GILBARCO VEEDER-ROOT

Passport™ V20 Network Addendum for HPS-Dallas CITGO®
July 2021

Introduction

Purpose

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

IMPORTANT INFORMATION

CITGO requires that Passport POS systems employ a CITGO-approved Managed Network Service Provider (MNSP) device. When configured properly, this single MNSP device will isolate and protect Gilbarco® devices and provide perimeter firewall services for the site while being managed by MNSP. Contact CITGO for a list of approved MNSP service providers. Before installing an Acumera device shipped with a new Passport POS system, contact Acumera to sign-up for MNSP perimeter firewall services.

The HPS-Dallas network requires notice in advance if the store is enabling EMV® functionality on Passport. EMV functionality affects inside and outside transactions. At least two full days before the scheduled upgrade, inform the merchant that they must contact the HPS-Dallas network and explain that the site is implementing an upgrade to Passport to enable EMV. The merchant should inform the network representative of the date the upgrade is to take place and request that the network be prepared 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.

If Passport V20.04 is being installed the ASC should contact the CITGO Help Desk (1-800-533-3421) **24 hours in advance** to inform them of the upgrade to V20.04 and the need for PDL 20.

On the day of the scheduled upgrade, ask the merchant or store manager if they 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 they can prepare for enabling EMV on the network within the next four hours, continue with the upgrade. Otherwise, consult the merchant or store manager regarding your options, which are:

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

Due to the End of Life of the Ingenico PIN Pads (iSC250 and iPP320) they were not certified with the HPS-Dallas network for Passport V20. Although, the iSC250 and iPP320 will still process EMV transactions on V20.02, it is recommended that a site upgrade their PIN Pads to Verifone® MX915 to remain in compliance with the approved HPS-Dallas network EMV configuration. Sites that continue using iSC250 or iPP320 after upgrading to Passport V20.02 will be at their own risk for receiving fraud liability chargebacks due to using a non-EMV certified solution. When upgrading to V20.04, Passport will check to see if an Ingenico PIN Pad is connected. If one is detected, an error message will be displayed and the upgrade will be aborted. For a clean install of V20.04, Ingenico will not be an option on the Register Set Up screen.

Intended Audience

The audience for this document includes merchants, cashiers, store managers, and Passport-certified Gilbarco Authorized Service Contractors (ASCs).

Note: Leave this manual at the store for the manager's reference. This manual is available for download by Passport-certified ASCs on the Gilbarco Online Documentation (GOLD℠) library.

REVIEW AND FULLY UNDERSTAND "Appendix B: Upgrading to Passport V20", BEGINNING ON page 49, BEFORE BEGINNING UPGRADE OR INSTALLATION OF PASSPORT V20 FOR CITGO.

Table of Contents

Related Documents

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

Abbreviations and Acronyms

Term	Description
AID	Application Identifier
ASC	Authorized Service Contractor
BOS	Back Office System
CNG	Compressed Natural Gas
COM	Communication
CRIND®	Card Reader in Dispenser
CWS	Cashier Workstation
EDH	Enhanced Dispenser Hub
EMV	Europay®, MasterCard®, and Visa®
GOLD	Gilbarco Online Documentation
HPS	Heartland Payment Systems
IP	Internet Protocol
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, Parameter Download
POS	Point of Sale
PPU	Price per Unit
RAS	Remote Access Service
SZR	Secure Zone Router
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security

Technical Support

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

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

To contact the CITGO Help Desk, call 1-800-533-3421.

Network Data Retention

Passport'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 Manager Workstation (MWS) Backup Journals/Reports utility to save up to one month of Passport system data to a single CD. For more information on saving journals and reports to CD, refer to *MDE-5025 Passport V9+ POS System Reference Manual.*

What's New in Passport V20 at CITGO Stores

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

CITGO Plus Renamed to CITGO Rewards

Beginning with V20.04, the "CITGO Plus" card has been renamed to "CITGO Rewards".

- The new card name will be reflected in the following locations:
  - Card Information screen
  - Fuel Discount Configuration screen
  - Receipts
  - Various reports, including the Network Configuration report and the Site Level Card-Based Fuel Discount report.
- Any Card Based Fuel Discounts that were configured for CITGO Plus will automatically be transferred to CITGO Rewards.

WEX EMV Cards

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

Process Unsupported Chip Card as Magstripe Outside

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

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

This enhancement applies to any unsupported chip card that is inserted at the dispenser.

Heartland Prepaid Gift Cards

Beginning with V20.02, Passport supports the Heartland Gift Card Program on the HPS-Dallas CITGO brand. This feature allows for the sale of prepaid Heartland gift cards and the acceptance of Heartland prepaid gift cards for payment. Refer to Figure 8 on page 15 for configuration parameters.

Wayne iX Pay™ Terminal

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

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

1 Navigate to **Set Up** > **Forecourt** > **Forecourt Installation**.

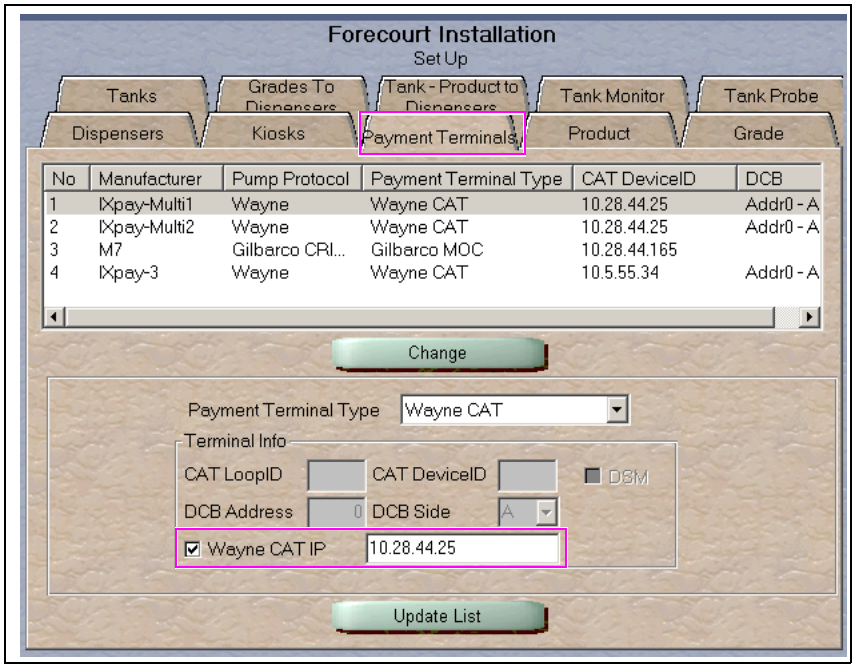
2 Select the **Payment Terminals** tab.

3 Select **Wayne CAT** for the Payment Terminal Type.

4 Select the **Wayne CAT IP** check box to enable the text box for the IP address.

5 Enter the IP address of the payment terminal. If the Wayne CAT IP check box is cleared, the payment terminal can be configured via the serial protocol.
Note: If a single IX pay board controls both sides of a dispenser, enter the same IP address for both sides.

Figure 1: Forecourt Installation - Payment Terminal



Passport V20 Core Feature Enhancements

For information on any of the new core features, refer to *MDE-5519 What's New in Passport V20*.

What's New in Passport V12 at CITGO Stores

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

FIS Payment Card as Loyalty

Beginning with V12.03, Passport supports a single swipe or insert of payment card that also serves as a loyalty card. This FIS Loyalty is available for CRIND sales only. The FIS payment loyalty program can be used in the same transaction with another loyalty program, which allows multiple loyalty discounts in a single transaction. FIS Loyalty is not supported for inside payment transactions. For more information, refer "FIS Payment Card as Loyalty" on page 24.

WEX Bulletin

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

Passport V12 Core Feature Enhancements

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

Assigning Product Codes

After configuring products or grades in Forecourt Installation, 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 fleet cards, as fleet cards often apply fuel restrictions to the transaction.

Based on the payment type the customer uses, Passport translates the product codes you assign in Forecourt Installation to the product code CITGO requires, based on the type of payment the customer uses. Use the following table to assign correct Passport product codes during setup or confirm correct product code assignment after upgrade:

Fuel Grade Description	Code
Unleaded	001
Mid-Grade 1	002
Mid-Grade 2	028
Mid-Grade 3	029
Premium	003
Premium 2	073
Diesel (taxed)	019
Diesel 2 (taxed)	021
Diesel (Off Road, Non-taxed)	032
Diesel 2 (Off Road, Non-taxed)	033
Kerosene	300
Compressed Natural Gas (CNG)	022
Gasohol	006
Gasohol 2	007
Gasohol 3	008
Ethanol	011
Ethanol 2	012
Ethanol 3	013

Do not use other fuel product codes. If you have questions or concerns about fuel product codes, contact the CITGO Help Desk at 1-800-533-3421.

Programming Network Site Configuration

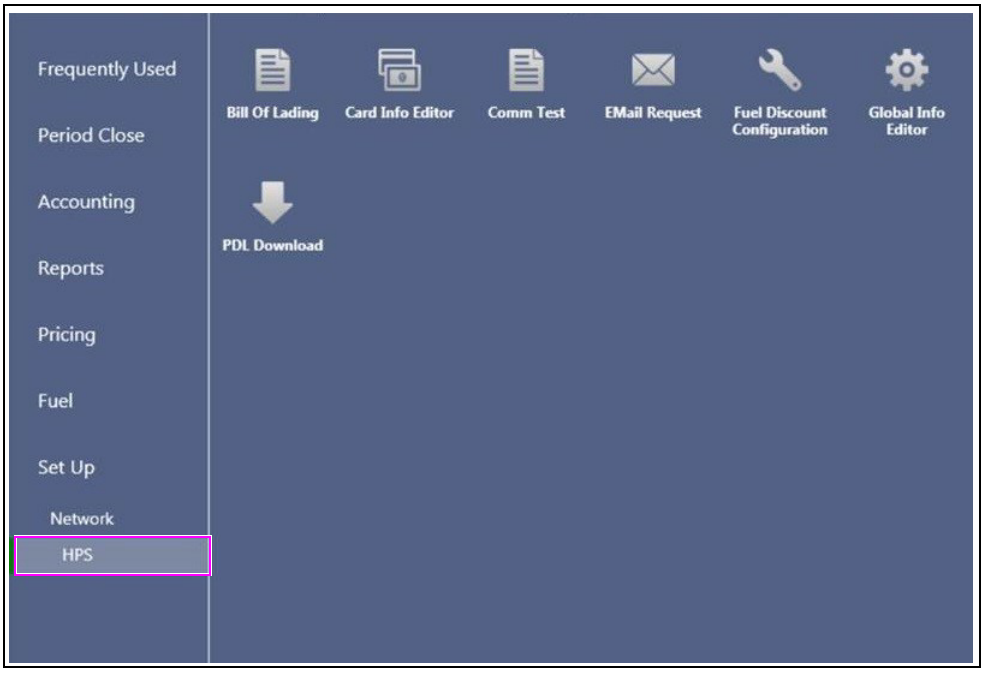
IMPORTANT INFORMATION
The Enhanced Dispenser Hub (EDH) must be installed and running before performing programming in **MWS** > **Set Up** > **Network**.

To communicate with the HPS-Dallas network, network site configuration must be programmed correctly.

To program network site configuration, proceed as follows:

1 From the MWS main menu, go to **Set Up > Network > HPS**. The CITGO Network Configuration menu opens.

Figure 2: HPS-Dallas Network Configuration Menu

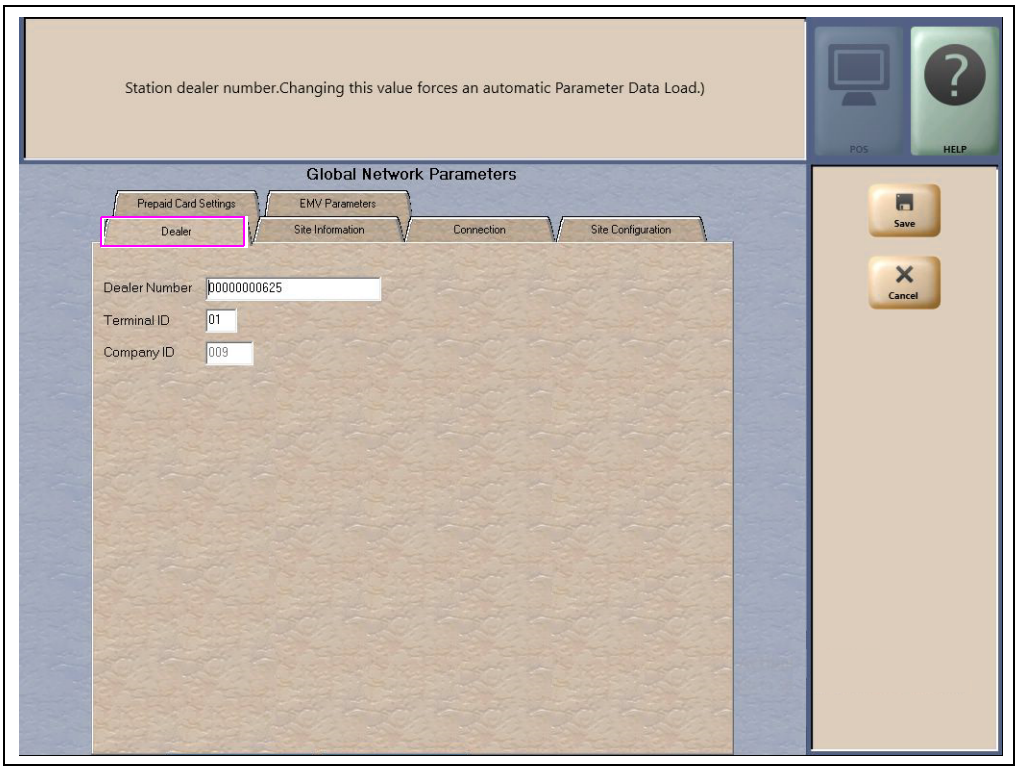


The following option buttons are displayed in the CITGO Network Configuration menu:

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

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

Figure 3: Global Network Parameters - Dealer Tab



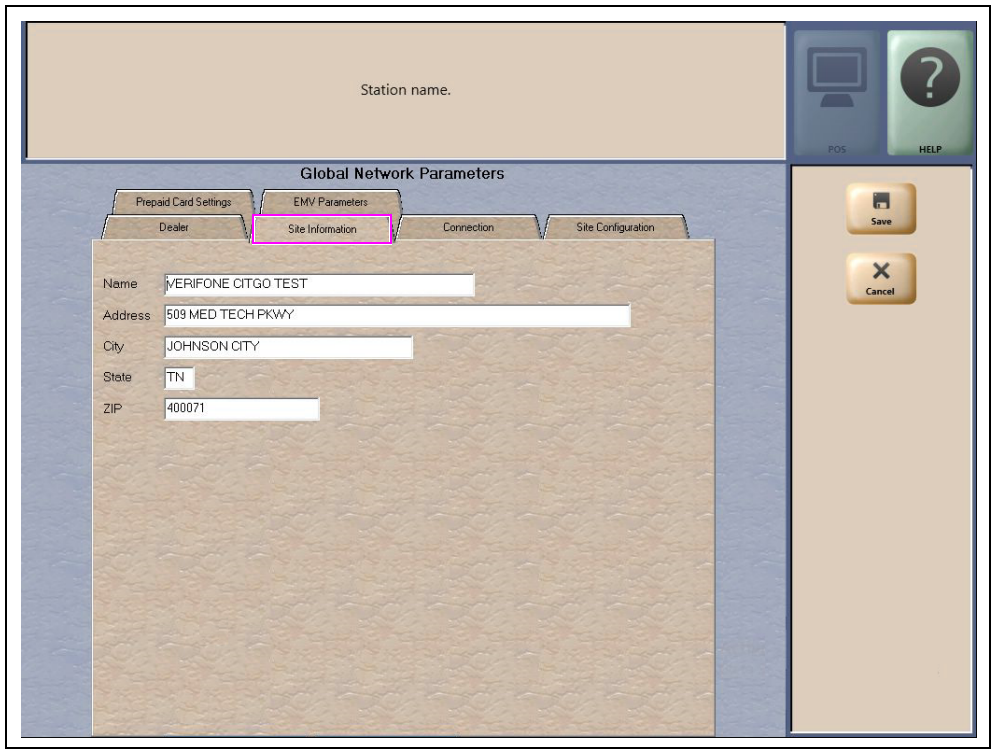
Fields on the Dealer Tab

Field	Description
Dealer Number	An 11-digit number the HPS-Dallas CITGO 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	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.*
Company ID	A three-digit number the HPS-Dallas network assigns to the company handling transactions for the store. The value for CITGO is 009 and is not editable.

3 After programming the Dealer tab, select the **Site Information** tab.

Note: Although the HPS-Dallas CITGO PDL populates the Site Information tab, these fields are editable. If you correct and save the information on this tab, you must notify the CITGO Help Desk at 1-800-533-3421 to avoid reverting to invalid data again in a subsequent PDL.

Figure 4: 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.

4 After programming the Site Information tab, select the **Connection** tab.

Programming the fields on the Connection tab varies, depending upon the Connection Type value selected on the Page 1 tab. When you access the Connection tab the first time, only the Connection Type field is displayed on the Page 1 tab. Selecting a Connection Type value causes the other fields to be displayed. Available Connection Type selections are NONE, 02 - Dial, and 06 - TCP. Select the appropriate Connection Type.

Note: A connection type of DIAL is no longer supported by CITGO. All stores must select 06 - TCP.

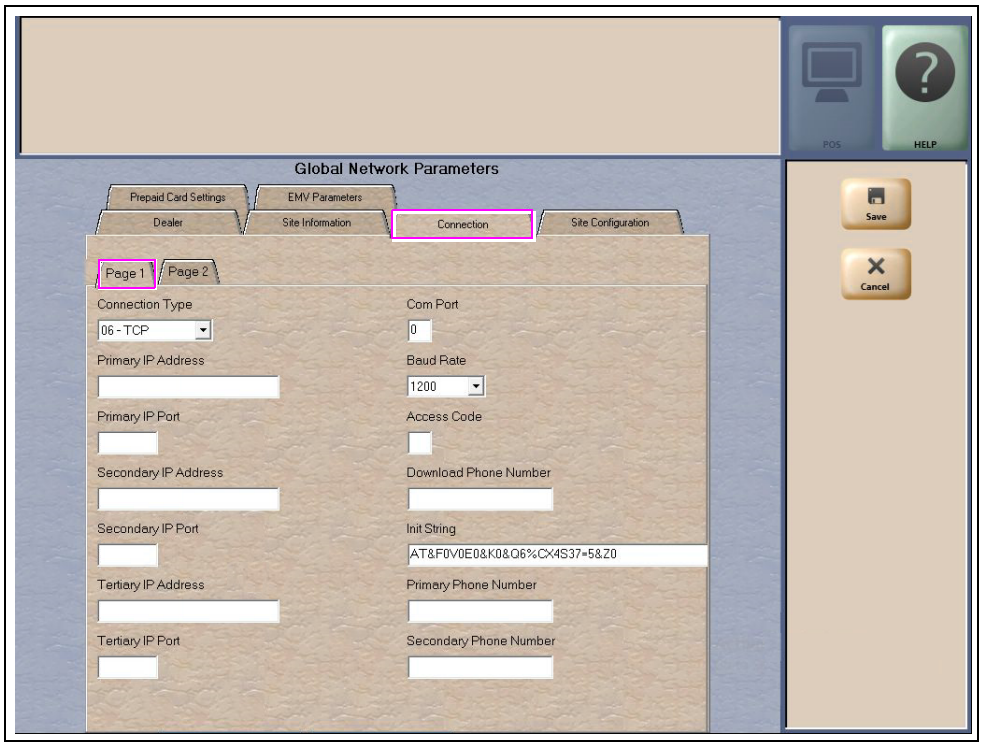
For TCP/IP Connections

For stores using TCP/IP network connection, proceed as follows:

1 Contact the CITGO Help Desk at 1-800-533-3421 to obtain the correct TCP/IP network settings for your location.

2 On the Page 1 tab, select **06 - TCP** from the Connection Type field drop-down list.

Figure 5: Connection - Page 1 Tab (For TCP/IP Connections)



Fields on the Connection - Page 1 Tab (for TCP/IP Connections)

Field	Description
Connection Type	Select 06 - TCP as the Connection Type.
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 (up to five characters). 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 (up to five characters). 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 (up to five characters). Verify with the HPS-Dallas network the value to key as the Tertiary IP Port.
Com Port*	Not used
Baud Rate*	Not used
Access Code*	Not used
Download Phone Number*	Not used
Init String*	Not used
Primary Phone Number*	Not used
Secondary Phone Number*	Not used

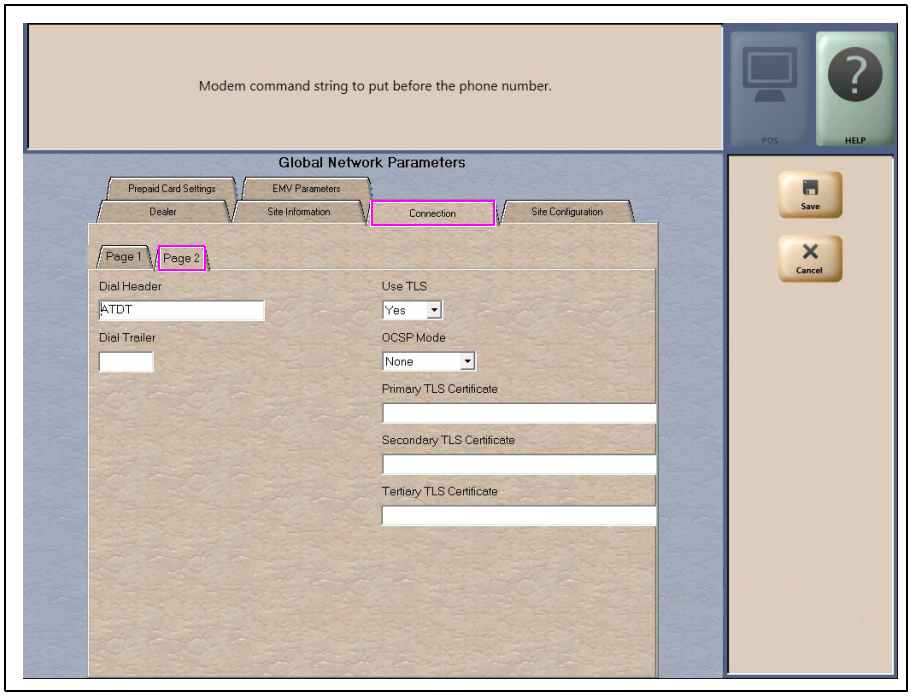
**Not used as a connection type of DIAL is no longer supported by CITGO.*

3 If one of the following Earth Stations is at the site, contact CITGO or the appropriate Help Desk for removal of that equipment.

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.

4 If the site will utilize an ISP for network traffic, TLS is required. TLS allows the merchant to use a direct secure network communication path over their store's Internet Service Provider (ISP). Continue to **Page 2** tab for TLS programming. Contact the CITGO Help Desk at 1-800-533-3421. Press **Option 2** > **Option 2** > **Option 6** for the appropriate TCP/IP and TLS programming.

Figure 6: Connection - Page 2 Tab (For TLS Connections)

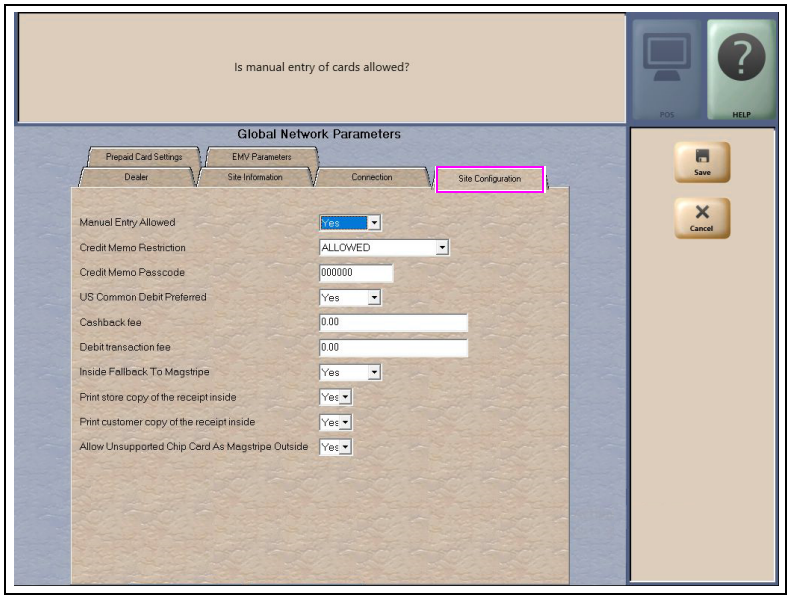


Fields on the Connection - Page 2 Tab

Field	Description
Dial Header	Not used
Dial Trailer	Not used
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.

5 After programming the Connection tab, select the **Site Configuration** tab.

Figure 7: Site Configuration Tab



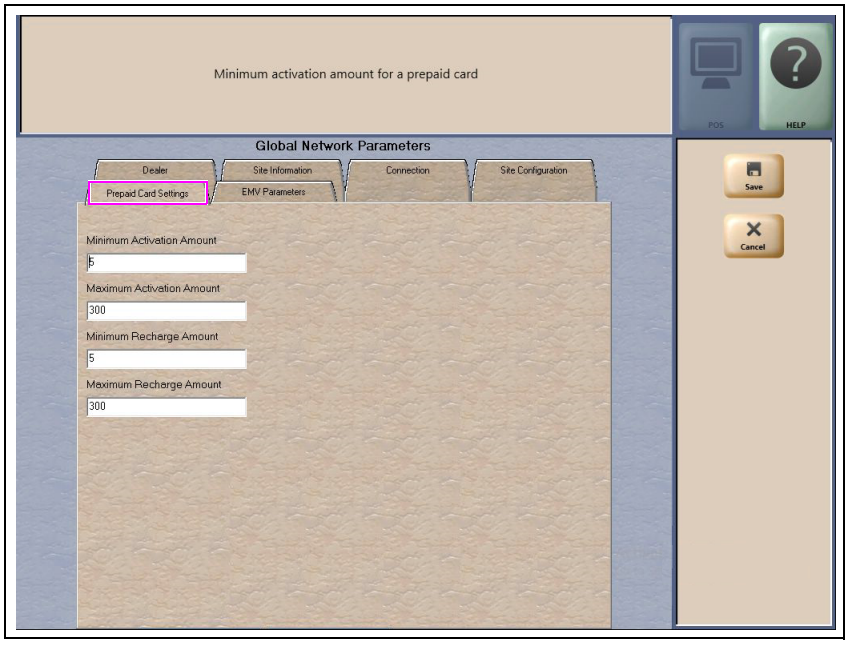
Fields on the Site Configuration Tab

Field	Description
Manual Entry Allowed	If set to **Yes**, manual entry of Credit Card transactions is allowed.
Credit Memo Restriction	Indicates restrictions placed on the ability to do credit memos. Options for this field are NOT ALLOWED, ALLOWED, and WITH PASSCODE.
Credit Memo Passcode	The code the cashier must enter to perform a credit memo.
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.
Cashback fee	Dollar amount charged if the customer requests cash back while using his debit card as payment for a transaction. Passport prompts the customer to approve the fee. When the customer approves the fee, Passport adds the fee to the sale total, receipt, and Department Sales Report. If the customer declines the fee, Passport removes the cash back item from the transaction.
Debit transaction fee	Dollar amount charged if the customer uses a debit card as payment for a transaction Passport prompts the customer to approve the fee. When the customer approves the fee, Passport adds the fee to the sale total, receipt, and Department Sales Report. If the customer declines the fee, Passport declines the tender and prompts for payment again.
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 magstripe 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 CITGO 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 CITGO 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.
Allow Unsupported Chip Card As Magstripe Outside	When set to **Yes**, and an EMV card which has an unsupported AID is inserted at the CRIND, the customer will be prompted to remove the card. The mag tripe will be read as the card is being removed, and the sale will be processed as a magstripe transaction. When set to **No**, and an unsupported chip card is inserted at the CRIND, an error message will display at the CRIND and on the cashier workstation. The default setting is Yes.

6 After programming the Site Configuration tab, select the **Prepaid Card Settings** tab. The fields on this tab provide parameters on activation and recharge of prepaid cards sold at the store.

Figure 8: Prepaid Card Settings Tab

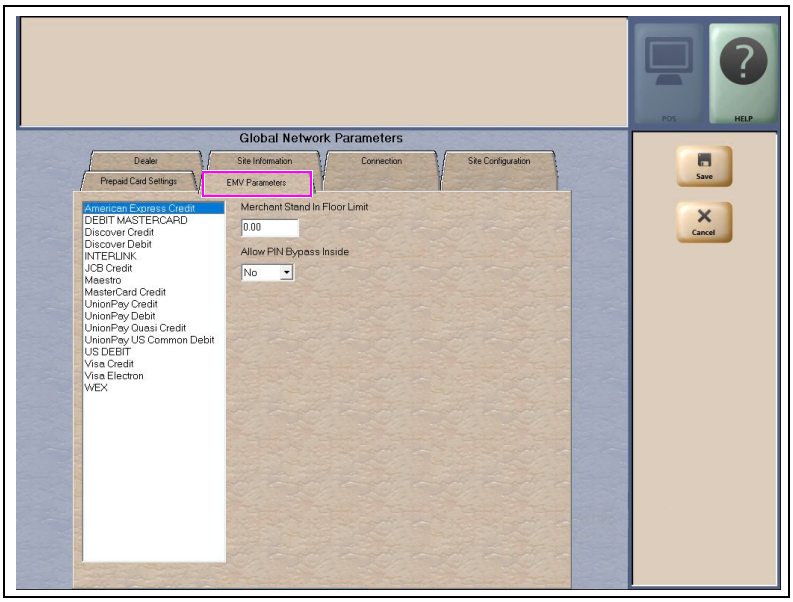


Fields on the Prepaid Card Settings Tab

Field	Description
Minimum Activation Amount	The minimum dollar amount required to activate Prepaid Cards. This field defaults to $5. *Note: Setting this field to "0" disables Prepaid Card Activation*.
Maximum Activation Amount	The maximum dollar amount allowed for Prepaid Card activation. This field defaults to $300. *Note: Setting this field to "0" disables Prepaid Card Activation.*
Minimum Recharge Amount	The minimum dollar amount required to recharge Prepaid Cards. This field defaults to $5. *Note: Setting this field to "0" disables Prepaid Card Recharge.*
Maximum Recharge Amount	The maximum dollar amount allowed for Prepaid Card recharges. This field defaults to $300. *Note: Setting this field to "0" disables Prepaid Card Recharge.*

7 After programming the Prepaid Card Settings tab, select the **EMV Parameters** tab.

Figure 9: 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, the inside PIN Pad prompts the customer to enter the PIN, but allows the customer to press the **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.*

8 After configuring all Global Network Parameters tabs, select **Save** to save all settings in the Passport database and exit from Global Network Parameters.

Programming Network Card Configuration

Follow this procedure to program the Response Authorization processing option for each payment card type CITGO accepts on Passport. The HPS-Dallas CITGO PDL controls all other acceptance programming for payment cards. Review the Network Configuration Report for information on card acceptance parameters.

Card Information

To configure Card Information, proceed as follows:

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

Figure 10: Card Information Screen

2 Select a card name from the list on the left to view or change the Response Auth setting for that card type.

The Response Auth field determines when Passport authorizes a dispenser to begin fueling on a CRIND transaction. Some card types display as read-only; the user cannot edit the field.

Options are:

- CARD ID - Passport authorizes the dispenser to begin fueling when it recognizes the card data is valid.
- ON TRANS - Passport authorizes the dispenser to begin fueling after transmitting the Authorization Request to the HPS-Dallas CITGO network.
- HOST RSP - Passport authorizes the dispenser to begin fueling after the HPS-Dallas network returns approval.

3 Select **Save** to save changes and return to the CITGO network menu.

Requesting PDL Download

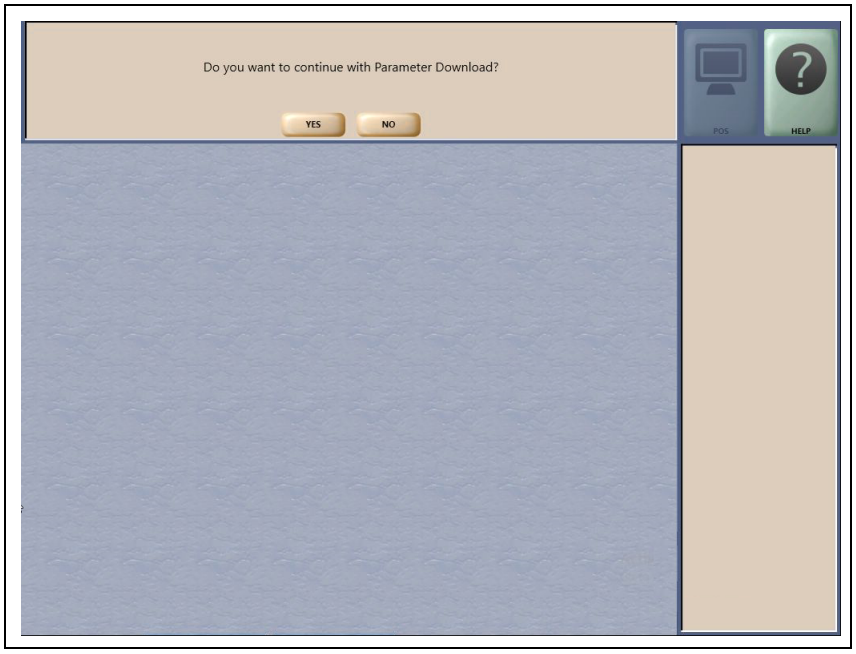
A PDL Download is a transfer of data from the HPS-Dallas CITGO network to Passport. A valid PDL contains card configuration information and is required for operation. You must request a PDL during system installation. Passport cannot process network transactions until it successfully receives a PDL from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

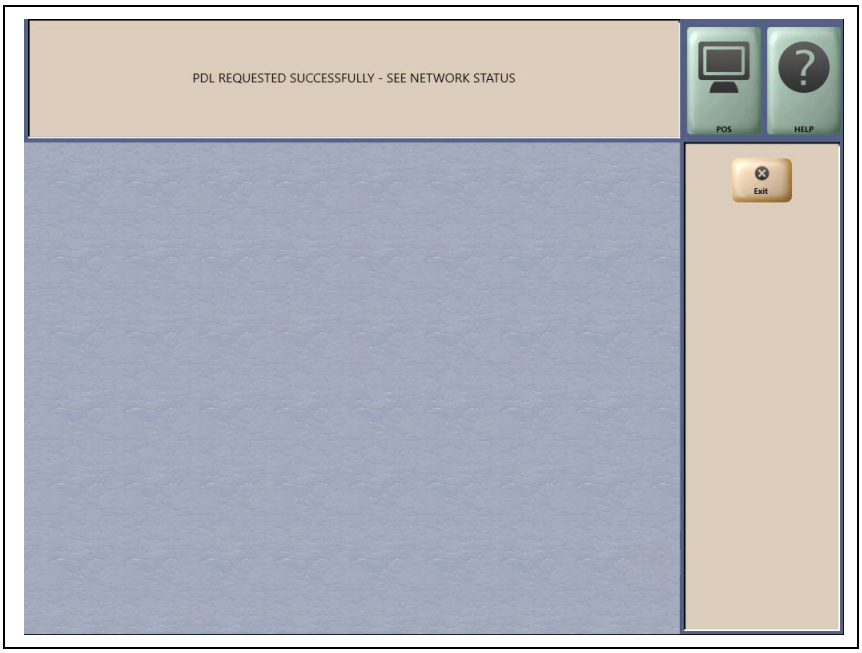
1 Navigate to **MWS** > **Set Up** > **Network** > **HPS** > **PDL Download**. Passport prompts: “Do you want to continue with Parameter Download?”

Figure 11: PDL Download Prompt



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

Figure 12: 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.

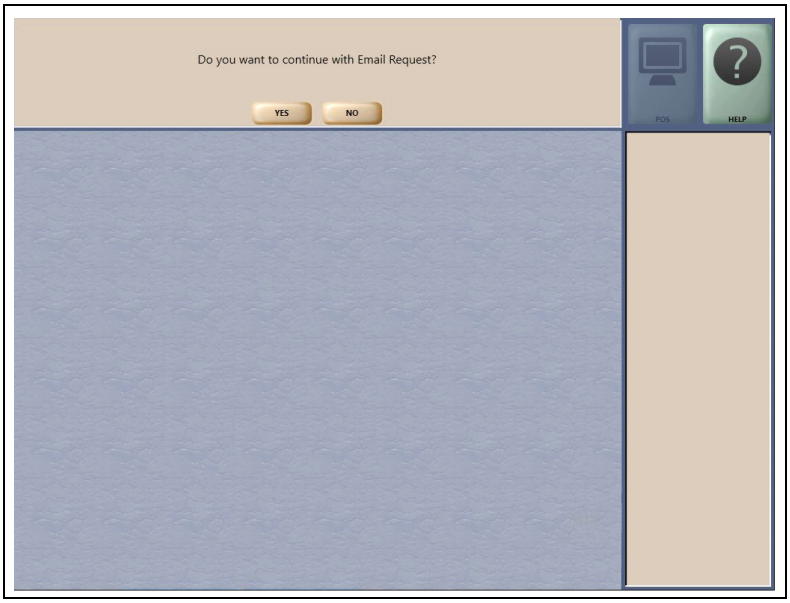
To review the PDL information sent from the network to Passport, view or print the Network Configuration Report.

Requesting Email

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

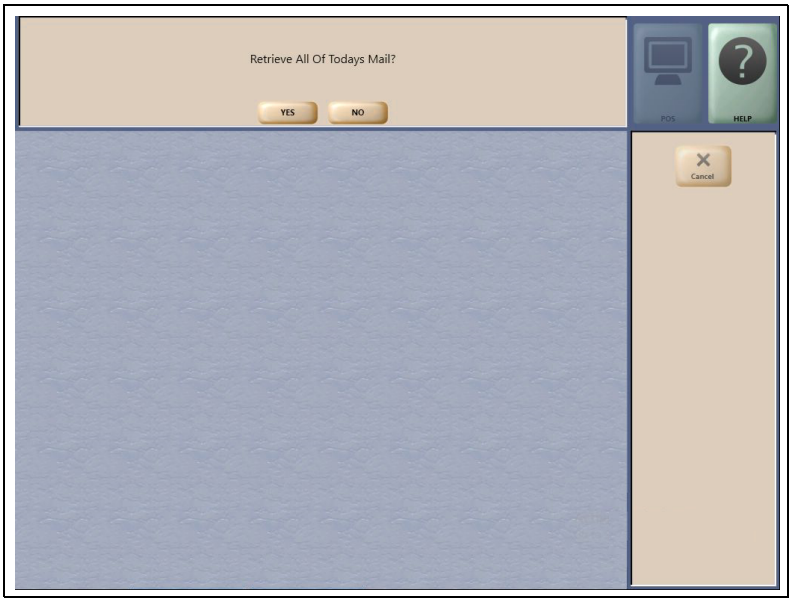
1 From the MWS main menu, go to **Set Up > Network > HPS > Email Request**. Passport prompts: “Do you want to continue with Email Request?”

Figure 13: Email Request Prompt



2 Select **No** to abandon the request or **Yes** to submit the request. Passport prompts: “Retrieve All Of Today’s Mail?”

Figure 14: All Mail Prompt



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

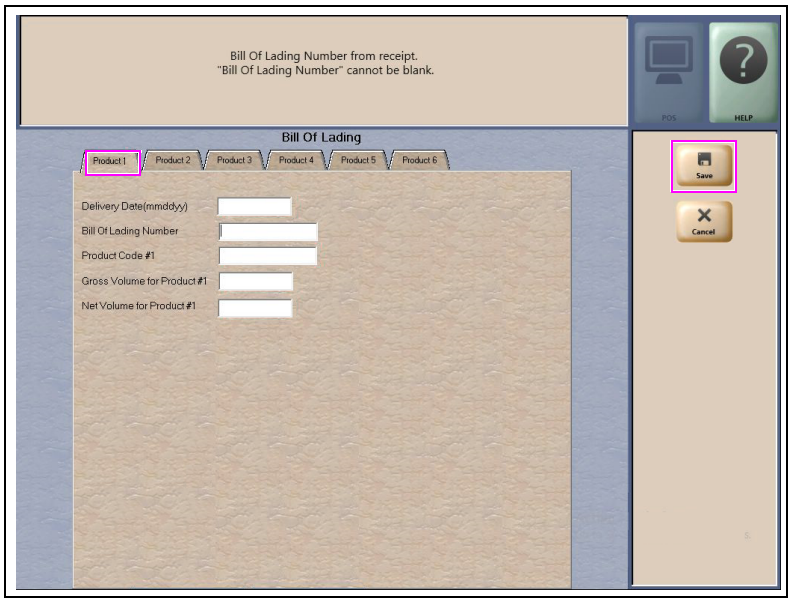
Bill of Lading

The Bill of Lading feature allows Passport to send fuel delivery information to CITGO electronically through the MWS when the store receives fuel deliveries.

To send the fuel delivery information to CITGO, proceed as follows:

1 From the MWS main menu, navigate to **Set Up > Network > HPS > Bill of Lading**. The Bill of Lading screen opens.

Figure 15: Bill of Lading Screen - Product 1 Tab



2 Complete each field. Use one tab for each fuel product or Bill of Lading that you want to send to the CITGO network.

Fields on the Bill of Lading Screen tabs

Field	Description	Length
Delivery Date	Date the fuel delivery was made.	6
Bill of Lading Number	Bill of Lading number from the fuel delivery invoice.	6 - 8
Product Code #1	PCATS Product code for the fuel grade delivered.	2 - 8
Gross Volume for Product #1	Gross fuel volume delivered (optional).	0 - 6
Net Volume for Product #1	Net fuel volume delivered.	4 - 6

The remaining tabs (Product 2 through Product 6) each contain similar fields. Complete these tabs, as necessary, for additional fuel products or bills of lading.

3 After entering the fuel delivery information, press **Save**. Passport sends the Fuel Volume information to the HPS-Dallas CITGO network and prints a report of the fuel delivery information.

Comm Test

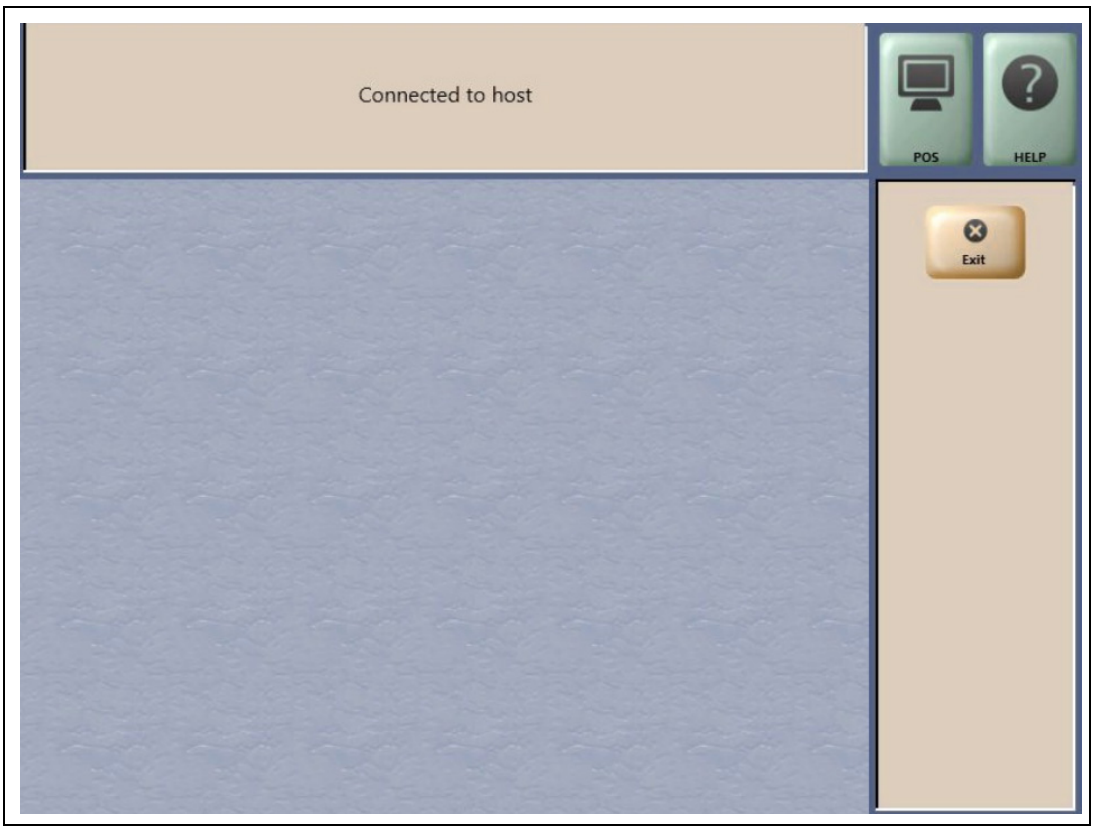
The Comm Test feature allows a site to validate that the HPS Network TCP/IP with TLS is online and working.

To validate, proceed as follows:

1 From the MWS main menu, navigate to **Set Up** > **Network** > **HPS** > **Comm Test**.

2 When Passport is online with the HPS-Dallas network, the following message is displayed. (see Figure 16).

Figure 16: Comm Test Screen



Fuel Discounts

Fuel Discount Configuration

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

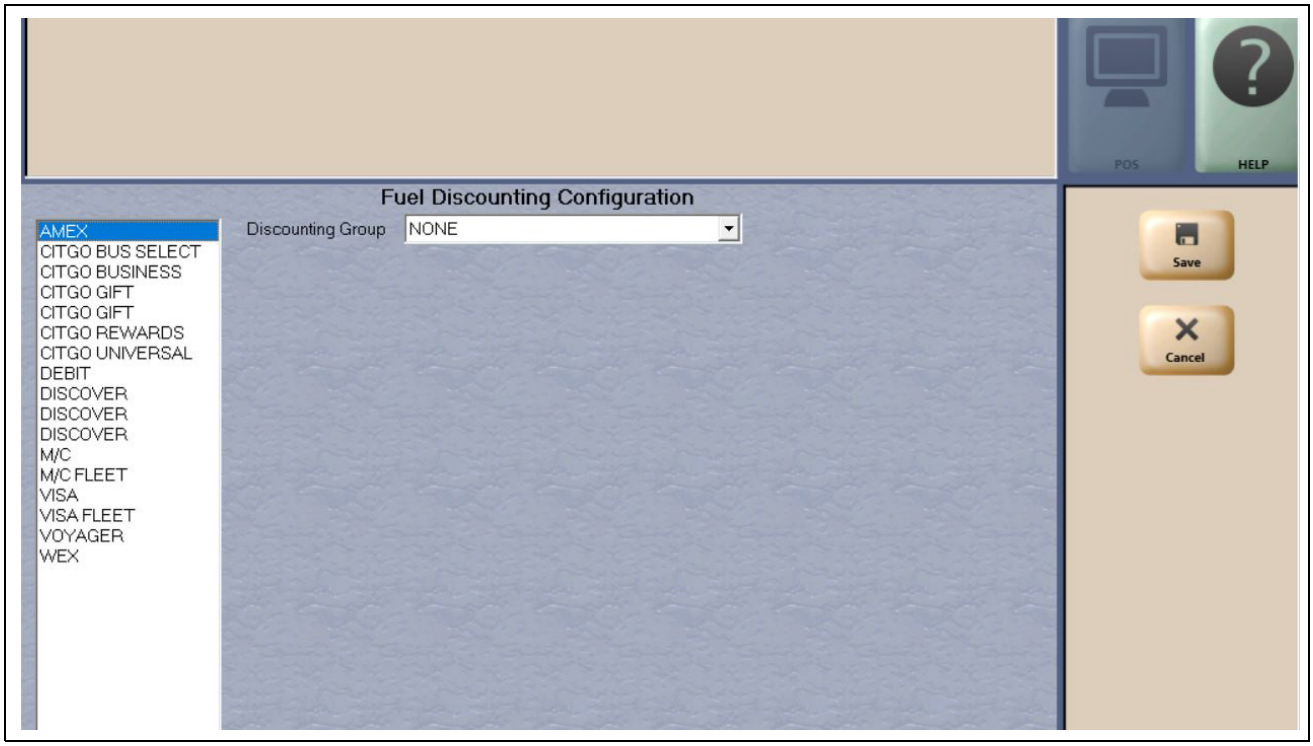
1 From the MWS main menu, select **Fuel** > **Fuel Discount Maintenance**. On the Fuel Discount Groups tab, configure PPU discounts to be applied to fuel grades available at the store.

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

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

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

Figure 17: Fuel Discounting Configuration



CITGO Setup for FIS Loyalty

FIS Payment Card as Loyalty

Passport supports a single swipe or insertion of a payment card that also serves as a loyalty card when paired with FIS Global Business Solutions Loyalty program. The FIS payment loyalty program can be used in the same transaction with another loyalty program, which allows multiple loyalty discounts in a single transaction. FIS Loyalty is not supported for inside payment transactions.

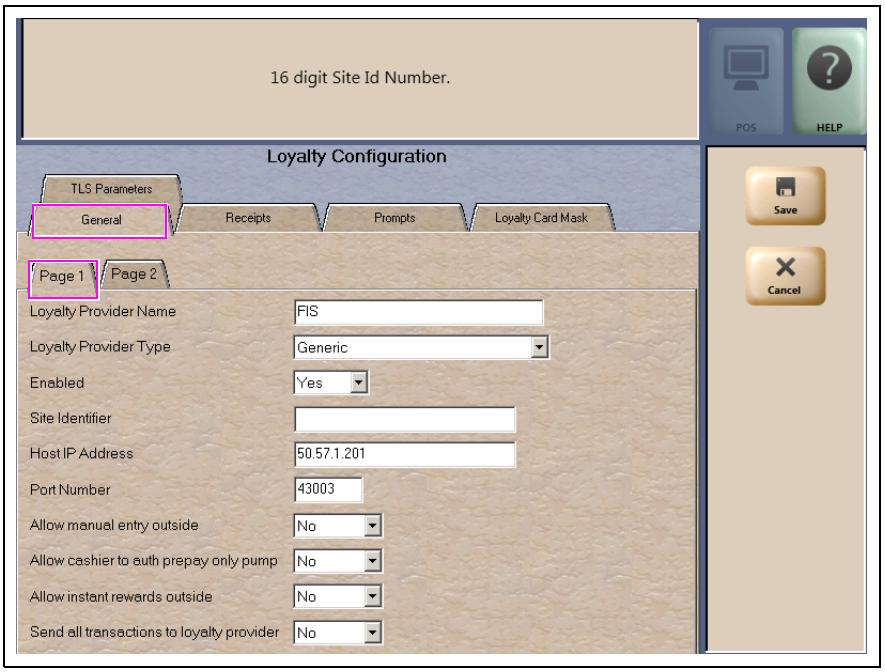
IMPORTANT INFORMATION
The merchant must contract with FIS to perform necessary onboarding processes before configuring the FIS Loyalty on Passport. The site's router/firewall devices must also be updated to allow messages to be sent to FIS. If using an Acumera SZR, certified technicians should contact Acumera to have the required router rules enabled; site personnel should contact Gilbarco's Help Desk. If not using an Acumera SZR, contact the site's MNSP. Any other firewall device(s) at the site might also need to be updated.

General Tab

To configure properties in the General tab, proceed as follows:

1 From the MWS main menu, navigate to **Set Up > Store > Loyalty Interface > General**. Enter the settings as shown in Figure 18.

Figure 18: Loyalty Configuration - Page 1

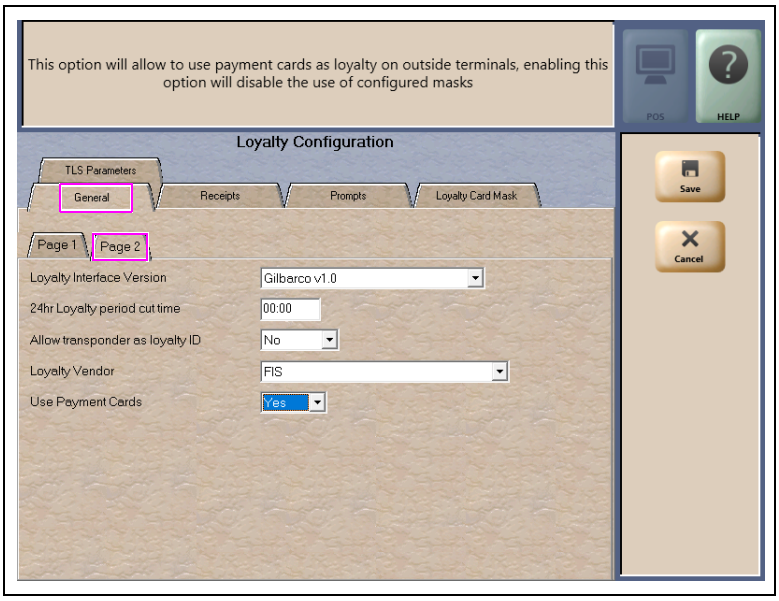


CITGO Setup

Field	Setting
Loyalty Provider Name	FIS
Loyalty Provider Type	Generic
Enabled	Yes
Site Identifier	Obtain from CITGO or FIS
Host IP Address	50.57.1.201
Port Number	43003
Allow manual entry outside	No
Allow cashier to auth prepay only pump	No
Allow instant rewards outside	No
Send all transactions to loyalty provider	No

2 Select **Page 2** and enter the settings as shown in Figure 19.

Figure 19: Loyalty Configuration - Page 2



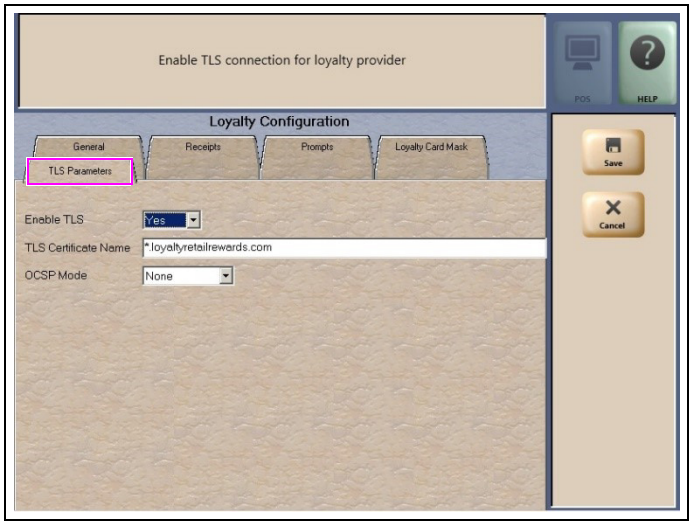
Field	Setting
Loyalty Interface Version	Gilbarco v1.0
24hr Loyalty period cut time	00:00
Allow transponder as loyalty ID	No
Loyalty Vendor	FIS
Use Payment Cards	Yes

*Note: When an FIS payment loyalty provider is configured and the option **Use Payment Cards** is set to **Yes**, the **Loyalty Card Mask** tab is not configured. When Passport is connected to the FIS host, the payment card bin ranges are sent from the FIS Host.*

TLS Parameters Tab

Select the **TLS Parameters** tab from the Loyalty Configuration screen and enter the settings as shown in Figure 20.

Figure 20: TLS Parameters

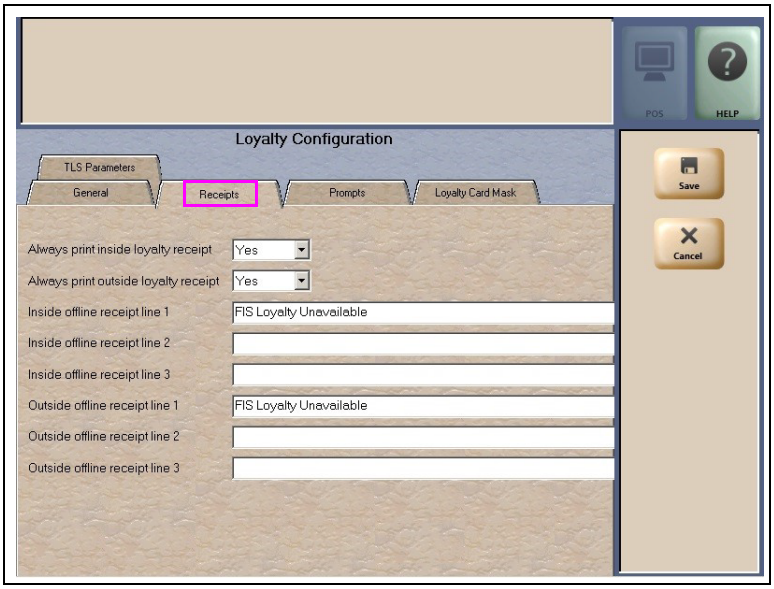


Field	Setting
Enable TLS	Yes
TLS Certificate Name	*.loyaltyretailrewards.com
OCSP Mode	None

Receipts Tab

Select the **Receipts** tab from the Loyalty Configuration screen and enter the settings as shown in Figure 21.

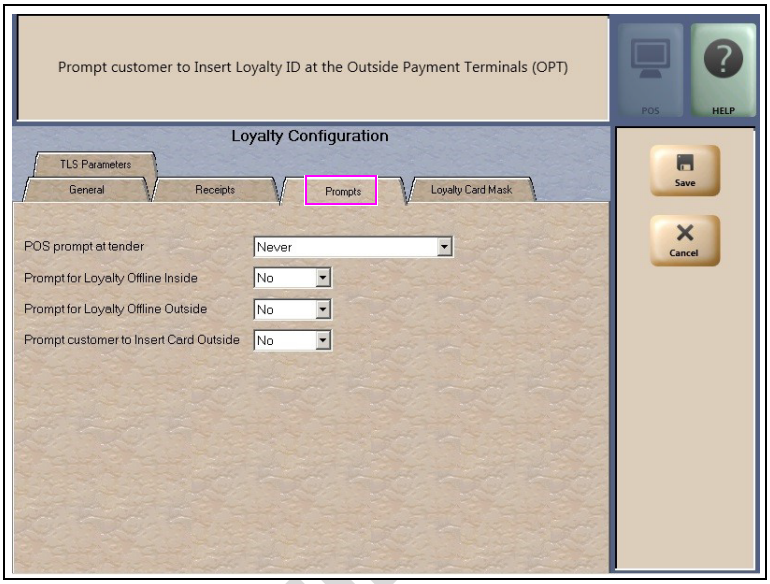
Figure 21: Receipts Tab



Prompts Tab

Select the **Prompts** tab from the Loyalty Configuration screen and enter the settings as shown in Figure 22.

Figure 22: Prompts Tab



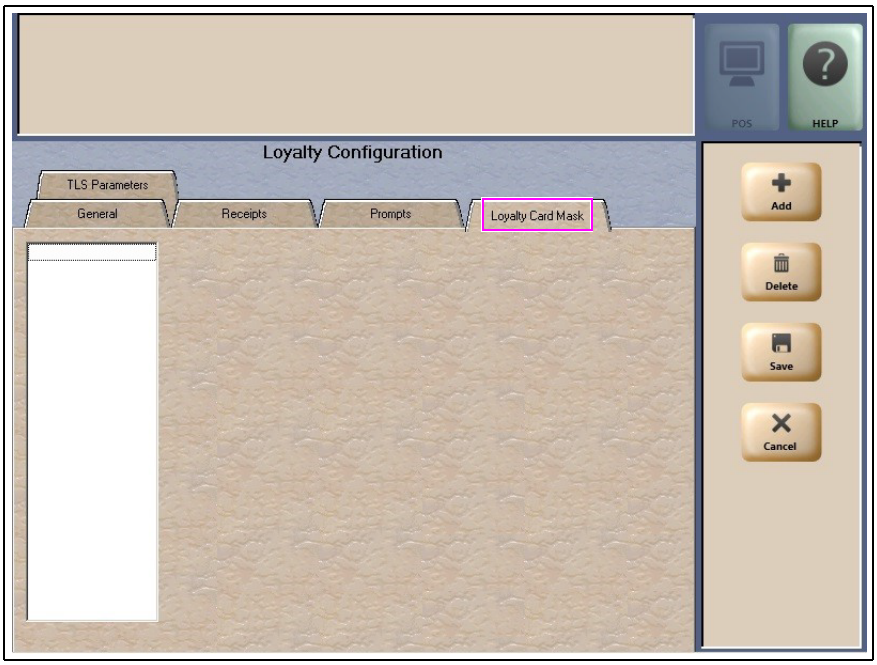
Field	Setting
POS prompt at tender	Never
Prompt for Loyalty Offline Inside	No
Prompt for Loyalty Offline Outside	No
Prompt customer to Insert Card Outside	No

Loyalty Card Mask Tab

1 Select the **Loyalty Card Mask** tab from the Loyalty Configuration screen and enter the settings as shown in Figure 23.

*Note: When an FIS payment loyalty provider is configured and the option **Use Payment Cards** is set to **Yes**, the **Loyalty Card Mask** tab is not configured. When Passport is connected to the FIS host the payment card bin ranges are sent from the FIS Host.*

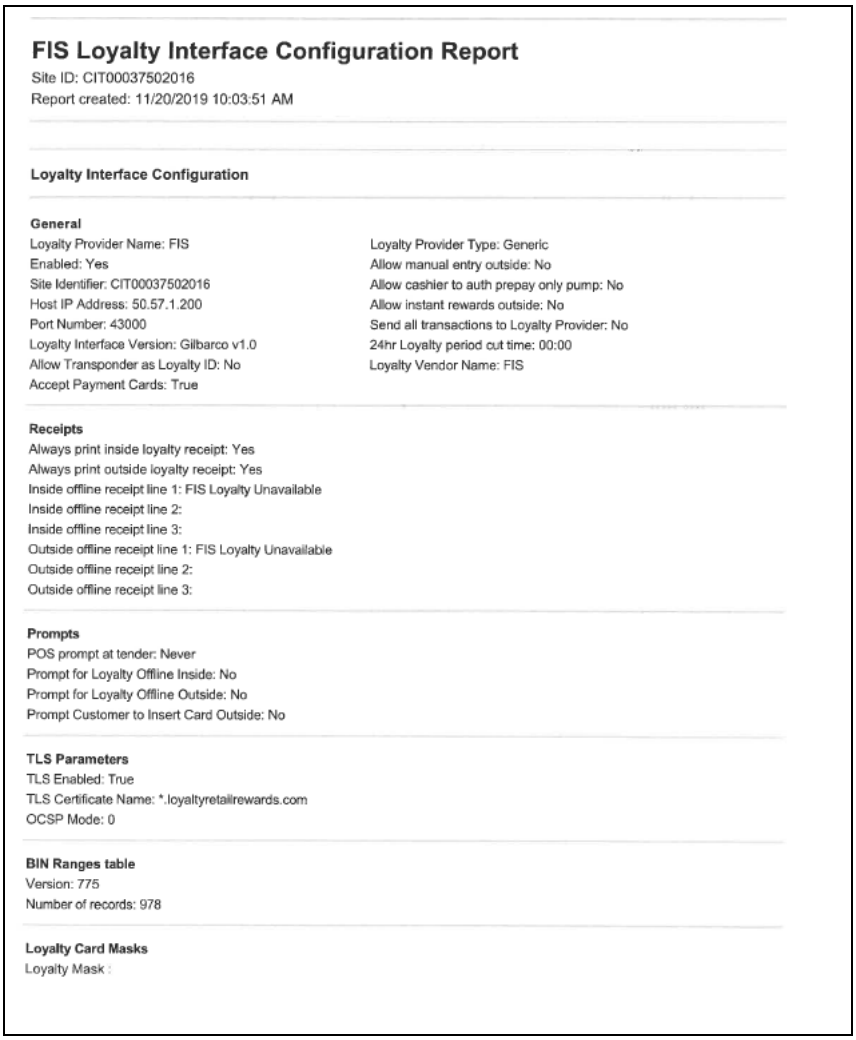
Figure 23: Loyalty Card Mask Tab



2 Select **Save**.

3 To validate connection and BIN download, review the FIS Loyalty Interface Configuration Report.

Figure 24: FIS Loyalty Interface Configuration Report



FIS Loyalty Interface Configuration Report

Site ID: CIT00037502016
Report created: 11/20/2019 10:03:51 AM

Loyalty Interface Configuration

General

Loyalty Provider Name: FIS
Enabled: Yes
Site Identifier: CIT00037502016
Host IP Address: 50.57.1.200
Port Number: 43000
Loyalty Interface Version: Gilbarco v1.0
Allow Transponder as Loyalty ID: No
Accept Payment Cards: True
Loyalty Provider Type: Generic
Allow manual entry outside: No
Allow cashier to auth prepay only pump: No
Allow instant rewards outside: No
Send all transactions to Loyalty Provider: No
24hr Loyalty period cut time: 00:00
Loyalty Vendor Name: FIS

Receipts

Always print inside loyalty receipt: Yes
Always print outside loyalty receipt: Yes
Inside offline receipt line 1: FIS Loyalty Unavailable
Inside offline receipt line 2:
Inside offline receipt line 3:
Outside offline receipt line 1: FIS Loyalty Unavailable
Outside offline receipt line 2:
Outside offline receipt line 3:

Prompts

POS prompt at tender: Never
Prompt for Loyalty Offline Inside: No
Prompt for Loyalty Offline Outside: No
Prompt Customer to Insert Card Outside: No

TLS Parameters

TLS Enabled: True
TLS Certificate Name: *.loyaltyretailrewards.com
OCSP Mode: 0

BIN Ranges table

Version: 775
Number of records: 978

Loyalty Card Masks

Loyalty Mask :

Integrated EBT Tenders

The HPS-Dallas Network supports processing EBT Food and EBT Cash. Call the CITGO POS Help Desk (1-866-398-6150) or email to POShelp@citgo.com and provide the site's FNS number and a copy of the certificate for EBT to be enabled on the PDL. EBT Food and EBT Cash tenders have been added to Tender Maintenance with the status of **Inactive**.

For stores that desire to process EBT tenders with Passport on the HPS-Dallas network, a user should go to **MWS** > **Set Up** > **Store** > **Tender Maintenance** and highlight the EBT Cash tender and select **Activate** and highlight the EBT Food tender and select **Activate**.

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

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

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

EBT Card Transactions

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

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

Passport also allows cash back for EBT Cash and applies a debit cash back transaction fee (similar to Debit transactions), based on programming in Network Site Configuration. If the customer requests cash back with EBT Cash tender, Passport does not allow split tender. The EBT Cash card must cover the entire amount of the transaction, including cash back. If Passport receives partial approval for EBT Cash in which the customer requested cash back, the Cashier Workstation (CWS) prompts the cashier to perform a manual refund of the partially approved EBT Cash tender. The manual refund is necessary because of the PIN entry requirement on the sale transaction.

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

Network Journal Report

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

Figure 25: Network Journal Report Screen

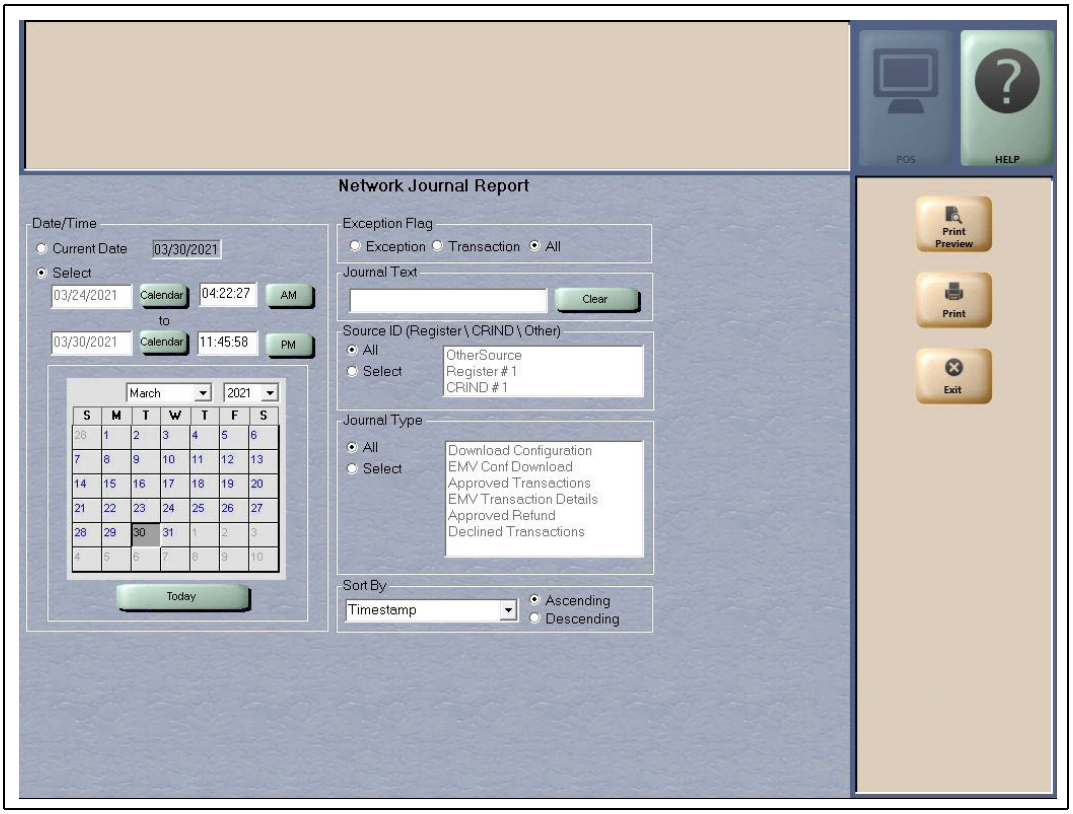
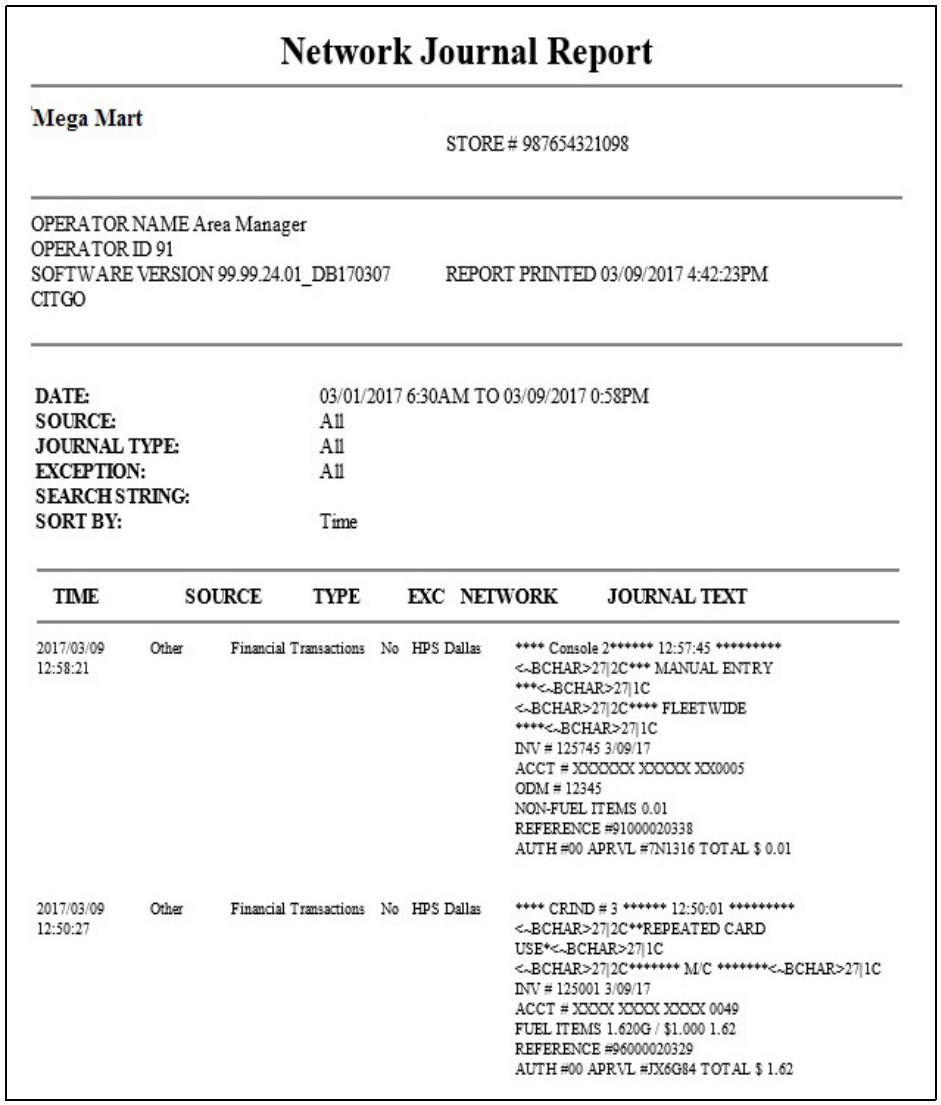


Figure 26: Network Journal Report



Network Journal Report

Mega Mart

STORE # 987654321098

OPERATOR NAME Area Manager
OPERATOR ID 91
SOFTWARE VERSION 99.99.24.01_DB170307 REPORT PRINTED 03/09/2017 4:42:23PM
CITGO

DATE: 03/01/2017 6:30AM TO 03/09/2017 0:58PM
SOURCE: All
JOURNAL TYPE: All
EXCEPTION: All
SEARCH STRING:
SORT BY: Time

TIME	SOURCE	TYPE	EXC	NETWORK	JOURNAL TEXT
2017/03/09 12:58:21	Other	Financial Transactions	No	HPS Dallas	**** Console 2****** 12:57:45 ********* <~BCHAR>27|2C*** MANUAL ENTRY ***<~BCHAR>27|1C <~BCHAR>27|2C**** FLEETWIDE ****<~BCHAR>27|1C INV # 125745 3/09/17 ACCT # XXXXXX XXXXX XX0005 ODM # 12345 NON-FUEL ITEMS 0.01 REFERENCE #91000020338 AUTH #00 APRVL #7N1316 TOTAL $ 0.01
2017/03/09 12:50:27	Other	Financial Transactions	No	HPS Dallas	**** CRIND # 3 ****** 12:50:01 ********* <~BCHAR>27|2C**REPEATED CARD USE*<~BCHAR>27|1C <~BCHAR>27|2C******* M/C *******<~BCHAR>27|1C INV # 125001 3/09/17 ACCT # XXXX XXXX XXXX 0049 FUEL ITEMS 1.620G / $1.000 1.62 REFERENCE #96000020329 AUTH #00 APRVL #JX6G84 TOTAL $ 1.62

Network Reports

Network reports show data on transactions transmitted to the HPS-Dallas CITGO network. Some network reports provide information on the status of transactions while others provide summary 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 Conflicts Report		✓		
Electronic Mail Report		✓		
EMV Chip Fallback Report		✓		
EMV Configuration 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			✓	

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

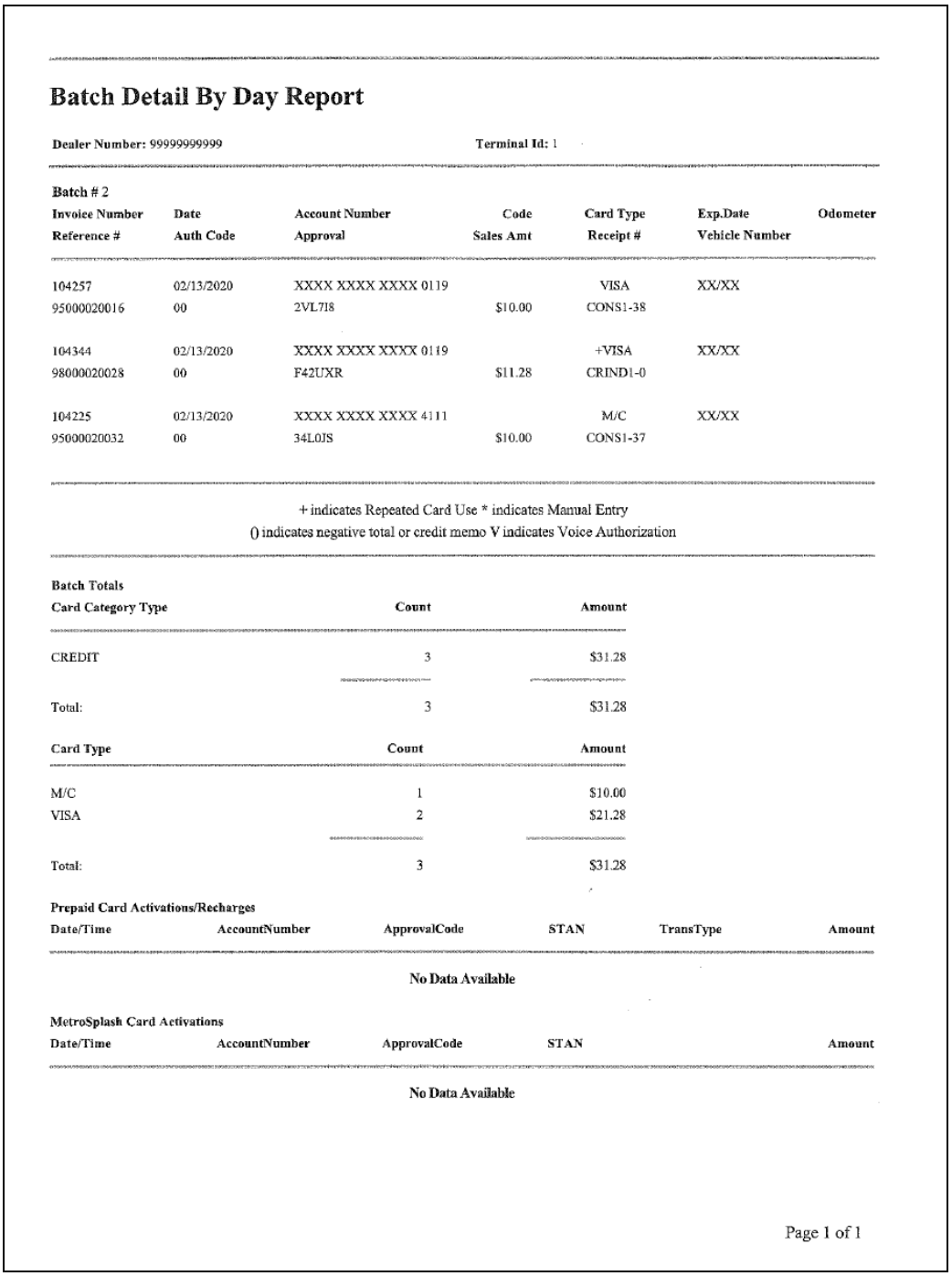
IMPORTANT INFORMATION

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 additional information on secure reports, refer to *MDE-5545 Passport EDH (Heartland Dallas) V11.24.01.* Implementation Guide for PA-DSS V3.2.*

Batch Detail by Day Report

The Batch Detail by Day Report is available at Store 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. Figure 27 shows 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 27: Batch Detail by Day Report



Batch Detail By Day Report

Dealer Number: 99999999999 **Terminal Id:** 1

Batch # 2

Invoice Number	Date	Account Number	Code	Card Type	Exp.Date	Odometer
Reference #	Auth Code	Approval	Sales Amt	Receipt #	Vehicle Number	
104257	02/13/2020	XXXX XXXX XXXX 0119		VISA	XX/XX	
95000020016	00	2VL7I8	$10.00	CONS1-38		
104344	02/13/2020	XXXX XXXX XXXX 0119		+VISA	XX/XX	
98000020028	00	F42UXR	$11.28	CRIND1-0		
104225	02/13/2020	XXXX XXXX XXXX 4111		M/C	XX/XX	
95000020032	00	34L0JS	$10.00	CONS1-37		

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

Batch Totals

Card Category Type	Count	Amount
CREDIT	3	$31.28
Total:	3	$31.28

Card Type	Count	Amount
M/C	1	$10.00
VISA	2	$21.28
Total:	3	$31.28

Prepaid Card Activations/Recharges

Date/Time	AccountNumber	ApprovalCode	STAN	TransType	Amount

No Data Available

MetroSplash Card Activations

Date/Time	AccountNumber	ApprovalCode	STAN	Amount

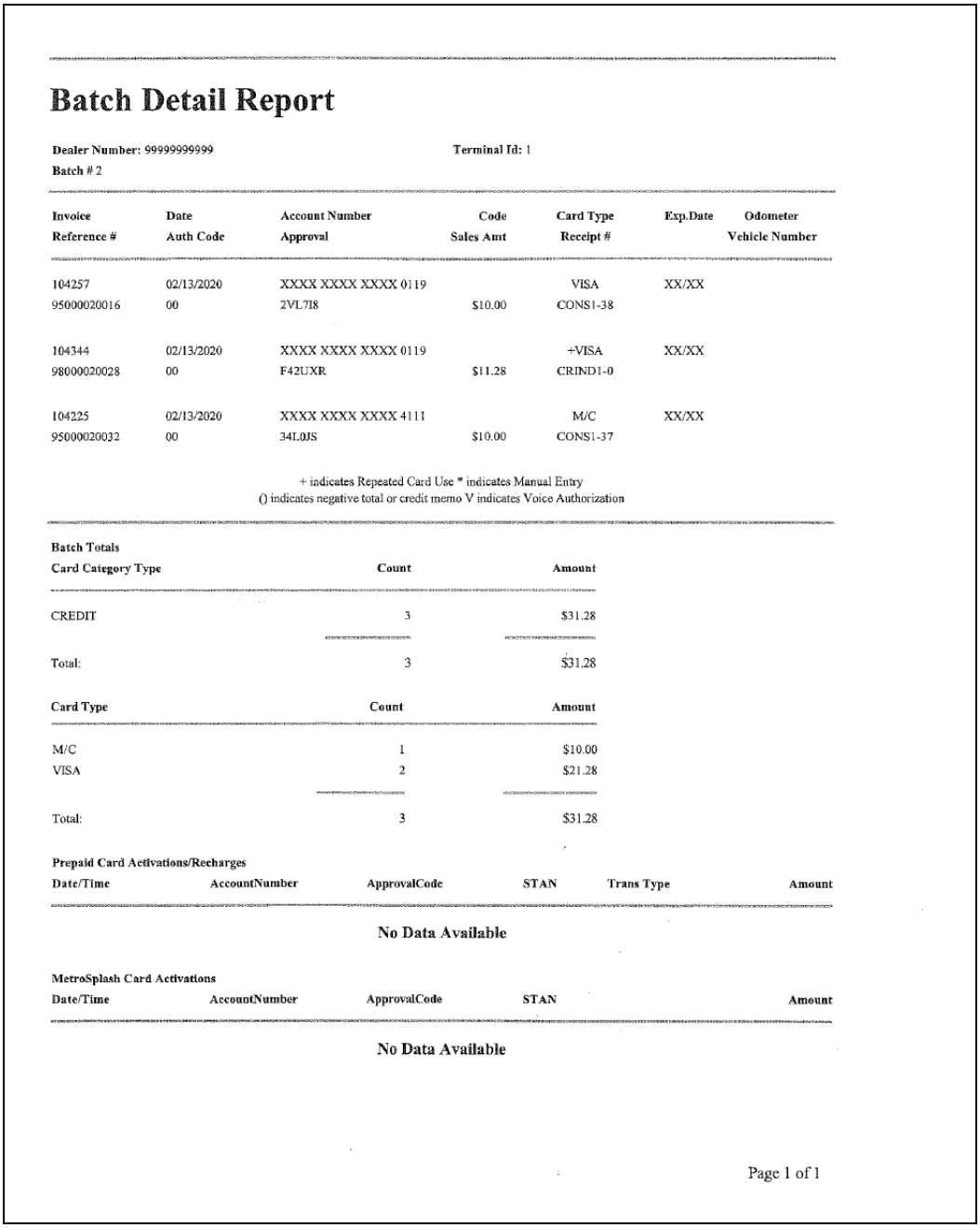
No Data Available

Page 1 of 1

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. Figure 28 shows 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 28: Batch Detail Report



Batch Detail Report

Dealer Number: 99999999999 **Terminal Id:** 1
Batch # 2

Invoice / Reference #	Date / Auth Code	Account Number / Approval	Code / Sales Amt	Card Type / Receipt #	Exp.Date	Odometer / Vehicle Number
104257	02/13/2020	XXXX XXXX XXXX 0119		VISA	XX/XX	
95000020016	00	2VL7I8	$10.00	CONS1-38		
104344	02/13/2020	XXXX XXXX XXXX 0119		+VISA	XX/XX	
98000020028	00	F42UXR	$11.28	CRIND1-0		
104225	02/13/2020	XXXX XXXX XXXX 4111		M/C	XX/XX	
95000020032	00	34L0JS	$10.00	CONS1-37		

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

Batch Totals

Card Category Type	Count	Amount
CREDIT	3	$31.28
Total:	3	$31.28

Card Type	Count	Amount
M/C	1	$10.00
VISA	2	$21.28
Total:	3	$31.28

Prepaid Card Activations/Recharges

Date/Time	AccountNumber	ApprovalCode	STAN	Trans Type	Amount

No Data Available

MetroSplash Card Activations

Date/Time	AccountNumber	ApprovalCode	STAN	Amount

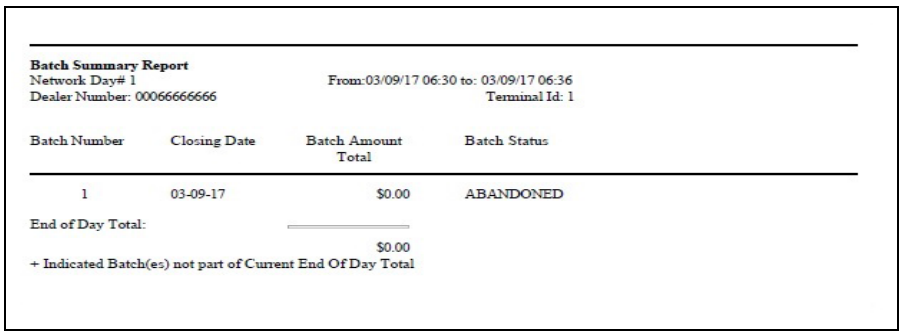
No Data Available

Page 1 of 1

Batch Summary Report

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

Figure 29: Batch Summary Report



Batch Summary Report
Network Day# 1 From:03/09/17 06:30 to: 03/09/17 06:36
Dealer Number: 00066666666 Terminal Id: 1

Batch Number	Closing Date	Batch Amount Total	Batch Status
1	03-09-17	$0.00	ABANDONED

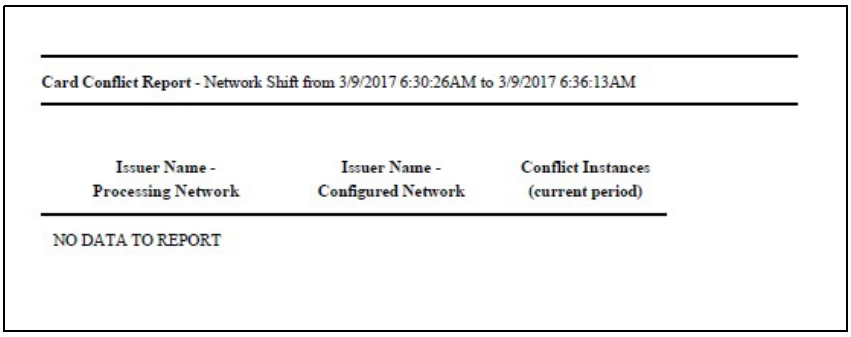
End of Day Total: $0.00
+ Indicated Batch(es) not part of Current End Of Day Total

Notes: 1) When the fallback file is more than 50% full, a message similar to "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 CITGO Help Desk at 1-800-533-3421 for procedures to process the batch manually.

Card Conflicts 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 30: Card Conflict Report



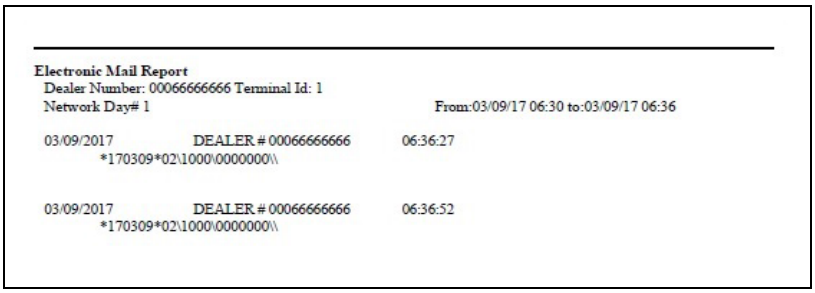
Card Conflict Report - Network Shift from 3/9/2017 6:30:26AM to 3/9/2017 6:36:13AM

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 31: Electronic Mail Report



Electronic Mail Report
Dealer Number: 00066666666 Terminal Id: 1
Network Day# 1 From:03/09/17 06:30 to:03/09/17 06:36

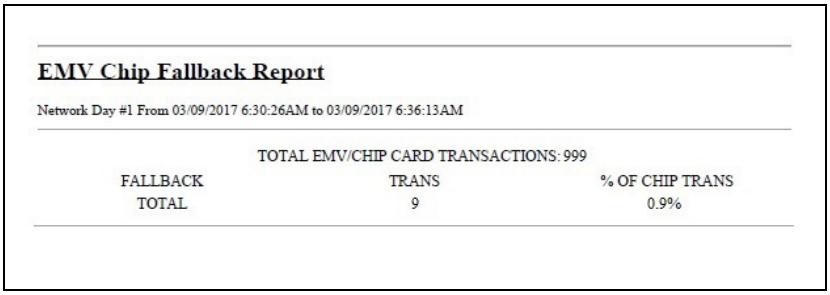
03/09/2017 DEALER # 00066666666 06:36:27
*170309*02\1000\0000000\\

03/09/2017 DEALER # 00066666666 06:36:52
*170309*02\1000\0000000\\

EMV Chip Fallback Report

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

Figure 32: EMV Chip Fallback Report



EMV Chip Fallback Report

Network Day #1 From 03/09/2017 6:30:26AM to 03/09/2017 6:36:13AM

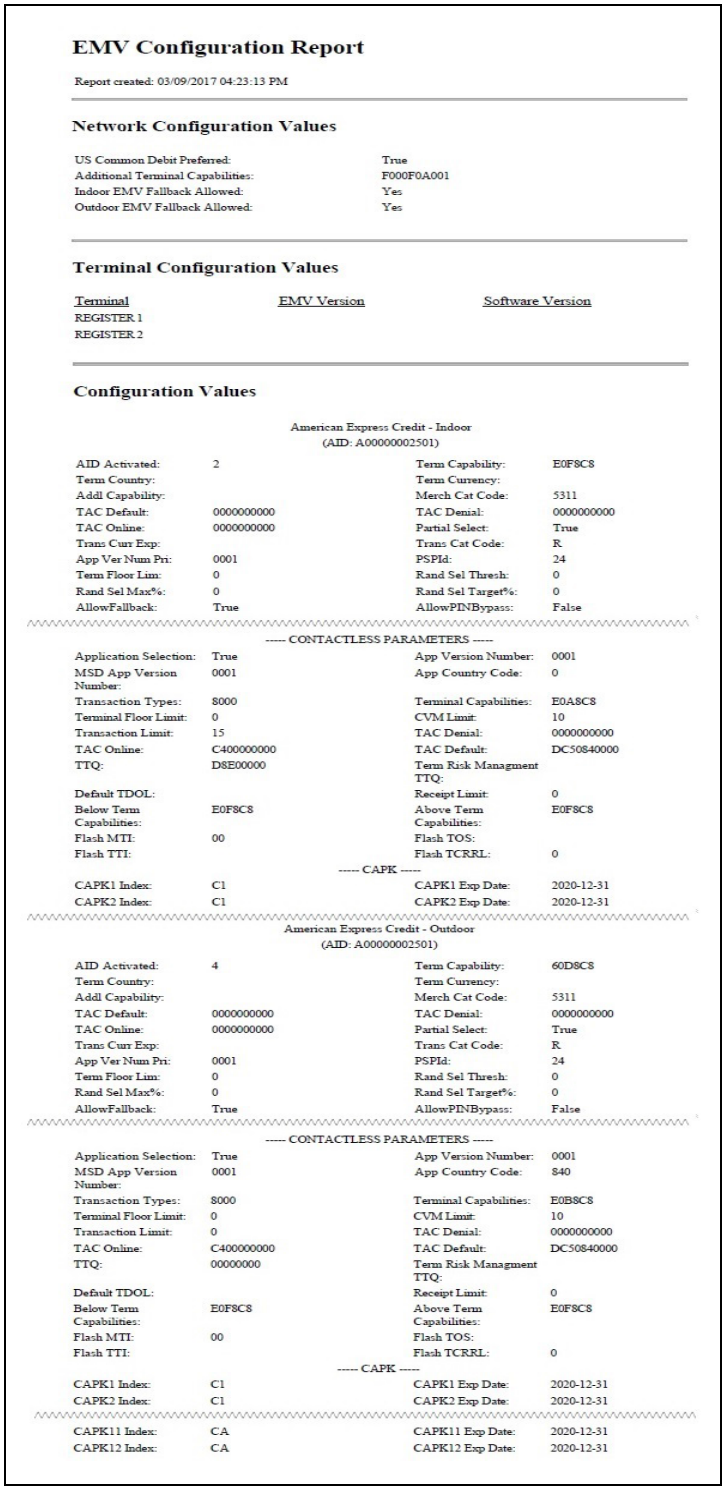
TOTAL EMV/CHIP CARD TRANSACTIONS: 999

FALLBACK	TRANS	% OF CHIP TRANS
TOTAL	9	0.9%

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 > HPS > Global Network Parameters > EMV Parameters** tab.

Figure 33: EMV Configuration Report



EMV Configuration Report

Report created: 03/09/2017 04:23:13 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		
REGISTER 2		

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:	E0A8C8
Terminal Floor Limit:	0	CVM Limit:	10
Transaction Limit:	15	TAC Denial:	0000000000
TAC Online:	C400000000	TAC Default:	DC50840000
TTQ:	D8E00000	Term Risk Managment TTQ:	
Default TDOL:		Receipt Limit:	0
Below Term Capabilities:	E0F8C8	Above Term Capabilities:	E0F8C8
Flash MTI:	00	Flash TOS:	
Flash TTI:		Flash TCRRL:	0

----- CAPK -----

CAPK1 Index:	C1	CAPK1 Exp Date:	2020-12-31
CAPK2 Index:	C1	CAPK2 Exp Date:	2020-12-31

American Express Credit - Outdoor
(AID: A00000002501)

AID Activated:	4	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:	840
Transaction Types:	8000	Terminal Capabilities:	E0B8C8
Terminal Floor Limit:	0	CVM Limit:	10
Transaction Limit:	0	TAC Denial:	0000000000
TAC Online:	C400000000	TAC Default:	DC50840000
TTQ:	00000000	Term Risk Managment TTQ:	
Default TDOL:		Receipt Limit:	0
Below Term Capabilities:	E0F8C8	Above Term Capabilities:	E0F8C8
Flash MTI:	00	Flash TOS:	
Flash TTI:		Flash TCRRL:	0

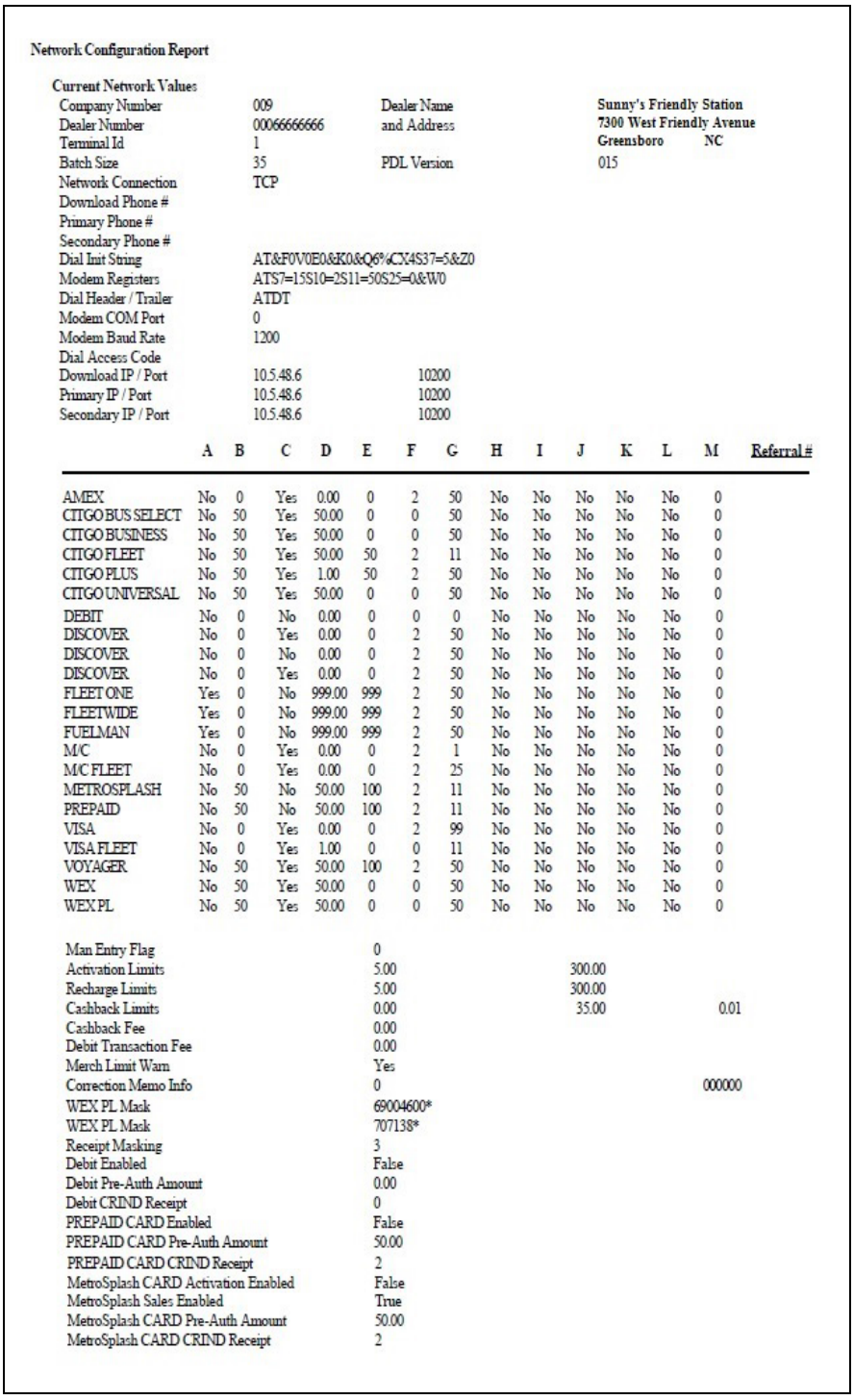
----- CAPK -----

CAPK1 Index:	C1	CAPK1 Exp Date:	2020-12-31
CAPK2 Index:	C1	CAPK2 Exp Date:	2020-12-31
CAPK11 Index:	CA	CAPK11 Exp Date:	2020-12-31
CAPK12 Index:	CA	CAPK12 Exp Date:	2020-12-31

Network Configuration Report

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

Figure 34: Network Configuration Report



Network Configuration Report

Current Network Values

Company Number	009	Dealer Name	Sunny's Friendly Station
Dealer Number	00066666666	and Address	7300 West Friendly Avenue
Terminal Id	1		Greensboro NC
Batch Size	35	PDL Version	015
Network Connection	TCP		
Download Phone #			
Primary Phone #			
Secondary Phone #			
Dial Init String	AT&F0V0E0&K0&Q6%CX4S37=5&Z0		
Modem Registers	ATS7=15S10=2S11=50S25=0&W0		
Dial Header / Trailer	ATDT		
Modem COM Port	0		
Modem Baud Rate	1200		
Dial Access Code			
Download IP / Port	10.5.48.6	10200	
Primary IP / Port	10.5.48.6	10200	
Secondary IP / Port	10.5.48.6	10200	

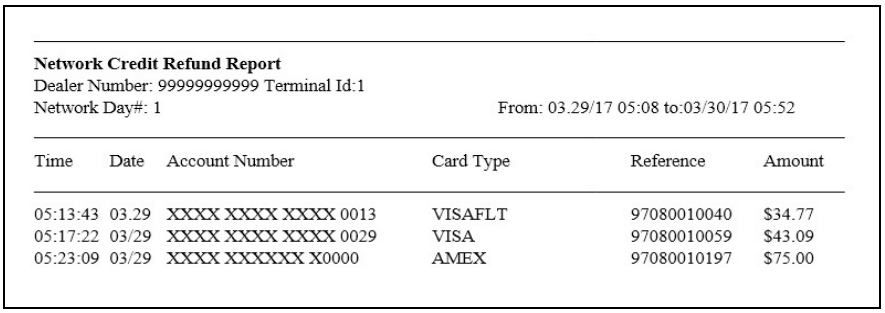
	A	B	C	D	E	F	G	H	I	J	K	L	M	Referral #
AMEX	No	0	Yes	0.00	0	2	50	No	No	No	No	No	0	
CITGO BUS SELECT	No	50	Yes	50.00	0	0	50	No	No	No	No	No	0	
CITGO BUSINESS	No	50	Yes	50.00	0	0	50	No	No	No	No	No	0	
CITGO FLEET	No	50	Yes	50.00	50	2	11	No	No	No	No	No	0	
CITGO PLUS	No	50	Yes	1.00	50	2	50	No	No	No	No	No	0	
CITGO UNIVERSAL	No	50	Yes	50.00	0	0	50	No	No	No	No	No	0	
DEBIT	No	0	No	0.00	0	0	0	No	No	No	No	No	0	
DISCOVER	No	0	Yes	0.00	0	2	50	No	No	No	No	No	0	
DISCOVER	No	0	No	0.00	0	2	50	No	No	No	No	No	0	
DISCOVER	No	0	Yes	0.00	0	2	50	No	No	No	No	No	0	
FLEET ONE	Yes	0	No	999.00	999	2	50	No	No	No	No	No	0	
FLEETWIDE	Yes	0	No	999.00	999	2	50	No	No	No	No	No	0	
FUELMAN	Yes	0	No	999.00	999	2	50	No	No	No	No	No	0	
M/C	No	0	Yes	0.00	0	2	1	No	No	No	No	No	0	
M/C FLEET	No	0	Yes	0.00	0	2	25	No	No	No	No	No	0	
METROSPLASH	No	50	No	50.00	100	2	11	No	No	No	No	No	0	
PREPAID	No	50	No	50.00	100	2	11	No	No	No	No	No	0	
VISA	No	0	Yes	0.00	0	2	99	No	No	No	No	No	0	
VISA FLEET	No	0	Yes	1.00	0	0	11	No	No	No	No	No	0	
VOYAGER	No	50	Yes	50.00	100	2	50	No	No	No	No	No	0	
WEX	No	50	Yes	50.00	0	0	50	No	No	No	No	No	0	
WEX PL	No	50	Yes	50.00	0	0	50	No	No	No	No	No	0	

Man Entry Flag	0			
Activation Limits	5.00		300.00	
Recharge Limits	5.00		300.00	
Cashback Limits	0.00		35.00	0.01
Cashback Fee	0.00			
Debit Transaction Fee	0.00			
Merch Limit Warn	Yes			
Correction Memo Info	0			000000
WEX PL Mask	69004600*			
WEX PL Mask	707138*			
Receipt Masking	3			
Debit Enabled	False			
Debit Pre-Auth Amount	0.00			
Debit CRIND Receipt	0			
PREPAID CARD Enabled	False			
PREPAID CARD Pre-Auth Amount	50.00			
PREPAID CARD CRIND Receipt	2			
MetroSplash CARD Activation Enabled	False			
MetroSplash Sales Enabled	True			
MetroSplash CARD Pre-Auth Amount	50.00			
MetroSplash CARD CRIND Receipt	2			

Network Credit Refund Report

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

Figure 35: Network Credit Refund Report



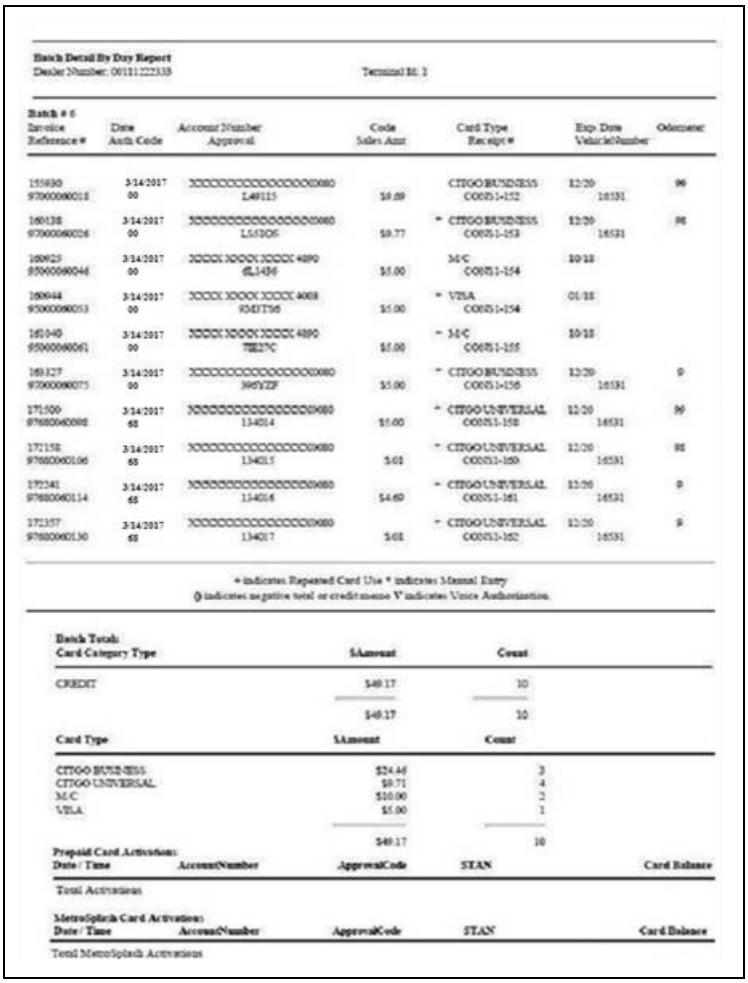
Network Credit Refund Report
Dealer Number: 99999999999 Terminal Id:1
Network Day#: 1 From: 03.29/17 05:08 to:03/30/17 05:52

Time	Date	Account Number	Card Type	Reference	Amount
05:13:43	03.29	XXXX XXXX XXXX 0013	VISAFLT	97080010040	$34.77
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 36: Network Day Report



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

Batch # 6

Invoice Reference #	Date Auth Code	Account Number Approval	Code Sales Amt	Card Type Receipt #	Exp Date Vehicle Number	Odometer
155930 97000060018	3/14/2017 00	XXXXXXXXXXXXXXXX0080 L49115	$8.69	CITGO BUSINESS C00351-152	12/20 16531	99
160138 97000060026	3/14/2017 00	XXXXXXXXXXXXXXXX0080 L51305	$9.77	* CITGO BUSINESS C00351-153	12/20 16531	98
160923 97000060046	3/14/2017 00	XXXX XXXX XXXX 4099 6L1436	$5.00	M/C C00351-154	10/18	
160944 97000060053	3/14/2017 00	XXXX XXXX XXXX 4008 95HT56	$5.00	* VISA C00351-154	01/18	
161040 97000060061	3/14/2017 00	XXXX XXXX XXXX 4099 7HE7C	$5.00	* M/C C00351-155	10/18	
169327 97000060075	3/14/2017 00	XXXXXXXXXXXXXXXX0080 3WYZF	$5.00	* CITGO BUSINESS C00351-156	12/20 16531	9
171509 97000060088	3/14/2017 68	XXXXXXXXXXXXXXXX0080 134014	$5.00	* CITGO UNIVERSAL C00351-158	12/20 16531	99
172158 97000060106	3/14/2017 68	XXXXXXXXXXXXXXXX0080 134015	$.01	* CITGO UNIVERSAL C00351-160	12/20 16531	98
172241 97000060114	3/14/2017 68	XXXXXXXXXXXXXXXX0080 134016	$4.60	* CITGO UNIVERSAL C00351-161	12/20 16531	9
172357 97000060130	3/14/2017 68	XXXXXXXXXXXXXXXX0080 134017	$.01	* CITGO UNIVERSAL C00351-162	12/20 16531	9

* 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	$49.17	10
	$49.17	10

Card Type	$Amount	Count
CITGO BUSINESS	$24.46	3
CITGO UNIVERSAL	$9.71	4
M/C	$10.00	2
VISA	$5.00	1
	$49.17	10

Prepaid Card Activation:

Date / Time	AccountNumber	ApprovalCode	STAN	Card Balance
Total Activations				

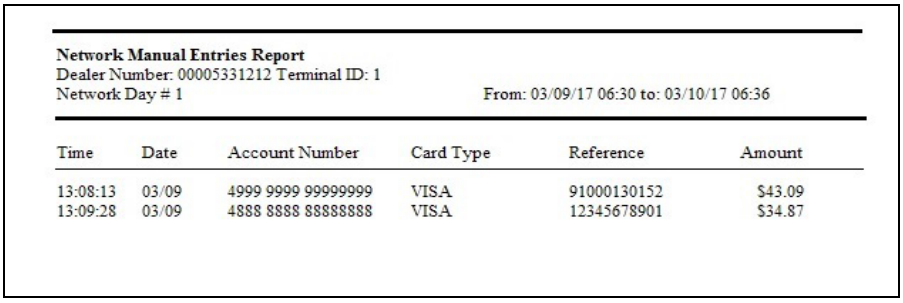
MetroSplash Card Activation:

Date / Time	AccountNumber	ApprovalCode	STAN	Card Balance
Total MetroSplash Activations				

Network Manual Entries Report

The Network Manual Entries Report is available for each day period and lists all network transactions for which the customer manually entered card information. Figure 37 shows a sample of the secure version of the Network Manual Entries Report. The non-secure version prints the account number masked except the last four digits.

Figure 37: Network Manual Entries Report



Network Manual Entries Report
Dealer Number: 00005331212 Terminal ID: 1
Network Day # 1 From: 03/09/17 06:30 to: 03/10/17 06:36

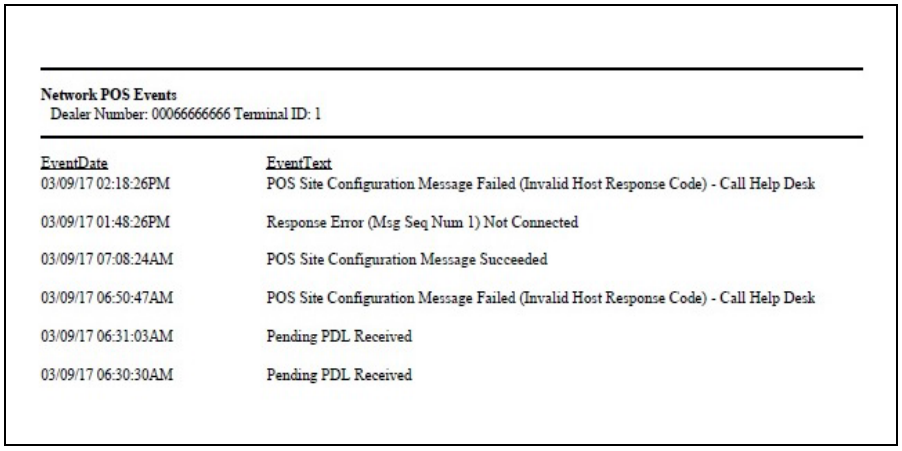
Time	Date	Account Number	Card Type	Reference	Amount
13:08:13	03/09	4999 9999 99999999	VISA	91000130152	$43.09
13:09:28	03/09	4888 8888 88888888	VISA	12345678901	$34.87

Network POS Events

The Network POS Events Report provides a list of significant POS processing events. This report records the following events:

- Network Response Errors
- Hot Catch-up Start and End
- PDL Messages
- Out of Balance Batches
- Batch Removal
- Fallback File Full Conditions

Figure 38: Network POS Events



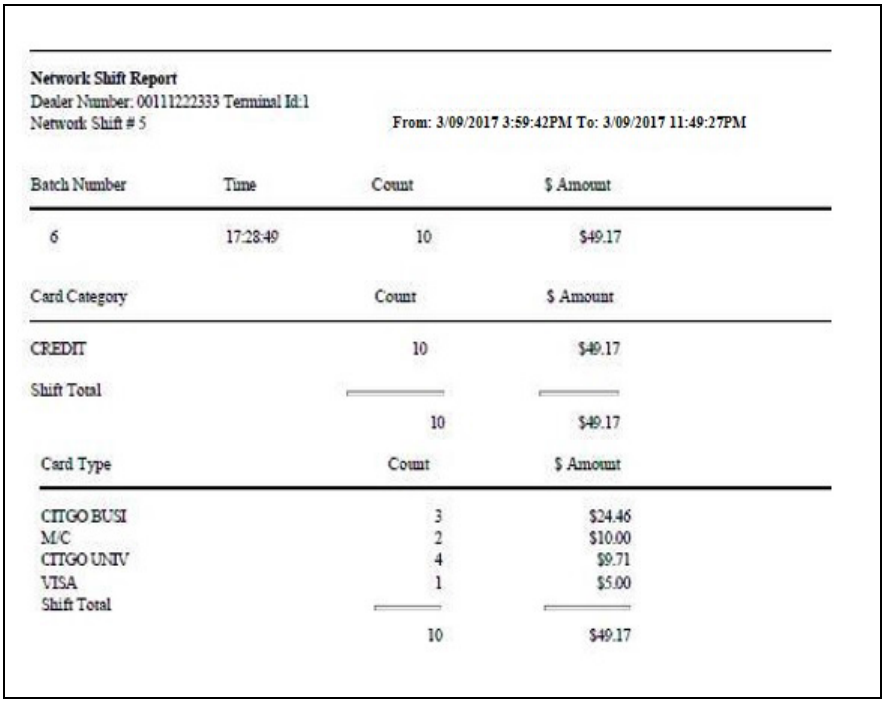
Network POS Events
Dealer Number: 00066666666 Terminal ID: 1

EventDate	EventText
03/09/17 02:18:26PM	POS Site Configuration Message Failed (Invalid Host Response Code) - Call Help Desk
03/09/17 01:48:26PM	Response Error (Msg Seq Num 1) Not Connected
03/09/17 07:08:24AM	POS Site Configuration Message Succeeded
03/09/17 06:50:47AM	POS Site Configuration Message Failed (Invalid Host Response Code) - Call Help Desk
03/09/17 06:31:03AM	Pending PDL Received
03/09/17 06:30:30AM	Pending PDL Received

Network Shift Report

The Network Shift Report is available for shift periods and provides network transaction information for the shift. Information includes batch summary totals, card category totals (CREDIT, CREDIT REFUND, DEBIT, PREPAID), and summary count and dollar amount totals by card type.

Figure 39: Network Shift Report



Network Shift Report
Dealer Number: 00111222333 Terminal Id:1
Network Shift # 5 **From: 3/09/2017 3:59:42PM To: 3/09/2017 11:49:27PM**

Batch Number	Time	Count	$ Amount
6	17:28:49	10	$49.17

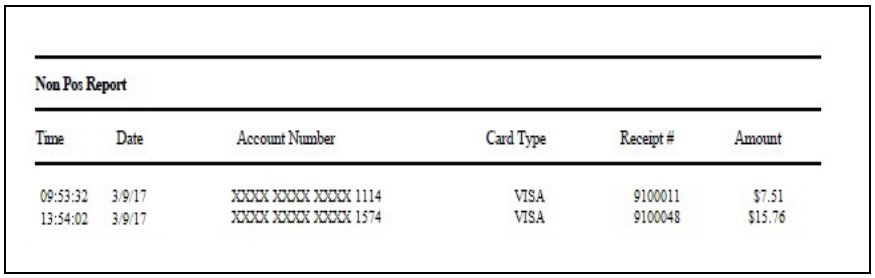
Card Category	Count	$ Amount
CREDIT	10	$49.17
Shift Total	10	$49.17

Card Type	Count	$ Amount
CITGO BUSI	3	$24.46
M/C	2	$10.00
CITGO UNIV	4	$9.71
VISA	1	$5.00
Shift Total	10	$49.17

Non-POS Report

The Non-POS Report is available for day periods and provides information on all credit card transactions not processed by the HPS-Dallas CITGO network, such as Imprinter transactions.

Figure 40: Non-POS Report



Non Pos Report

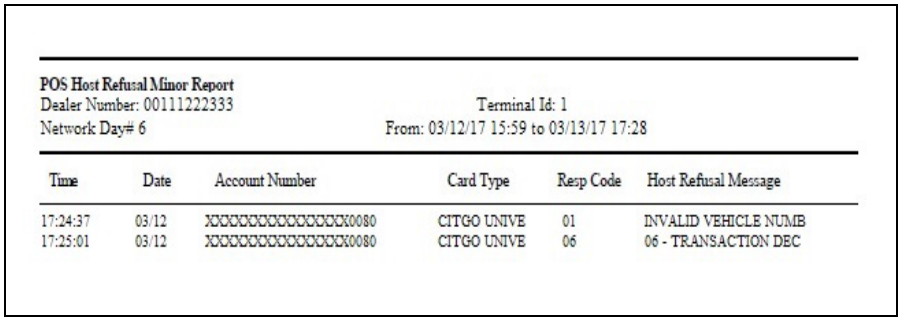
Time	Date	Account Number	Card Type	Receipt #	Amount
09:53:32	3/9/17	XXXX XXXX XXXX 1114	VISA	9100011	$7.51
13:54:02	3/9/17	XXXX XXXX XXXX 1574	VISA	9100048	$15.76

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 CITGO network. The 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 (repeat card use not included).

Figure 41: POS Host Refusal Minor Report



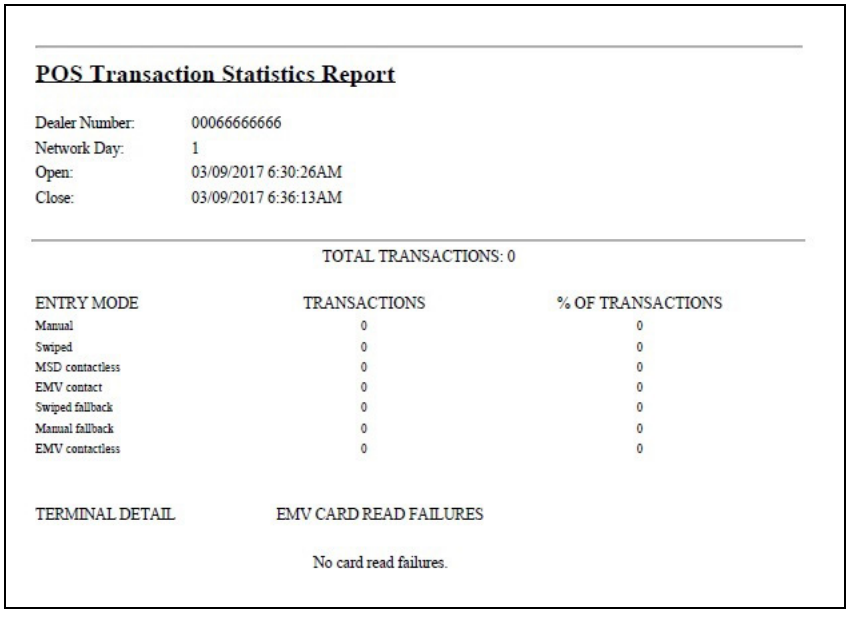
POS Host Refusal Minor Report
Dealer Number: 00111222333 Terminal Id: 1
Network Day# 6 From: 03/12/17 15:59 to 03/13/17 17:28

Time	Date	Account Number	Card Type	Resp Code	Host Refusal Message
17:24:37	03/12	XXXXXXXXXXXXXXX0080	CITGO UNIVE	01	INVALID VEHICLE NUMB
17:25:01	03/12	XXXXXXXXXXXXXXX0080	CITGO UNIVE	06	06 - TRANSACTION DEC

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 42: POS Transaction Statistics Report



POS Transaction Statistics Report

Dealer Number: 00066666666
Network Day: 1
Open: 03/09/2017 6:30:26AM
Close: 03/09/2017 6:36:13AM

TOTAL TRANSACTIONS: 0

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

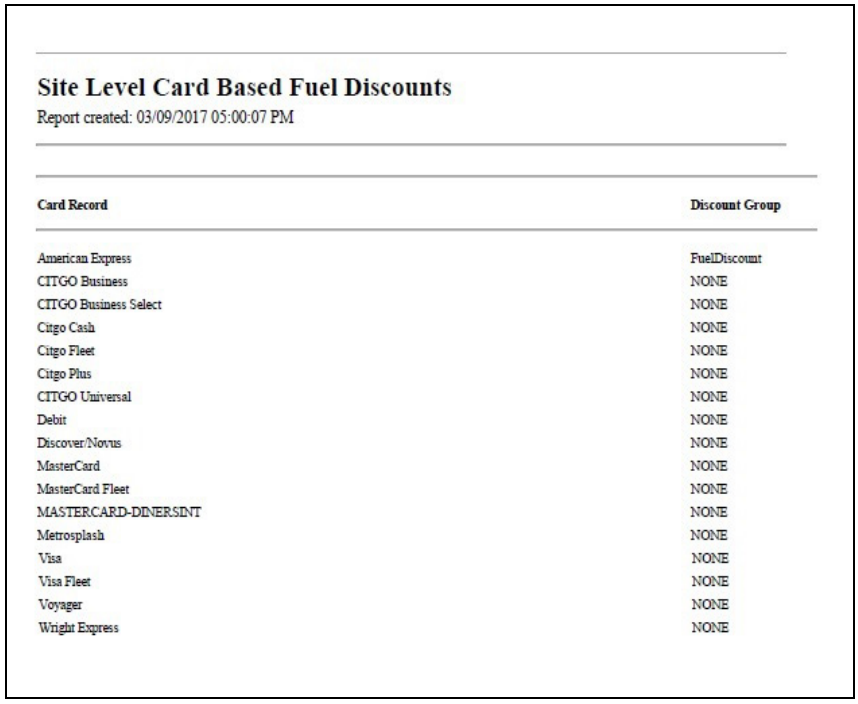
TERMINAL DETAIL EMV CARD READ FAILURES

No card read failures.

Site Level Card Based Fuel Discounts Report

The Site Level Card Based Fuel Discounts report is available on demand. It provides programming information for fuel discount by network card type as programmed in **MWS > Set Up > Network > HPS > Fuel Discount Configuration**.

Figure 43: Site Level Card Based Fuel Discounts Report



Site Level Card Based Fuel Discounts

Report created: 03/09/2017 05:00:07 PM

Card Record	Discount Group
American Express	FuelDiscount
CITGO Business	NONE
CITGO Business Select	NONE
Citgo Cash	NONE
Citgo Fleet	NONE
Citgo Plus	NONE
CITGO Universal	NONE
Debit	NONE
Discover/Novus	NONE
MasterCard	NONE
MasterCard Fleet	NONE
MASTERCARD-DINERSINT	NONE
Metrosplash	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 may view the Network Status and access the following tools:

- Batch Close
- Balance Request
- Electronic Mail
- Comm Test

Accessing Network Functions

You can access the Network Status screen by selecting the **Network** button. For more information, refer to "Checking Network Status" on page 46.

Figure 44: Network Button

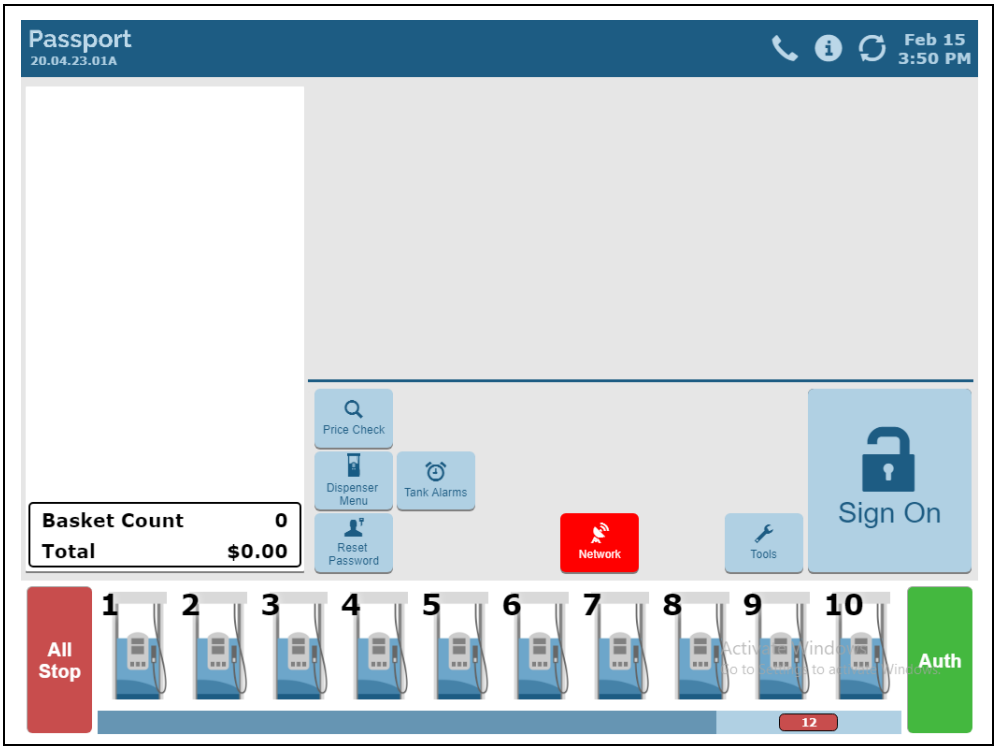
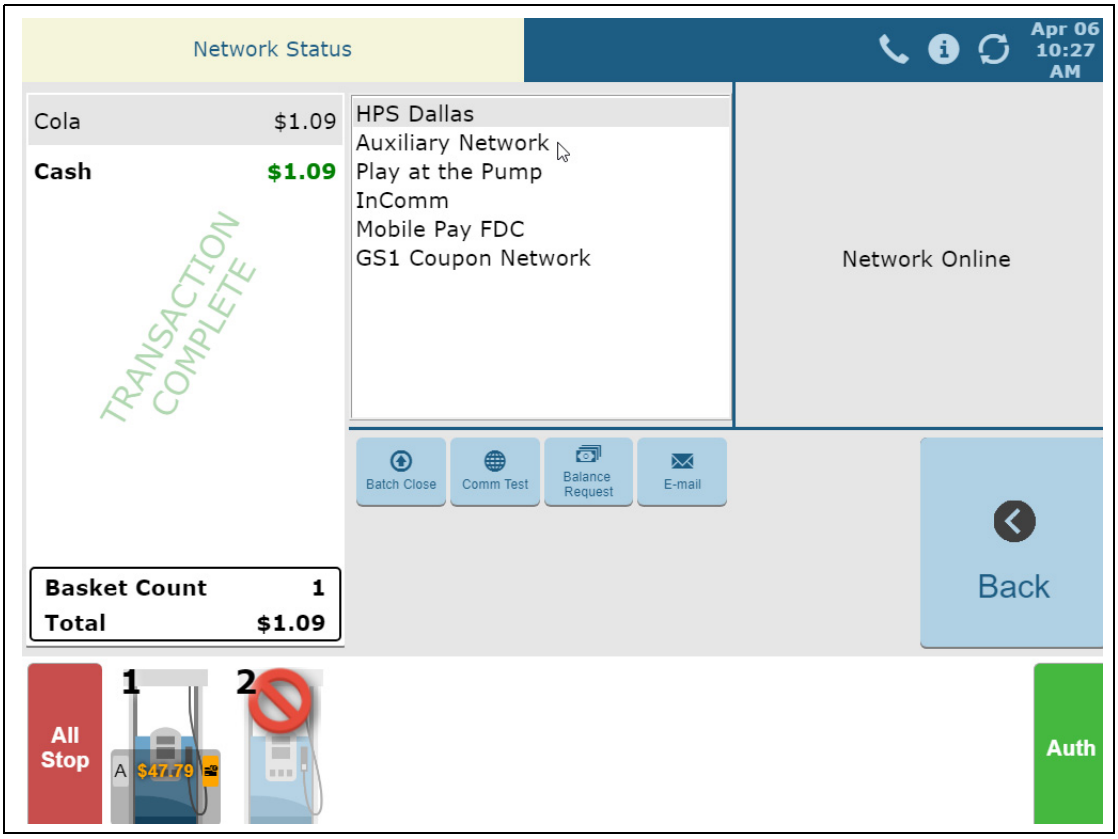


Figure 45: CWS Network Status Screen



The Network Status screen provides information on all networks connected to Passport. Select a network in the middle pane and its status appears in the right pane.

Checking 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
Blue	Low
Yellow	Medium
Red	High

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

Performing a 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 sales transaction by selecting the **Batch Close** button.

You can perform a batch close whenever you are not in a 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**.

Receiving Email from CWS

Passport notifies you when it receives an email from the HPS-Dallas CITGO network. Passport saves all emails for 60 days.
Note: You can receive an email 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.

Checking Card Balance

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

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

2. Swipe the cash card/EBT card
   *Note: If Passport cannot identify the card as a cash card, Passport prompts the cashier if the card is an EBT Cash card. If the cashier responds with **Yes**, Passport makes an EBT Cash card balance request; otherwise, Passport makes an EBT Food card balance inquiry.*

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

Checking Comm Test

To test communications with the HPS-Dallas network, proceed as follows:

1. From the Network Status screen, select **COMM TEST** (see Figure 45 on page 46).

2. If Passport is communicating properly with the HPS-Dallas network, "Connected to Host" message is displayed.

Appendix A: Network Events Messages

Message	Priority	Meaning
Network Connection Offline	N/A	For TCP/IP (satellite) locations, this message means that a previous message expired and the site is waiting for confirmation that Passport is connected to the HPS-Dallas CITGO 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 Store 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 CITGO 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: Upgrading to Passport V20

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

Due to the End of Life of the Ingenico PIN Pads (iSC250 and iPP320) they were not certified with the HPS-Dallas network for Passport V20. Although, the iSC250 and iPP320 will still process EMV transactions on V20.02, it is recommended that a site upgrade their PIN Pads to Verifone MX915 to remain in compliance with the approved HPS-Dallas network EMV configuration. Sites that continue using iSC250 or iPP320 after upgrading to Passport V20.02 will be at their own risk for receiving fraud liability chargebacks due to using a non-EMV certified solution.

When upgrading to V20.04, Passport will check to see if an Ingenico PIN Pad is connected. If one is detected, an error message will be displayed and the upgrade will be aborted. For a clean install of V20.04, Ingenico will not be an option on the Register Set Up screen.

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

Step	Task Description
1	Ensure that all the dispenser software and firmware meet applicable requirements to support loyalty and other fuel discounting functionality (including support of $0.000 PPU).
2	Print the **Network Configuration Report**. This will be helpful if a clean install is required and to confirm all network settings (including Host Connection Type and other parameters in Global Information).
3	Perform Store Close and ensure all network transactions have completed by checking the Store and Forward Transactions Report for fallback transaction information.
4	Call the CITGO Help Desk at 1-800-533-3421 to ensure the Store Close is successful and confirm that the HPS-Dallas network is prepared to enable EMV PDL downloads or TLS, if applicable. *Note: If Passport V20.04 is being installed, the ASC should contact CITGO Help Desk (1-800-533-3421), 24 hours in advance to inform them of the upgrade to V20.04 and the need for PDL 20.*
5	Assist the merchant or store manager to print additional accounting and network reports as needed.
6	Ensure that all file transfers from Passport to the BOS have completed.

After the upgrade:
The ASC must perform the following steps after the upgrade:

Step	Task Description
1	Request a PDL Download by going to **MWS** > **Set Up** > **Network** > **HPS** > **PDL Download**. For more information on requesting a PDL Download, refer to "Requesting PDL Download" on page 18.
2	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.
3	Review the parameters on the EMV Parameters tab in **MWS** > **Set Up** > **Network** > **HPS** > **Global Info Editor** with the merchant or store manager. Advise them to contact the CITGO Help Desk at 1-800-533-3421 to discuss financial implications of the suggested settings on this screen.
4	If installing a VeriFone MX915 PIN Pad, ensure the **MWS** > **Set Up Register** > **Register Set Up** > **Device Configuration** > **EMV Capable** field is selected.
5	If enabling TCP/IP and TLS, call the CITGO Help Desk at 1-800-533-3421 to obtain new IP addresses, IP ports, and TLS settings for network site configuration on Passport.
6	Print a new **Site Level Card Based Fuel Discounts Report**. If some card types no longer have their fuel discount or if the manager wishes to target new card types with fuel discounts, go to **MWS > Set Up > Network > HPS > Fuel Discount Configuration** and update the fuel discounts accordingly. Select **Save** to save the changes to the Passport database and exit.

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

© 2021 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-5547B Passport™ V20 Network Addendum for HPS-Dallas CITGO® · July 2021