Introduction

Purpose

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

- Upgrading from Passport V10 with Service Pack P or later
- Upgrading from Passport V11.01 with Service Pack G or later
- Upgrading from Passport V11.02 with Service Pack P or later
- Installing V11.04 for the first time

Note: If an earlier version of Passport software is running, upgrade first to one of these minimum versions before upgrading to Marathon V11.04 or perform a clean install.

Upgrading to Passport or Edge V11.04 requires use of Gilbarco®-certified Managed Network Service Provider (MNSP). The MNSP allows a more simple configuration and footprint of your Passport or Edge 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 provide 4G cellular backup. The Marathon Managed Firewall solution provided by Cybera® is the preferred option.

IMPORTANT INFORMATION

Upgrading to Passport V11.04 requires advance notice to the HPS-Dallas network that the site is implementing EMV® functionality on Passport. 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 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 or Transport Layer Security (TLS) Encryption, 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.

Intended Audience

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

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 V11.04 FOR MARATHON.

Table of Contents

Related Documents

Document Number	Title	GOLD Library
MDE-3816	Passport Hardware Start-up and Service Manual	• Passport • Service Manual
MDE-4696	Ingenico® PIN Pad Kits (PA0379XXXXX, PA0380XXXXX, PA0412XXXXX, and PA0411XXXXX) Installation Instructions	POS Peripheral Devices
MDE-4826	Passport Card and Face-based Local Accounts Setup and Operations Manual	POS Peripheral Devices
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 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	• Passport • Service Manual
MDE-5167	Gilbarco Deployment Service Startup 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-5302	Passport V11.04 Upgrade Instructions	Passport
MDE-5303	Passport Software Installation Manual for V11.04 on PX60 Hardware Platforms	Passport
MDE-5323	Passport EDH (HPS-Dallas) V08.24 Implementation Guide for PA-DSS V3.2	Passport
MDE-5382	Secure Zone Router (Acumera) Installation Instructions	Passport

Abbreviations and Acronyms

Term	Description
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
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
SPG	Secure Payment Gateway
SZR	Secure Zone Router
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol

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 if you have any issue while 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. Besides 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 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 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 Manager Workstation (MWS) and POS

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

What's New in Passport V11.02 for Marathon Stores

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

Network Connection Type

Stores running Passport V8.03 that are configured for User Datagram Protocol (UDP) communication with the HPS-Dallas network are configured for TCP/IP after an upgrade to Passport V11.01 or V11.02 software. This change occurs automatically as part of the upgrade to V11.01 or V11.02. No manual intervention is required. Your ASC, however, must make necessary adjustments on the Passport Firewall Router to complete the migration from UDP to TCP/IP communication.

V11 Core Feature Enhancements

The following is a high-level description of core Passport features introduced in V11. For more information on any of the new features, refer to *MDE-5266 What's New in Passport Version 11*.

EMV Compliance

Passport V11.01 was the first release in the US to support EMV chip card compliance for inside transactions. Passport V11.02 is the first release in the US to support EMV chip card compliance outside at the dispenser. The customer and store associate experience changes greatly with these Passport features. Customers using a credit or debit card with an embedded microchip must insert the card into the chip reader on the PIN pad inside or the card reader on the dispenser outside and leave it until the chip reader displays instructions to remove the card. Cashiers at the Cashier Workstation (CWS) and customers inside and at the dispenser will notice new prompting beginning with these Passport versions.

Enabling EMV inside may require new PIN pads or new PIN pad software. EMV-capable PIN pads are:

- VeriFone MX915
- Ingenico iSC250
- Ingenico iPP320

Enabling EMV outside at the dispenser requires Gilbarco FlexPay™ II, FlexPay IV, or FlexPay IV Retrofit Kit for Wayne® dispensers. Each of these Gilbarco platforms also require CRIND via TCP/IP.

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 which 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. The network 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.

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 displays.

Receipt Printer Settings for Faster Printing

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

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.

The following table contains an excerpt of the PCATS Payment Systems Product Code fuel product codes along with their description:

Fuel Grade Description	Code	Fuel Grade Description	Code
Regular Unleaded	001	Super Methanol 7.7%	037
Midgrade Unleaded	002	Unl. Methanol 10%	038
Premium Unleaded	003	Plus Methanol 10%	039
Unl. Methanol 5.7%	006	Super Methanol 10%	040
Plus Methanol 5.7%	007	Super Ethanol 7.7%	041
Super Methanol 5.7%	008	Unl. Ethanol 10%	042
Unl. Methanol 7.7%	009	Plus Ethanol 10%	043
Plus Methanol 7.7%	010	Super Ethanol 10%	044
Unl. Ethanol 5.7%	011	Non-Tax (Off-road)	071
Plus Ethanol 5.7%	012	Unleaded 2	072
Super Ethanol 5.7%	013	Premium/Super 2	073
Unl. Ethanol 7.7%	014	Premium/Super 3	074
Plus Ethanol 7.7%	015	Premium/Super 4	075
Leaded Regular	018	Refrigerated Fuel and Off-road Non-farming	076
Diesel 1 (Taxed)	019	Farm (Off-road Farming Equipment)	077
Diesel 2 (Taxed)	020	Misc. Fuel	099
CNG	022	Aviation Jet	150
LPG	023	Aviation Gas	151-174
LNG	024	Misc. Fuel	225-229
E-85	026	Marine (Two-stroke)	230
Midgrade Unld. 2	028	Misc.	231-249
Midgrade Unld. 3	029	Misc.	255-299
Diesel 1 (Off-road)	032	Kerosene	300
Diesel 2 (Off-road)	033	White Gas	301
Racing	036	Propane	303

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 MWS main menu, select **Set Up** > **Network** > **Marathon**. The Marathon Network Configuration menu opens.

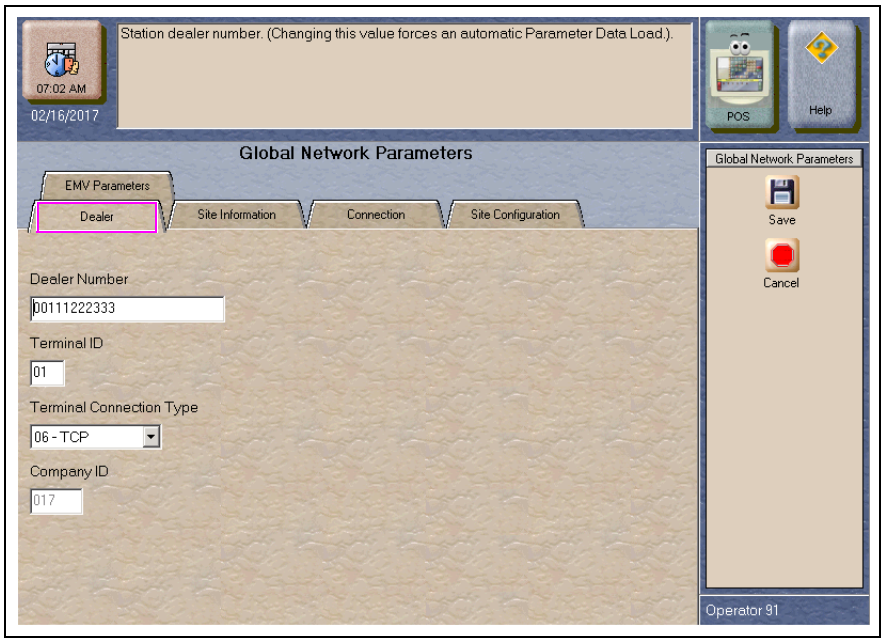
Figure 1: Marathon Network Configuration Menu

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

- Global Info Editor
- Card Info Editor
- PDL Download
- E-Mail Request
- Fuel Discount Configuration

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

Figure 2: Global Network Parameters - Dealer Tab

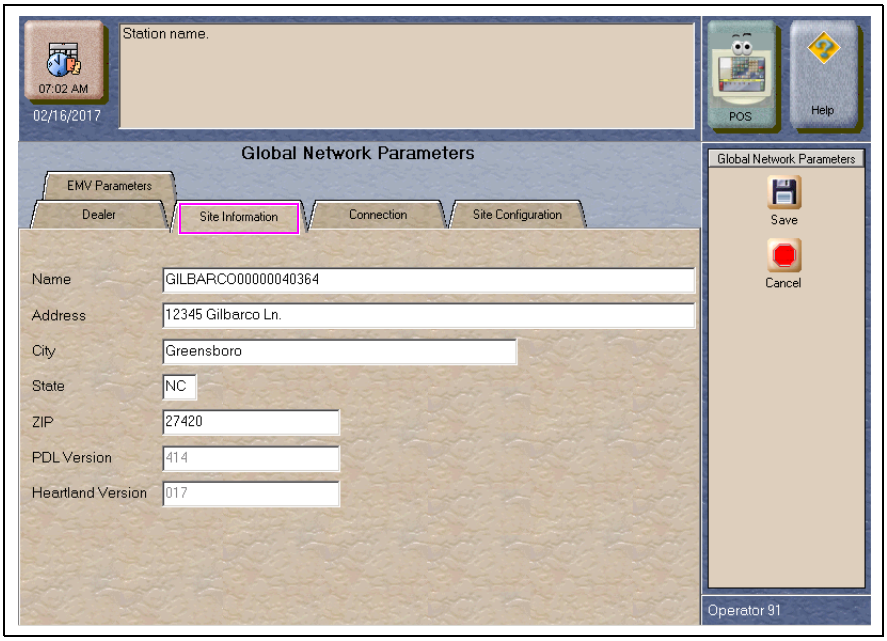


Fields on the Dealer Tab

Field	Description
Dealer Number	An 11-digit number the HPS-Dallas network uses to identify the store. *Notes: 1) Enter the dealer number before receiving initial PDL* *2) Change Dealer Number only after Store Close*
Terminal ID	The terminal identification number the HPS-Dallas network assigns to the store. *Notes: 1) The default Terminal ID is "01".* *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 3: Site Information Tab



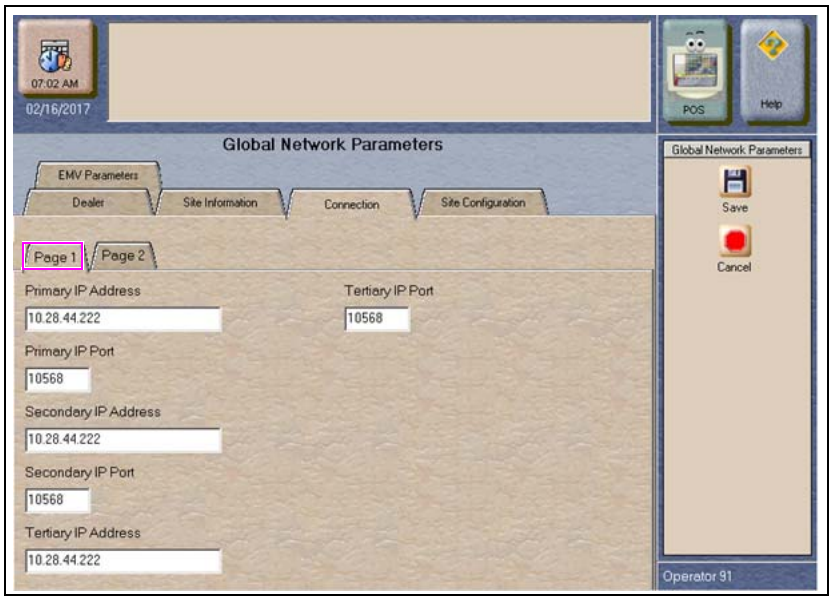
Fields on the Site Information Tab

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.
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.

Figure 4: Connection - Page 1 Tab (for TCP/IP Connections)



The following table contains information on fields that is 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.

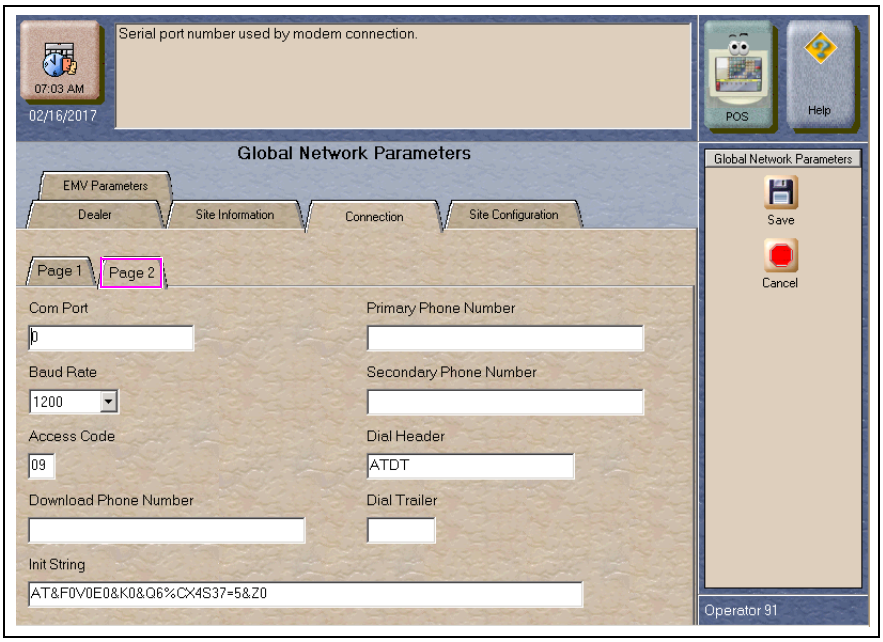
i Obtain the IP addresses from the HPS-Dallas or EchoSat℠ Help Desk, depending upon the kind of Earth Station used at the site (refer to the following table).

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 Select the **Page 2** tab to complete programming for a Dial connection.

Figure 5: Connection - Page 2 Tab



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

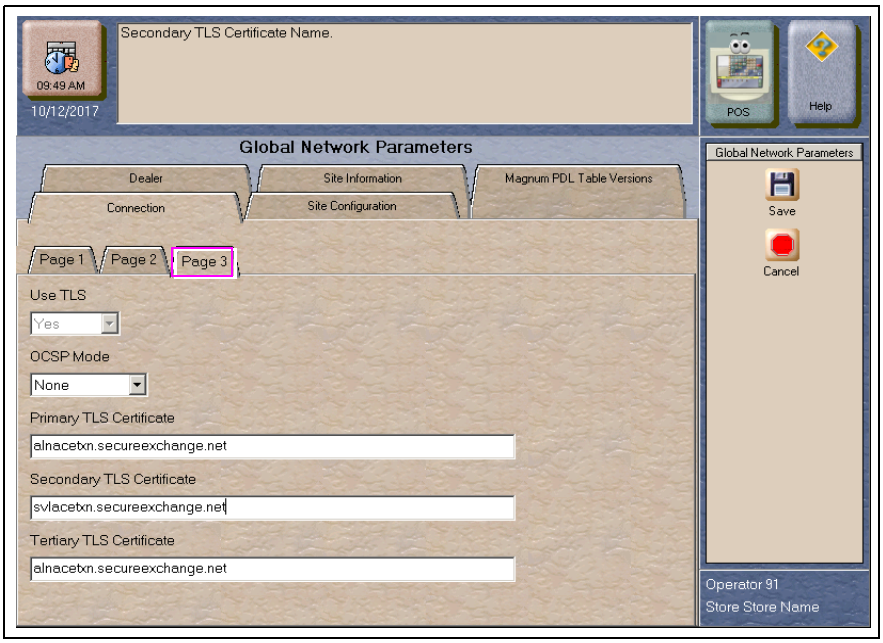
Field	Description
COM Port	The COM port to which the modem is connected on the EDH. Default is 0.
Baud Rate	Dial baud rate used by the modem; Options are 300, 1200, 2400, 4800, 9600, 14400, 19200, 38400, 56000, 57600, 115200, 128000, and 256000. Default rate is 1200.
Access Code	Numbers that must be 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. Default is AT&F0V0E0&K0&Q6%CX4S37=5&Z0. • MultiTech® 009: use default value • 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. • MultiTech 009: ATS7=15S10=2S11=50S25=0&W0 • 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.

Complete the Download Phone Number, Primary Phone Number, and Secondary Phone Number fields. Refer to the following table for phone numbers:

Download	Primary	Secondary	Alternate
1-800-221-2455 (use Alternate if this number does not work)	1-800-221-2455 (use Alternate if this number does not work)	1-800-454-6103	1-800-454-6103

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

Figure 6: Connection - Page 3 Tab (for TLS Connections)



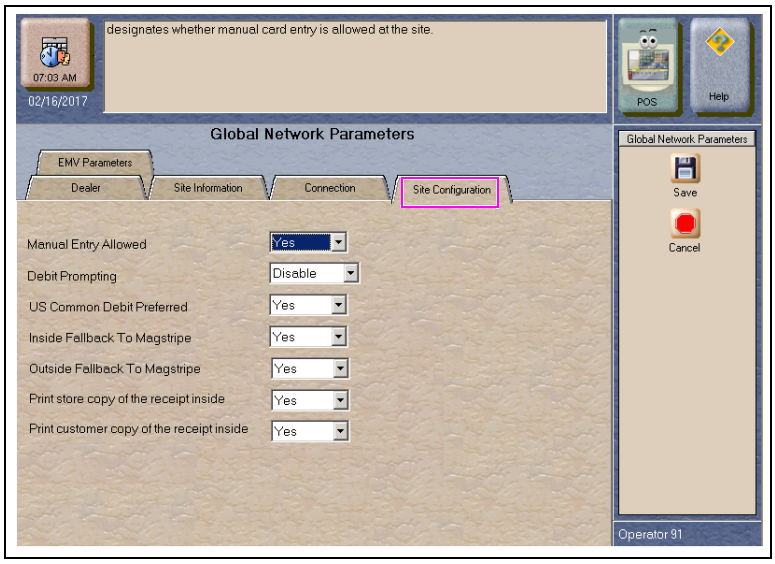
Note: Contact the Marathon Help Desk at 1-800-378-1204 for the appropriate TLS programming.

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.

3 Select the **Site Configuration** tab.

Figure 7: Site Configuration Tab



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

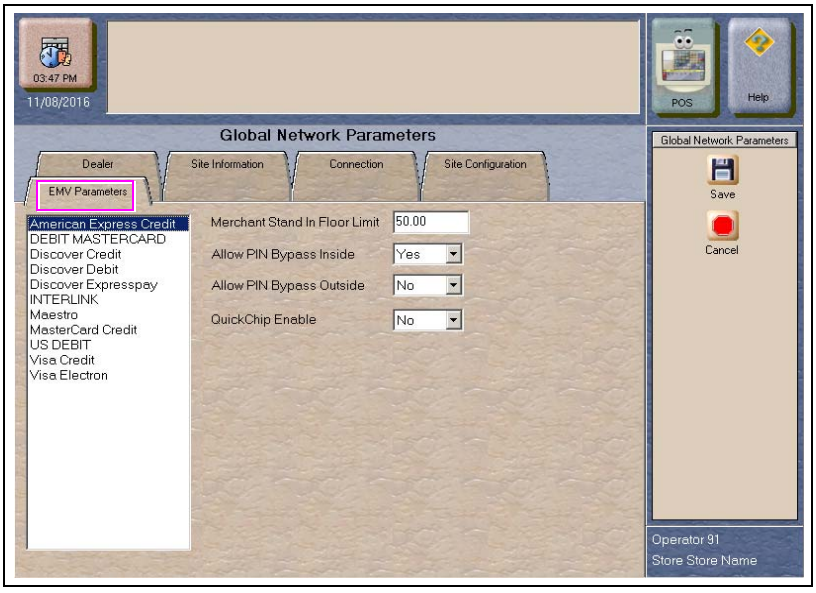
Fields on the Site Configuration Tab

Field	Description
Manual Entry Allowed	If set to Yes, manual entry of Credit Card transactions is allowed.
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. 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 Application Identifiers (AID), Passport displays or uses the US Common Debit AID. 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. 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. 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.
Outside Fallback to Magstripe	If set to No, when the customer inserts a chip card into the chip reader on the CRIND and a chip error occurs, Passport declines the card. If set to Yes, when the customer inserts a chip card into the chip reader on the CRIND 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.

4 Select the **EMV Parameters** tab.

Figure 8: 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. *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. 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. *Note: Some debit AIDs set this field to Yes by default and the merchant cannot change this setting.*

Field	Description
Allow PIN Bypass Outside	If set to Yes and the EMV application requires PIN entry, the CRIND prompts the customer to enter the PIN, but allows the customer to press the **ENTER** key on the CRIND keypad without entering a PIN. If set to No and the EMV application requires PIN entry, the CRIND prompts the customer to enter the PIN and the customer must enter a PIN to move forward in the transaction. *Note: Some debit AIDs set this field to Yes by default and the merchant cannot change this setting.*
QuckChip Enable	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. 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. 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. Defaults to No. Enable “QuickChip” functionality at time of installation for faster EMV transactions.

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

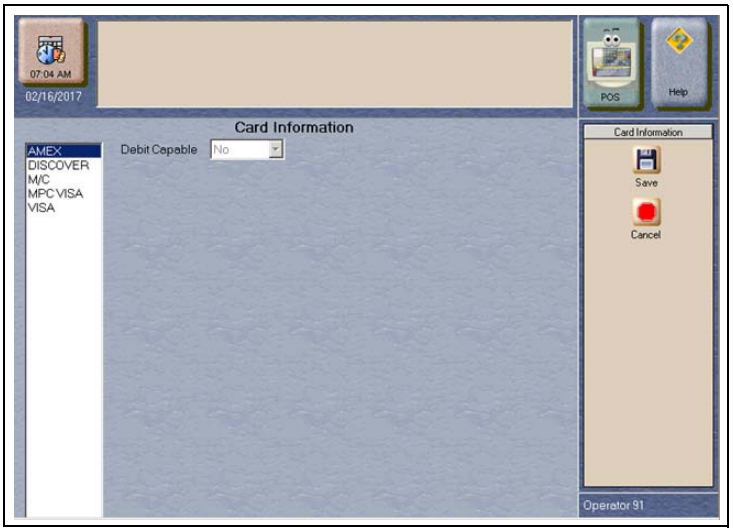
Programming Network Card Configuration

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 **Setup** > **Network** > **Marathon** > **Card Info Editor**. The **Card Information** screen opens.

Figure 9: 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.

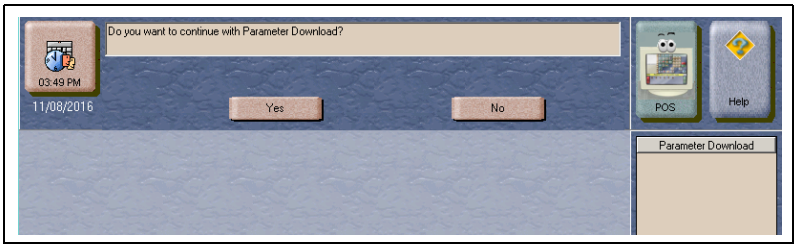
IMPORTANT INFORMATION
When upgrading software, call HPS-Dallas Help Desk (1-800-533-3421) to inform them that you need a new PDL. Then, request a PDL Download through the MWS.

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?”

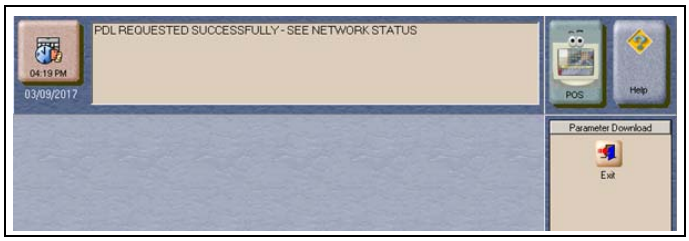
Figure 10: PDL Download Screen



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 11: 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.

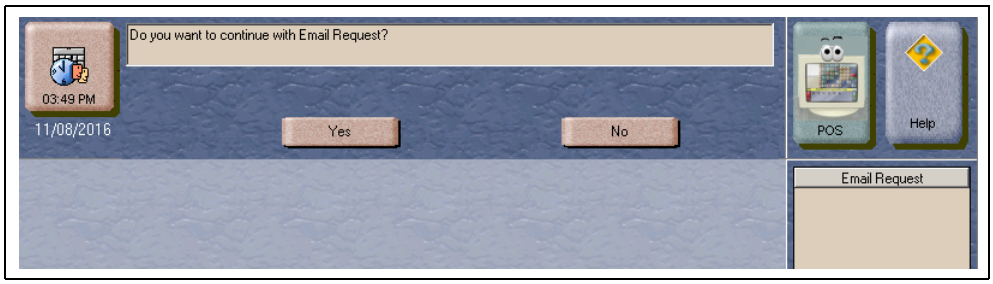
Requesting E-Mail

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

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

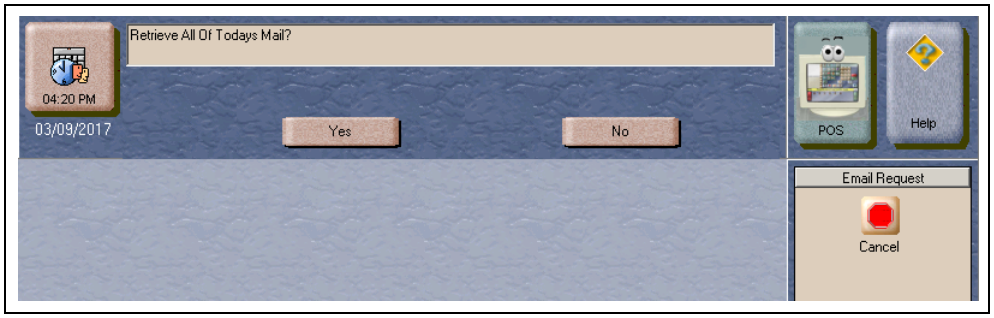
2 The Passport system prompts: “Do you want to continue with Email Request?”

Figure 12: E-Mail Request Prompt



3 Select **Yes** to submit the request. Passport prompts: “Retrieve all of today's mail?”

Figure 13: All Mail Prompt



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

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 14: Network Journal Report Screen

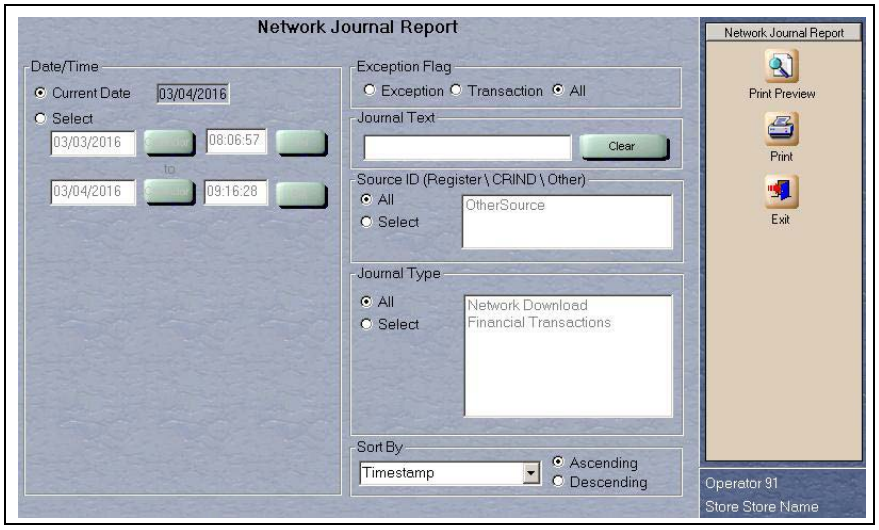
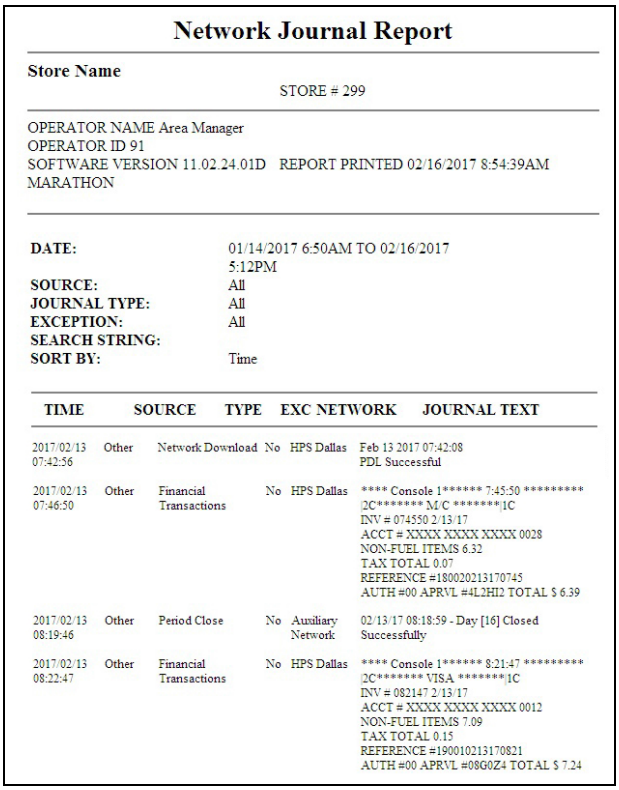


Figure 15: Network Journal Report Sample



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 PDL Successful
2017/02/13 07:46:50	Other	Financial Transactions	No	HPS Dallas	**** Console 1****** 7:45:50 ********* |2C******* M/C *******|1C INV # 074550 2/13/17 ACCT # XXXX XXXX XXXX 0028 NON-FUEL ITEMS 6.32 TAX TOTAL 0.07 REFERENCE #180020213170745 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 ********* |2C******* VISA *******|1C INV # 082147 2/13/17 ACCT # XXXX XXXX XXXX 0012 NON-FUEL ITEMS 7.09 TAX TOTAL 0.15 REFERENCE #190010213170821 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.*

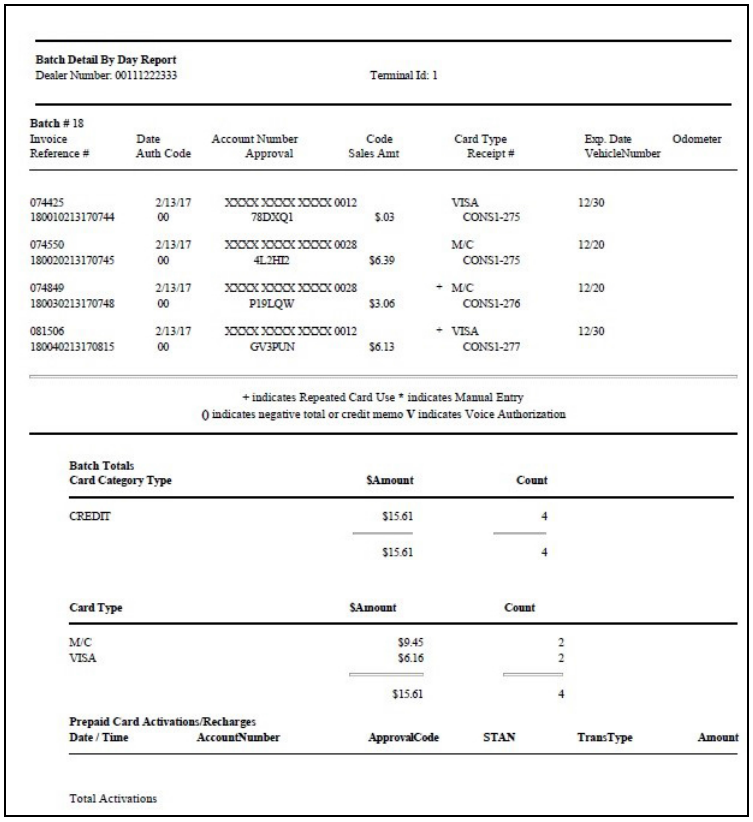
IMPORTANT INFORMATION

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-5323 Passport EDH (HPS-Dallas) V08.24 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 16: Batch Detail by Day Report



Batch Detail By Day Report
Dealer Number: 00111222333 Terminal Id: 1

Batch # 18

Invoice Reference #	Date Auth Code	Account Number Approval	Code Sales Amt	Card Type Receipt #	Exp. Date VehicleNumber	Odometer
074425	2/13/17	XXXX XXXX XXXX 0012		VISA	12/30	
180010213170744	00	78DXQ1	$.03	CONS1-275		
074550	2/13/17	XXXX XXXX XXXX 0028		M/C	12/20	
180020213170745	00	4L2HI2	$6.39	CONS1-275		
074849	2/13/17	XXXX XXXX XXXX 0028		+ M/C	12/20	
180030213170748	00	P19LQW	$3.06	CONS1-276		
081506	2/13/17	XXXX XXXX XXXX 0012		+ VISA	12/30	
180040213170815	00	GV3PUN	$6.13	CONS1-277		

+ 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	$15.61	4
	$15.61	4

Card Type	$Amount	Count
M/C	$9.45	2
VISA	$6.16	2
	$15.61	4

Prepaid Card Activations/Recharges

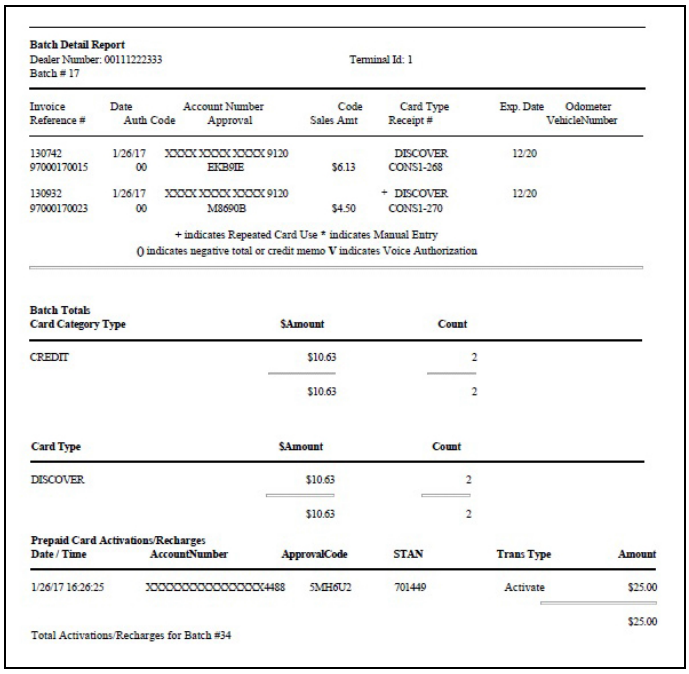
Date / Time	AccountNumber	ApprovalCode	STAN	TransType	Amount

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 17: 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

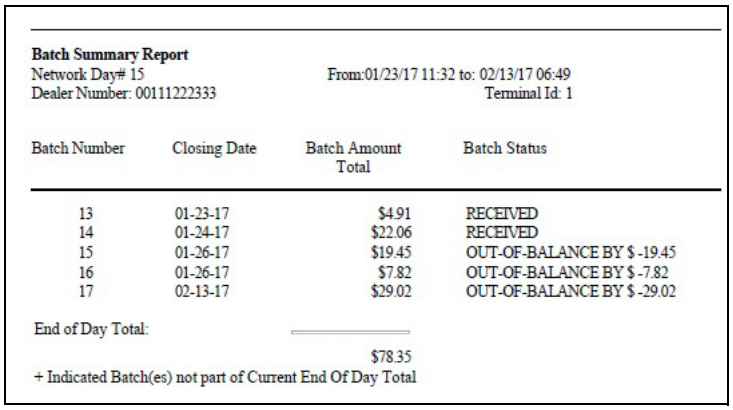
Date / Time	AccountNumber	ApprovalCode	STAN	Trans Type	Amount
1/26/17 16:26:25	XXXXXXXXXXXXXXX4488	5MH6U2	701449	Activate	$25.00
					$25.00

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 18: 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

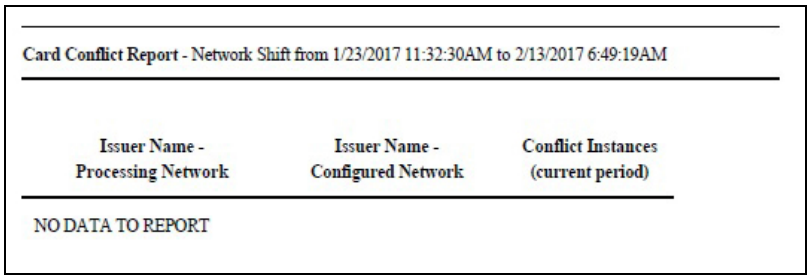
End of Day Total: $78.35
+ Indicated Batch(es) not part of Current End Of Day Total

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 19: Card Conflict Report



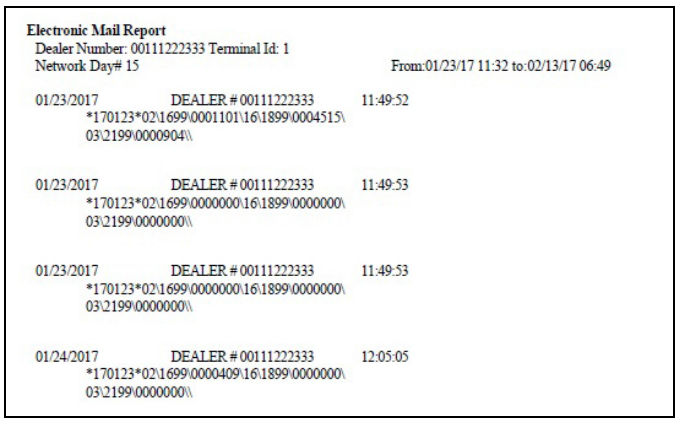
Card Conflict Report - Network Shift from 1/23/2017 11:32:30AM to 2/13/2017 6:49:19AM

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 20: 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\\

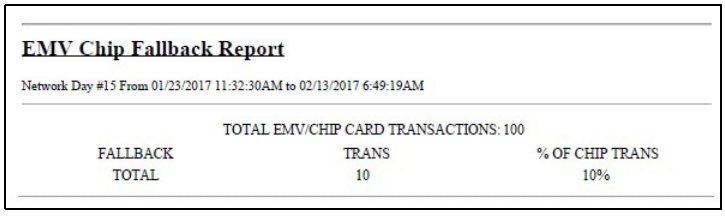
01/23/2017 DEALER # 00111222333 11:49:53
*170123*02\1699\0000000\16\1899\0000000\
03\2199\0000000\\

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 21: 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

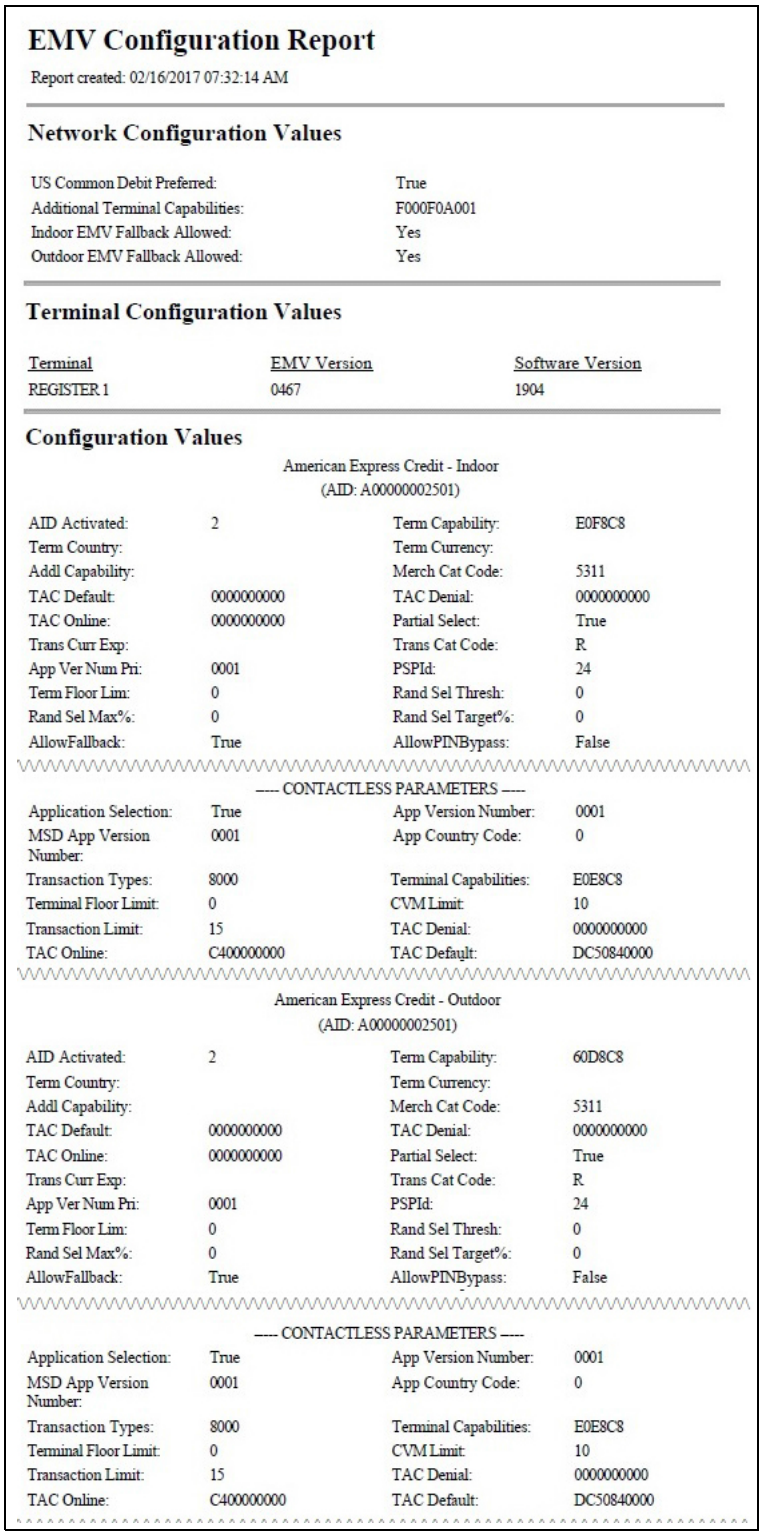
TOTAL EMV/CHIP CARD TRANSACTIONS: 100

FALLBACK	TRANS	% OF CHIP TRANS
TOTAL	10	10%

EMV Configuration Report

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

Figure 22: 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

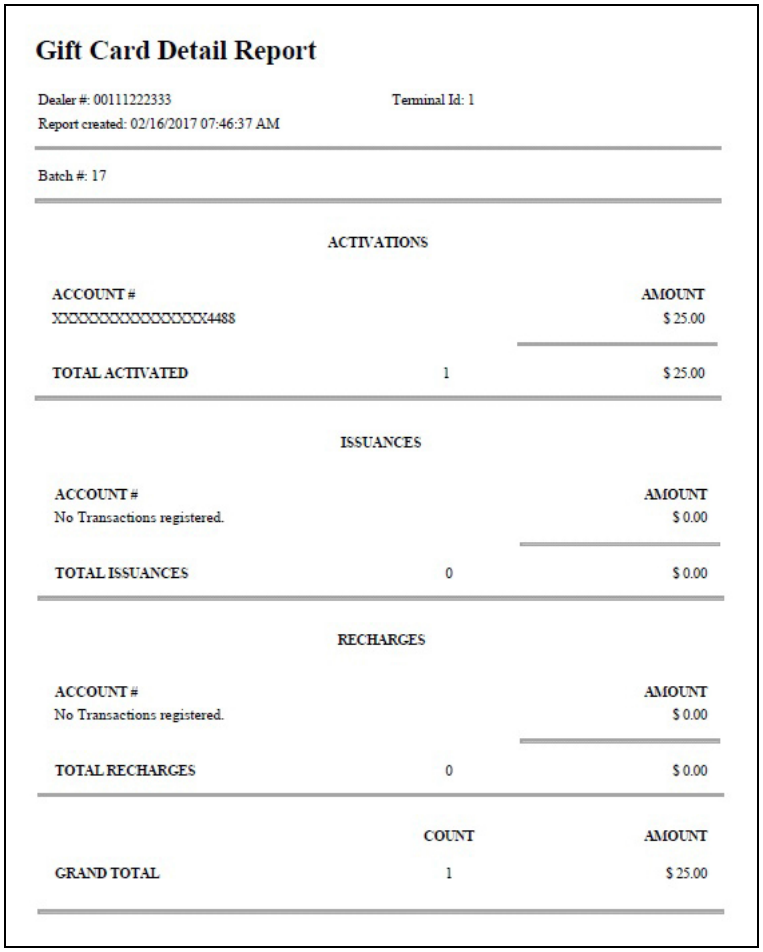
---- CONTACTLESS PARAMETERS ----

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 23: 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
XXXXXXXXXXXXXXX4488		$ 25.00
TOTAL ACTIVATED	1	$ 25.00

ISSUANCES

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

RECHARGES

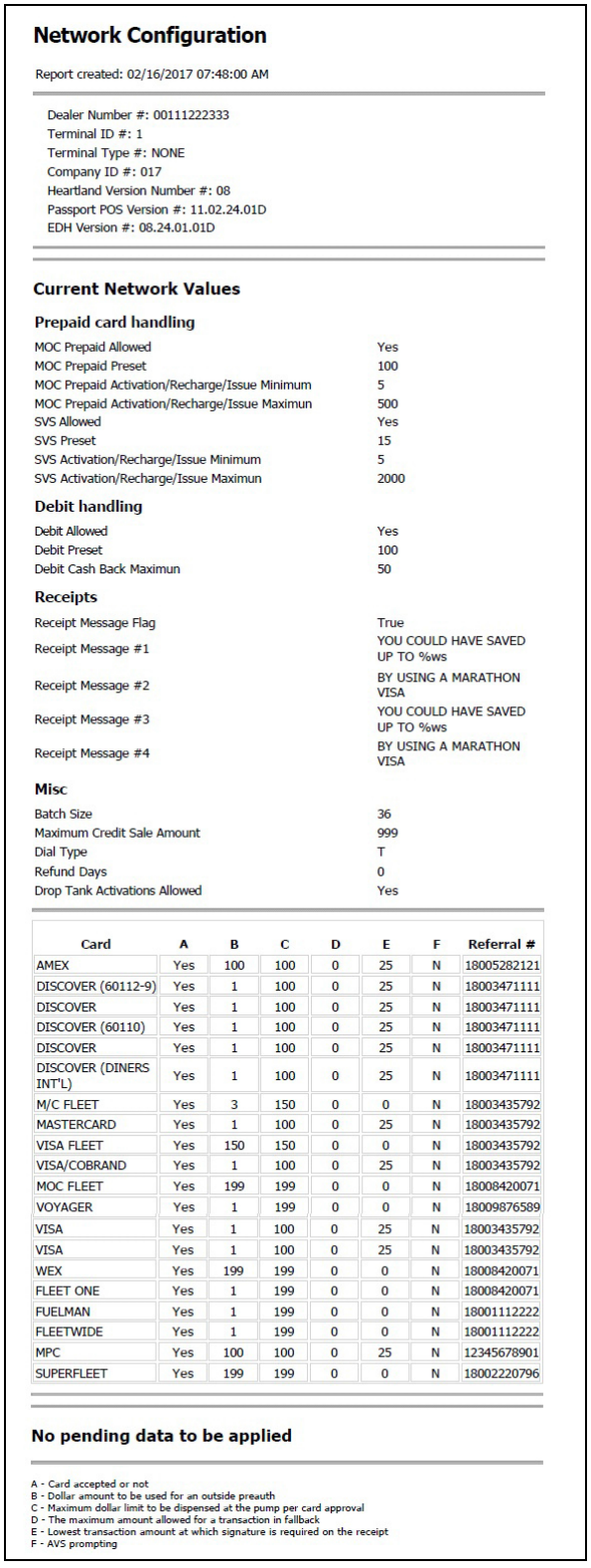
ACCOUNT #		AMOUNT
No Transactions registered.		$ 0.00
TOTAL RECHARGES	0	$ 0.00

	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 24: 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

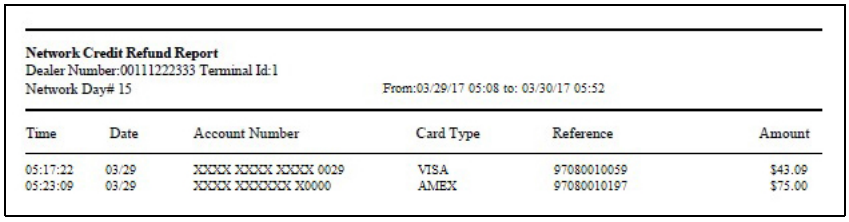
No pending data to be applied

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 25: Network Credit Refund Report



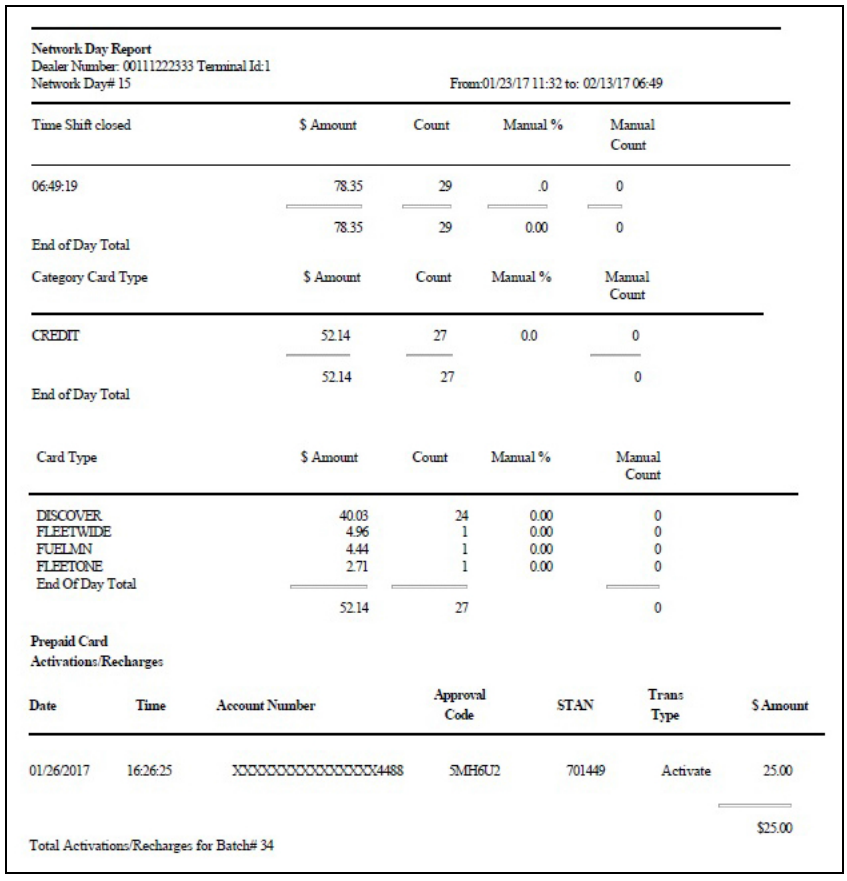
Network Credit Refund Report
Dealer Number:00111222333 Terminal Id:1
Network Day# 15 From:03/29/17 05:08 to: 03/30/17 05:52

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 26: 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

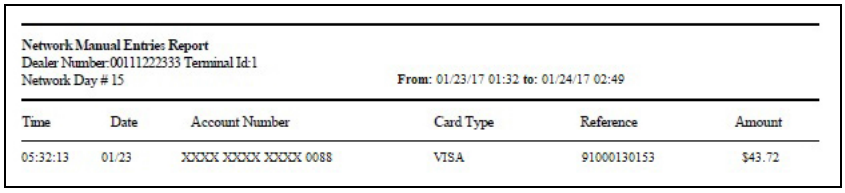
Date	Time	Account Number	Approval Code	STAN	Trans Type	$ Amount
01/26/2017	16:26:25	XXXXXXXXXXXXXXX4488	5MH6U2	701449	Activate	25.00
						$25.00

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 27: 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

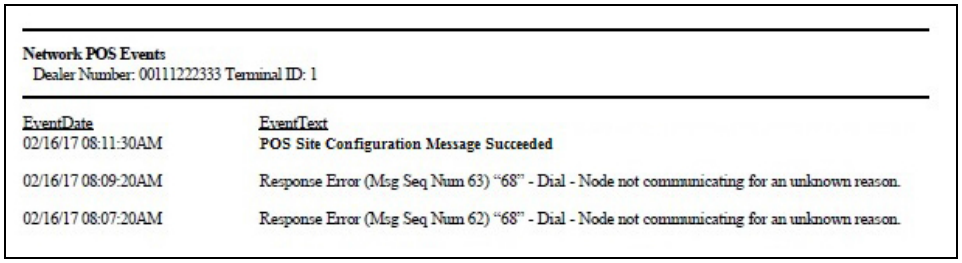
Time	Date	Account Number	Card Type	Reference	Amount
05:32:13	01/23	XXXX XXXX XXXX 0088	VISA	91000130153	$43.72

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 28: Network POS Events



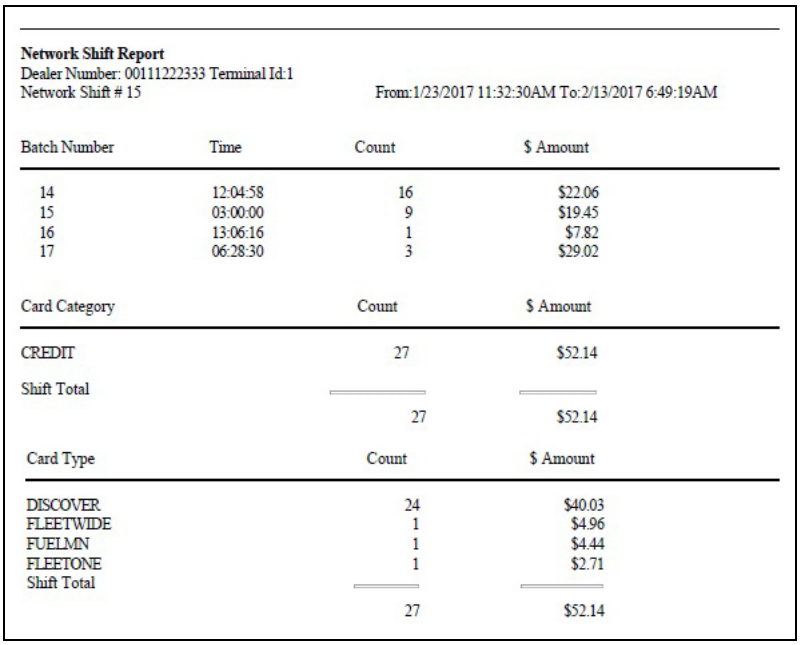
Network POS Events
Dealer Number: 00111222333 Terminal ID: 1

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 29: 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

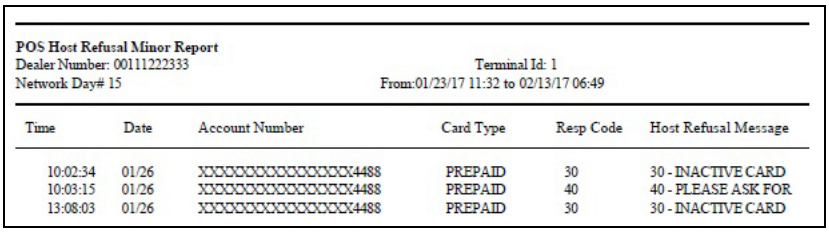
Card Type	Count	$ Amount
DISCOVER	24	$40.03
FLEETWIDE	1	$4.96
FUELMN	1	$4.44
FLEETONE	1	$2.71
Shift Total	27	$52.14

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 secure version of the POS Host Refusal Minor Report. A non-secure version prints the account number masked except for the last four digits. 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 30: POS Host Refusal Minor Report



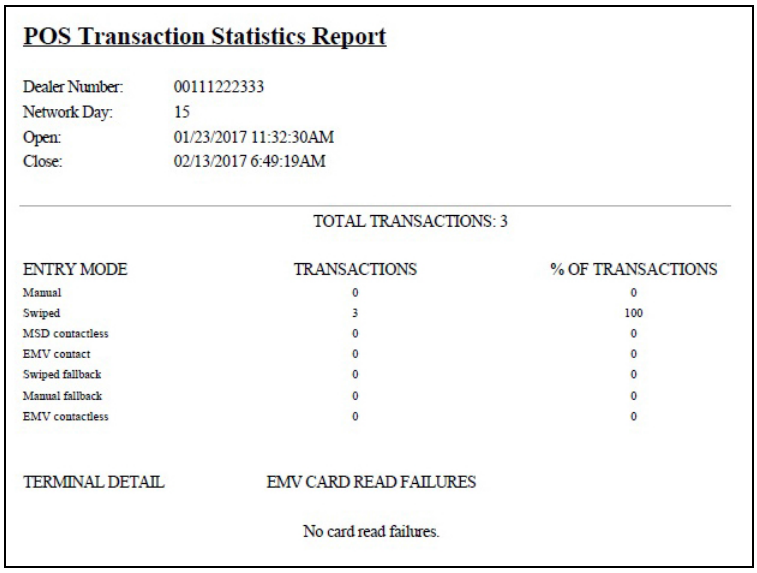
POS Host Refusal Minor Report
Dealer Number: 00111222333 Terminal Id: 1
Network Day# 15 From:01/23/17 11:32 to 02/13/17 06:49

Time	Date	Account Number	Card Type	Resp Code	Host Refusal Message
10:02:34	01/26	XXXXXXXXXXXXXXX4488	PREPAID	30	30 - INACTIVE CARD
10:03:15	01/26	XXXXXXXXXXXXXXX4488	PREPAID	40	40 - PLEASE ASK FOR
13:08:03	01/26	XXXXXXXXXXXXXXX4488	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 31: 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

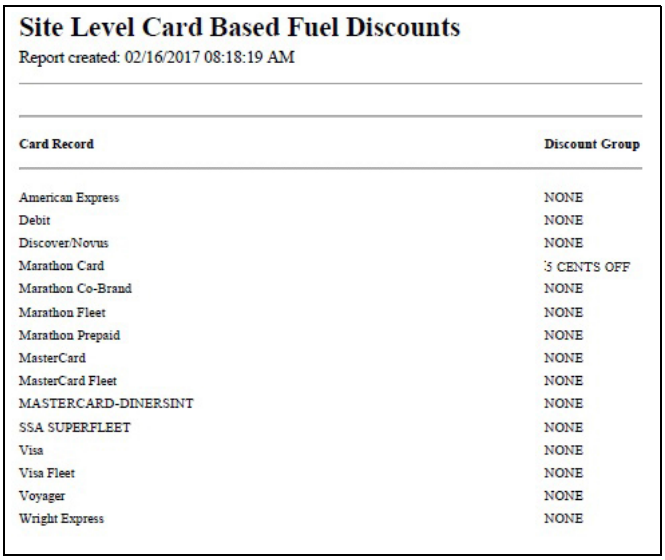
TERMINAL DETAIL EMV CARD READ FAILURES

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 Menu > 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 32: 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 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
- Credit Card Balance Inquiry
- E-mail Request

Accessing Network Functions

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

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

Figure 33: Network Functions Button

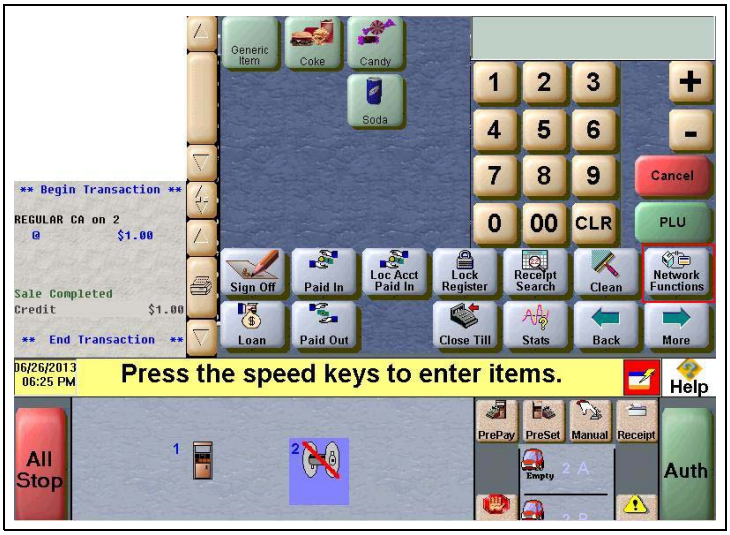
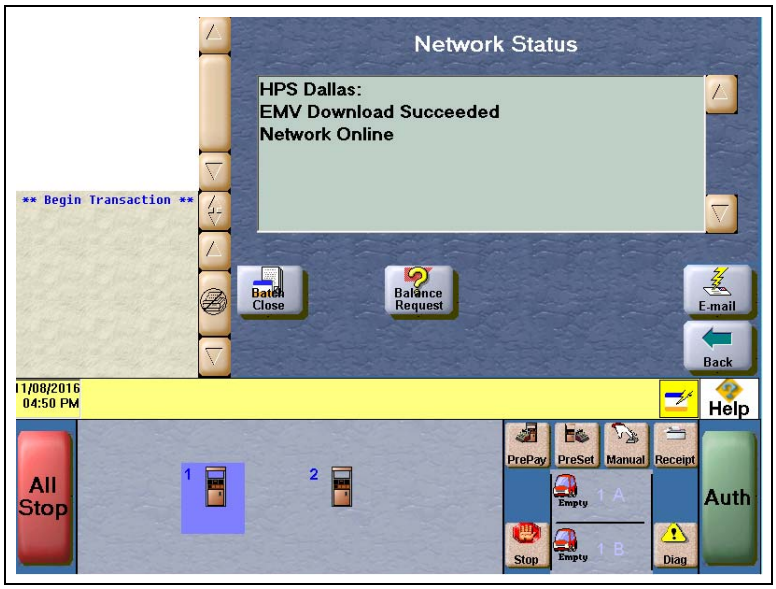


Figure 34: CWS Network Status Indicator

With either action the Network Status screen opens.

Figure 35: CWS Network Status Screen



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

Checking the Network Status

The Network Status tool 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.

Performing a Batch Close

A network batch close may occur automatically after a certain number of transactions. You may also perform a batch close at any time outside a sales transaction by selecting the **Batch Close** button.

You can perform a batch close whenever you are not in a sales transaction. On the Network Functions screen, select **Batch Close**. The message "**Processing Batch Close. Please Wait.**" is displayed on the message bar.

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 Cash Card Balance

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

1. On the Network Functions screen, select **Balance Inquiry**.
2. Swipe the cash card.
3. The balance is displayed and Passport prints a customer receipt with the balance amount.

Receiving E-Mail from CWS

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

1. On the Network Functions screen, select **E-mail**. 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.

Frequently Asked Questions

Q:1 I think Passport is not connected to the HPS-Dallas network. What should I do?

A:1 Check the Network Status screen. If the Network Status screen displays Network Offline and you use a dial connection, check the phone numbers displayed in **MWS** > **Setup** > **Network** > **Marathon** > **Global Info Editor** > **Connection** > **Page 2** tab. If the phone numbers are not correct, call the HPS-Dallas Help Desk for assistance.

Appendix A: Network Events Messages

The following table lists the network event messages:

Message	Priority	Meaning
Network Connection Offline	N/A	For Dial locations, this message means that no modem connection is present. For TCP/IP (satellite) locations, this message means that 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 ADS-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 ADS-Dallas Help Desk for help.
Fallback File Warning - Call Help Desk	Medium	This message indicates that the fallback file has 200 or more transactions in it. Check the network connection and call the ADS-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	This message indicates that the fallback file is full. Check the network connection and call the ADS-Dallas Help Desk for help in clearing transactions. When the file is no longer full, the message will clear.

Appendix B: Upgrading to Passport V11.04

This section provides Marathon-specific information to the ASC for upgrading from Passport V8.03, V10, or V11.01, V11.02 to V11.04.

IMPORTANT INFORMATION

Upgrades to HPS-Dallas V11.04 are supported only for locations running:

- Marathon V8.03 with Service Pack M or later
- Marathon V10 with Service Pack K or later
- Marathon V11.01 with Service Pack C or later
- Upgrading from Passport V11.02 with Service Pack P or later

If the Passport system is running an earlier version or service pack, the first upgrade to one of these minimum versions or perform a clean install.

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 or Edge V11.04 requires use of Gilbarco-certified MNSP. The MNSP allows a more simple configuration and footprint of your Passport or Edge 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 provide 4G cellular backup. The Marathon Managed Firewall solution provided by Cybera is the preferred option.

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

- If upgrading from V8.03:
  - If the **MWS > Fuel > Fuel Discount Maintenance > Fuel Discounts by Card Type** tab is configured, print the Fuel Discount Configuration report. This report aids in confirming and reconfiguring fuel discounting after the upgrade to V11.04 in **Fuel Discount Maintenance** and in **Fuel Discount Configuration**.
  - If a generic loyalty provider is configured in **MWS > Set Up > Store > Loyalty Interface**, advise the manager that during the upgrade all historical Loyalty sales data will be lost and Loyalty period reports must be printed before the upgrade begins.
  - In **MWS > Set Up > Network > Marathon > Global Info Editor > Connection > Page 1** tab, if the Connection Type field is set to 06 - UDP, Passport will change this setting to 06 - TCP/IP and delete the IP Addresses and IP Ports as part of the upgrade process. You must contact the Marathon Help Desk after the software upgrade completes to obtain new Primary, Secondary, and Tertiary IP Addresses and IP Ports.
- 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.
- Perform Store Close and ensure all network transactions have completed by checking the Batch Summary Report for fallback transaction information.
- 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.
- Assist the merchant or store manager to print all additional accounting and network reports needed.
- Ensure all file transfers from Passport to the BOS have completed.

After the upgrade, the ASC must perform the following:

- Perform a PDL request by going to **MWS** > **Set Up** > **Network** > **Marathon** and select **PDL Download**.

  Note: Contact the Marathon Network Support to set the download flag. For more information, refer to "Requesting a PDL Download" on page 20.
- 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.
- On the EMV Parameters tab of the Global Network Parameters screen (**MWS** > **Set Up** > **Network** > **Marathon** > **Global Info Editor**), enable QuickChip functionality for faster EMV transactions.
- Review the parameters on the **EMV Parameters** 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.
- If installing a VeriFone MX915, Ingenico iSC250, or Ingenico iPP320 PIN pad, ensure the **MWS > Set Up Register > Register Set Up > Device Configuration >** EMV Capable field is selected.
- 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.

GILBARCO VEEDER-ROOT

© 2019 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-5450A Passport™ V11.04 Network Addendum for Marathon® · July 2019