Introduction

Purpose

This manual provides network-specific information for stores running Passport™ V12 systems at Phillips 66® stores using the HPS-Dallas network.

IMPORTANT INFORMATION

Upgrading to Passport V12 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 to 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 the network to 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, verify the merchant or store manager has 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 they can expedite enabling EMV functionality for the store within four hours. If the network representative indicates that there is a possibility of enabling EMV on the network within the next four hours, continue with the upgrade. Otherwise, consult the merchant or store manager regarding your options, that are:

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

Intended Audience

The audience for this document includes 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 Online Documentation (GOLD℠).

REVIEW AND FULLY UNDERSTAND THE MANUAL BEFORE BEGINNING THE UPGRADE OR INSTALLATION OF PASSPORT V12 FOR PHILLIPS 66.

Table of Contents

Related Documents

Document Number	Title	GOLD Library
MDE-4696	Ingenico® PIN Pad Kits (PA0379XXXXX and PA0380XXXXX) Installation Instructions	Passport
MDE-4826	Passport Card and Face-based Local Accounts Setup and Operations Manual	Passport
MDE-4834	Passport System Recovery Guide for Passport V8.02+	Passport
MDE-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-5213	VeriFone® MX915 PIN Pad Kit Installation Instructions	Passport
MDE-5218	MX915 PIN Pad to Passport Configuration Poster with RV042 Firewall Router	Passport
MDE-5266	What's New in Passport Version 11	Passport
MDE-5302	Passport V11.02 Upgrade Instructions	Passport
MDE-5303	Passport Software Installation Manual for V11.02 on PX60 Hardware Platforms	Passport
MDE-5332	Passport V11.02 Network Addendum for HPS-Dallas for Phillips 66	Passport
MDE-5470	What's New in Passport Version 12	Passport
MDE-5487	Passport EDH (HPS-Dallas) V10.24 Implementation Guide for PA-DSS V3.2	Passport

Abbreviations and Acronyms

Term	Description
AID	Application Identifier
ANSI	American National Standards Institute
ASC	Authorized Service Contractor
BOS	Back Office System
CAT5	Category 5
CD	Compact Disc
CRIND®	Card Reader in Dispenser
CWS	Cashier Workstation
DMZ	Demilitarized Zone
EDH	Enhanced Dispenser Hub
EMV	Europay®, MasterCard®, and Visa®
FDC	First Data Corporation
GDS	Gilbarco Deployment Service
GOLD	Gilbarco Online Documentation
MWS	Manager Workstation
PA-DSS	Payment Application Data Security Standard
PC	Personal Computer
PCATS	Petroleum Convenience Alliance for Technology Standards
PDL	Parameter Data Load or Parameter Download
PLU	Price Look Up
POS	Point of Sale
PPU	Price per Unit
RAS	Remote Access Service
SAF	Store and Forward
SDES	Single Data Encryption Standard
SR	System Recovery
SVC	Stored Value Card
TCP	Transmission Control Protocol
TDES	Triple Data Encryption Standard
TLS	Tank Level Sensor (Tank Layer Security)
UDP	User Datagram Protocol
UPC	Universal Product Code
WAN	Wide Area Network
WEX	Wright Express
W&M	Weights and Measures

Technical Support

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

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

To contact the Phillips 66 Help Desk, contact 1-800-426-3696.

Network Data Retention

Phillips 66 determines the length of time the Passport system must save network transaction details. The HPS-Dallas network transmits this value to the Passport system in the Table 30 download. This network setting is not editable on the Passport system. To determine the number of days Passport keeps network transactions for your store, refer to the value in the STORAGE LIMIT field within the Table 30 section of the Network Configuration Report.

In addition to meeting the Payment Application Data Security Standard (PA-DSS) compliance requirements, network data retention allows retailers to use the Backup Journals/Reports utility to save one full month of Passport system data on a single CD. For additional information on saving journals and reports to CD, refer to *MDE-5025 Passport V9+ System Reference Manual*.

What's New in Passport V12 at Phillips 66 Stores

WEX Merchant Bulletin No. 20171001-2

Starting with version 12, 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.
Host Base Discounts are now being applied on mobile transactions.

What's New in Passport V11.02 for Phillips 66 Stores

The following features have been updated or are new for Phillips 66 stores.

Network Connection Type

Stores that are configured for User Datagram Protocol (UDP) communication with the HPS-Dallas network are configured for TCP/IP after an upgrade to Passport V10 software. This change occurs automatically as part of the V8.03 to V11.01 upgrade. The store does not need to make any changes. Your ASC, will make the necessary adjustments on the Passport Firewall Router to complete the migration from UDP to TCP/IP communication.

In addition, as part of the migration to V11.02, Passport automatically enables Tank Level Sensor (TLS) encryption for the HPS-Dallas network connection. Phillips 66 requires all stores to move to TCP/IP with TLS encryption beginning with V11.02. For more information about **Global Network Parameters**, refer to "Site Configuration Programming" on page 7.

PDL Initiated Fuel Discounts

Beginning with V11.02 Service Pack P, Phillips 66 includes information in the network Parameter Download (PDL) that Passport uses to apply discounts to a transaction based on the card type the customer uses as tender. For each card type in the PDL, Phillips 66 includes the following information:

- Type of discount to apply (no discount, cents per gallon, percent per gallon, percent of total sale, cents per gallon and percent on non-fuel)
- Dollar amount per gallon discount
- Percent discount

To review the discounts that Passport automatically applies based on card type, review Table 40 of the Network Configuration Report.

Mandatory TCP/IP Network Connection Using TLS Encryption with HPS-Dallas

Also beginning with V11.02 with Service Pack P, Phillips 66 requires a TCP/IP connection using TLS encryption with the HPS-Dallas network. For more information about Global Network Parameters, refer to "Site Configuration Programming" on page 7.

Assigning Product Codes

Phillips 66 sends a list of valid fuel grade names and product codes to Passport in Table 60 of the network PDL. The ASC does not associate product codes to fuel grades, as the correct product code is already associated with the fuel grade names that can be selected. To configure the fuel grades (and their product codes) that Passport sends to the network in transaction messages, proceed as follows:

1. Select **MWS** > **Set Up** > **Forecourt** > **Forecourt Installation**.

2. From the Forecourt Installation screen, select **Set Up**. The Forecourt Installation configuration screen opens.

3. Select the **Grade** tab.

4. Select **Add** or highlight an existing Grade. Select the fuel grade name from the Name list. Passport uses the product code associated with the fuel grade name from the PDL when sending transactions to the HPS-Dallas network.

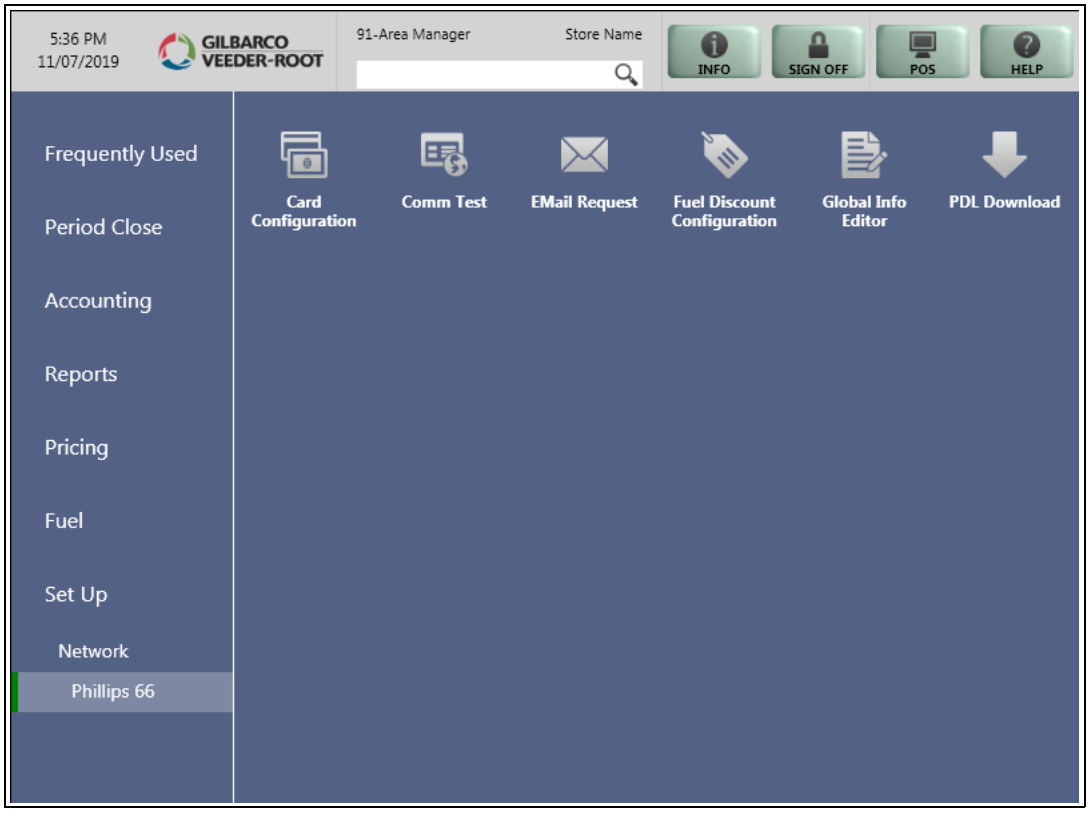
Site Configuration Programming

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

To program Site Configuration to communicate with the network, proceed as follows:

1 From the Manager Workstation (MWS) main menu, select **Set Up > Network > Phillips 66**. The Phillips 66 Network Configuration menu is displayed.

Figure 1: Phillips 66 Network Configuration Menu



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

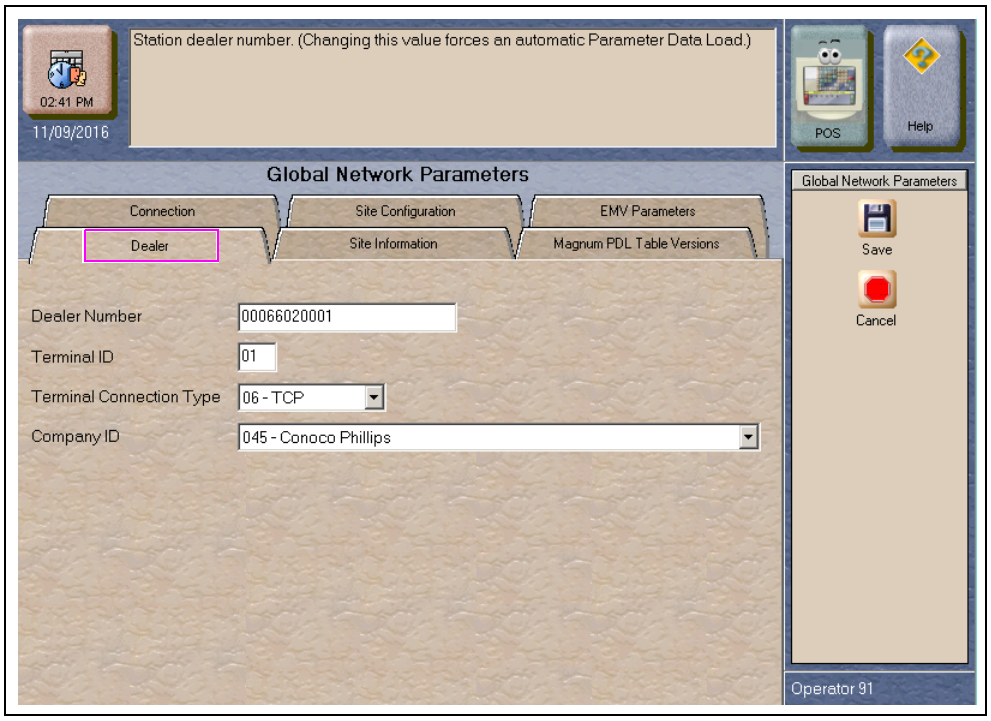
- Card Configuration
- Comm Test
- Email Request
- Fuel Discount Configuration
- Global Info Editor
- PDL Download

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

Dealer Tab

Figure 2 shows the Dealer tab on the Global Network Parameters screen.

Figure 2: Dealer Tab



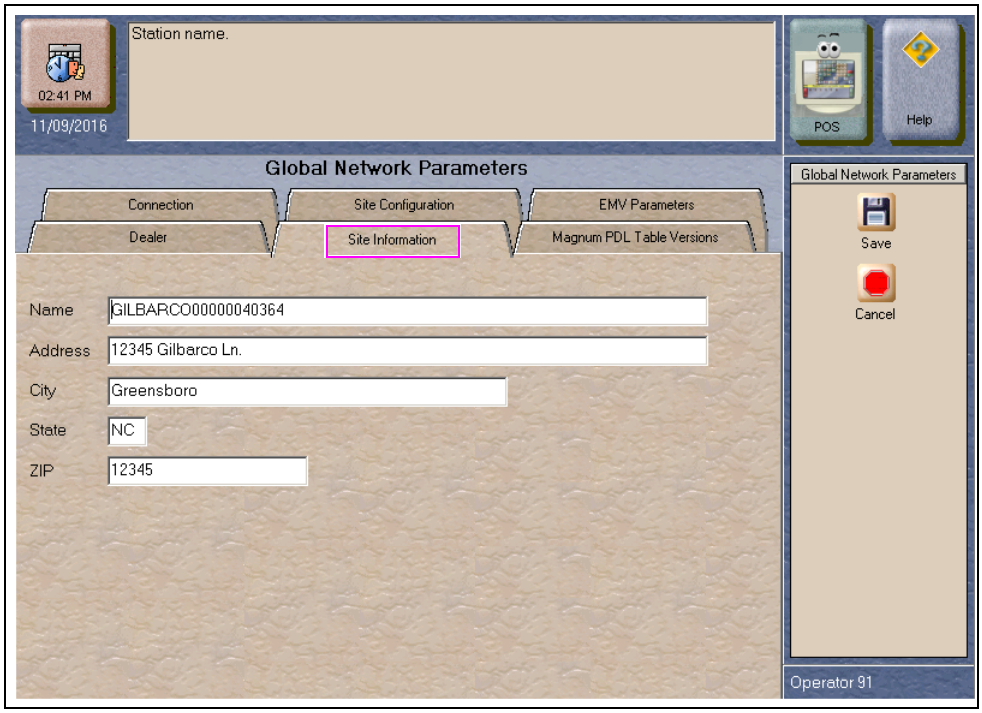
Fields on the Dealer Tab

Field	Description
Dealer Number	Eleven-digit number the HPS-Dallas network uses to identify the store. *Notes: 1) Enter the dealer number before receiving the initial PDL* *2) Change Dealer Number only after Store Close*
Terminal ID	Two-digit terminal identification number the HPS-Dallas network assigns to the store. The field can be modified only if all tills and the batches are closed. Ensure all batch files have been sent to the HPS-Dallas network before changing the value. Defaults to 01.
Terminal Connection Type	Specifies how the store connects to the network. Options are: • None • 02 - Dial • 06 - TCP/IP *Note: Beginning with V11.02 Service Pack P, all Phillips 66 stores must use Terminal Connection Type of 06 - TCP.*
Company ID	A three-digit number associated with the company handling transactions for the site. The HPS-Dallas network assigns the value. Options are: • 045 - Conoco Phillips 66 • 046 - Pacific Convenience and Fuels

Site Information Tab

After programming the Dealer tab, select the **Site Information** tab. Although the data on the **Site Information** tab comes from the HPS-Dallas PDL, the fields are editable. Contact the Phillips 66 Help Desk at 1-800-426-3696, before modifying fields on the **Site Information** tab to avoid the data being overwritten in a subsequent PDL.

Figure 3: Site Information Tab



Fields on the Site Information Tab

Field	Description
Name	Store name (up to 30 characters), which is displayed on network transaction receipts.
Address	Street address (up to 30 characters) for the store, which is displayed on network transaction receipts.
City	City (up to 20 characters) in which the store is located, which is displayed on network transaction receipts.
State	Two-character abbreviation for state where the store is located, which is displayed on network transaction receipts.
ZIP	ZIP Code assigned to the store, which is displayed on network transaction receipts.

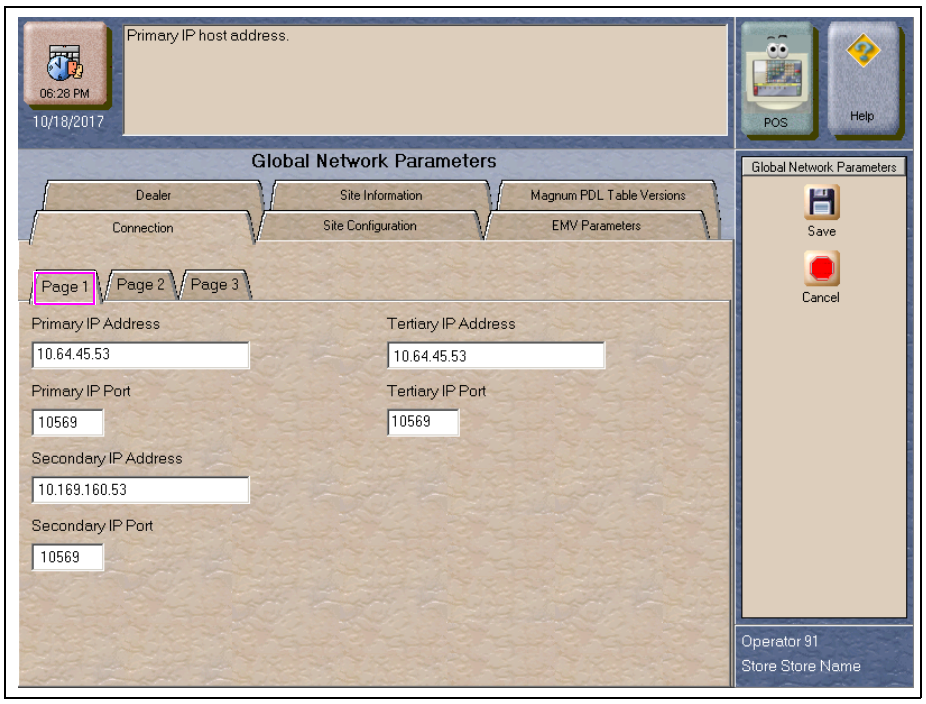
Connection Tab

After programming the **Site Information** tab, select the **Connection** tab. The Connection tab contains **Page 1**, **Page 2**, and **Page 3** tabs for programming network communication parameters, based on the Terminal Connection Type selected on the **Dealer** tab. Use the **Page 1** and **Page 3** tabs for configuring a TCP/IP connection. Use the **Page 2** tab for configuring a Dial connection.

Note: Beginning with V11.02 Service Pack P, all Phillips 66 sites must use TCP/IP connection with TLS encryption.

IMPORTANT INFORMATION
For stores using TCP/IP connection, contact the Phillips 66 Help Desk at 1-800-426-3696 to obtain IP addresses and ports.

Figure 4: Page 1 Tab - TCP/IP Connection Type

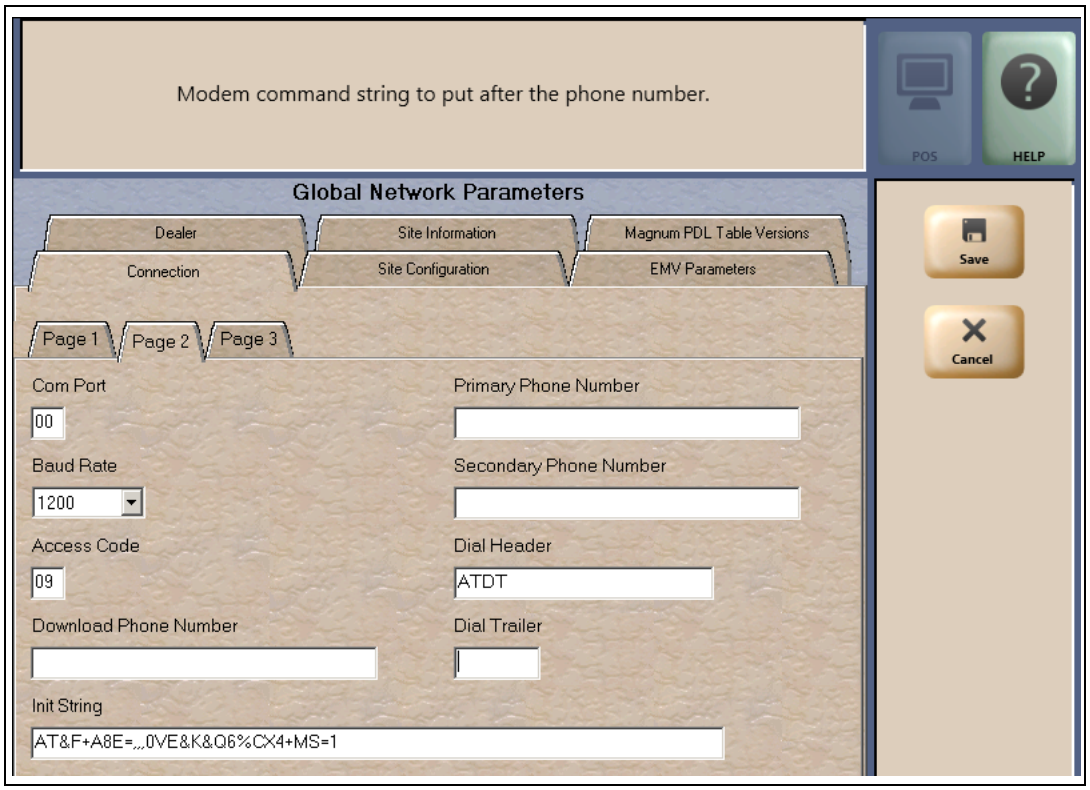


Fields on the Connection - Page 1 Tab

Field	Description
Primary IP Address	IP address Passport uses to exchange financial transaction messages with the HPS-Dallas network. HPS-Dallas may change the value in this field through PDL Download.
Primary IP Port	Port (up to 5 digits) Passport uses to exchange financial transaction messages with the HPS-Dallas network. Defaults to 10569.
Secondary IP Address	First alternate IP address Passport uses to exchange financial transaction messages with the HPS-Dallas network if the primary IP address and port fail. HPS-Dallas may change the value in this field through PDL Download.
Secondary IP Port	First alternate port Passport uses to exchange financial transaction messages with the HPS-Dallas network if the primary IP address and port fail. Defaults to 10569.
Tertiary IP Address	Second alternate IP address Passport uses to exchange financial transaction messages with the HPS-Dallas network. HPS-Dallas may change the value in this field through PDL Download.

Field	Description
Tertiary IP Port	Second alternate port Passport uses to exchange financial transaction messages with the HPS-Dallas network if the primary IP address and port fail. Defaults to 10569.

Figure 5: Page 2 Tab - Dial Connection Type

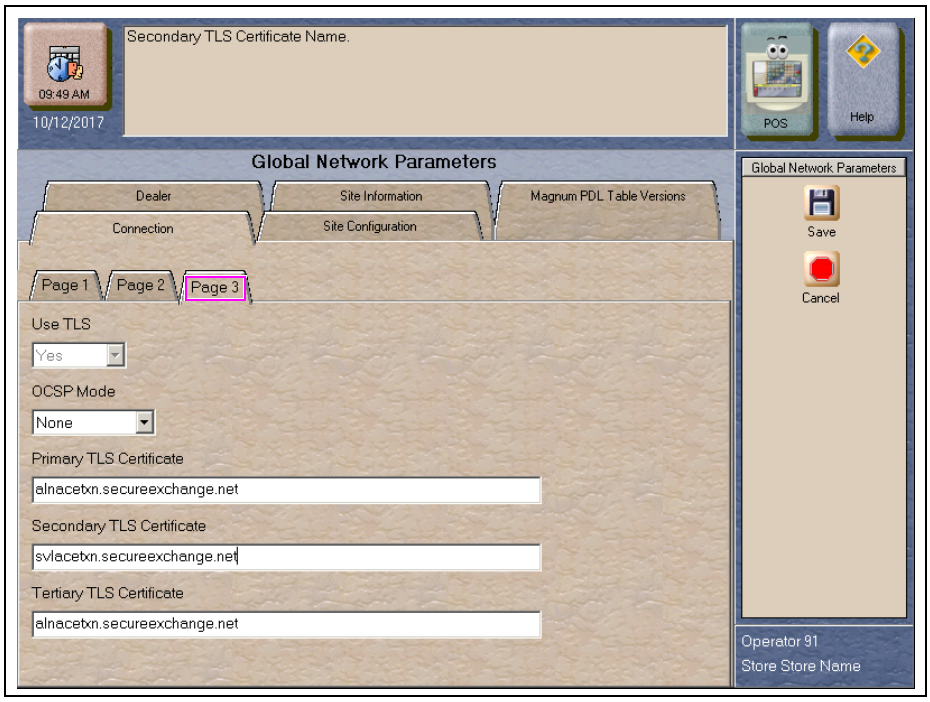


Fields on the Connection - Page 2 Tab

Field	Description
Com Port	Serial port number used by modem connection.
Baud Rate	Baud rate for the dial-up connection.
Access Code	Digits required for dial to get an outside line.
Download Phone Number	Phone number to get a table download. Automatically updated on download.
Init String	Initial string to send to the modem, prior to the phone number.
Primary Phone Number	First number to dial for transactions. Automatically updated on download.
Secondary Phone Number	Second number to dial for transactions. Automatically updated on download.
Dial Header	Modem command string to put before the phone number.
Dial Trailer	Modem command string to put after the phone number.

Note: Beginning with V11.02 Service Pack P, Dial connections are no longer valid for Phillips 66 stores.

Figure 6: Page 3 Tab - TCP/IP Connection Type



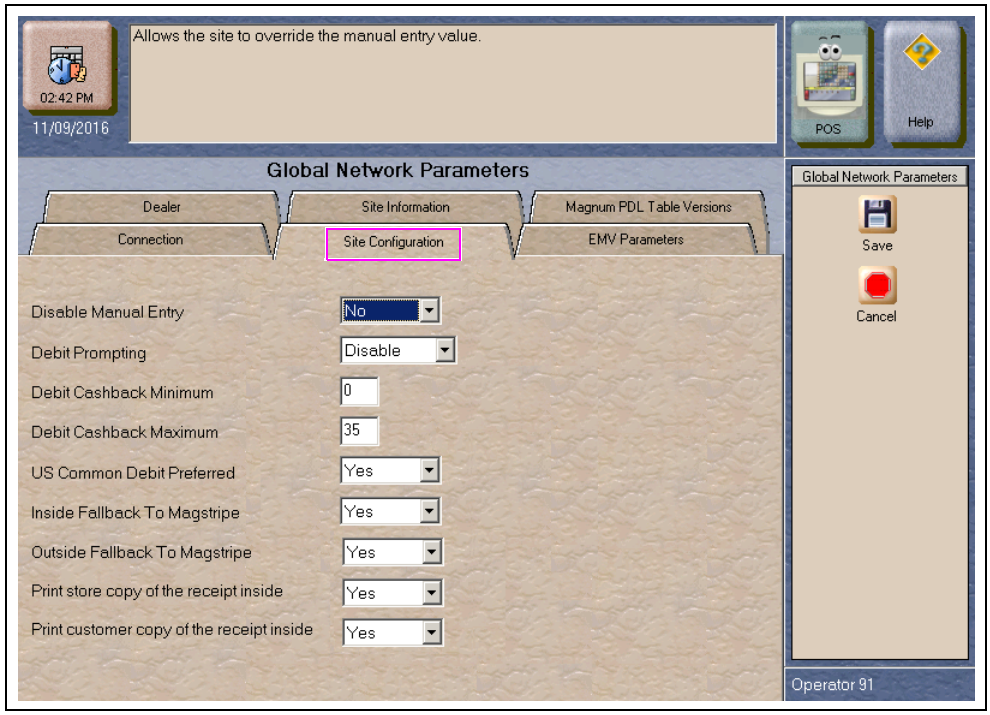
Fields on the Connection - Page 3 Tab

Field	Description
Use TLS	This field defaults to Yes and is not 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

Site Configuration Tab

After programming the Connection tab, select the **Site Configuration** tab. The Site Configuration tab allows the store to override manual entry and debit parameters received in the HPS-Dallas PDL.

Figure 7: Site Configuration Tab



Fields on the Site Configuration Tab

Field	Description
Disable Manual Entry	If set to Yes, allows the site to override the manual entry value received from the PDL.
Debit Prompting	Allows the site to disable whether the CRIND devices prompt the customer “Is this a debit card?” for dual use (Credit and Debit) cards.
Debit Cashback Minimum	Minimum dollar amount allowed for debit cash back.
Debit Cashback Maximum	Maximum dollar amount allowed for debit cash back.
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.

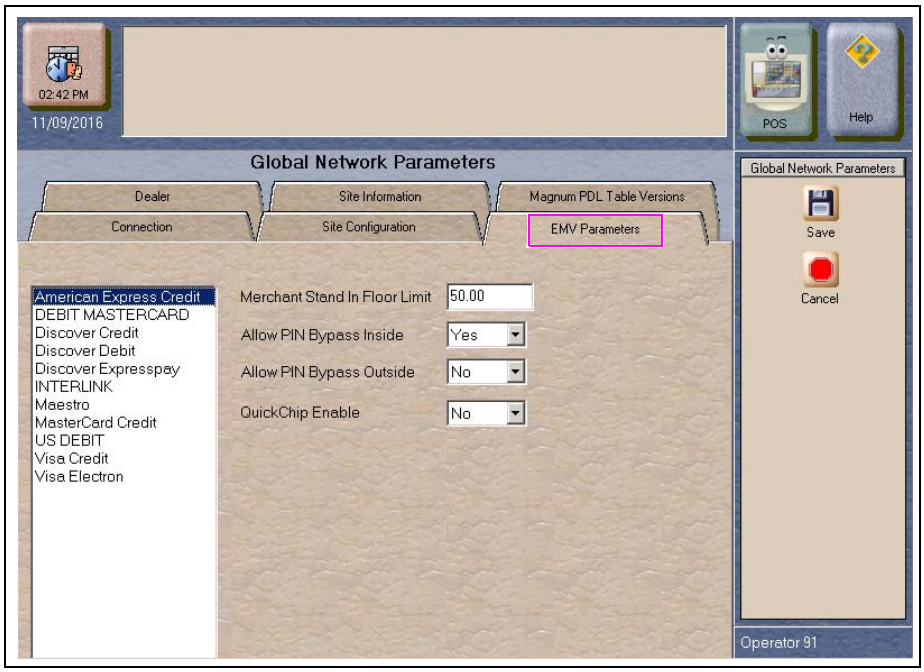
Field	Description
Outside Fallback to Magstripe	If set to No, when the customer inserts a chip card into the chip reader on the CRIND and a chip error occurs, Passport declines the card. If set to Yes, when the customer inserts a chip card into the chip reader on the CRIND and a chip error occurs, Passport 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.
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.

EMV Parameters Tab

The EMV Parameters tab provides information about the EMV parameters.

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.

Figure 8: EMV Parameters Tab



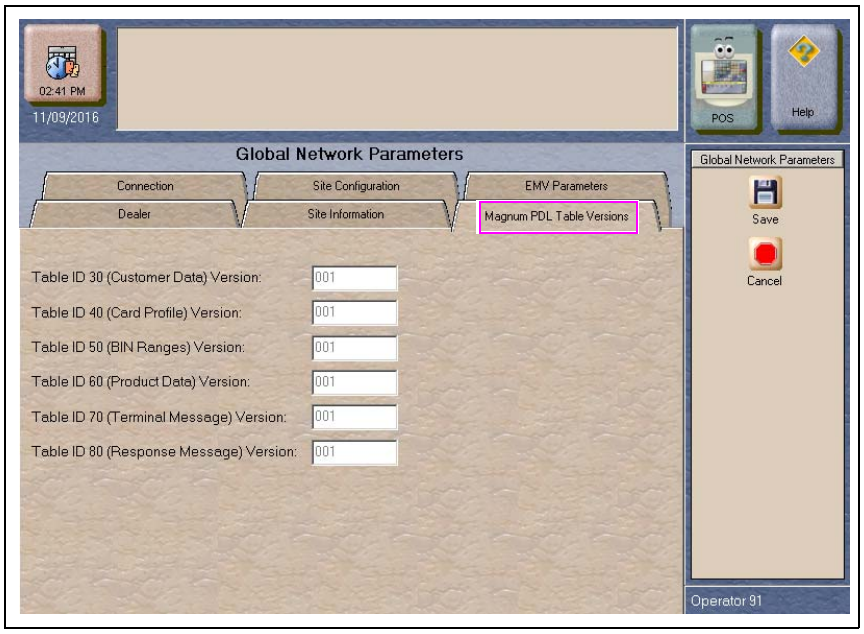
Fields on the EMV Parameters Tab

Field	Description
Merchant Stand In Floor Limit	Maximum transaction dollar amount for this EMV card AID the merchant will accept locally to SAF when the HPS-Dallas network is offline. Defaults to $0.00. This field is not editable for any debit AID. $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, the inside PIN Pad prompts the customer to enter the PIN, but allows the customer to press **ENTER** key on the PIN Pad without entering a PIN. If set to No and the EMV application requires PIN entry, the inside PIN Pad 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 the setting.*
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 the setting.*
QuickChip 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.

Magnum PDL Table Versions Tab

After completing all **Global Network Parameters** tabs, select **Save** to save the settings and exit from **Global Info Editor**. One additional tab is displayed within the Global Info Editor screens; however, the Magnum PDL Table Versions tab provides information about the currently existing Magnum PDL Table ID versions. These values are not editable.

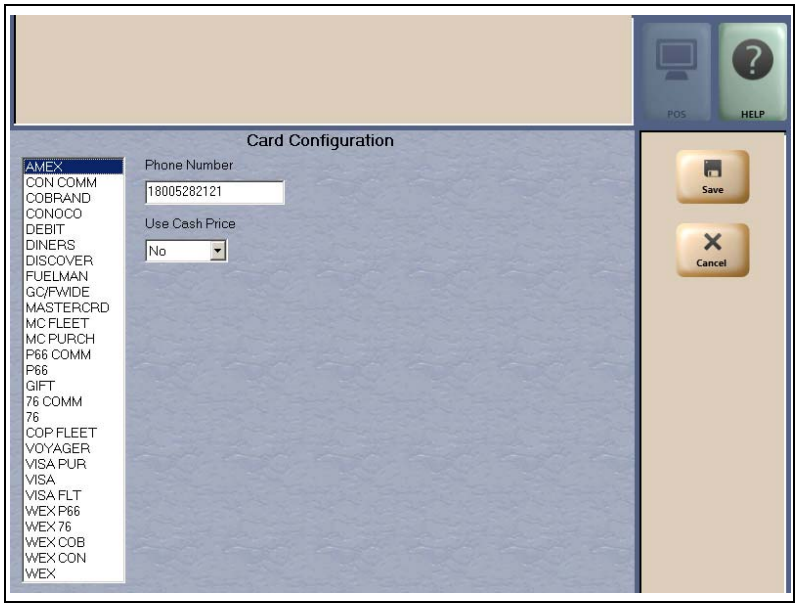
Figure 9: Magnum PDL Table Versions Tab



Programming Call for Auth Phone #s

To configure phone numbers that display when Passport invokes the Call for Authorization process, select **MWS** > **Set Up** > **Network** > **Phillips 66** > **Call for Auth #s**. Each card type that requires Call for Auth displays on the Call for Auth Phone #s screen, along with a field for programming the telephone number the cashier must dial.

Figure 10: Call For Auth Phone #s Screen



Field	Description
Phone Number	• Phone number used to call for authorization. • Enter only numbers.
Use Cash Price	Transactions with this card, use the cash price when buying fuel.

Default Phone Numbers

Card Type	Phone Number
American Express®	800-528-2121
Discover℠/Novus®	800-347-1111
MasterCard	800-622-3858
Phillips 66, Conoco, 76 Commercial	800-323-2952
Phillips 66, Conoco, 76 Fleet	800-767-1917
Phillips 66, Conoco, 76 MasterCard	800-622-3858
Phillips 66, Conoco, 76 Personal	800-323-2952
Visa	800-622-3858
Voyager® Universal Fleet	800-987-6589
Wright Express® (WEX) Universal Fleet	800-842-0071

Contact the Phillips 66 Help Desk at 1-800-426-3696 for assistance with other Call for Auth phone numbers.

Requesting PDL Download

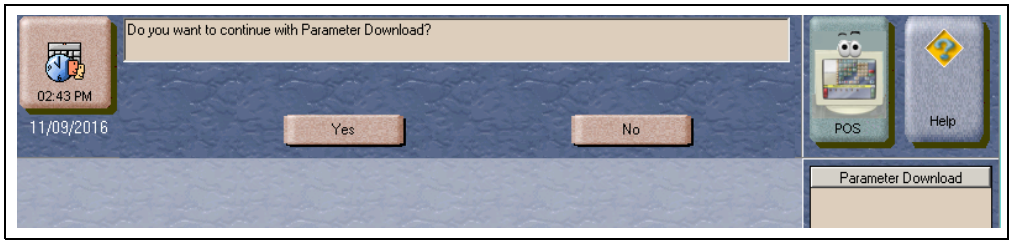
The PDL Download is a transfer of data from the HPS-Dallas network to Passport. A valid PDL contains card configuration information and is required for operation. You must request a PDL during system installation. Passport cannot process network transactions until it successfully receives a PDL from 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, contact the 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 Go to **MWS** > **Set Up** > **Network** > **Phillips 66** > **PDL Download**. The Passport prompts: "Do you want to continue with Parameter Download?"

Figure 11: PDL Download Prompt Screen



2 Select **No** to abandon the PDL Download request or select **Yes** to request the HPS-Dallas network for the PDL Download. Passport provides status of the PDL Download request on the MWS screen. 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.

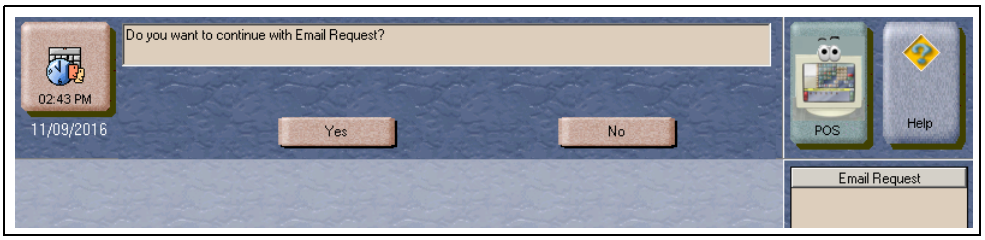
3 To review the PDL information sent from the network to Passport, view or print the Network Configuration Report.

Requesting Email

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

1 From **MWS** > **Set Up** > **Network** > **Phillips 66**, select **Email Request** to request e-mail from the HPS-Dallas network. The Email Request screen displays with the user prompt "Do you want to continue with Email Request?"

Figure 12: E-Mail Request Prompt



2 Select **Yes** to initiate an e-mail request. The Passport system displays status of the request. Select **No** to return to the Phillips 66 network screen.

Watch Dog Reboot Warning

To avoid a conflict between Watch Dog Reboot and the nightly 2:00AM Site Oversight message, program Watch Dog to occur at 2:30AM. For more information on changing the Watch Dog Reboot schedule, refer to *MDE-5025 Passport V9+ POS System Reference Manual.*

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 13: Network Journal Report Filter Screen

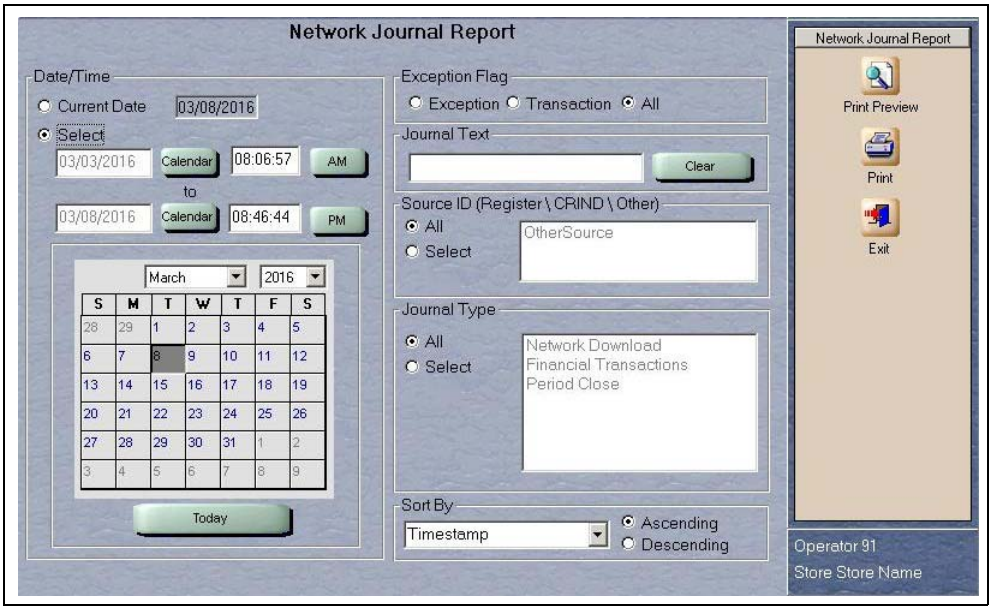
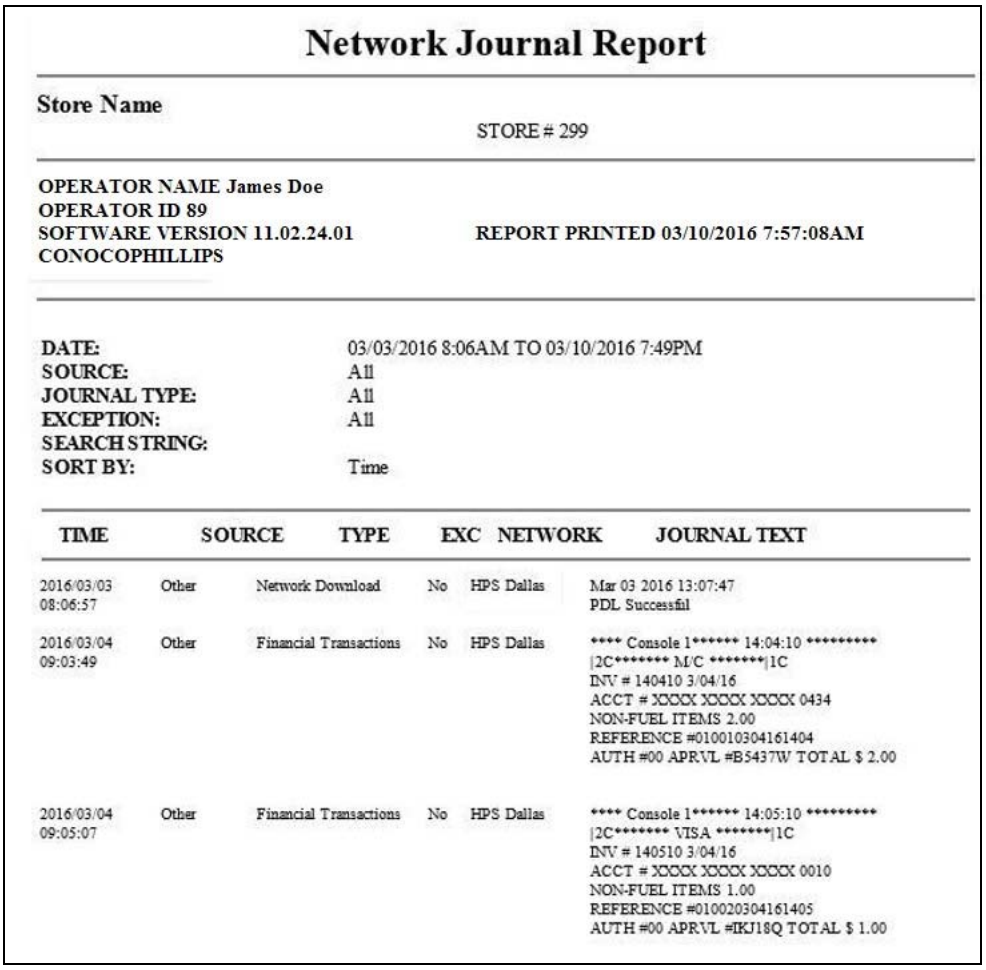


Figure 14: Network Journal Report Sample



Network Journal Report

Store Name

STORE # 299

OPERATOR NAME James Doe
OPERATOR ID 89
SOFTWARE VERSION 11.02.24.01 **REPORT PRINTED 03/10/2016 7:57:08AM**
CONOCOPHILLIPS

DATE:	03/03/2016 8:06AM TO 03/10/2016 7:49PM
SOURCE:	All
JOURNAL TYPE:	All
EXCEPTION:	All
SEARCH STRING:	
SORT BY:	Time

TIME	SOURCE	TYPE	EXC	NETWORK	JOURNAL TEXT
2016/03/03 08:06:57	Other	Network Download	No	HPS Dallas	Mar 03 2016 13:07:47 PDL Successful
2016/03/04 09:03:49	Other	Financial Transactions	No	HPS Dallas	**** Console 1****** 14:04:10 ********* |2C******* M/C *******|1C INV # 140410 3/04/16 ACCT # XXXX XXXX XXXX 0434 NON-FUEL ITEMS 2.00 REFERENCE #010010304161404 AUTH #00 APRVL #B5437W TOTAL $ 2.00
2016/03/04 09:05:07	Other	Financial Transactions	No	HPS Dallas	**** Console 1****** 14:05:10 ********* |2C******* VISA *******|1C INV # 140510 3/04/16 ACCT # XXXX XXXX XXXX 0010 NON-FUEL ITEMS 1.00 REFERENCE #010020304161405 AUTH #00 APRVL #IKJ18Q TOTAL $ 1.00

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 the time the report was printed.

Report Name	Shift Close	Store Close	Current	Secure
Batch Detail Report	✓	✓		✓
Batch Summary Report*		✓	✓	
Card Conflict Report			✓	✓
Day Batch Detail Report	✓	✓	✓	
Day Batch Summary Report	✓	✓	✓	
Day Summary Report		✓	✓	
Electronic Mail Report	✓			
EMV Chip Fallback Report		✓		
EMV Configuration Report			✓	
Fallback Detail Report*		✓	✓	✓
Gift Card Detail Report		✓		✓
Network Configuration Report			✓	
Network POS Events Report		✓		✓
POS Transaction Statistics Report		✓	✓	
Site Level Card Based Fuel Discounts			✓	
Unpaid Transactions Report				✓

**This report must 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-5487 Passport EDH (HPS-Dallas) V10.24 Implementation Guide for PA-DSS V3.2*.

Batch Detail Report

The Day Batch Detail report is available at Shift Close and Store Close. It contains all details necessary to reconstruct the transaction for the shift or day, including for the current batch. The Batch Status provides information on whether the batch is In Balance or Out of Balance. If a batch is in balance, Passport deletes all account number information pertaining to transactions within the batch. This report also contains a breakdown of batch totals by card category type, and card type, as well as prepaid card activations, deactivations, and recharges.

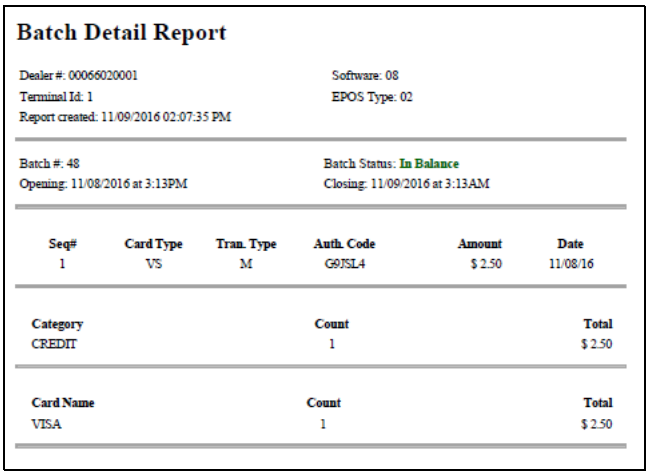
This report also contains a breakdown of batch totals by card category type, card type, and all prepaid card activations, deactivations, and recharges.

Definitions for Trans. Type Field Abbreviations

Abbreviation	Definition	Abbreviation	Definition
U	Unattended	C	Contactless
M	Manually entered	F	Fallback
D	Duplicate	R	Refund
S	Swiped	V	Void

Note: Multiple abbreviations may apply to a single transaction.

Figure 15: Batch Detail Report



Batch Detail Report

Dealer #: 00066020001
Terminal Id: 1
Report created: 11/09/2016 02:07:35 PM
Software: 08
EPOS Type: 02

Batch #: 48
Opening: 11/08/2016 at 3:13PM
Batch Status: In Balance
Closing: 11/09/2016 at 3:13AM

Seq#	Card Type	Tran. Type	Auth. Code	Amount	Date
1	VS	M	G9JSL4	$ 2.50	11/08/16

Category	Count	Total
CREDIT	1	$ 2.50

Card Name	Count	Total
VISA	1	$ 2.50

Day Batch Detail Report

This report provides similar information as the Batch Detail Report, except for a given day period.

Batch Summary Report

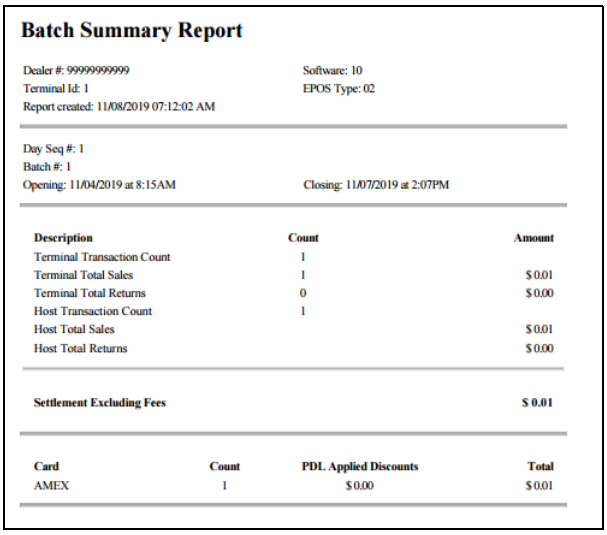
The Batch Summary Report provides information for the current batch. The information includes the category description, total count, and total amount:

- The FuelMan®/Gas Card category lists all FuelMan and Gas Card transactions in the batch.
- The Settlement Excluding Fees amount determines the settlement with the Customer. If the batch is out of balance, this line indicates “Out of Balance”.

  Host Total Sales
  + PDL Applied Discounts
  - Host Total Returns
  - FuelMan/Gas Card
  Settlement Excluding Fees

- The lines below Settlement Excluding Fees shows the dollar amount by card type. These lines display for each card type used in the batch.

Figure 16: Batch Summary Report



Batch Summary Report

Dealer #: 99999999999 Software: 10
Terminal Id: 1 EPOS Type: 02
Report created: 11/08/2019 07:12:02 AM

Day Seq #: 1
Batch #: 1
Opening: 11/04/2019 at 8:15AM Closing: 11/07/2019 at 2:07PM

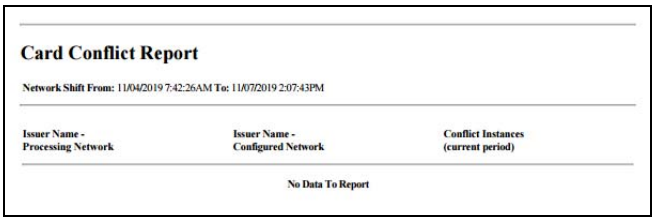
Description	Count	Amount
Terminal Transaction Count	1	
Terminal Total Sales	1	$ 0.01
Terminal Total Returns	0	$ 0.00
Host Transaction Count	1	
Host Total Sales		$ 0.01
Host Total Returns		$ 0.00
Settlement Excluding Fees		**$ 0.01**

Card	Count	PDL Applied Discounts	Total
AMEX	1	$ 0.00	$ 0.01

Card Conflict Report

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. The Card Conflict Report provides information on transactions affected by card conflicts.

Figure 17: Card Conflict Report



Card Conflict Report

Network Shift From: 11/04/2019 7:42:26AM To: 11/07/2019 2:07:43PM

Issuer Name - Processing Network	Issuer Name - Configured Network	Conflict Instances (current period)

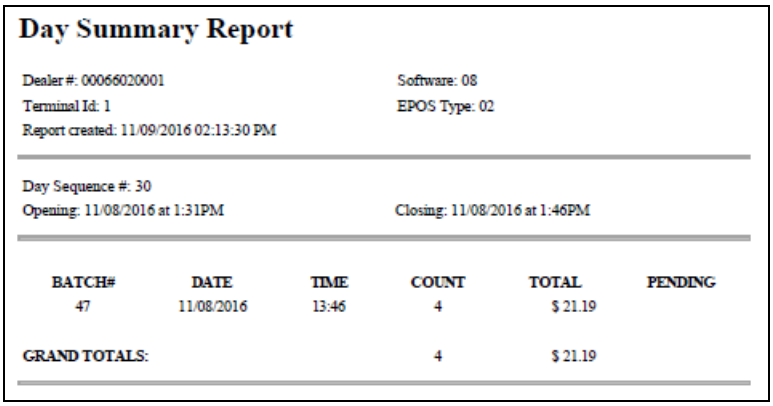
No Data To Report

Day Summary Report

This report is available for each POS day period and contains Network totals for the given day:

- The header includes the date and time of the POS day closure with which it is associated
- The report provides information for all batches with the associated day including batch number, date batch was closed, time batch was closed, transaction count, and batch transaction total

Figure 18: Day Summary Report



Day Summary Report

Dealer #: 00066020001 Software: 08
Terminal Id: 1 EPOS Type: 02
Report created: 11/09/2016 02:13:30 PM

Day Sequence #: 30
Opening: 11/08/2016 at 1:31PM Closing: 11/08/2016 at 1:46PM

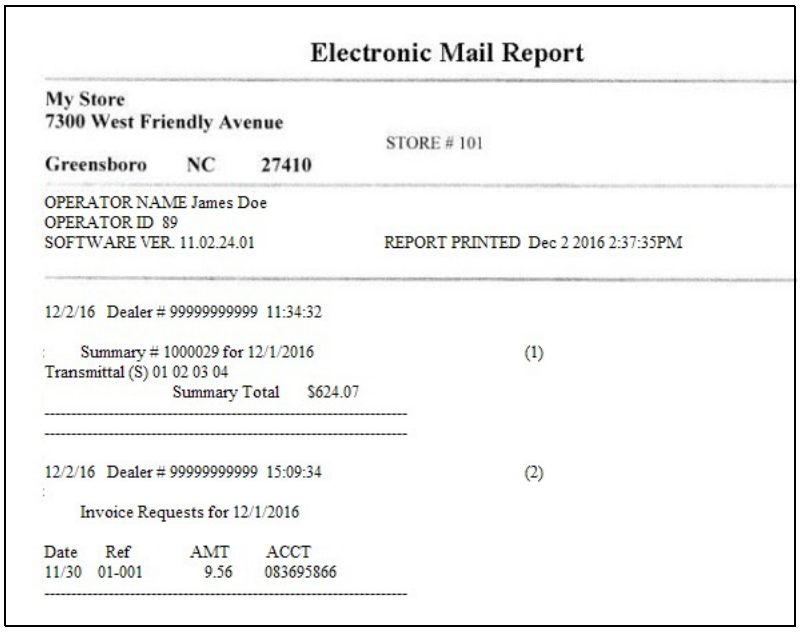
BATCH#	DATE	TIME	COUNT	TOTAL	PENDING
47	11/08/2016	13:46	4	$ 21.19	
GRAND TOTALS:			4	$ 21.19	

Electronic Mail Report

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

- Each mail message can be from 2-11 lines in length.
- When there is no mail to print the following message is displayed: ***No Mail available for current day***

Figure 19: Electronic Mail Report



Electronic Mail Report

My Store
7300 West Friendly Avenue
STORE # 101
Greensboro NC 27410

OPERATOR NAME James Doe
OPERATOR ID 89
SOFTWARE VER. 11.02.24.01 REPORT PRINTED Dec 2 2016 2:37:35PM

12/2/16 Dealer # 99999999999 11:34:32

Summary # 1000029 for 12/1/2016 (1)
Transmittal (S) 01 02 03 04
Summary Total $624.07

12/2/16 Dealer # 99999999999 15:09:34 (2)

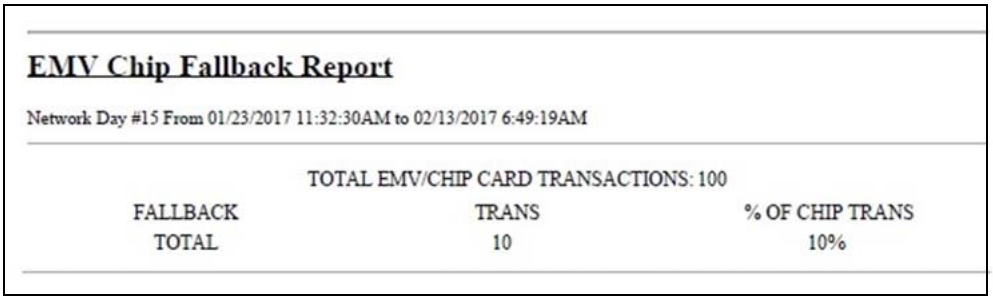
Invoice Requests for 12/1/2016

Date	Ref	AMT	ACCT
11/30	01-001	9.56	083695866

EMV Chip Fallback Report

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

Figure 20: 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 AID Passport supports, along with the fields programmed in the **MWS** > **Set Up** > **Network Menu** > **Phillips 66** > **Global Network Parameters** > **EMV Parameters** tab.

Figure 21: EMV Configuration Report

EMV Configuration Report

Report created: 11/09/2016 02:15:26 PM

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	5300n4	4.5.2-20160526
REGISTER 2	0467	1904
CRIND 2	EMV 02.09	30.5.0
CRIND 3	42.05.13	40.1.1
CRIND 4	42.05.14	40.1.1

Configuration Values

American Express Credit - Indoor
(AID: A00000002501)

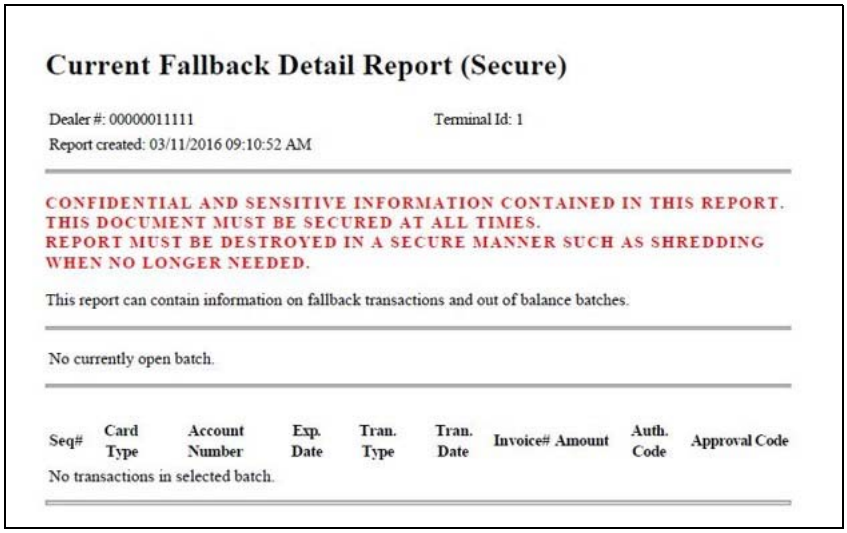
AID Activated:	2	Term Capability:	E0F8C8
Term Country:		Term Currency:	
Addl Capability:		Merch Cat Code:	5311
TAC Default:	0000000000	TAC Denial:	0000000000
TAC Online:	0000000000	Partial Select:	True
Trans Curr Exp:		Trans Cat Code:	R
App Ver Num Pri:	0001	PSPId:	24
Term Floor Lim:	0	Rand Sel Thresh:	0
Rand Sel Max%:	0	Rand Sel Target%:	0
AllowFallback:	True	AllowPINBypass:	False
Fallback expiry:	2099-12-31	Acquirer ID:	
Default DDOL:	9F3704	Default TDOL:	
Merchant stand-in floor limit:	99.99	Is debit Card:	False
Application Account Selection:	False	Trans Refer Currency Conv:	61000000
Terminal Risk Managment TTQ:		Transaction Types:	8000
Application Selection:	True	Card Type:	03
Quick Chip Enabled:	False		

Fallback Detail Report

The Fallback Detail Report provides information on all transactions in a batch, not only those transactions that occur in fallback (SAF) or for batches that close Out of Balance. The report is available on demand for the current batch, as well as for previous batches.

- The report contains the message: ***This report can contain information on fallback transactions and out of balance batches***.
- Information in the report includes the Batch Number, Sequence Number, Card Type, Transaction Type (as defined in the Batch Detail Report), Transaction Amount, Invoice Number, and an Out of Balance indicator.
- Host refusals are not included on this report.
- The non-secure version of the report uses the encryption algorithm defined in the Phillips 66 EPOS Payment Interface Addendum to encrypt account numbers and expiration dates.
- The secure version of the report prints the account number and expiration date unencrypted. To view or print the secure version of the report requires entry of the Secure Report Password. In this situation, the report prints the following message in the header: **Confidential and sensitive information contained in this report. This document must be secured at all times. Report must be destroyed in a secure manner such as shredding when no longer needed**.

Figure 22: Fallback Detail Report



Current Fallback Detail Report (Secure)

Dealer #: 00000011111 Terminal Id: 1
Report created: 03/11/2016 09:10:52 AM

CONFIDENTIAL AND SENSITIVE INFORMATION CONTAINED IN THIS REPORT.
THIS DOCUMENT MUST BE SECURED AT ALL TIMES.
REPORT MUST BE DESTROYED IN A SECURE MANNER SUCH AS SHREDDING WHEN NO LONGER NEEDED.

This report can contain information on fallback transactions and out of balance batches.

No currently open batch.

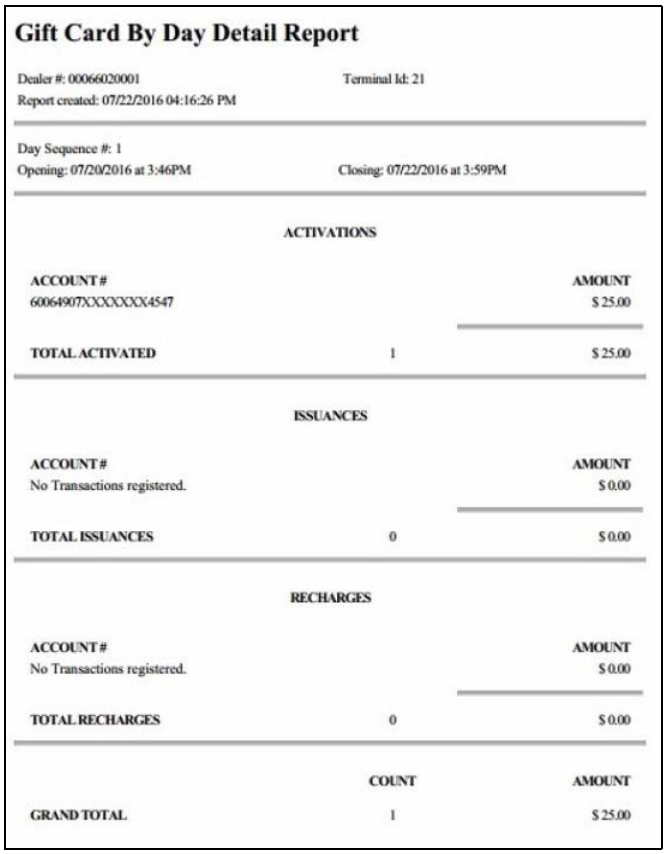
Seq#	Card Type	Account Number	Exp. Date	Tran. Type	Tran. Date	Invoice#	Amount	Auth. Code	Approval Code

No transactions in selected batch.

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 By Day Detail Report

Dealer #: 00066020001 Terminal Id: 21
Report created: 07/22/2016 04:16:26 PM

Day Sequence #: 1
Opening: 07/20/2016 at 3:46PM Closing: 07/22/2016 at 3:59PM

ACTIVATIONS

ACCOUNT #		AMOUNT
60064907XXXXXXX4547		$ 25.00
TOTAL ACTIVATED	1	$ 25.00

ISSUANCES

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

RECHARGES

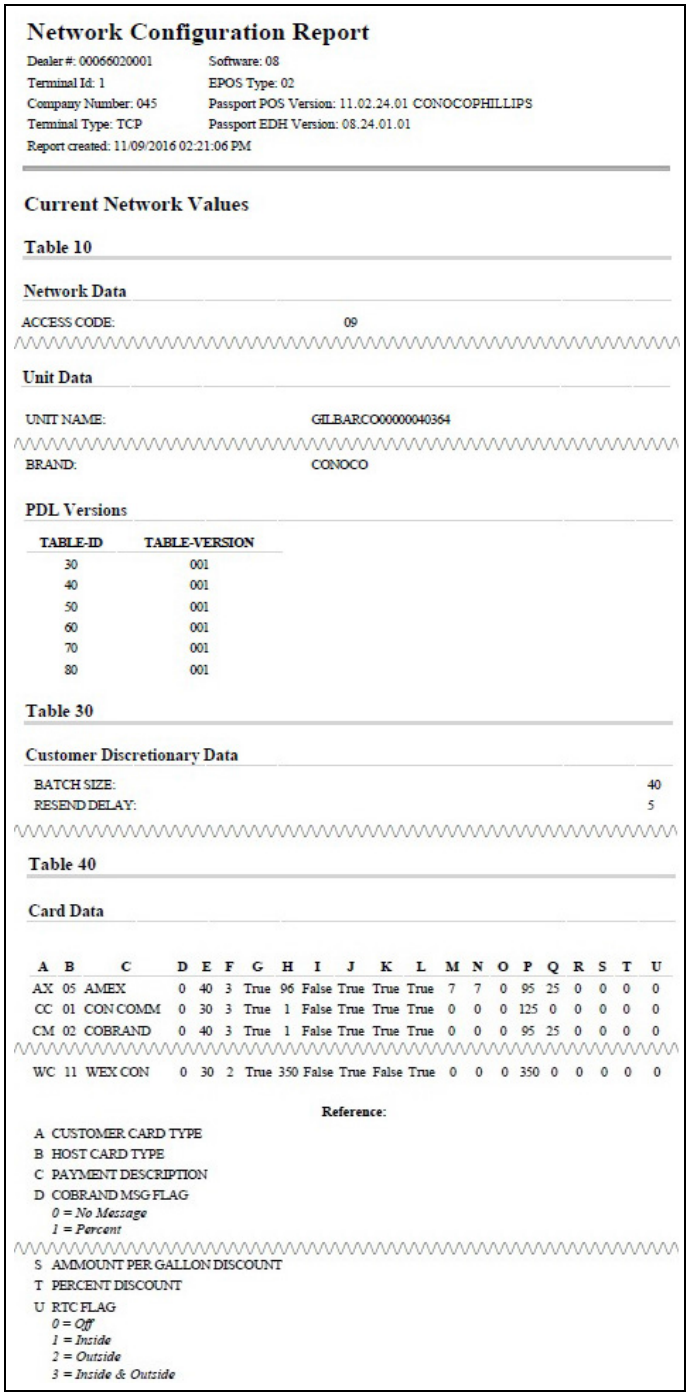
ACCOUNT #		AMOUNT
No Transactions registered.		$ 0.00
TOTAL RECHARGES	0	$ 0.00

	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 Passport received from the HPS-Dallas network PDL Download and programmed in **MWS** > **Set Up** > **Network** > **Phillips 66** > **Global Info Editor**. This report may contain information regarding host discounting parameters, as well.

Figure 24: Network Configuration Report Sample - Page 1



Network Configuration Report

Dealer #: 00066020001 Software: 08
Terminal Id: 1 EPOS Type: 02
Company Number: 045 Passport POS Version: 11.02.24.01 CONOCOPHILLIPS
Terminal Type: TCP Passport EDH Version: 08.24.01.01
Report created: 11/09/2016 02:21:06 PM

Current Network Values

Table 10

Network Data

ACCESS CODE: 09

Unit Data

UNIT NAME: GILBARCO00000040364
BRAND: CONOCO

PDL Versions

TABLE-ID	TABLE-VERSION
30	001
40	001
50	001
60	001
70	001
80	001

Table 30

Customer Discretionary Data

BATCH SIZE: 40
RESEND DELAY: 5

Table 40

Card Data

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
AX	05	AMEX	0	40	3	True	96	False	True	True	True	7	7	0	95	25	0	0	0	0
CC	01	CON COMM	0	30	3	True	1	False	True	True	True	0	0	0	125	0	0	0	0	0
CM	02	COBRAND	0	40	3	True	1	False	True	True	True	0	0	0	95	25	0	0	0	0
WC	11	WEX CON	0	30	2	True	350	False	True	False	True	0	0	0	350	0	0	0	0	0

Reference:

A CUSTOMER CARD TYPE
B HOST CARD TYPE
C PAYMENT DESCRIPTION
D COBRAND MSG FLAG
0 = No Message
1 = Percent
S AMMOUNT PER GALLON DISCOUNT
T PERCENT DISCOUNT
U RTC FLAG
0 = Off
1 = Inside
2 = Outside
3 = Inside & Outside

Figure 25: Network Configuration Report Sample - Page 2

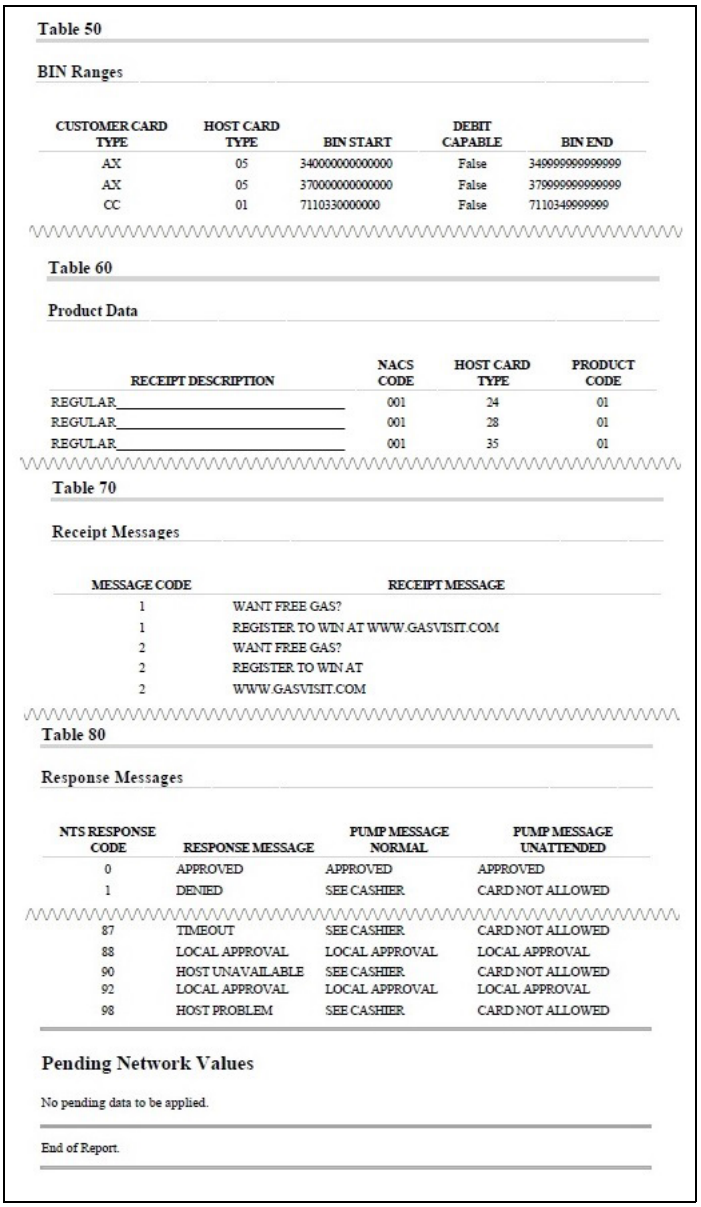


Table 50

BIN Ranges

CUSTOMER CARD TYPE	HOST CARD TYPE	BIN START	DEBIT CAPABLE	BIN END
AX	05	340000000000000	False	349999999999999
AX	05	370000000000000	False	379999999999999
CC	01	7110330000000	False	7110349999999

Table 60

Product Data

RECEIPT DESCRIPTION	NACS CODE	HOST CARD TYPE	PRODUCT CODE
REGULAR	001	24	01
REGULAR	001	28	01
REGULAR	001	35	01

Table 70

Receipt Messages

MESSAGE CODE	RECEIPT MESSAGE
1	WANT FREE GAS?
1	REGISTER TO WIN AT WWW.GASVISIT.COM
2	WANT FREE GAS?
2	REGISTER TO WIN AT
2	WWW.GASVISIT.COM

Table 80

Response Messages

NTS RESPONSE CODE	RESPONSE MESSAGE	PUMP MESSAGE NORMAL	PUMP MESSAGE UNATTENDED
0	APPROVED	APPROVED	APPROVED
1	DENIED	SEE CASHIER	CARD NOT ALLOWED
87	TIMEOUT	SEE CASHIER	CARD NOT ALLOWED
88	LOCAL APPROVAL	LOCAL APPROVAL	LOCAL APPROVAL
90	HOST UNAVAILABLE	SEE CASHIER	CARD NOT ALLOWED
92	LOCAL APPROVAL	LOCAL APPROVAL	LOCAL APPROVAL
98	HOST PROBLEM	SEE CASHIER	CARD NOT ALLOWED

Pending Network Values

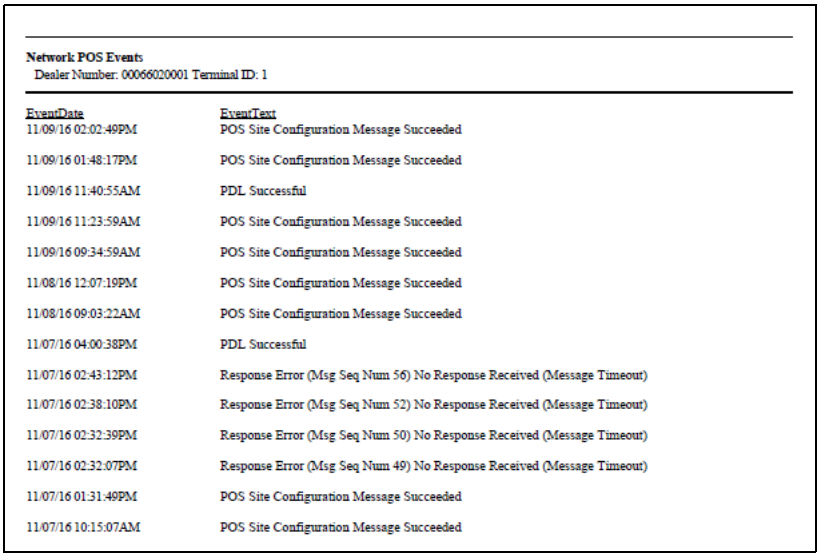
No pending data to be applied.

End of Report.

Network POS Events Report

The Network POS Events Report provides information on the most recent 250 messages between Passport and the HPS-Dallas network.

Figure 26: Network POS Events Report



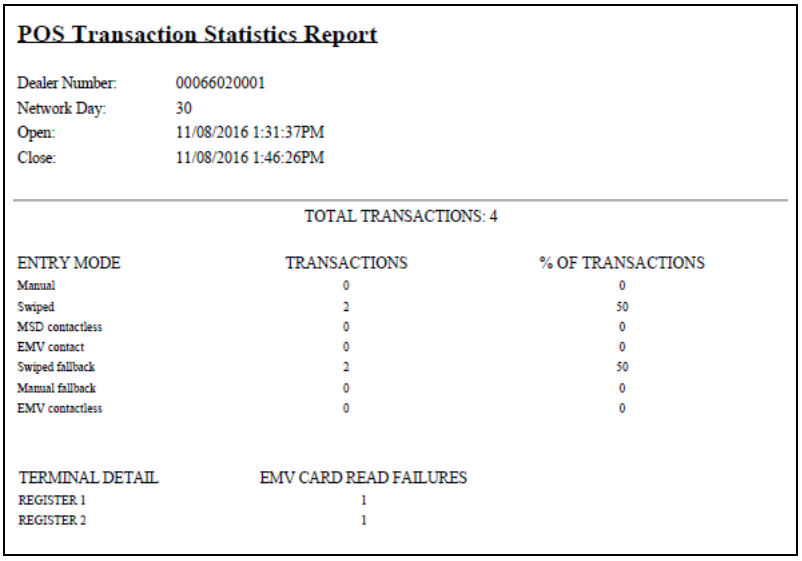
Network POS Events
Dealer Number: 00066020001 Terminal ID: 1

EventDate	EventText
11/09/16 02:02:49PM	POS Site Configuration Message Succeeded
11/09/16 01:48:17PM	POS Site Configuration Message Succeeded
11/09/16 11:40:55AM	PDL Successful
11/09/16 11:23:59AM	POS Site Configuration Message Succeeded
11/09/16 09:34:59AM	POS Site Configuration Message Succeeded
11/08/16 12:07:19PM	POS Site Configuration Message Succeeded
11/08/16 09:03:22AM	POS Site Configuration Message Succeeded
11/07/16 04:00:38PM	PDL Successful
11/07/16 02:43:12PM	Response Error (Msg Seq Num 56) No Response Received (Message Timeout)
11/07/16 02:38:10PM	Response Error (Msg Seq Num 52) No Response Received (Message Timeout)
11/07/16 02:32:39PM	Response Error (Msg Seq Num 50) No Response Received (Message Timeout)
11/07/16 02:32:07PM	Response Error (Msg Seq Num 49) No Response Received (Message Timeout)
11/07/16 01:31:49PM	POS Site Configuration Message Succeeded
11/07/16 10:15:07AM	POS Site Configuration Message Succeeded

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 27: POS Transaction Statistics Report



POS Transaction Statistics Report

Dealer Number: 00066020001
Network Day: 30
Open: 11/08/2016 1:31:37PM
Close: 11/08/2016 1:46:26PM

TOTAL TRANSACTIONS: 4

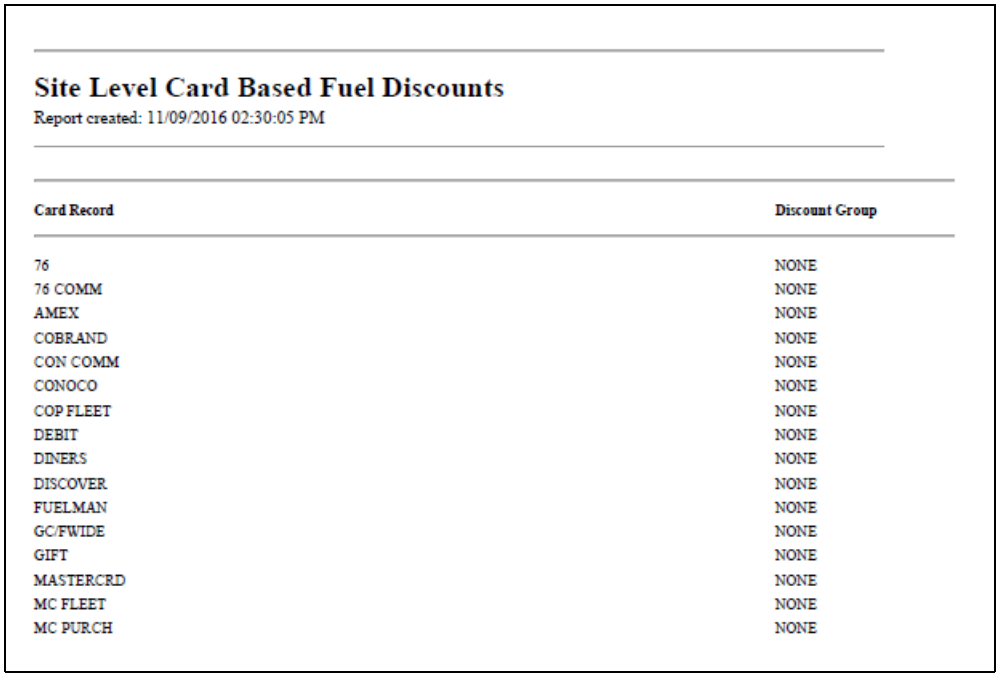
ENTRY MODE	TRANSACTIONS	% OF TRANSACTIONS
Manual	0	0
Swiped	2	50
MSD contactless	0	0
EMV contact	0	0
Swiped fallback	2	50
Manual fallback	0	0
EMV contactless	0	0

TERMINAL DETAIL	EMV CARD READ FAILURES
REGISTER 1	1
REGISTER 2	1

Site Level Card Based Fuel Discounts

This report provides information on the fuel discounts by card type configured in **MWS** > **Set Up** > **Network Menu** > **Phillips 66** > **Fuel Discount Configuration**. It lists each card type the network accepts, and the Fuel Discount Group assigned to the card type, or NONE if the card type has no discount configured.

Figure 28: Site Level Card Based Fuel Discounts Report



Site Level Card Based Fuel Discounts

Report created: 11/09/2016 02:30:05 PM

Card Record	Discount Group
76	NONE
76 COMM	NONE
AMEX	NONE
COBRAND	NONE
CON COMM	NONE
CONOCO	NONE
COP FLEET	NONE
DEBIT	NONE
DINERS	NONE
DISCOVER	NONE
FUELMAN	NONE
GC/FWIDE	NONE
GIFT	NONE
MASTERCRD	NONE
MC FLEET	NONE
MC PURCH	NONE

Unpaid Transactions Report

The Unpaid Transactions Report contains information on transactions initiated through the HPS Dallas network but declined at completion during the current open network day. This report consists of two sections: detail lines (two lines for each transaction) and summary transaction totals.

Figure 29: Unpaid Transaction Report

Unpaid Transactions Report (Secure)

Dealer #: 00066020001 Software: 07
Terminal Id: 1 EPOS Type: 02
Report created: 10/08/2017 04:14:03 AM

CONFIDENTIAL AND SENSITIVE INFORMATION CONTAINED IN THIS REPORT.
THIS DOCUMENT MUST BE SECURED AT ALL TIMES.
REPORT MUST BE DESTROYED IN A SECURE MANNER SUCH AS SHREDDING
WHEN NO LONGER NEEDED.

Day Sequence #: 15
Opening: 10/08/2015 at 4:08AM Closing: 10/08/2015 at 4:10AM

Batch #: 4 Batch Status: In Balance
Opening: 10/08/2015 at 4:08AM Closing: 10/08/2015 at 4:10AM

Seq#	Card Type	Account Number	Exp. Date	Tran. Type	Tran. Date	Invoice#	Amount	Auth. Code	Approval Code
1	MC	88PDD876LGM60328	46/PM	F	10/08/2015	040831	$5.00		

CWS Network Functions

The Network Functions screen contains the Network Status window and the Network Functions buttons. On this screen, you may view the Network Status and access the following tools:

- Batch Close
- Balance Request
- E-mail

Accessing Network Functions

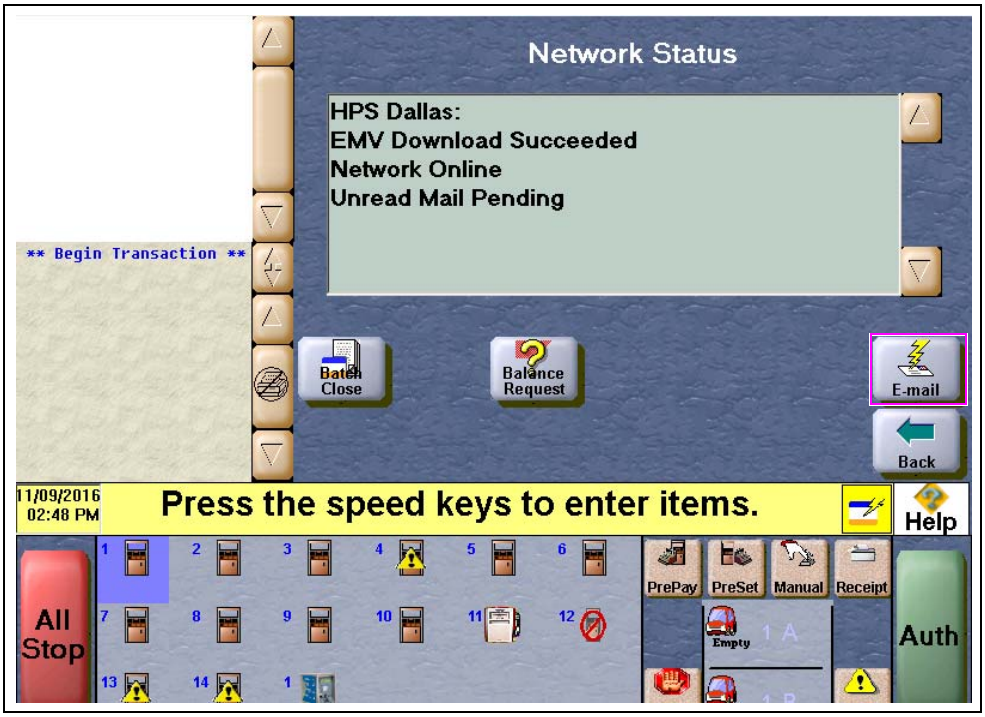
You can access this screen in one of the following ways:

- Select the **Network Status Indicator** when it is displayed on the message bar (for more information, refer to "Checking the Network Status" on page 36).
- On the Cashier Workstation (CWS) idle screen, select **More** > **Network Functions**.

Figure 30: Network Functions Button

With either action, the Network Status screen opens.

Figure 31: 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 screen allows you to view a record of network events such as communication errors that occurred. Each network event is assigned a severity rating (low, medium, or high). When a new event occurs and has been added to the list, the **Network Status** button is also updated. The color of the Network Status button indicates the severity of the rating of the event.

Color	Severity
Green	Low
Yellow	Medium
Red	High

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

The following table lists some of the network messages that may be displayed:

Situation	Status Indicator Color	Display Time
Passport successfully receives a Magnum PDL.	Green (low rating)	The status indicator is green and the “PDL Successful” message displays for one hour.
Intermittent failures - the first or second attempt.	Yellow (medium rating)	The status indicator color remains yellow and the “PDL Unavailable, Will Retry in 30 Minutes” message displays until the next attempt. After 3 failures, the Passport system moves to red.
End failures - the site’s first or original PDL fails, or there is a failure on the third attempt.	Red (high rating)	The status indicator color remains red and the “PDL Unavailable After 3rd Attempt, contact Network Help Desk” message displays until the problem is fixed and Passport receives a successful Magnum PDL.

Performing Batch Close

A Network Batch Close may occur automatically after a certain number of transactions. You also may perform a Batch Close at any time outside a transaction by selecting the **Batch Close** button. The following message is displayed on the yellow message bar: **Processing Batch Close**. **Please Wait**.

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 Request**.
2. Swipe the Cash Card.
3. The balance is displayed and the Passport system prints a customer receipt with the balance amount.

Receiving E-mail from the CWS

The Passport system notifies you when it receives an electronic message from the HPS-Dallas network. The Passport system saves all e-mails for 60 days.
Note: You can only receive electronic mail.

To retrieve electronic mail, proceed as follows:

1. On the **Network Functions** screen, select **E-mail**. The following prompt is displayed: **Retrieve all of today’s mail?**
2. Select **Yes** to retrieve all of the current day’s mail. Select **No** to retrieve only the unread mail. The mail prints on the receipt printer.

Frequently Asked Questions

Q1: I think the Passport system is not connected to the HPS-Dallas network. What should I do?

A1: 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** > **Set Up** > **Network** > **Phillips 66** > **Global Info Editor** > **Connection** > **Page 2** tab. If the phone numbers are not correct, contact the Phillips 66 Help Desk at 1-800-426-3696 for assistance.

Appendix A: Network Events 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 HPS-Dallas Help Desk and ask that the PDL be re-sent. 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	This message indicates that 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	This message indicates that 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: Programming Passport for the BOS

IMPORTANT INFORMATION

All WAN and Back Office PC IP addresses are unique for each site. Before you begin the procedure, you must read and understand the following steps for each site. Do not program an IP address from another site. When making network changes that affect the BOS, contact the owner or manager two days before the changes are implemented to allow store management time to notify the Back Office vendor.

Phillips 66 allows the BOS to interface to Passport through one of two broadband environments:

- LinkSafe 1.0 with access through the FortiGate® DMZ Port
- LinkSafe 2.0 with access through FortiGate Port 3

The following instructions cover both environments, using the term “FortiGate Port”

To set up Back Office, proceed as follows:

1. Contact the Phillips 66 Help Desk at 1-800-426-3696 to request the store’s FortiGate Port IP Address. Be prepared to provide the Help Desk agent with the store’s MNSP Firewall Router WAN IP Address and Dealer Number programmed on the **MWS** > **Set Up** > **Network** > **Phillips 66** > **Global Info Editor** > **Dealer** tab.

2. Add 1 to the value of the fourth octet of the FortiGate IP Address to derive the IP Address to use for the BOS PC. For instance, if the IP Address that the agent provides is 172.20.164.129, then the IP Address for the BOS PC is 172.20.164.130.

3. Plug the Back Office PC into the FortiGate port using a standard CAT5 cable (not a crossover cable).

4. Configure the Network Interface Card (NIC) for the BOS PC. In a dual NIC setup, the second network card is no longer supported and should be removed.
   - Single NIC (not connected to the Internet): use the FortiGate IP Address as the BOS PC Default Gateway.
   - Ensure that the IP settings for the network card are configured as provided by the Managed Network Service Provider (MNSP) vendor.

5. From the desktop of the Back Office PC, select **Start** > **Run** and type **ncpa.cpl** to access the Network Connections.

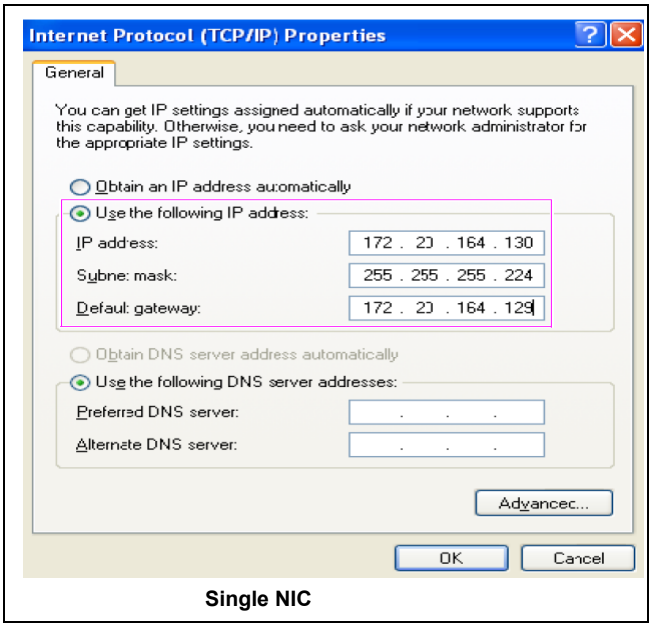
6. Right-click and select **Properties**.

7. From the **General** tab under “This connection uses following items”, scroll the menu and select **Internet Protocol (TCP/IP)**.

8. Select **Properties**.

9 From the **General** tab under **Internet Protocol (TCP/IP) Properties**, select the **Use the following IP address** option and type the values for the **IP address**, **Subnet mask**, and **Default gateway** fields (see Figure 32).

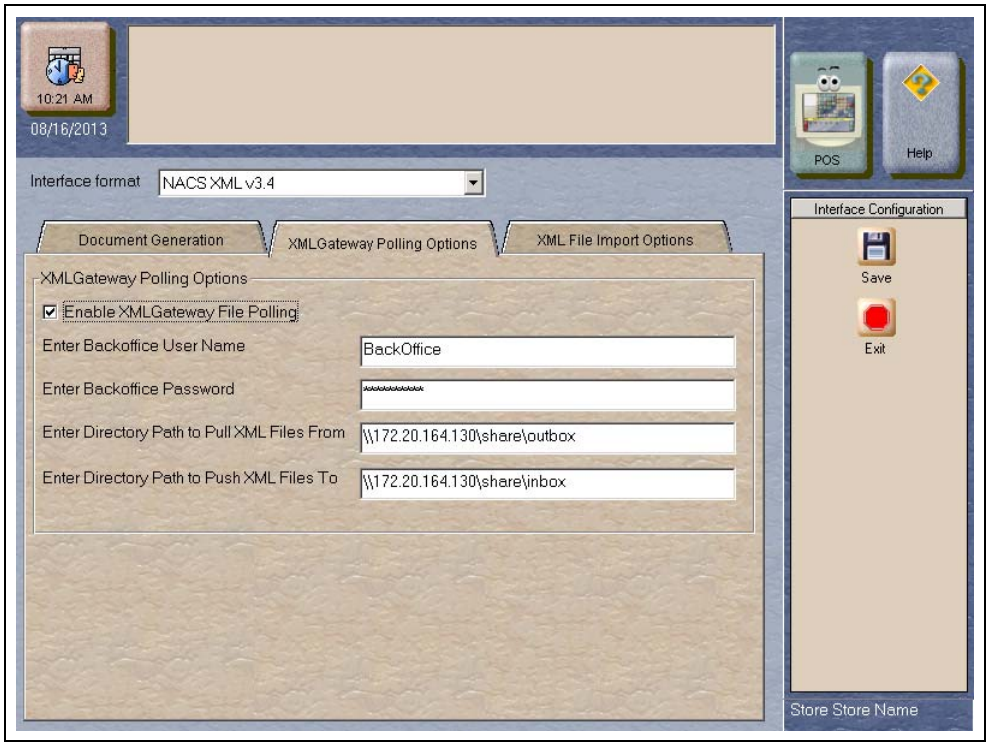
Figure 32: Single NIC - Sample Only



Single NIC

10 For a BOS that requires Passport to manage pushing sales data files and pulling price book files reconfigure the BOS IP Address in the Pull and Push paths on the **MWS** > **Set Up** > **Store** > **Back Office** > **Back Office Interface** > **XMLGateway Polling Options** fields.

Figure 33: XMLGateway Polling Options



The directory path must include the specific IP address of the Back Office (For example, 172.20.164.130). Ensure you do not change the remaining values in the path names.

11 For a BOS that manages pushing price book files and pulling sales date files, proceed as follows:

a Contact the MNSP vendor to ensure that the Firewall Router Access Rule settings are correctly configured for the Back Office software to communicate with the Passport Server.

b Change the Back Office drive mapping for all drives mapped to the Passport server from 10.5.60.1 to the Passport Server IP of 10.5.48.2. When the Back Office PC prompts for User Name and Password, enter **BackOffice** as the User Name and **BackOffice** as the Password.

Note: Contact the Back Office vendor for instructions to change the mapped drives, as they may prefer to connect to the Back Office PC to make these changes.

Appendix C: Upgrading to Passport V12

This section provides Phillips 66-specific information to the ASC for upgrading to Passport **V12**.

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

- Ensure that all dispenser software and firmware meet applicable requirements to support loyalty and other fuel discounting functionality, including support of $0.000 PPU.
- Print the **Network Configuration Report**. This will be helpful if a clean install is required and to confirm all network settings (including Host Connection Type and other parameters in Global Information).
- Perform Store Close and ensure all network transactions have completed by checking the SAF Transactions Report for fallback transaction information.
- Contact the HPS-Dallas Help Desk at 1-800-767-5258 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 that all file transfers from Passport to the BOS have completed.

After the upgrade, the ASC must perform the following:

- Beginning with V11.02 Service Pack P, Passport defaults to TCP/IP Connection with TLS encryption. If enabling TLS for the first time, contact the HPS-Dallas Help Desk and 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** > **Phillips 66** > **Global Network Parameters** > **Connection** - **Page 1** and **Page 3** tabs to confirm the settings with the HPS-Dallas network.
- Request a PDL Download by going to **MWS** > **Set Up** > **Network** > **Phillips 66** > **PDL Download**. For more information on requesting PDL download, refer to "Requesting PDL Download" on page 18.
- 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.

  Note: These first two steps are especially important for stores that were running a version of Passport earlier than V10 Service Pack K and upgrading to V12, as Passport supports new credit card types beginning with V10 Service Pack K.
- Review the parameters on **MWS** > **Set Up** > **Network** > **Phillips 66** > **Global Network Parameters** > **EMV Parameters** tab with the merchant or store manager. Advise them to contact the Phillips 66 Help Desk at 1-800-426-3696 to discuss the financial implications and suggested settings on this screen.
- If installing a VeriFone MX915 or Ingenico iSC250 PIN Pad, ensure the EMV Capable field is selected in **MWS** > **Set Up** > **Register** > **Register Set Up** > **Device Configuration**.

- If the upgrade was from V8.03:
  - Use the Fuel Discount Configuration report that you printed before the upgrade to assist the manager in reviewing and renaming Fuel Discount Groups in **MWS** > **Fuel** > **Fuel Discount Maintenance** and reconfiguring **MWS** > **Set Up** > **Network** > **Marathon** > **Fuel Discounting by Card Type**.
  - Assist in activating the Multiple Loyalty Interface feature, if applicable; and advise the manager of the Loyalty Provider Name in **MWS** > **Set Up** > **Store** > **Loyalty Interface** that migrated from V8.03 and assist in changing the name if the manager requests.
- 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** > **Phillips 66** > **Fuel Discount Configuration** and update the fuel discounts accordingly. Select **Save** to save the changes to the Passport database and exit.

GILBARCO VEEDER-ROOT

© 2020 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-5466A Passport™ V12 Network Addendum HPS-Dallas for Phillips 66® · February 2020