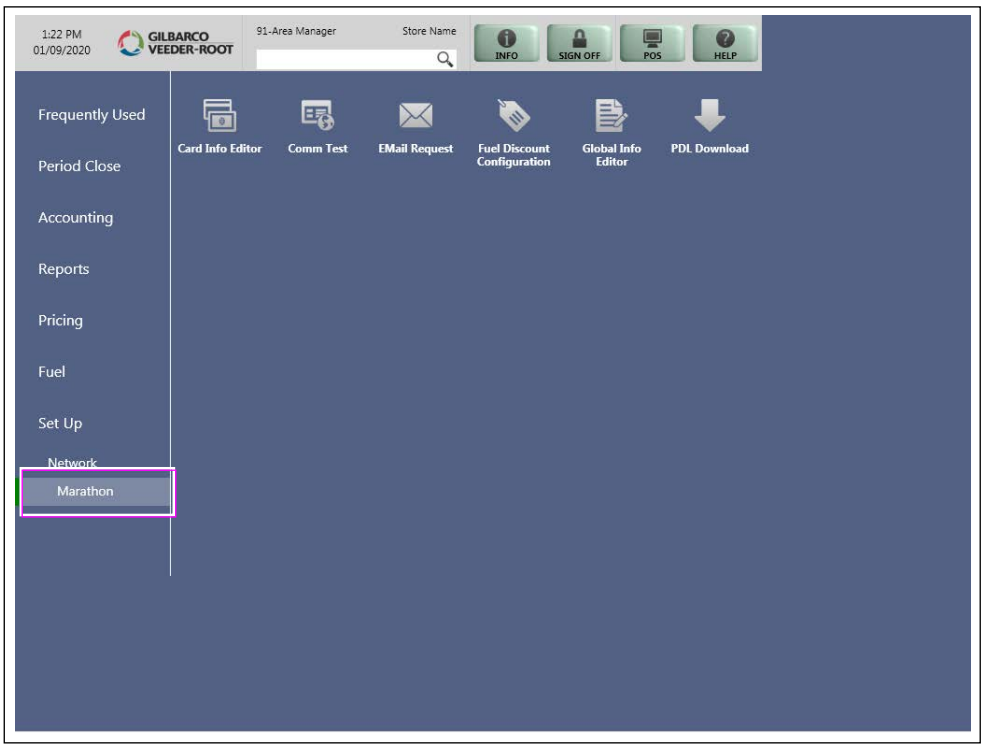
# Programming Network Site Configuration

| IMPORTANT INFORMATION |
| --- |
| The Enhanced Dispenser Hub (EDH) must be installed and running before programming in **MWS** > **Set Up** > **Network**. |

To program network site configuration, proceed as follows:

1 From the Manager Workstation (MWS) main menu, select **Set Up** > **Network** > **Marathon**. The Marathon Network Configuration menu opens.

**Figure 4: Marathon Network Configuration Menu**

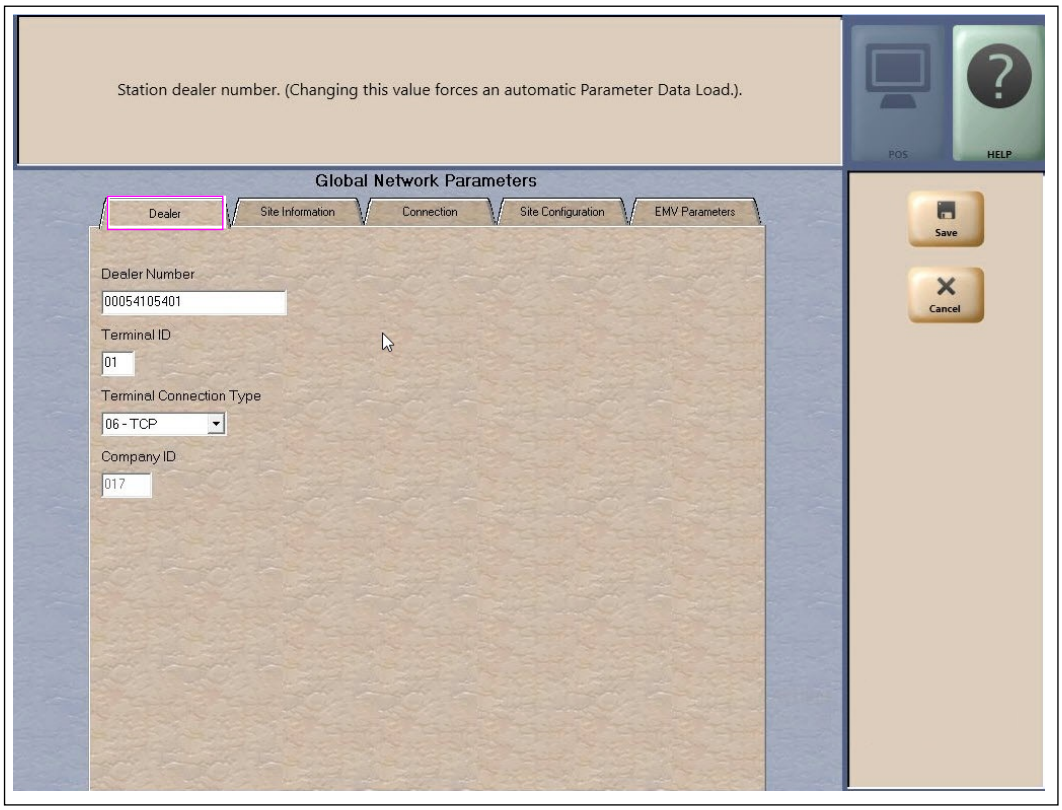



The following option buttons are displayed in the Network Configuration menu:

- Card Info Editor
- Comm Test
- EMail Request
- Fuel Discount Configuration
- Global Info Editor
- PDL Download

**2** Select **Global Info Editor**. The **Global Network Parameters** screen opens. Select the **Dealer** tab.

**Figure 5: Global Network Parameters - Dealer Tab**

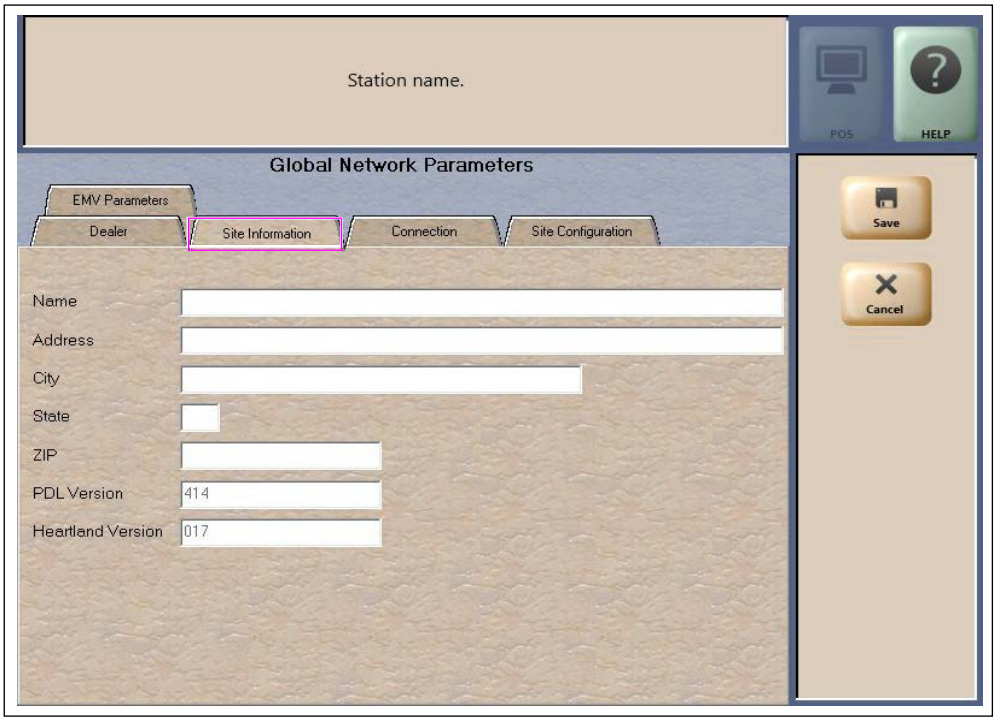



## Fields on the Dealer Tab

| Field | Description |
|---|---|
| Dealer Number | An 11-digit number the HPS-Dallas network uses to identify the store.<br>*Notes: 1) Enter the dealer number before receiving initial PDL.*<br>*2) Change Dealer Number only after Store Close.* |
| Terminal ID | The terminal identification number the HPS-Dallas network assigns to the store.<br>*Notes: 1) The default Terminal ID is "01".*<br>*2) Change Terminal ID only after Store Close.* |
| Terminal Connection Type | A drop-down menu for selecting the type of connection used to communicate with the HPS-Dallas network. Options are None, 02 – Dial, and 06 – TCP. |
| Company ID | A 3-digit number assigned by the HPS-Dallas network to the company handling transactions for the site. This field defaults to 017 for Marathon and is not editable. |

3 After programming the **Dealer** tab, select the **Site Information** tab. Although the HPS-Dallas PDL populates the **Site Information** tab, many of the fields are editable. If you change and save information on the **Site Information** tab, you must notify the Marathon Help Desk at 1-800-378-1204 to avoid reverting to invalid data in a subsequent PDL.

**Figure 6: Site Information Tab**




## Fields on the Site Information Tab

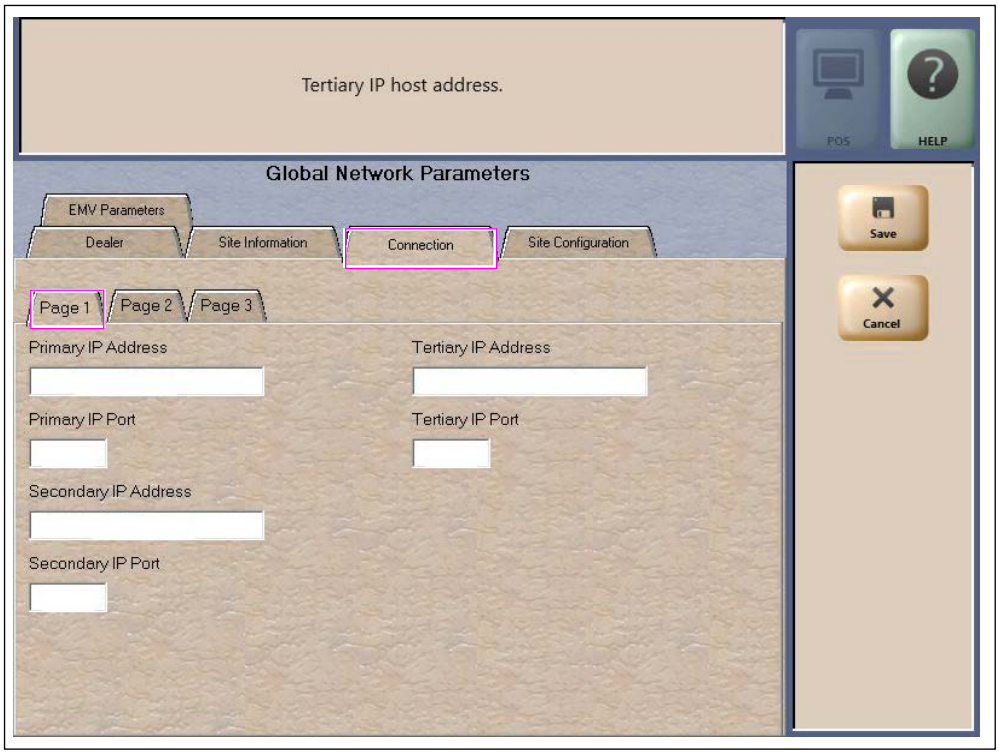
| Field | Description |
|---|---|
| Name | The store name. The name displays here and appears on all receipts for network transactions. This field is editable. |
| Address | The street address for the store. The street address displays here and appears on all receipts for network transactions. This field is editable. |
| City | The city in which the store is located. The city displays here and appears on all receipts for network transactions. This field is editable. |
| State | The state in which the store is located. The state displays here and appears on all receipts for network transactions. This field is editable. |
| ZIP | The ZIP code assigned to the store. The ZIP displays here and appears on all receipts for network transactions. This field is editable. |
| PDL Version | The version of the PDL sent to the site. This field is not editable. Default value is 414. |
| Heartland Version | The version of the EDH version. This field is not editable. |

4 After programming the **Site Information** tab, select the **Connection** tab. Programming the Connection tab varies depending on the Terminal Connection type selected on the Dealer tab.
The Page 1 tab contains parameters for Terminal Connection Type of 06 - TCP.
The Page 2 tab contains parameters for Terminal Connection Type of 02 - Dial.

**a** Select the **Page 1** tab to complete programming for a TCP/IP connection.
*Note: All Marathon sites must use TCP/IP connection with TLS encryption.*

| IMPORTANT INFORMATION |
| --- |
| Contact the Marathon Help Desk at 1-800-378-1204 to obtain IP addresses and ports. |

**Figure 7: Connection - Page 1 Tab (for TCP/IP Connections)**




The following table contains information on fields that are displayed on the **Page 1** tab (for TCP/IP Connections):

| Field | Description |
| --- | --- |
| Primary IP Address | The main IP address used to connect to the HPS-Dallas network. The format of this field is four sets of numbers in the range of 1 through 255, each separated by a decimal point, for example 255.255.255.255. Verify with the HPS-Dallas network the value to key as the Primary IP Address. |
| Primary IP Port | The main IP port used to connect to the HPS-Dallas network (five characters maximum). Verify with the HPS-Dallas network the value to key as the Primary IP Port. |
| Secondary IP Address | The first alternate IP address used to connect to the HPS-Dallas network if the Primary IP Address is unavailable. The format of this field is four sets of numbers in the range of 1 through 255, each separated by a decimal point, for example 255.255.255.255. Verify with the HPS-Dallas network the value to key as the Secondary IP Address. |
| Secondary IP Port | The first alternate IP port used to connect to the HPS-Dallas network (five characters maximum). Verify with the HPS-Dallas network the value to key as the Secondary IP Port. |
| Tertiary IP Address | The second alternate IP address used to connect to the HPS-Dallas network for transaction processing if the Primary IP Address is unavailable. The format of this field is four sets of numbers in the range of 1 through 255, each separated by a decimal point, for example 255.255.255.255. The HPS-Dallas network supplies the Tertiary IP Address. |
| Tertiary IP Port | The second alternate IP port used to connect to the HPS-Dallas network if the Primary IP Address is unavailable (five characters maximum). Verify with the HPS-Dallas network the value to key as the Tertiary IP Port. |

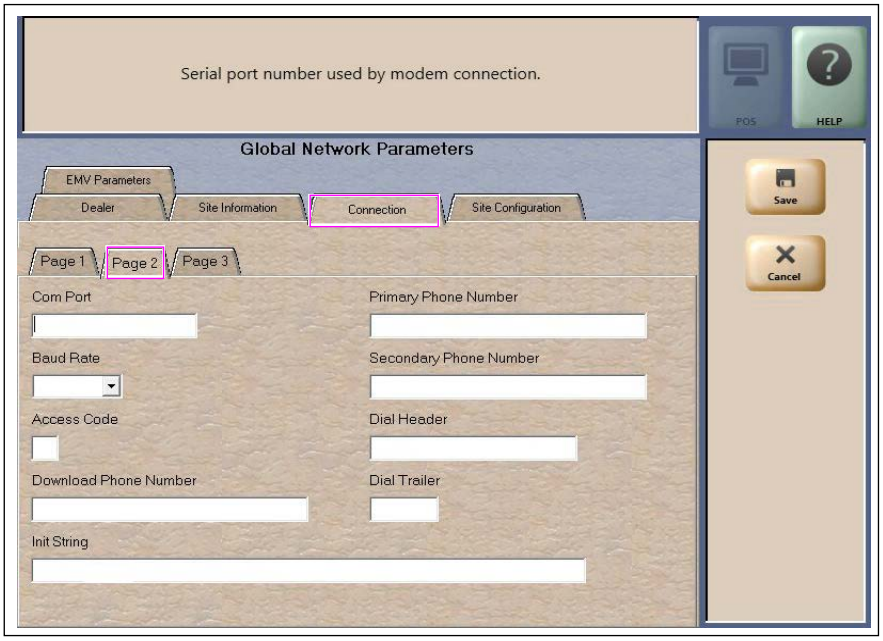
**i** Obtain the IP addresses from the HPS-Dallas or EchoSat℠ Help Desk, depending upon the kind of Earth Station used at the site (refer to the following table).

| Connection Type | Procedure |
|---|---|
| EchoSat℠ | Call the EchoSat Help Desk at 1-800-393-3246. |
| Hughes® | Call the HPS-Dallas Help Desk at 1-800-767-5258. |

**ii** Ensure that the site's router allows communication with the IP addresses and ports obtained in step i. At sites using an Acumera Secure Zone Router (SZR), call 1-800-743-7501 (select option **3** and then option **1**). Otherwise, contact the site's MNSP.

**b** The **Page 2** tab contains configuration fields for a Dial connection, which is no longer valid at Marathon sites. Continue to step c on page 17.

**Figure 8: Connection - Page 2 Tab**



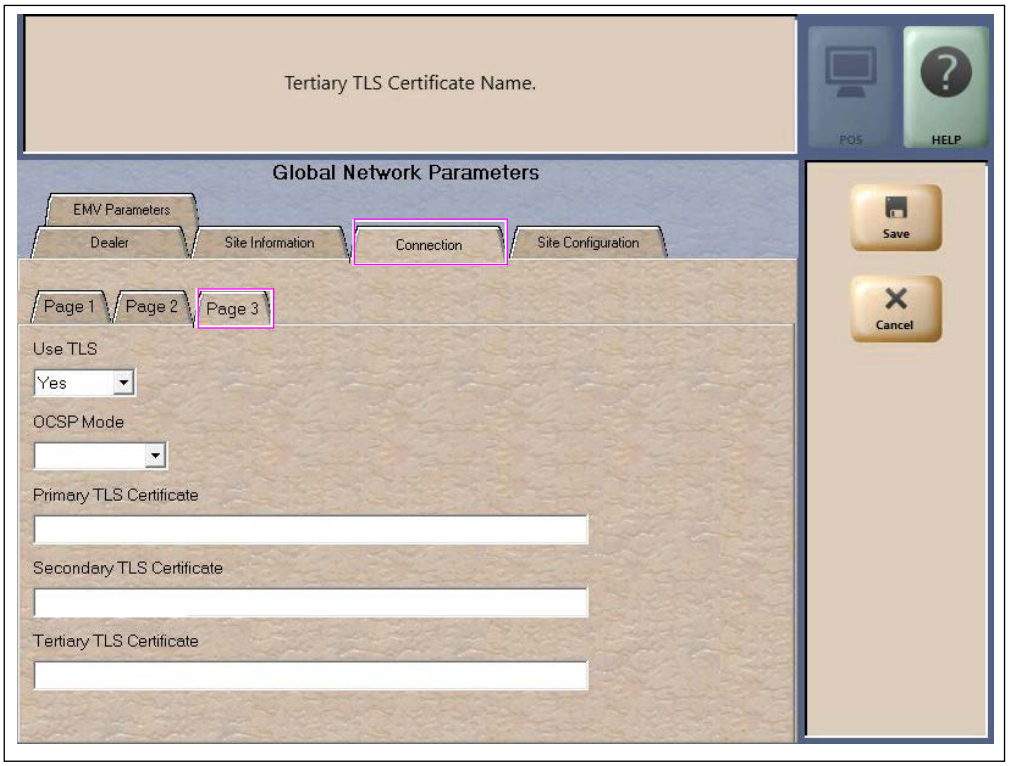
## Fields on the Connection - Page 2 Tab (for Dial Connections)

| Field | Description |
|---|---|
| COM Port | The COM port to which the modem is connected on the EDH. Default is 0. |
| Baud Rate | Dial baud rate used by the modem;<br>Options are 300, 1200, 2400, 4800, 9600, 14400, 19200, 38400, 56000, 57600, 115200, 128000, and 256000.<br>Default rate is 1200. |
| Access Code | Numbers that must be dialed in order to reach an outside phone line for the modem (that is, if you must dial a “9” to reach an outside line) |
| Download Phone Number | The main phone number used to dial the HPS-Dallas network for initial PDL processing (maximum 20 digits). May be the same as the Primary Phone. |
| Init String | The 40-character initialization string sent to the modem each time a link is established.<br>Default is AT&F0V0E0&K0&Q6%CX4S37=5&Z0.<br>• MultiTech® 009: use default value<br>• MultiTech 007: AT&F+A8E=,,,0VE&K&Q6%CX4+MS=1 |
| Primary Phone Number | The main phone number used to dial the HPS-Dallas network for transaction processing (maximum 20 digits). |
| Secondary Phone Number | The alternate phone number used to dial the HPS-Dallas network for transaction processing if the Primary Phone number is busy or not responding (maximum 20 digits). |
| Dial Header | The dial command to the modem, including tone generation. Default is.<br>• MultiTech 009: ATS7=15S10=2S11=50S25=0&W0<br>• MultiTech 007: use default value |
| Dial Trailer | Up to five characters are added to the end of the dial string. Defaults to blank. Enter # if the site’s modem requires it. |

*Note: Dial connections are no longer valid for Marathon stores.*

**c** Select the **Page 3** tab to complete TLS programming.

**Figure 9: Connection - Page 3 Tab (for TLS Connections)**



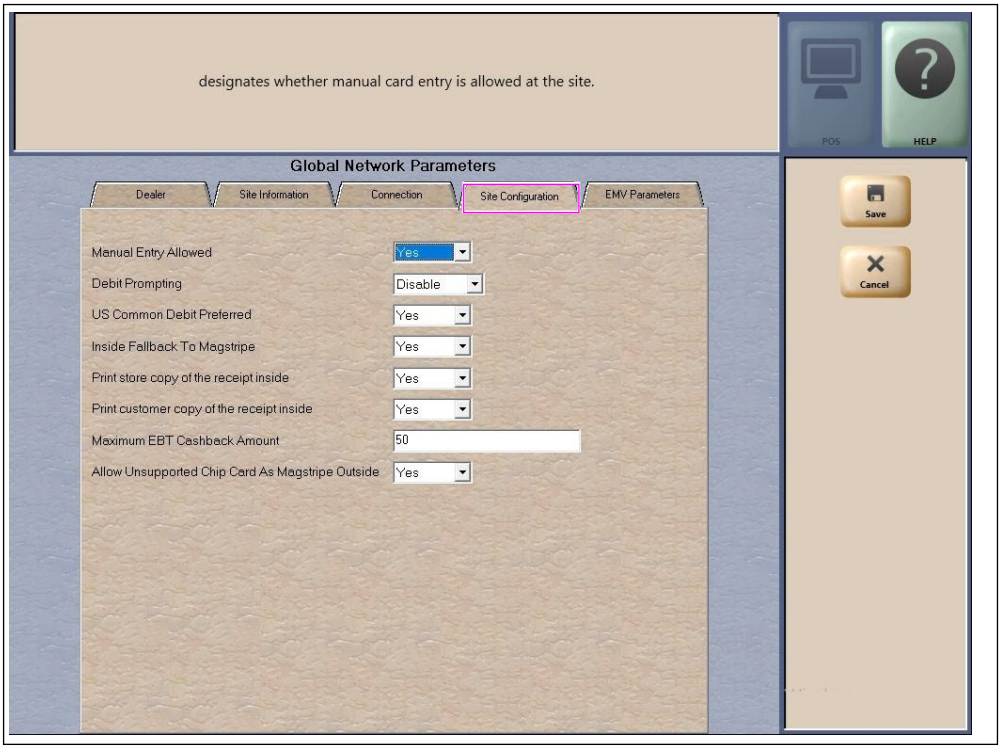

*Note: Contact the Marathon Help Desk at 1-800-378-1204 for the appropriate TLS programming.*

## Fields on the Connection - Page 3 Tab

| Field | Description |
|---|---|
| Use TLS | This field is a drop-down with YES/NO as options. Defaults to NO and is editable. |
| OCSP Mode | Options are None, Lenient, or Strict. Defaults to None. |
| Primary TLS Certificate | TLS certificate name used to validate TLS. |
| Secondary TLS Certificate | TLS certificate name used to validate TLS if the primary TLS certificate fails. |
| Tertiary TLS Certificate | TLS certificate name used to validate TLS if the primary and secondary TLS certificates fail. |

**5** Select the **Site Configuration** tab.

**Figure 10: Site Configuration Tab**




The following table provides information regarding completion of the fields on the **Site Configuration** tab:

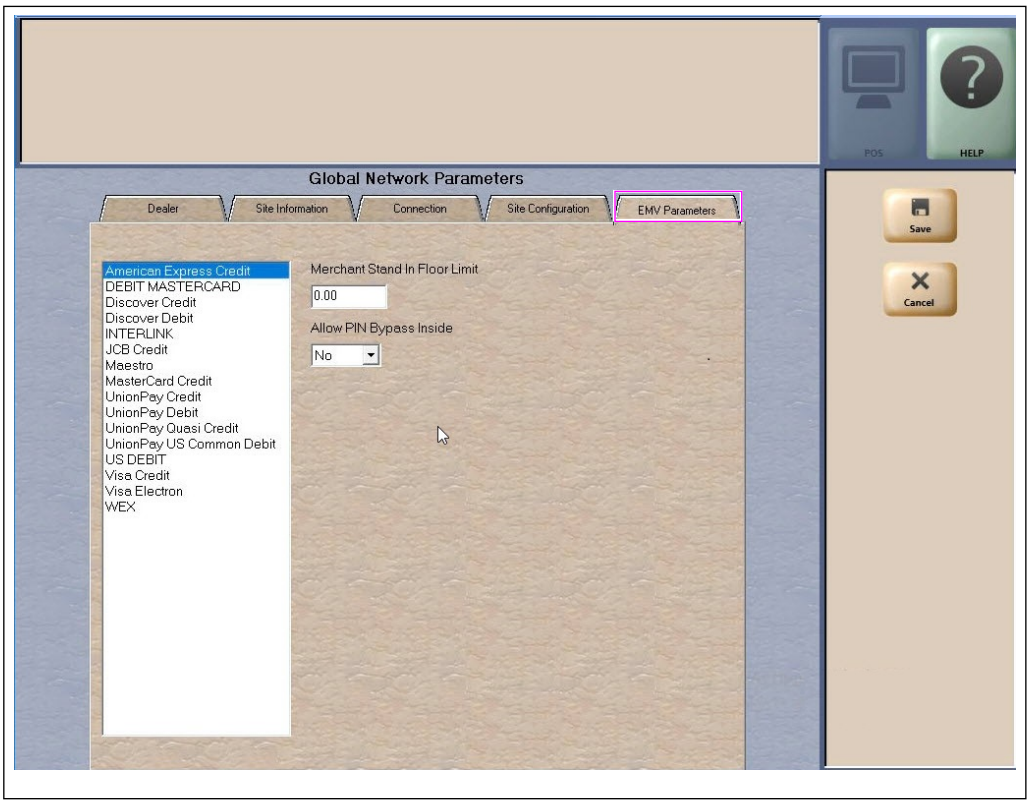
## Fields on the Site Configuration Tab

| Field | Description |
|---|---|
| Manual Entry Allowed | If set to Yes, manual entry of credit card transactions is allowed.<br>Manual entry should be set to “No” by default, unless specified by the dealer. |
| Debit Prompting | If set to Enable, Passport prompts the customer to choose credit or debit for dual use cards configured as debit capable in Card Information programming.<br><br>If set to Disable, Passport overrides all settings in Card Information programming and accepts dual use cards only as credit. |
| US Common Debit Preferred | If set to Yes, when the customer presents an EMV card that contains both US Common and International Debit AID, Passport displays or uses the US Common Debit AID.<br><br>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.<br>If the card contains only one debit AID, Passport displays or uses it without regard to the setting for this field. |
| Inside Fallback to Magstripe | 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.<br><br>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 HPS-Dallas network for the card type to determine whether to prompt the customer to remove the card from the chip reader and swipe it. |

| Field | Description |
|---|---|
| Print store copy of the receipt inside | If set to Yes, the merchant copy of the receipt prints automatically for all inside HPS-Dallas network transactions. This may be especially important for stores that enable electronic signature capture at the PIN Pad. The customer signature prints as part of the receipt. |
| Print customer copy of the receipt inside | If set to Yes, the customer copy of the receipt prints automatically for all inside HPS-Dallas network transactions. This may be especially important for stores that enable electronic signature capture at the PIN Pad. The customer signature prints as part of the receipt. |
| Maximum EBT Cashback Amount | Maximum dollar amount that can be returned as cash in an EBT transaction. |
| Allow Unsupported Chip Card As Magstripe Outside | If set to **Yes** and an EMV card which has an unsupported AID is inserted at the CRIND, the customer is prompted to remove the card. The magstripe is read as the card is being removed, and the sale is processed as a magstripe transaction. If set to **No**, an error message is displayed at the CRIND and on the cashier workstation when the unsupported chip card is inserted at the CRIND. The default setting is **Yes**. |

**6** Select the **EMV Parameters** tab.

**Figure 11: EMV Parameters Tab**




The fields on this tab are used to set options for using EMV cards. To change the settings for an EMV card AID, select the AID from the listing on the left and program the values in the fields to the right.

### Fields on the EMV Parameters Tab

| Field | Description |
|---|---|
| Merchant Stand In Floor Limit | Maximum transaction dollar amount for this EMV card AID the merchant will accept locally to store and forward when the HPS-Dallas network is offline. Defaults to $0.00. This field is not editable for any debit AID.<br>*Note: $0.00 means Passport relies on the EMV chip card for authorization when the HPS-Dallas network is not communicating. If the merchant configures an amount other than $0.00 for this field, Passport may approve the transaction based on chip card validation. The network may decline the transaction when communication resumes. The merchant is responsible for the charge back if the transaction is locally approved and then the network declines.* |
| Allow PIN Bypass Inside | If set to Yes, and the EMV application requires PIN entry, Passport prompts for PIN, but allows the customer to press the **ENTER** key on the PIN Pad without first entering digits for a PIN.<br><br>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.<br>*Note: Some debit AIDs set this field to Yes by default and the merchant cannot change this setting.* |

**7** After completing all the necessary programming for Global Network Parameters, select **Save** to save all programming and return to the Network menu.

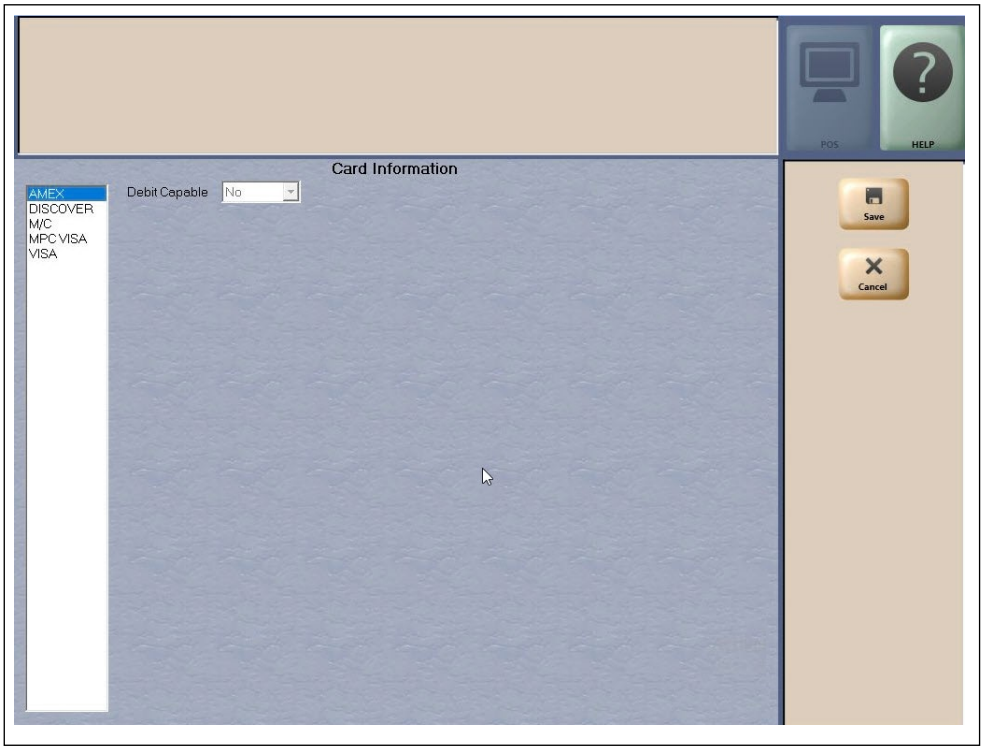
# Programming Network Card Configuration

The HPS-Dallas Marathon PDL controls most card acceptance parameters for payment cards. Review the Network Configuration Report for information on card acceptance parameters. Passport allows the merchant or store manager to configure each dual use card accepted at the store as debit capable in the **Card Info Editor** screen.

To configure debit capability for dual use cards, proceed as follows:

1 From the MWS main menu, select **Set Up** > **Network** > **Marathon** > **Card Info Editor**. The **Card Information** screen opens.

**Figure 12: Card Information**




2 Select a dual use card type from the list on the left to view or change the Debit Capable setting for that card type. If the Debit Capable parameter for a card type is set to **Yes**, when the customer uses the card type Passport prompts the customer to select whether to use the card as credit or debit.

*Note: If the Debit Prompting field on the **MWS** > **Set Up** > **Network** > **Marathon** > **Global Info Editor** > **Site Configuration** tab is set to Disable, the Passport system overrides all settings in Card Information and recognizes dual use cards as credit.*

3 After completing updates to the **Card Information** screen, select **Save** to save changes and exit from **Card Information**.

# Requesting a PDL Download

A PDL Download is a transfer of data from the HPS-Dallas network to Passport. A valid PDL contains card configuration information and is required for operation. You must request a PDL during system installation. Passport cannot process network transactions until it successfully receives a PDL from the network. The HPS-Dallas network can initiate a PDL Download by sending a message to Passport. Passport automatically requests a PDL when the HPS-Dallas network indicates a new PDL is ready.

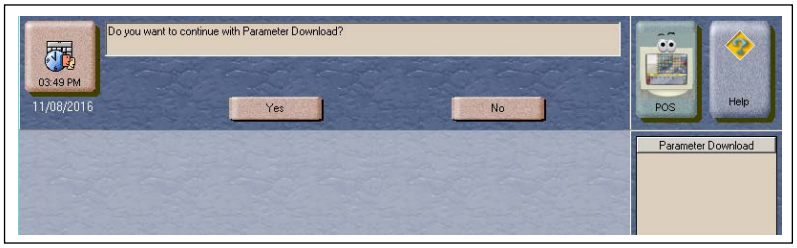
| IMPORTANT INFORMATION |
| --- |
| When upgrading software, call HPS-Dallas Help Desk (1-800-533-3421) to inform them that you need a new PDL. Then request a PDL Download through the MWS. |

To request a PDL download, proceed as follows:

1 From the MWS main menu, select **Set Up > Network > Marathon > PDL Download**.

2 The Passport system prompts: “Do you want to continue with Parameter Download?”

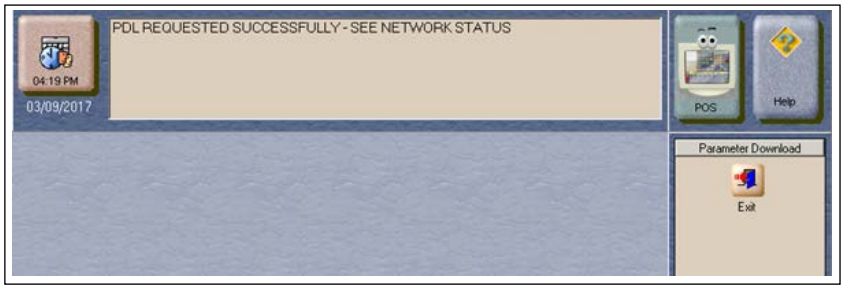
**Figure 13: PDL Download Screen**




a If you select **No**, the system returns to the Network Menu screen.

b If you select **Yes**, the system requests a download from the HPS-Dallas network. Passport provides status of the PDL Download request on the MWS screen.

**Figure 14: Successful PDL Download Request**




3 When Passport receives the PDL, it stores the file until the next Store Close. For new installations, in which Passport requests an initial PDL, Passport applies the PDL immediately.

*Note: To review the PDL information sent from the network to Passport, view or print the Network Configuration Report.*

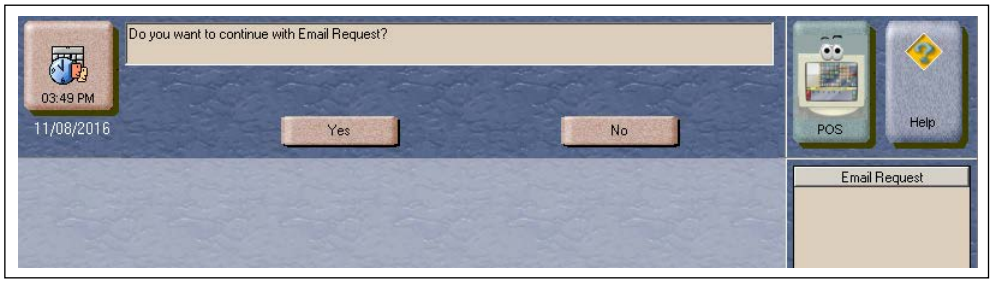
# Requesting Email

The network can communicate with store personnel by transmitting email messages. To access email messages, proceed as follows:

1 From the MWS main menu, select **Set Up** > **Network** > **Marathon** > **Email Request**.

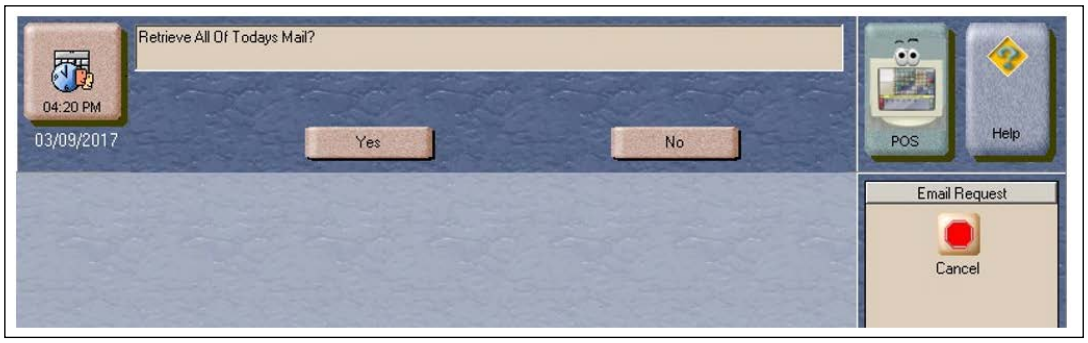
2 The Passport system prompts: “Do you want to continue with Email Request?”

**Figure 15: Email Request Prompt**




3 Select **Yes** to submit the request. Passport prompts: “Retrieve All Of Todays Mail?”

**Figure 16: All Mail Prompt**




4 Select **Yes** to retrieve all of today’s mail. Select **No** to retrieve only the unread mail.

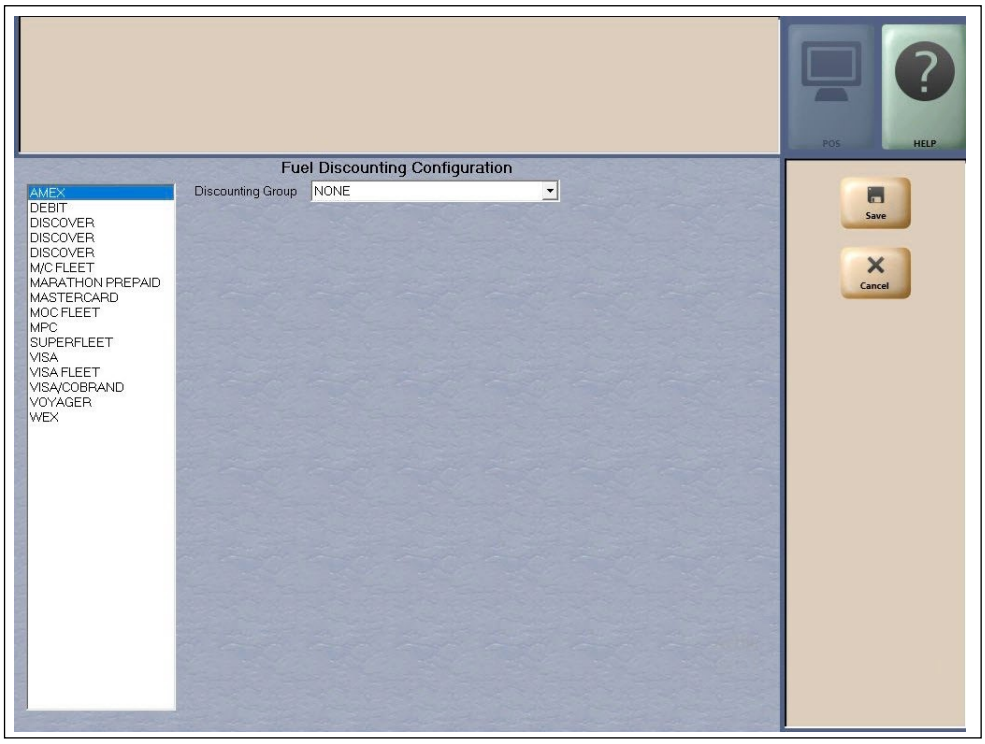
# Fuel Discount Configuration

To configure fuel discounts by card type, proceed as follows:

1. From the MWS main menu, select **Fuel > Fuel Discount Maintenance**. On the **Fuel Discount Groups** tab, configure PPU discounts to be applied to fuel grades available at the store.

2. From the MWS main menu, select **Set Up > Network > Marathon > Fuel Discount Configuration**. The Fuel Discounting Configuration screen opens.

**Figure 17: Fuel Discounting Configuration Screen**




3. Select the desired card type in the left pane. From the drop-down list, select the **Discounting Group** to be applied to that card type.

4. Select **Save** to save your changes.

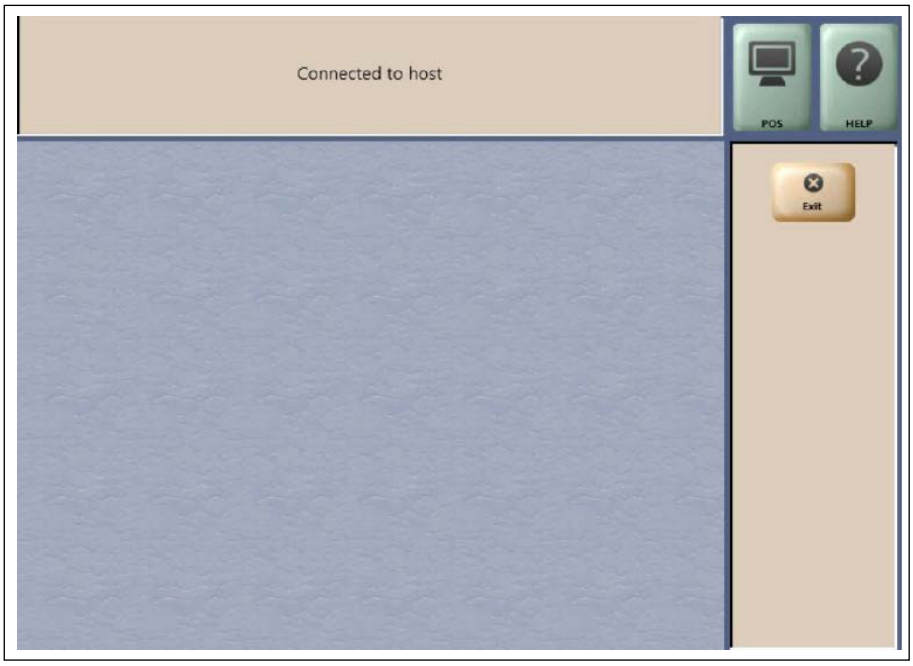
# Comm Test

The Comm Test feature allows a site to validate that the HPS-Dallas network is online and communicating with the Passport system. To execute a Comm Test, proceed as follows:

1 From the MWS main menu, select **Set Up > Network > Marathon > Comm Test**.

If the Passport is online with the HPS-Dallas network, **Connected to Host** message is displayed on the screen.

**Figure 18: Connected to Host**



# 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 19: Network Journal Report Screen**

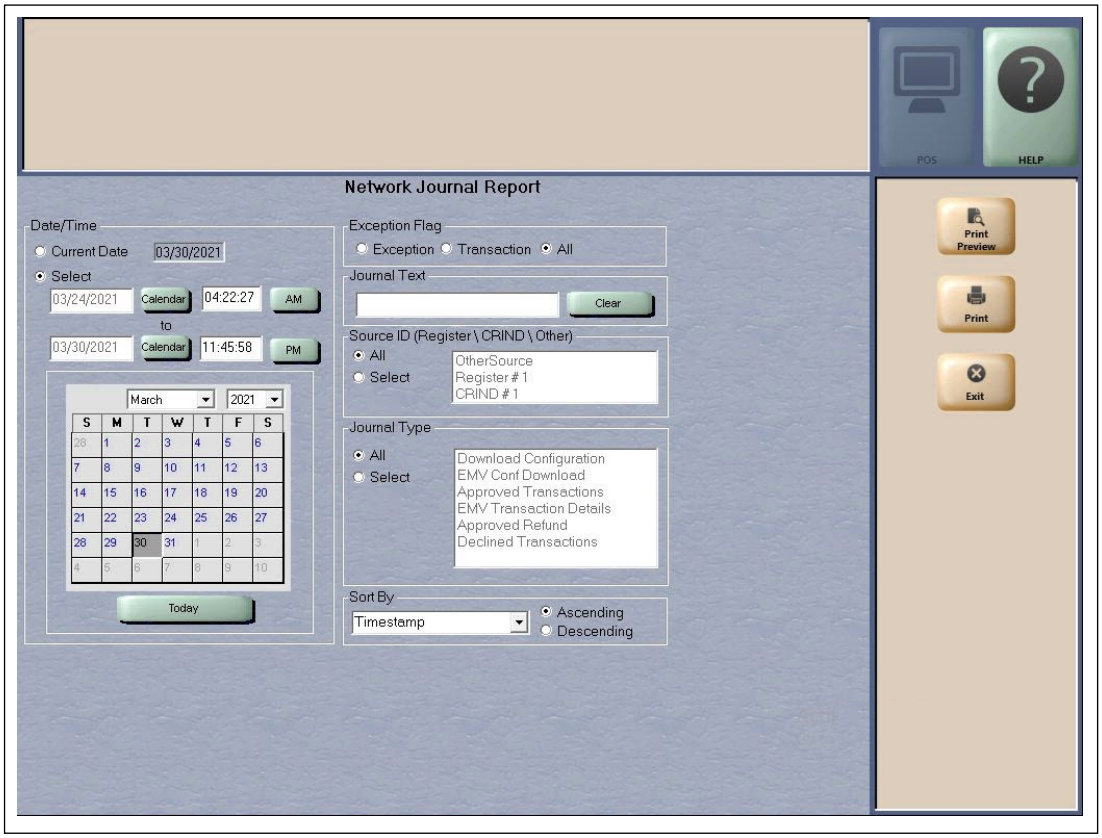


**Figure 20: Network Journal Report Sample**

# Network Journal Report

**Store Name**

STORE # 299

OPERATOR NAME Area Manager
OPERATOR ID 91
SOFTWARE VERSION 11.02.24.01D REPORT PRINTED 02/16/2017 8:54:39AM
MARATHON

| | |
|---|---|
| **DATE:** | 01/14/2017 6:50AM TO 02/16/2017 5:12PM |
| **SOURCE:** | All |
| **JOURNAL TYPE:** | All |
| **EXCEPTION:** | All |
| **SEARCH STRING:** | |
| **SORT BY:** | Time |

| TIME | SOURCE | TYPE | EXC | NETWORK | JOURNAL TEXT |
|---|---|---|---|---|---|
| 2017/02/13 07:42:56 | Other | Network Download | No | HPS Dallas | Feb 13 2017 07:42:08<br>PDL Successful |
| 2017/02/13 07:46:50 | Other | Financial Transactions | No | HPS Dallas | **** Console 1****** 7:45:50 *********<br>2C******* M/C *******\|1C<br>INV # 074550 2/13/17<br>ACCT # XXXX XXXX XXXX 0028<br>NON-FUEL ITEMS 6.32<br>TAX TOTAL 0.07<br>REFERENCE #180020213170745<br>AUTH #00 APRVL #4L2HI2 TOTAL $ 6.39 |
| 2017/02/13 08:19:46 | Other | Period Close | No | Auxiliary Network | 02/13/17 08:18:59 - Day [16] Closed Successfully |
| 2017/02/13 08:22:47 | Other | Financial Transactions | No | HPS Dallas | **** Console 1****** 8:21:47 *********<br>2C******* VISA *******\|1C<br>INV # 082147 2/13/17<br>ACCT # XXXX XXXX XXXX 0012<br>NON-FUEL ITEMS 7.09<br>TAX TOTAL 0.15<br>REFERENCE #190010213170821<br>AUTH #00 APRVL #08G0Z4 TOTAL $ 7.24 |

# Network Reports

Network reports show data on transactions transmitted to the HPS-Dallas network. Some network reports provide information on the status of transactions while others list total amounts for transmitted transactions. Each report prints with a heading that includes the name of the report, the date, and time the report was printed.

The following network reports are available:

| Report Name | Shift Close | Store Close | Current | Secure |
|---|---|---|---|---|
| Batch Detail by Day Report | | ✓ | | ✓ |
| Batch Detail Report | ✓ | | | ✓ |
| Batch Summary Report* | | ✓ | | |
| Card Conflict Report | | ✓ | | |
| Electronic Mail Report | | ✓ | | |
| EMV Chip Fallback Report | | ✓ | | |
| EMV Configuration Report | | | ✓ | |
| Gift Card Detail Report | | ✓ | | |
| Network Configuration Report | | | ✓ | |
| Network Credit Refund Report | | ✓ | | ✓ |
| Network Day Report* | | ✓ | | ✓ |
| Network Manual Entries Report | | ✓ | | ✓ |
| Network POS Events Report | | ✓ | | |
| Network Shift Report* | ✓ | | | |
| Non POS Report | | ✓ | | |
| POS Host Refusal Minor Report | | ✓ | | ✓ |
| POS Transaction Statistics Report | | ✓ | | |
| Site Level Card Based Fuel Discounts Report | | | ✓ | |

**This report should be printed on each Store Close or Batch Close and read closely.*

## IMPORTANT INFORMATION

Secure reports may contain sensitive customer data, such as card account number and expiration date. These reports are password protected and available to print on demand only. For more information on secure reports, refer to *MDE-5545 Passport EDH (Heartland-Dallas) V11.24.01* Implementation Guide for PA-DSS V3.2.*

# Batch Detail by Day Report

The Batch Detail by Day Report is available at Day Close and contains all detail necessary to reconstruct a transaction for the day. This report also contains a breakdown of all prepaid card activations and recharges. Below is a sample of the non-secure version of the Batch Detail Report, which prints the account numbers masked except for the last four digits. A secure version prints the account numbers unmasked.

**Figure 21: Batch Detail by Day Report**

| | | | | | | |
|---|---|---|---|---|---|---|
| 9S000040204 | 00 | 00561Z | $25.00 | CONS1-68 | | |
| 150707 | 5/30/17 | XXXX XXXX XXXX 3727 | | + M/C | | 12/25 |
| 9S000040220 | 00 | 00561Z | $20.00 | CONS1-69 | | |
| 151007 | 5/30/17 | XXXX XXXX XXXX 3743 | | M/C | | 12/25 |
| 9S000040238 | 00 | 00561Z | $10.00 | CONS1-70 | | |
| 151156 | 5/30/17 | XXXX XXXX XXXX 3743 | | + M/C | | 12/25 |
| 9S000040246 | 00 | 00561Z | $5.00 | CONS1-71 | | |
| 065239 | 6/2/17 | XXXX XXXX XXXX 0521 | | DISCOVER | | 12/17 |
| 97000040259 | 00 | 006430 | $36.00 | CONS1-72 | | |

+ indicates Repeated Card Use * indicates Manual Entry
() indicates negative total or credit memo **V** indicates Voice Authorization

**Batch Totals**

| Card Category Type | $Amount | Count |
|---|---|---|
| CREDIT | $442.02 | 23 |
| CREDIT REFUND | ($10.00) | 1 |
| | $432.02 | 24 |

| Card Type | $Amount | Count |
|---|---|---|
| DISCOVER | $56.00 | 2 |
| M/C | $376.02 | 22 |
| | $432.02 | 24 |

**Prepaid Card Activations/Recharges**

| Date / Time | AccountNumber | ApprovalCode | STAN | TransType | Amount |
|---|---|---|---|---|---|

Total Activations

# Batch Detail Report

The Batch Detail report is available at Shift Close and contains all detail necessary to reconstruct a transaction for the shift. This report also contains a breakdown of all prepaid card activations and recharges. Below is a sample of the non-secure version of the Batch Detail Report, which prints the account numbers masked except for the last four digits. A secure version prints the account numbers unmasked.

**Figure 22: Batch Detail Report**

**Batch Detail Report**
Dealer Number: 00111222333 Terminal Id: 1
Batch # 17

| Invoice Reference # | Date Auth Code | Account Number Approval | Code Sales Amt | Card Type Receipt # | Exp. Date | Odometer VehicleNumber |
|---|---|---|---|---|---|---|
| 130742 | 1/26/17 | XXXX XXXX XXXX 9120 | | DISCOVER | 12/20 | |
| 97000170015 | 00 | EKB9IE | $6.13 | CONS1-268 | | |
| 130932 | 1/26/17 | XXXX XXXX XXXX 9120 | | + DISCOVER | 12/20 | |
| 97000170023 | 00 | M8690B | $4.50 | CONS1-270 | | |

+ indicates Repeated Card Use * indicates Manual Entry
() indicates negative total or credit memo **V** indicates Voice Authorization

**Batch Totals**

| Card Category Type | $Amount | Count |
|---|---|---|
| CREDIT | $10.63 | 2 |
| | $10.63 | 2 |

| Card Type | $Amount | Count |
|---|---|---|
| DISCOVER | $10.63 | 2 |
| | $10.63 | 2 |

**Prepaid Card Activations/Recharges**

| Date / Time | AccountNumber | ApprovalCode | STAN | Trans Type | Amount |
|---|---|---|---|---|---|
| 1/26/17 16:26:25 | XXXXXXXXXXXXXXXX4488 | 5MH6U2 | 701449 | Activate | $25.00 |
| | | | | | $25.00 |

Total Activations/Recharges for Batch #34

## Batch Summary Report

The Batch Summary Report prints at Store Close to provide totals for the current batch.

**Figure 23: Batch Summary Report**

**Batch Summary Report**
Network Day# 15 From:01/23/17 11:32 to: 02/13/17 06:49
Dealer Number: 00111222333 Terminal Id: 1

| Batch Number | Closing Date | Batch Amount Total | Batch Status |
|---|---|---|---|
| 13 | 01-23-17 | $4.91 | RECEIVED |
| 14 | 01-24-17 | $22.06 | RECEIVED |
| 15 | 01-26-17 | $19.45 | OUT-OF-BALANCE BY $ -19.45 |
| 16 | 01-26-17 | $7.82 | OUT-OF-BALANCE BY $ -7.82 |
| 17 | 02-13-17 | $29.02 | OUT-OF-BALANCE BY $ -29.02 |
| End of Day Total: | | $78.35 | |

+ Indicated Batch(es) not part of Current End Of Day Total

*Notes: 1) When the fallback file is more than 50% full, a warning message, "WARNING: There are 240 transactions in fallback which is 60% full" is displayed at the end of the Batch Summary Report.*
*2) When the message, "FINAL OUT-OF-BALANCE" is displayed, call the HPS-Dallas Help Desk for procedures to process the batch manually.*

## Card Conflict Report

Card conflicts can occur when a card configured for acceptance in Auxiliary Network Card Configuration processes through the HPS-Dallas network, or a card configured for acceptance by the HPS-Dallas network processes through the Auxiliary Network. This report provides information on transactions affected by card conflicts.

**Figure 24: Card Conflict Report**

**Card Conflict Report** - Network Shift from 1/23/2017 11:32:30AM to 2/13/2017 6:49:19AM

| Issuer Name - Processing Network | Issuer Name - Configured Network | Conflict Instances (current period) |
|---|---|---|
| NO DATA TO REPORT | | |

## Electronic Mail Report

The Electronic Mail Report records all electronic mail messages received from HPS-Dallas during the Day period.

**Figure 25: Electronic Mail Report**

```
Electronic Mail Report
 Dealer Number: 00111222333 Terminal Id: 1
 Network Day# 15                                  From:01/23/17 11:32 to:02/13/17 06:49

 01/23/2017          DEALER # 00111222333        11:49:52
        *170123*02\1699\0001101\16\1899\0004515\
        03\2199\0000904\\

 01/23/2017          DEALER # 00111222333        11:49:53
        *170123*02\1699\0000000\16\1899\0000000\
        03\2199\0000000\\

 01/23/2017          DEALER # 00111222333        11:49:53
        *170123*02\1699\0000000\16\1899\0000000\
        03\2199\0000000\\

 01/24/2017          DEALER # 00111222333        12:05:05
        *170123*02\1699\0000409\16\1899\0000000\
        03\2199\0000000\\
```

## EMV Chip Fallback Report

The EMV Chip Fallback Report provides information on EMV transactions that occurred during a specific network day.

**Figure 26: EMV Chip Fallback Report**

```
EMV Chip Fallback Report

Network Day #15 From 01/23/2017 11:32:30AM to 02/13/2017 6:49:19AM

                    TOTAL EMV/CHIP CARD TRANSACTIONS: 100
FALLBACK                    TRANS                    % OF CHIP TRANS
  TOTAL                       10                          10%
```

# EMV Configuration Report

This report provides information regarding EMV processing parameters for each EMV card that Passport supports, along with the fields programmed in the **MWS** > **Set Up** > **Network** > **Marathon** > **Global Network Parameters** > **EMV Parameters** tab.

**Figure 27: EMV Configuration Report**

## EMV Configuration Report

Report created: 02/16/2017 07:32:14 AM

### Network Configuration Values

| | |
|---|---|
| US Common Debit Preferred: | True |
| Additional Terminal Capabilities: | F000F0A001 |
| Indoor EMV Fallback Allowed: | Yes |
| Outdoor EMV Fallback Allowed: | Yes |

### Terminal Configuration Values

| Terminal | EMV Version | Software Version |
|---|---|---|
| REGISTER 1 | 0467 | 1904 |

### Configuration Values

American Express Credit - Indoor
(AID: A00000002501)

| | | | |
|---|---|---|---|
| AID Activated: | 2 | Term Capability: | E0F8C8 |
| Term Country: | | Term Currency: | |
| Addl Capability: | | Merch Cat Code: | 5311 |
| TAC Default: | 0000000000 | TAC Denial: | 0000000000 |
| TAC Online: | 0000000000 | Partial Select: | True |
| Trans Curr Exp: | | Trans Cat Code: | R |
| App Ver Num Pri: | 0001 | PSPId: | 24 |
| Term Floor Lim: | 0 | Rand Sel Thresh: | 0 |
| Rand Sel Max%: | 0 | Rand Sel Target%: | 0 |
| AllowFallback: | True | AllowPINBypass: | False |

----- CONTACTLESS PARAMETERS -----

| | | | |
|---|---|---|---|
| Application Selection: | True | App Version Number: | 0001 |
| MSD App Version Number: | 0001 | App Country Code: | 0 |
| Transaction Types: | 8000 | Terminal Capabilities: | E0E8C8 |
| Terminal Floor Limit: | 0 | CVM Limit: | 10 |
| Transaction Limit: | 15 | TAC Denial: | 0000000000 |
| TAC Online: | C400000000 | TAC Default: | DC50840000 |

American Express Credit - Outdoor
(AID: A00000002501)

| | | | |
|---|---|---|---|
| AID Activated: | 2 | Term Capability: | 60D8C8 |
| Term Country: | | Term Currency: | |
| Addl Capability: | | Merch Cat Code: | 5311 |
| TAC Default: | 0000000000 | TAC Denial: | 0000000000 |
| TAC Online: | 0000000000 | Partial Select: | True |
| Trans Curr Exp: | | Trans Cat Code: | R |
| App Ver Num Pri: | 0001 | PSPId: | 24 |
| Term Floor Lim: | 0 | Rand Sel Thresh: | 0 |
| Rand Sel Max%: | 0 | Rand Sel Target%: | 0 |
| AllowFallback: | True | AllowPINBypass: | False |

----- CONTACTLESS PARAMETERS -----

| | | | |
|---|---|---|---|
| Application Selection: | True | App Version Number: | 0001 |
| MSD App Version Number: | 0001 | App Country Code: | 0 |
| Transaction Types: | 8000 | Terminal Capabilities: | E0E8C8 |
| Terminal Floor Limit: | 0 | CVM Limit: | 10 |
| Transaction Limit: | 15 | TAC Denial: | 0000000000 |
| TAC Online: | C400000000 | TAC Default: | DC50840000 |

# Gift Card Detail Report

This report provides information on gift card activations, issuances, and recharges, including count and amount totals.

**Figure 28: Gift Card Detail Report**

## Gift Card Detail Report

Dealer #: 00111222333 Terminal Id: 1
Report created: 02/16/2017 07:46:37 AM

Batch #: 17

ACTIVATIONS

| ACCOUNT # | | AMOUNT |
|---|---|---|
| XXXXXXXXXXXXXXXX4488 | | $ 25.00 |
| TOTAL ACTIVATED | 1 | $ 25.00 |

ISSUANCES

| ACCOUNT # | | AMOUNT |
|---|---|---|
| No Transactions registered. | | $ 0.00 |
| TOTAL ISSUANCES | 0 | $ 0.00 |

RECHARGES

| ACCOUNT # | | AMOUNT |
|---|---|---|
| No Transactions registered. | | $ 0.00 |
| TOTAL RECHARGES | 0 | $ 0.00 |

| | COUNT | AMOUNT |
|---|---|---|
| GRAND TOTAL | 1 | $ 25.00 |

# Network Configuration Report

The Network Configuration Report provides the current and pending, if applicable, settings and dealer information received from HPS-Dallas.

**Figure 29: Network Configuration Report**

## Network Configuration

Report created: 02/16/2017 07:48:00 AM

Dealer Number #: 00111222333
Terminal ID #: 1
Terminal Type #: NONE
Company ID #: 017
Heartland Version Number #: 08
Passport POS Version #: 11.02.24.01D
EDH Version #: 08.24.01.01D

### Current Network Values

**Prepaid card handling**

| | |
|---|---|
| MOC Prepaid Allowed | Yes |
| MOC Prepaid Preset | 100 |
| MOC Prepaid Activation/Recharge/Issue Minimum | 5 |
| MOC Prepaid Activation/Recharge/Issue Maximun | 500 |
| SVS Allowed | Yes |
| SVS Preset | 15 |
| SVS Activation/Recharge/Issue Minimum | 5 |
| SVS Activation/Recharge/Issue Maximun | 2000 |

**Debit handling**

| | |
|---|---|
| Debit Allowed | Yes |
| Debit Preset | 100 |
| Debit Cash Back Maximun | 50 |

**Receipts**

| | |
|---|---|
| Receipt Message Flag | True |
| Receipt Message #1 | YOU COULD HAVE SAVED UP TO %ws |
| Receipt Message #2 | BY USING A MARATHON VISA |
| Receipt Message #3 | YOU COULD HAVE SAVED UP TO %ws |
| Receipt Message #4 | BY USING A MARATHON VISA |

**Misc**

| | |
|---|---|
| Batch Size | 36 |
| Maximum Credit Sale Amount | 999 |
| Dial Type | T |
| Refund Days | 0 |
| Drop Tank Activations Allowed | Yes |

| Card | A | B | C | D | E | F | Referral # |
|---|---|---|---|---|---|---|---|
| AMEX | Yes | 100 | 100 | 0 | 25 | N | 18005282121 |
| DISCOVER (60112-9) | Yes | 1 | 100 | 0 | 25 | N | 18003471111 |
| DISCOVER | Yes | 1 | 100 | 0 | 25 | N | 18003471111 |
| DISCOVER (60110) | Yes | 1 | 100 | 0 | 25 | N | 18003471111 |
| DISCOVER | Yes | 1 | 100 | 0 | 25 | N | 18003471111 |
| DISCOVER (DINERS INT'L) | Yes | 1 | 100 | 0 | 25 | N | 18003471111 |
| M/C FLEET | Yes | 3 | 150 | 0 | 0 | N | 18003435792 |
| MASTERCARD | Yes | 1 | 100 | 0 | 25 | N | 18003435792 |
| VISA FLEET | Yes | 150 | 150 | 0 | 0 | N | 18003435792 |
| VISA/COBRAND | Yes | 1 | 100 | 0 | 25 | N | 18003435792 |
| MOC FLEET | Yes | 199 | 199 | 0 | 0 | N | 18008420071 |
| VOYAGER | Yes | 1 | 199 | 0 | 0 | N | 18009876589 |
| VISA | Yes | 1 | 100 | 0 | 25 | N | 18003435792 |
| VISA | Yes | 1 | 100 | 0 | 25 | N | 18003435792 |
| WEX | Yes | 199 | 199 | 0 | 0 | N | 18008420071 |
| FLEET ONE | Yes | 1 | 199 | 0 | 0 | N | 18008420071 |
| FUELMAN | Yes | 1 | 199 | 0 | 0 | N | 18001112222 |
| FLEETWIDE | Yes | 1 | 199 | 0 | 0 | N | 18001112222 |
| MPC | Yes | 100 | 100 | 0 | 25 | N | 12345678901 |
| SUPERFLEET | Yes | 199 | 199 | 0 | 0 | N | 18002220796 |

**No pending data to be applied**

A - Card accepted or not
B - Dollar amount to be used for an outside preauth
C - Maximum dollar limit to be dispensed at the pump per card approval
D - The maximum amount allowed for a transaction in fallback
E - Lowest transaction amount at which signature is required on the receipt
F - AVS prompting

# Network Credit Refund Report

The Network Credit Refund Report is available for each Day period and lists each credit refund transaction.

**Figure 30: Network Credit Refund Report**

**Network Credit Refund Report**
Dealer Number:00111222333 Terminal Id:1
Network Day# 15 From:03/29/17 05:08 to: 03/30/17 05:52

| Time | Date | Account Number | Card Type | Reference | Amount |
|---|---|---|---|---|---|
| 05:17:22 | 03/29 | XXXX XXXX XXXX 0029 | VISA | 97080010059 | $43.09 |
| 05:23:09 | 03/29 | XXXX XXXXXX X0000 | AMEX | 97080010197 | $75.00 |

# Network Day Report

The Network Day Report is available for each Day period and provides network totals for the specified Day period.

**Figure 31: Network Day Report**

**Network Day Report**
Dealer Number: 00111222333 Terminal Id:1
Network Day# 15 From:01/23/17 11:32 to: 02/13/17 06:49

| Time Shift closed | $ Amount | Count | Manual % | Manual Count |
|---|---|---|---|---|
| 06:49:19 | 78.35 | 29 | .0 | 0 |
| | 78.35 | 29 | 0.00 | 0 |
| End of Day Total | | | | |

| Category Card Type | $ Amount | Count | Manual % | Manual Count |
|---|---|---|---|---|
| CREDIT | 52.14 | 27 | 0.0 | 0 |
| | 52.14 | 27 | | 0 |
| End of Day Total | | | | |

| Card Type | $ Amount | Count | Manual % | Manual Count |
|---|---|---|---|---|
| DISCOVER | 40.03 | 24 | 0.00 | 0 |
| FLEETWIDE | 4.96 | 1 | 0.00 | 0 |
| FUELMN | 4.44 | 1 | 0.00 | 0 |
| FLEETONE | 2.71 | 1 | 0.00 | 0 |
| End Of Day Total | 52.14 | 27 | | 0 |

**Prepaid Card Activations/Recharges**

| Date | Time | Account Number | Approval Code | STAN | Trans Type | $ Amount |
|---|---|---|---|---|---|---|
| 01/26/2017 | 16:26:25 | XXXXXXXXXXXXXXXX4488 | 5MH6U2 | 701449 | Activate | 25.00 |
| | | | | | | $25.00 |

Total Activations/Recharges for Batch# 34

## Network Manual Entries Report

The Network Manual Entries Report is available for Day periods and lists all network transactions for which the cashier manually entered card information. The non-secure version prints the account number masked except for the last four digits.

**Figure 32: Network Manual Entries Report**

**Network Manual Entries Report**
Dealer Number:00111222333 Terminal Id:1
Network Day # 15 **From:** 01/23/17 01:32 **to:** 01/24/17 02:49

| Time | Date | Account Number | Card Type | Reference | Amount |
|---|---|---|---|---|---|
| 05:32:13 | 01/23 | XXXX XXXX XXXX 0088 | VISA | 91000130153 | $43.72 |

## Network POS Events

The POS Events Report provides a list of system events responses to significant POS processing events. This report documents the following events:

- Network Response Errors
- Hot Catch-up Start and End
- PDL Messages (Received, and so on)
- Out of Balance Batches
- Batch Removal
- Fallback File Full Conditions

**Figure 33: Network POS Events**

**Network POS Events**
Dealer Number: 00111222333 Terminal ID: 1

| EventDate | EventText |
|---|---|
| 02/16/17 08:11:30AM | **POS Site Configuration Message Succeeded** |
| 02/16/17 08:09:20AM | Response Error (Msg Seq Num 63) "68" - Dial - Node not communicating for an unknown reason. |
| 02/16/17 08:07:20AM | Response Error (Msg Seq Num 62) "68" - Dial - Node not communicating for an unknown reason. |

# Network Shift Report

The Network Shift Report is available for Shift periods and provides network transaction information for the shift.

**Figure 34: Network Shift Report**

**Network Shift Report**
Dealer Number: 00111222333 Terminal Id:1
Network Shift # 15 From:1/23/2017 11:32:30AM To:2/13/2017 6:49:19AM

| Batch Number | Time | Count | $ Amount |
|---|---|---|---|
| 14 | 12:04:58 | 16 | $22.06 |
| 15 | 03:00:00 | 9 | $19.45 |
| 16 | 13:06:16 | 1 | $7.82 |
| 17 | 06:28:30 | 3 | $29.02 |

| Card Category | Count | $ Amount |
|---|---|---|
| CREDIT | 27 | $52.14 |
| Shift Total | 27 | $52.14 |

| Card Type | Count | $ Amount |
|---|---|---|
| DISCOVER | 24 | $40.03 |
| FLEETWIDE | 1 | $4.96 |
| FUELMN | 1 | $4.44 |
| FLEETONE | 1 | $2.71 |
| Shift Total | 27 | $52.14 |

# POS Host Refusal Minor Report

The POS Host Refusal Minor Report is available for Shift periods and provides information on transactions refused by the HPS-Dallas network. Below is a sample of the non-secure version of the POS Host Refusal Minor which prints the account numbers masked except for the last four digits. A secure version prints the account numbers unmasked. This report includes transactions denied for the following reasons:

- Host refusal at any pay point (in-store or at the pump).
- Conditional approval at the CRIND.
- Conditional approval was granted at the POS, and the cashier elected to cancel the sale rather than continue (repeated card use not included).

**Figure 35: POS Host Refusal Minor Report**

**POS Host Refusal Minor Report**
Dealer Number: 00111222333 Terminal Id: 1
Network Day# 15 From:01/23/17 11:32 to 02/13/17 06:49

| Time | Date | Account Number | Card Type | Resp Code | Host Refusal Message |
|---|---|---|---|---|---|
| 10:02:34 | 01/26 | XXXXXXXXXXXXXXXX4488 | PREPAID | 30 | 30 - INACTIVE CARD |
| 10:03:15 | 01/26 | XXXXXXXXXXXXXXXX4488 | PREPAID | 40 | 40 - PLEASE ASK FOR |
| 13:08:03 | 01/26 | XXXXXXXXXXXXXXXX4488 | PREPAID | 30 | 30 - INACTIVE CARD |

## POS Transaction Statistics Report

This report provides summary count and percentage of network transactions, based on entry method, such as Manual, Swiped, MSD Contactless, EMV Contact, Swiped Fallback, Manual Fallback, and EMV Contactless.

**Figure 36: POS Transaction Statistics Report**

**POS Transaction Statistics Report**

Dealer Number: 00111222333
Network Day: 15
Open: 01/23/2017 11:32:30AM
Close: 02/13/2017 6:49:19AM

TOTAL TRANSACTIONS: 3

| ENTRY MODE | TRANSACTIONS | % OF TRANSACTIONS |
|---|---|---|
| Manual | 0 | 0 |
| Swiped | 3 | 100 |
| MSD contactless | 0 | 0 |
| EMV contact | 0 | 0 |
| Swiped fallback | 0 | 0 |
| Manual fallback | 0 | 0 |
| EMV contactless | 0 | 0 |

TERMINAL DETAIL EMV CARD READ FAILURES

No card read failures.

## Site Level Card Based Fuel Discounts

This report provides information on the fuel discounts by card type configured in **MWS** > **Set Up** > **Network** > **Marathon** > **Fuel Discount Configuration**. It lists each card type the network accepts, the Fuel Discount Group assigned to the card type, or NONE if the card type has no discount configured.

**Figure 37: Site Level Card Based Fuel Discounts Report**

**Site Level Card Based Fuel Discounts**

Report created: 02/16/2017 08:18:19 AM

| Card Record | Discount Group |
|---|---|
| American Express | NONE |
| Debit | NONE |
| Discover/Novus | NONE |
| Marathon Card | 5 CENTS OFF |
| Marathon Co-Brand | NONE |
| Marathon Fleet | NONE |
| Marathon Prepaid | NONE |
| MasterCard | NONE |
| MasterCard Fleet | NONE |
| MASTERCARD-DINERSINT | NONE |
| SSA SUPERFLEET | NONE |
| Visa | NONE |
| Visa Fleet | NONE |
| Voyager | NONE |
| Wright Express | NONE |

# CWS Network Functions

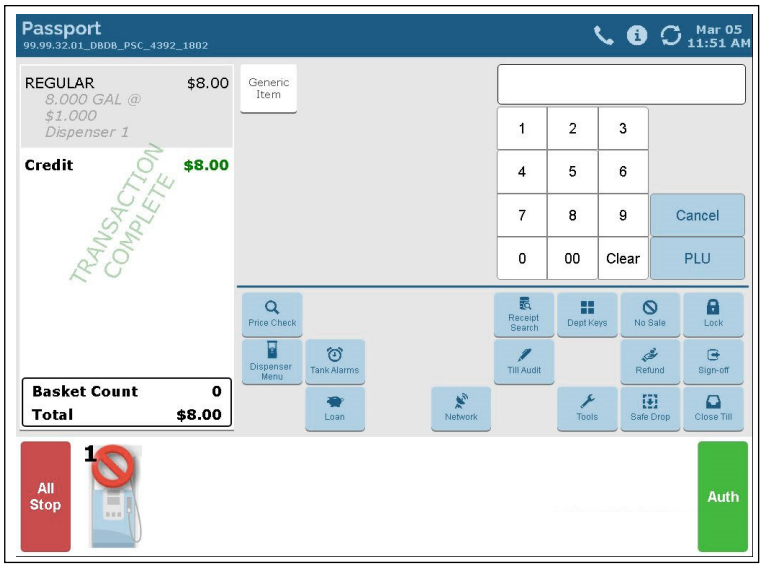
The Cashier Workstation (CWS) Network Functions screen contains the Network Status window and the Network Functions buttons. On this screen, you can view the Network Status and access the following tools:

- Batch Close
- Communication Test
- Card Balance Request
- Email Request

## Accessing Network Functions

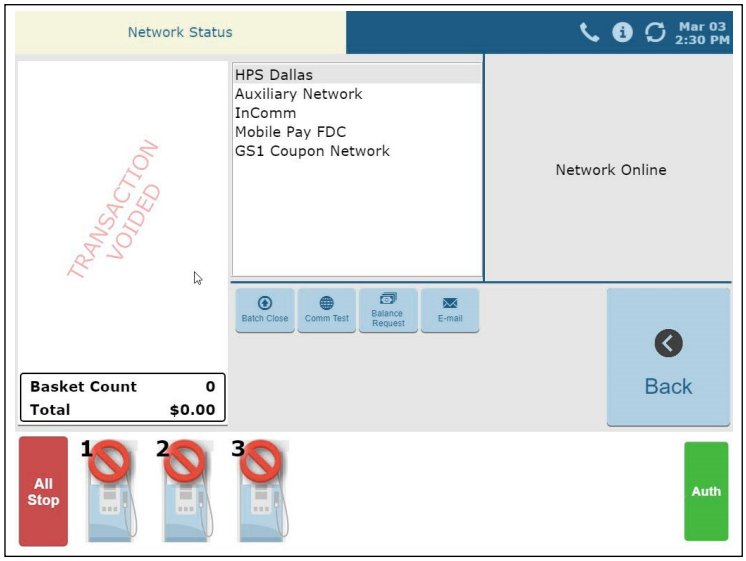
To access the Network Functions screen, select the Network button.

**Figure 38: Network Button**



The Network Status screen opens.

**Figure 39: CWS Network Status Screen**




## Checking the Network Status

The Network Status screen provides information on all networks connected to the Passport system. Select a network from the list in the middle pane to view its status in the right pane. 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 color of the Network button indicates the severity rating of the event:

| Color | Severity |
|---|---|
| Blue | Low |
| Yellow | Medium |
| Red | High |

If multiple events occurred, the color of the Network button indicates the highest severity rating of the events.

## Performing a Batch Close

A network batch close may occur automatically after a certain number of transactions. You may also perform a batch close whenever you are not in a sales transaction. On the Network Status screen, select **Batch Close**. The message "**Processing Batch Close. Please Wait.**" is displayed.

The Batch Close Report is available through MWS. The Batch Close Report prints at Shift close as part of the Shift Report if the manager has selected it as part of the Shift Close list of reports in **Period Maintenance**.

## Checking Card Balance

To find out how much money is available on a cash card or an EBT card, proceed as follows:

1. On the Network Functions screen, select **Balance Request**.

2. Swipe the card.
   - If Passport does not identify the card as a cash card, the cashier is prompted whether the card is an EBT Cash card. If the cashier responds with Yes, the card is handled as an EBT Cash card. Otherwise the card is handled as an EBT Food card.

3. The card balance is displayed and Passport prints a customer receipt with the balance amount.

## Receiving Email from CWS

Passport notifies you when it receives an email from the HPS-Dallas network. Passport saves all emails for 60 days.
*Note: You can receive electronic mail only; you cannot send one.*

1. On the Network Functions screen, select **Email**. The prompt, “Retrieve all of today's mail?” is displayed.

2. Select **Yes** to retrieve all the current day’s mail. Select **No** to retrieve only the unread mail. The mail prints on the receipt printer.

## Communication Test

Select **Comm Test** to validate that the HPS-Dallas network is online and communicating with the Passport system. A message will be displayed showing the status of this connection.

# EBT Food and EBT Cash Tenders

The HPS-Dallas Network supports processing EBT Food and EBT Cash. Please call your brand representative to engage HPS-Dallas for integrated EBT activation. If you do not belong to a branded network, contact your merchant services account manager to update EBT in their system. If you currently do not have an account manager assigned, please call the Toll-Free number on your merchant services statement for assistance and be sure to have your EBT/FNS number and merchant ID ready.

EBT Food and EBT Cash tenders have been added to Tender Maintenance with the status of “**Inactive**”. For stores that wish to process EBT tenders with Passport on the HPS-Dallas network, go to **MWS > Setup > Store > Tender Maintenance** and highlight the EBT Cash tender and select “**Activate**” and highlight the EBT Food tender and select “**Activate**”.

The tender options for EBT Cash and EBT Food have been preconfigured, with the exception of “**NACS Tender code**” and “**Allow safe drops**”. These may be configured as needed by the site. The tender group assigned to EBT Cash and EBT food should not be changed. Once the tender has a status of “**Active**” it is ready for use at the POS cashier workstation.

If the site had previously defined EBT tenders in an earlier version with the description EBT Food and EBT Cash, they have been renamed to have "**Non int**" appended to the front of the tender description. You can choose to deactivate those tenders and use the new EBT Tenders.

Inform Back Office partners of new EBT Cash and EBT Food tender configuration. After activating EBT Cash and EBT Food on Passport ensure your tender mapping with the back office is correct for reporting and tender restrictions. Go to **Reports > Backoffice Reports** and execute the Tender Code Report to view the Passport tender code and the NACS tender code.

## EBT Card Transactions

The EBT Food tender applies food stamp restrictions to the items in the transaction as well as forgives tax for the items that qualify for food stamps.

Passport allows EBT transactions inside only. EBT cards are not accepted outside at the dispenser. EBT Cash is accepted for all inside transactions including prepay fuel transactions. EBT Cash and EBT Food transactions do not require customer PIN entry.

Passport also allows cash back for EBT Cash based on programming in Network Site Configuration. The maximum amount of cash back allowed in a transaction is configurable in Global Network Parameters on the Site Configuration tab. If the customer requests cash back with EBT Cash tender, Passport does not allow split tender. The EBT Cash card must cover the entire amount of the transaction, including cash back.
If Passport receives partial approval for EBT Cash in which the customer requested cash back, the CWS prompts the cashier to perform a manual refund of the partially approved EBT Cash tender. The manual refund is necessary because of the PIN entry requirement on the sale transaction.

For split tender with EBT Food, the customer must present the EBT Food card as first payment.

## Balance Request

The cashier can use the Balance Request button that appears on the Network Status screen to obtain the remaining balance on cash cards as well as EBT cards. After the cashier swipes the card, if Passport cannot identify the card as a cash card, Passport prompts the cashier if the card is an EBT Cash card. If the cashier responds with Yes, Passport makes an EBT Cash card balance request; otherwise, Passport makes an EBT Food card balance request.

# Appendix A: Network Events Messages

The following table lists the network event messages:

| Message | Priority | Meaning |
|---|---|---|
| Network Connection Offline | N/A | A previous message expired and the site is waiting for confirmation that the Passport system is connected to the HPS-Dallas network. The message will clear when the network connection is confirmed or re-established. |
| Unread Mail Pending | Low | Mail has been received and is waiting to be printed. The message will clear when the mail is printed. |
| Pending PDL Received | Medium | A new PDL has been received. Perform a Day Close to update the PDL. The message will then clear. |
| PDL Error - Call Help Desk | Medium | The system has attempted to request a PDL from the HPS-Dallas network, but has failed. Check the network connection, then call the HPS-Dallas Help Desk and ask that the PDL be resent. The message will clear when the PDL is successfully downloaded. |
| 70-70-79 Data Error - Call Help Desk | Medium | A data collect error has occurred. Call the HPS-Dallas Help Desk for help. |
| Fallback File Warning - Call Help Desk | Medium | The fallback file has 200 or more transactions in it. Check the network connection and call the HPS-Dallas Help Desk for help in clearing transactions. When the network connection is established and the fallback file has fewer than 200 transactions in it, the message will clear. |
| Fallback File Full - Call Help Desk | High | The fallback file is full. Check the network connection and call the HPS-Dallas Help Desk for help in clearing transactions. When the file is no longer full, the message will clear. |

# Appendix B: Mobile Payment Configuration

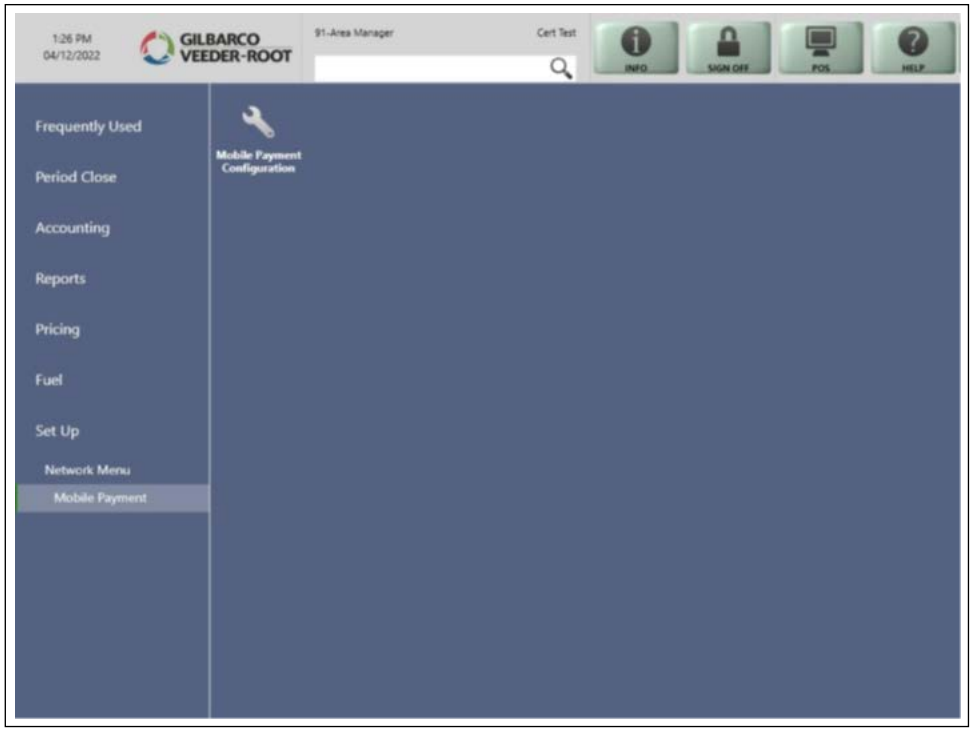
The following mobile payment configuration settings are to support Marathon Rewards Mobile Payment application functionality (ex. fuel prices and descriptions in the app). The Passport Mobile Payment feature bundle needs to be enabled at the site and the site connected to the mobile payment host; however, Mobile Payment is currently unavailable.

## Network Menu

To configure network menu, proceed as follows:

1 Go to **Set Up > Network Menu > Mobile Payment > Mobile Payment Configuration**.

**Figure 40: Network Menu**

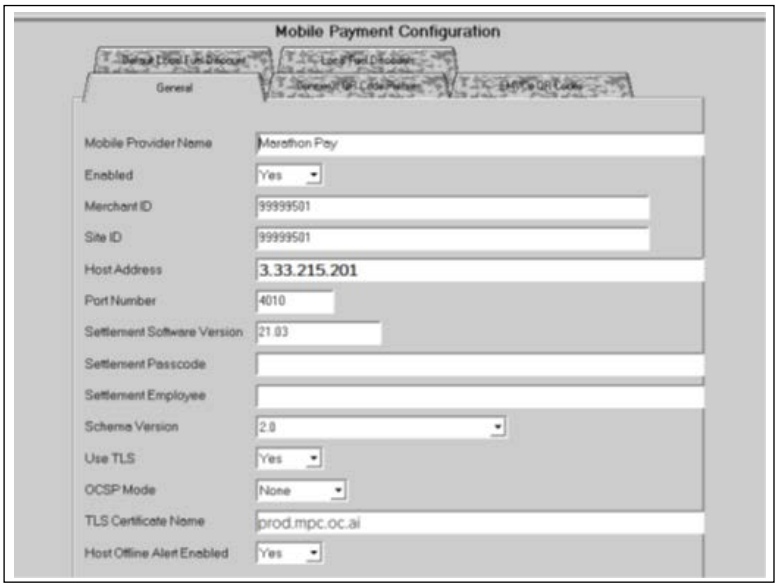



2 In the Mobile provider name, select **Add** and enter **Marathon pay**.

3 Click **Save**.

## General Tab

**Figure 41: General Tab**




Enter the following information on the General tab:

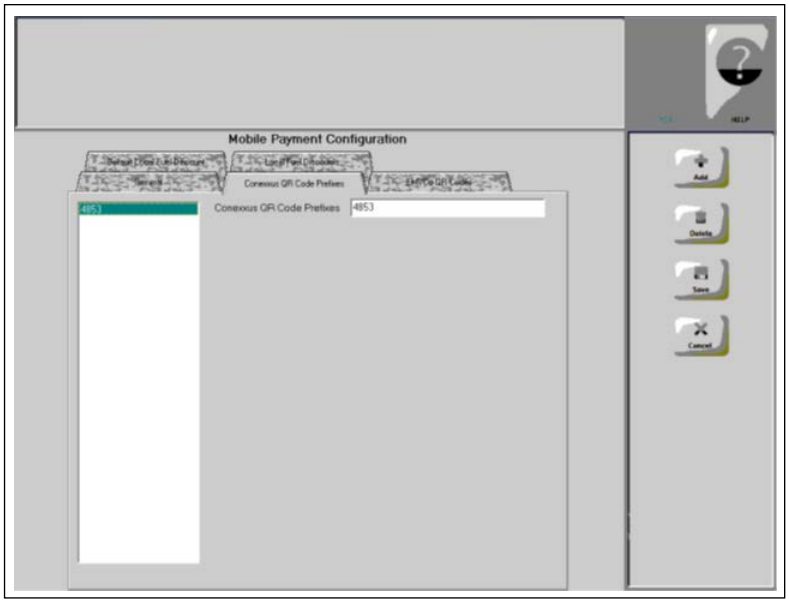
1. Mobile Provider Name: **Marathon Pay**
2. Enabled: **Yes**
3. Merchant ID: **Dealer # + 2-digit Term ID ex. 99999501 (no leading zeros)**
4. SiteID: **Same as Merchant ID**
5. Host IP: **3.33.215.201**
6. Port Number: **4010**
7. Settlement Software Version: **Passport Software Version**
8. Settlement Passcode: **Leave blank**
9. Settlement Employee: **Leave blank**
10. Schema Version: **2.0**
11. Use TLS: **Yes**
12. OCSP Mode: **None**
13. TLS Certificate: **prod.mpc.oc.ai**

**14** Host Offline Alert Enabled: **Yes**

## Conexxus QR Code Prefixes

Enter the prefix 4853 in the **Conexxus QR Code Prefixes** tab.

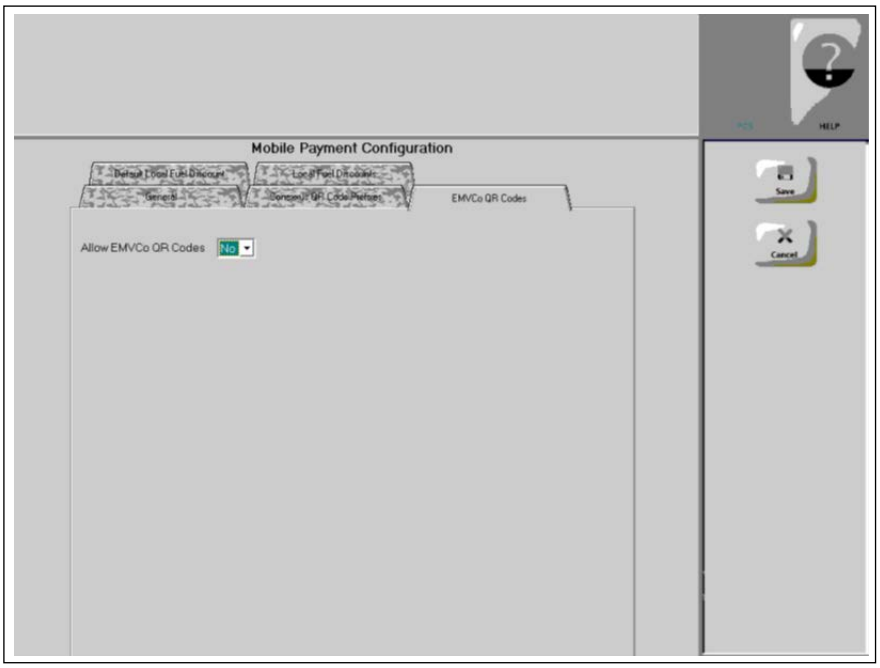
**Figure 42: Conexxus QR Code Prefixes Tab**




## EMVCo QR Codes

Select the Allow EMVCo QR Codes as **No** from the drop-down and select **Save**.

**Figure 43: EMVCo QR Codes Tab**



## Transaction Testing

After installing Marathon Rewards, make sure to validate the installation by completing at least two test transactions.

1. Buy any item or fuel inside the store using Marathon Rewards by entering a phone number at the PIN Pad.

2. Purchase at least 1 gallon of fuel at a dispenser using Marathon Rewards by entering your phone number at the PIN Pad.

   a. When at least 1 full gallon is pumped, the member will earn 5 cents, and a text should arrive to the number entered at the start of the transaction, confirming that 5 cents was earned.

# Appendix C: Loyalty Configuration Access

To configure Marathon Rewards Loyalty, proceed as follows:

1 Go to **MWS > Set Up > Store > Loyalty Interface**.
   - If a legacy Marathon loyalty program (MakeitCount, CentsOff, etc.) is already configured, select **Change**.
   - If the location has its own independent loyalty program, make sure you do not disable or delete that entry.
   - If no loyalty exists, select **Add**.

## Provider Details

1 Enter **Marathon Rewards** as the Loyalty Provider Name.

2 Select **Generic** from the Loyalty Provider Type drop-down menu.

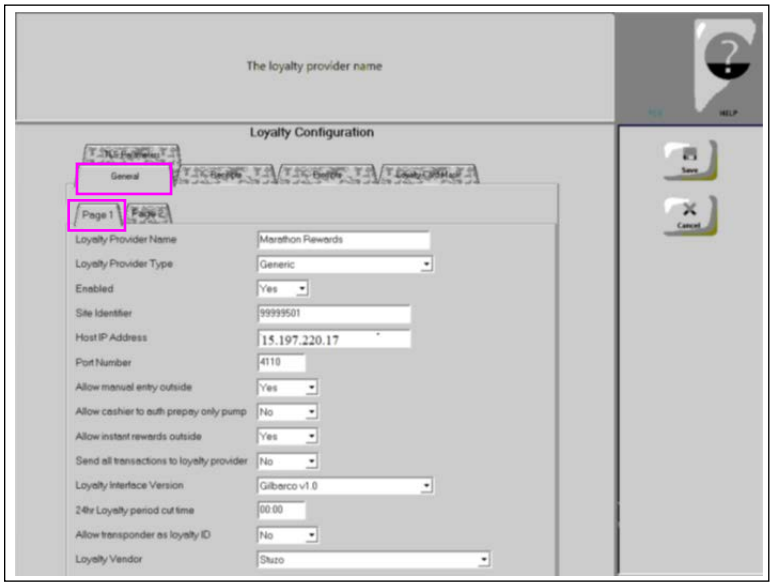
3 Select **Save** and move to the **Loyalty Configuration** screen.

**Figure 44: Provider Details**

## General

In the Loyalty Configuration section, begin with the **General** tab.

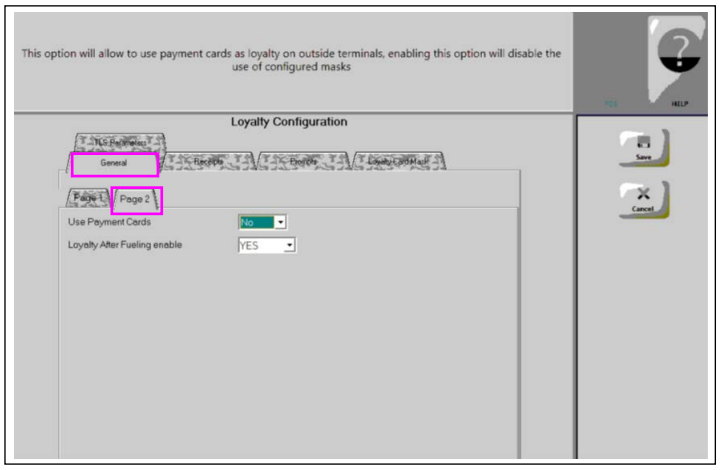
**Figure 45: Loyalty Configuration General Page 1 Tab**




Enter the following information on the **General** > **Page 1** tab:

1. Loyalty Provider Name: **Marathon Rewards**
2. Loyalty Provider Type: **Generic**
3. Enabled: **Yes**
4. Site Identifier: **Dealer # + 2-digit Term ID ex. 99999501 (no leading zeros)**
5. Host IP Address: **15.197.220.17**
6. Port Number: **4110**
7. Allow manual entry outside: **Yes**
8. Allow cashier to auth prepay only pump: **No**
9. Allow instant rewards outside: **Yes**
10. Send all transactions to loyalty provider: **No**
11. Loyalty Interface Version: **Gilbarco v1.0**
12. 24hr Loyalty period cut time: **00:00**
13. Allow transponder as loyalty ID: **No**
14. Loyalty Vendor: **Stuzo**

**Figure 46: Loyalty Configuration General Page 2 Tab**




Enter the following information on the **General > Page 2** tab

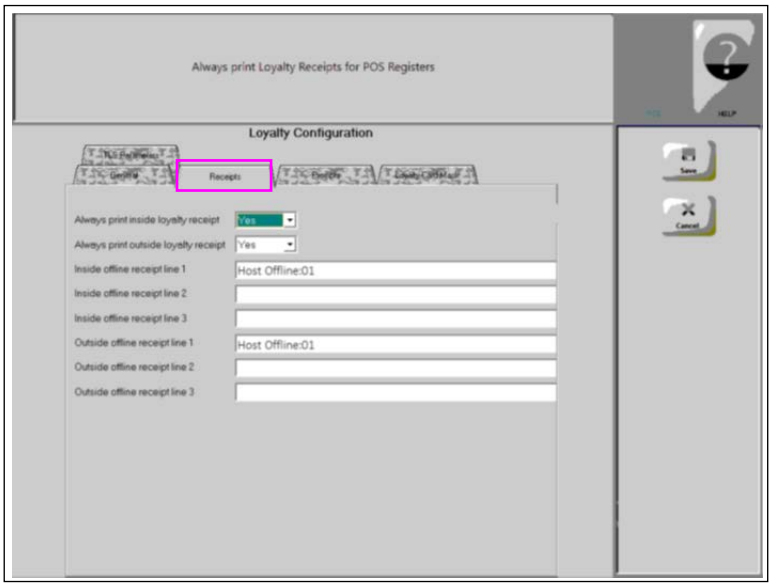
1 Use Payment Cards: **No**

2 Loyalty After Fueling enable: **Yes**

## Receipts

In the Loyalty Configuration section, navigate to the **Receipts** Tab.

**Figure 47: Receipts Tab**




Enter the following information on the Receipts tab:

1 Always print inside loyalty receipt: **Yes**

2 Always print outside loyalty receipt: **Yes**

3 Inside offline receipt line 1: **Host Offline:01**

4 Inside offline receipt line 2:

5 Inside offline receipt line 3:

6 Outside offline receipt line 1: **Host Offline:01**

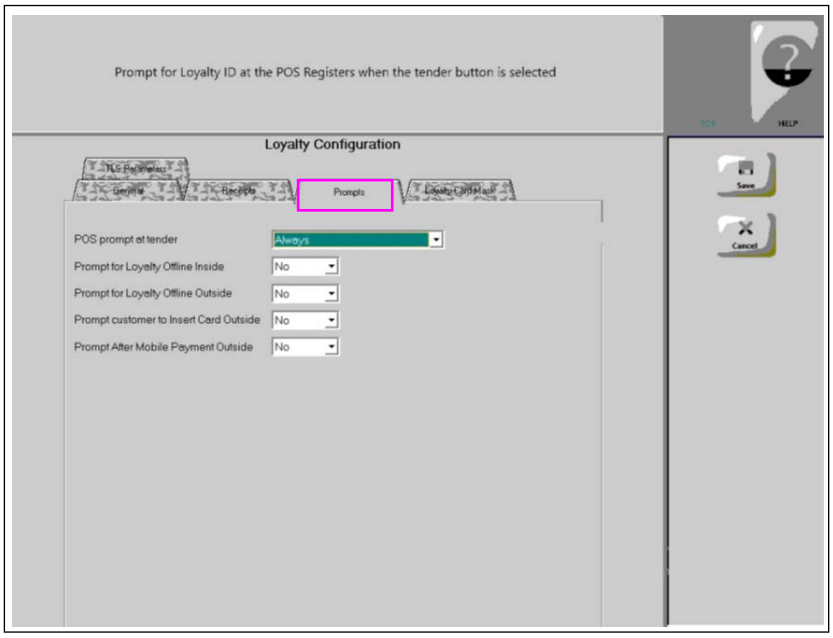
7 Outside offline receipt line 2:

8 Outside offline receipt line 3:

## Prompts

In the Loyalty Configuration section, navigate to the **Prompts** tab.

**Figure 48: Prompts Tab**




Enter the following information on the **Prompts** tab:

1 POS prompt at tender: **Always**

2 Prompt for Loyalty Offline Inside: **No**

3 Prompt for Loyalty Offline Outside: **No**

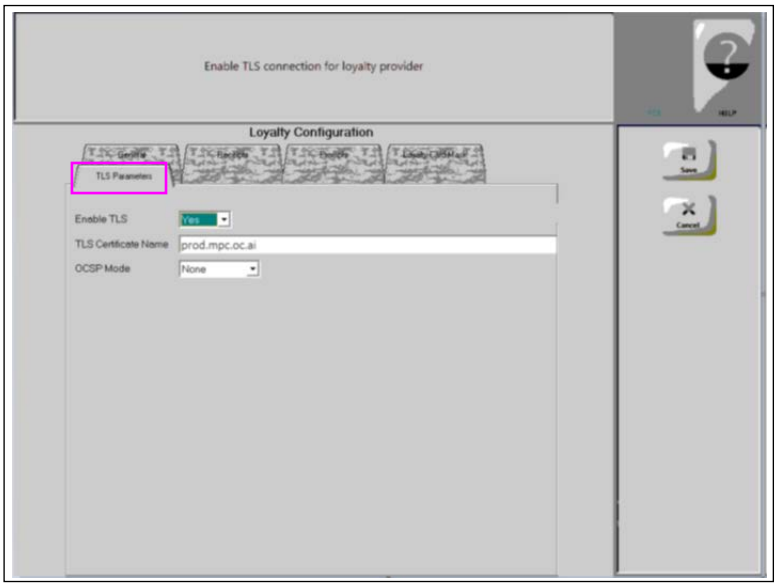
4 Prompt customer to Insert Card Outside: **No**

5 Prompt After Mobile Payment Outside: **No**

## TLS Parameters

In the Loyalty Configuration section, navigate to the **TLS Parameters** tab.

**Figure 49: TLS Parameters Tab**




Enter the following information on the **TLS Parameters** tab:

1. Enable TLS: **Yes**
2. TLS Certificate Name: **prod.mpc.oc.ai**
3. OCSP Mode: **None**

## Loyalty Card Mask

Remove any legacy Marathon loyalty configurations from the Loyalty Card Mask area. Marathon Rewards does not require any Loyalty Card Mask entries.

Select **Save**.

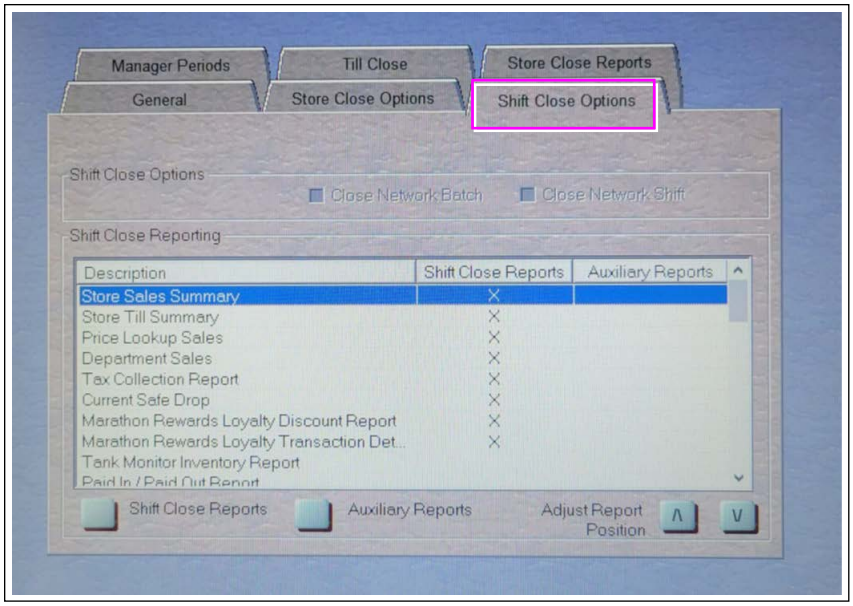
## Report Configuration

If the store wants to include loyalty reporting in their daily reports:

1 Go to **MWS >Set Up > Store > Period Maintenance Shift**.

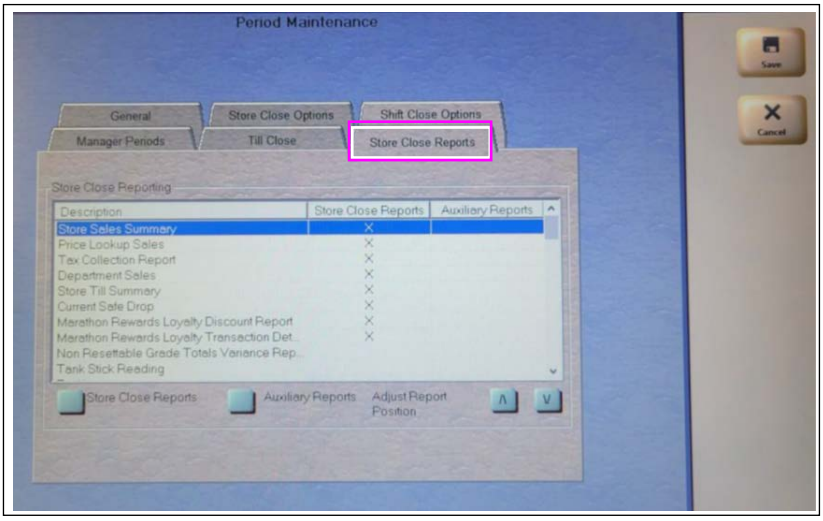
2 In the Shift Close Tab, ensure that Marathon Rewards reports are selected.

**Figure 50: Shift Close Options**




3 In the Store Close Tab, ensure that the Marathon Rewards reports are selected.

**Figure 51: Store Close Reports**




4 Select **Save**.

## IMPORTANT TECHNICIAN NOTES

- Marathon Rewards is intended to replace Marathon legacy loyalty configurations (MakeitCount, CentsOff, etc.).
- Please remove all references to any Marathon legacy loyalty (MakeitCount, CentsOff, etc.) and replace with the values represented in this guide.
- If the location has a Clapton device from a Marathon legacy loyalty program, remove it and call 888-654-6559 (option 2) to start the return process.
- At locations using Wayne Edge or Gilbarco Applause, make sure that no references to Marathon legacy loyalty programs are present.
- If the location has any custom dispenser prompting configured to reference Marathon legacy loyalty, it will need to be updated.
- Remove any images with references to Marathon legacy loyalty programs from the PIN Pads.
- Please be mindful of any independent loyalty programs at the site and do not disturb those configurations.

# Appendix D: Upgrading to Passport V21

This section provides Marathon-specific information to the ASC when upgrading from a Passport version which has been defined as an approved upgrade path.

| IMPORTANT INFORMATION |
| --- |
| If you are performing an upgrade and you are swapping out or installing new VeriFone MX915 PIN Pads, do not install the PIN Pads until you have completed the software upgrade. |

Upgrading to Passport V21 requires the use of a of Gilbarco-certified MNSP. The MNSP allows a more simple configuration and footprint of your Passport POS. The MNSP allows for removal of high-speed device MicroNode and removal of RV042 (store router). The MNSP combines these functions along with network communications and also provides 4G cellular backup. The Marathon Managed Firewall solution provided by Cybera is the preferred option.

Due to the End of Life of the Ingenico PIN Pads (iSC250 & iPP320), these devices were not certified with the HPS-Dallas network for Passport V21. When upgrading to V21.02, Passport will check to see if an Ingenico PIN Pad is connected. If one is detected, an error message will be displayed and the upgrade will be aborted. For a clean install of V21.02, Ingenico will not be an option on the Register Set Up screen. Although the iSC250 and iPP320 will still process EMV transactions on V20.02, it is recommended that a site upgrade their PIN Pads to Verifone MX915 to remain in compliance with the approved HPS-Dallas network EMV configuration. Sites that continue using iSC250 or iPP320 after upgrading to Passport V20.02 will do so at their own risk of receiving fraud liability charge backs due to using a non-EMV certified solution.

**Before beginning the upgrade:**
The ASC must perform the following steps before the upgrade:

| Step | Task Description |
| --- | --- |
| 1 | Ensure that all dispenser software and firmware meet applicable requirements to support loyalty and other fuel discounting functionality (including support of $0.000 PPU). |
| 2 | 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) |
| 3 | Perform Store Close and ensure all network transactions have completed by checking the Store and Forward Transactions Report for fallback transaction information. |
| 4 | Call the Marathon Help Desk at 1-800-378-1204 to ensure the Store Close is successful and confirm the HPS-Dallas network is prepared to enable EMV downloads for inside and outside transactions. If installing an MNSP, tell the Help Desk which MNSP is being installed and request IP addresses to be modified (which could take four hours). The Help Desk will provide new IP addresses depending on which MNSP is being installed. They will also provide TLS encryption certificate URLs if needed. |
| 5 | Assist the merchant or store manager to print additional accounting and network reports as needed. |
| 6 | Ensure that all file transfers from Passport to the BOS have completed. |

### After the upgrade:

The ASC must perform the following steps after the upgrade:

| Step | Task Description |
|---|---|
| 1 | If enabling TLS or installing an MNSP device for the first time, contact the Marathon Help Desk at 1-800-378-1204 to obtain new IP addresses, IP Ports, and TLS settings for network site configuration on Passport. Advise the agent to confirm the network is ready to communicate with the site using TCP/IP and TLS. Go to **MWS > Set Up > Network > Marathon > Global Network Parameters > Connection - Page 1** and **Page 3** tabs to confirm the settings. |
| 2 | Request a PDL Download by going to **MWS > Set Up > Network > Marathon > PDL Download**. For more information on requesting a PDL Download, refer to "Requesting a PDL Download" on page 22. |
| 3 | If the PDL download is successful, perform a Store Close. This triggers Passport to activate the new PDL and update the card table, including any new card types such as WEX EMV. |
| 4 | Review the parameters on the EMV Parameters tab and the Site Configuration tab in **MWS > Set Up > Network > Marathon > Global Info Editor** with the merchant or store manager. Advise him to contact the Marathon Help Desk to discuss financial implications of the suggested settings on this screen. |
| 5 | If installing a VeriFone MX915 or Ingenico iSC250 PIN Pad after the upgrade, ensure the EMV Capable field is selected in **MWS > Set Up > Register > Register Set Up > Device Configuration**. |
| 6 | Print a new Site Level Card Based Fuel Discounts Report. If some card types no longer have their fuel discount or if the manager wishes to target new card types with fuel discounts, go to **MWS > Set Up > Network > Marathon > Fuel Discount Configuration** and update the fuel discounts accordingly. Select **Save** to save the changes to the Passport database and exit. |

If the store manager or owner has operational questions outside Passport behavior, refer them to their Marathon representative.

*CRIND® and Gilbarco® are registered trademarks of Gilbarco Inc. GOLD℠ is service mark of Gilbarco Inc. Passport™ is a trademark of Gilbarco Inc.*

*All product names, logos, and brands are the property of their respective owners and are for identification purposes only. Use of these names, logos, and brands does not imply endorsement.*

GILBARCO VEEDER-ROOT

*© 2022 Gilbarco Inc.*
*7300 West Friendly Avenue · Post Office Box 22087*
*Greensboro, North Carolina 27410*
*Phone (336) 547-5000 · http://www.gilbarco.com · Printed in the U.S.A.*
*MDE-5583C Passport™ V21 Network Addendum for Marathon® · November 2022*