Mobile Payment

Feature Reference

Date: April 11, 2023

Verifone®

Mobile Payment

Using This Feature Reference

This Feature Reference provides detailed information on how to configure and use the Mobile Payment feature on the Verifone Commander.

This feature document contains the subsections listed below:

- **Overview** - This section contains a brief description, requirements and the supported hardware configurations for the Mobile Payment feature on the Verifone Commander.
- **Configuring** - This section contains information on how to configure the Mobile Payment feature on the Verifone Commander.
- **Using** - This section describes using the Mobile Payment feature.
- **Reporting** - This section contains sample reports with detailed report descriptions for the Mobile Payment feature on the Verifone Commander.
- **Troubleshooting** - This section provides basic troubleshooting steps.

The content of this document is subject to change without notice. The information contained herein does not represent a commitment on the part of VeriFone, Inc. All features and specifications are subject to change without notice.

Revision History

Date	Description
10/21/2015	Initial Documentation Release
05/25/2016	Updated format. 2016 Copyright. Updated partner list.
02/02/2017	2017 Copyright. Updated Reporting information.Updated network configuration.
02/23/2017	Update Mobile Payment Host Configuration.
05/01/2017	Updated Reporting information.
07/19/2019	Updated with Conexxus V2 updates.
01/04/2022	Added the Mobile Payment (Collected by Host) Report.
04/11/2023	Updated cover and copyright notice, Updated for Mobile Payment Configuration in Verifone C-Site Management. Added C18 references for POS support. Added touchscreen configuration for MOP.

Contents

Overview

Feature Description

The Mobile Payment feature reference provides information on the parameters used to setup a site to accept Mobile Payments with a Verifone Commander.

This feature enables mobile payment, loyalty, delivery and transaction processing using a consumer's smart phone with a loaded Mobile Payment Application (MPA), a third party FEP vendor and a third party Mobile Payment Processing Application (MPPA) host.

Mobile payment configurations are specific to the Mobile Payment Host, such as the merchant ID (MID). The specific parameters for each Mobile Payment Host are not documented in this feature reference manual and must be obtained from the Mobile Payment Host.

Hardware Requirements

- Verifone Commander with Topaz, Ruby2, and/or C18
- Verifone RubyCi with Topaz, Ruby2, and/or C18

Software Requirements

- Verifone Commander software base 39 and higher.
- Verifone C-Site Management configuration and updates support of Mobile Configuration available starting in software base 53.41.

Configuring Mobile Payments

Pre-Requisites

The following list of requirements must be met by the location prior to Mobile Payment setup:

- The site must setup connectivity to the MPPA using either a VPN or the latest TLS protocol.
- Contact the Mobile Host Provider (MPPA) for site onboarding information.

Site Onboarding Information

The following data fields should be obtained from the Mobile Application Partner and the site for identifying the site on the mobile application.

Mobile Host Provided

- Adapter (Mobile payment APIs used by site system for communication with MPPA)
- Program Name (Program name as defined by MPPA)
- Authentication Type (Generate Token, Display Token, Scan Token, Enter Token)
- Host IP Address
- Port
- TLS Enabled
- Site Terminal ID
- Merchant ID
- Location ID
- Settlement Employee Number (**optional)

Site Provided

- Phone: (store phone (xxx) xxx-xxxx)
- Welcome Message (may be left blank)

NOTE

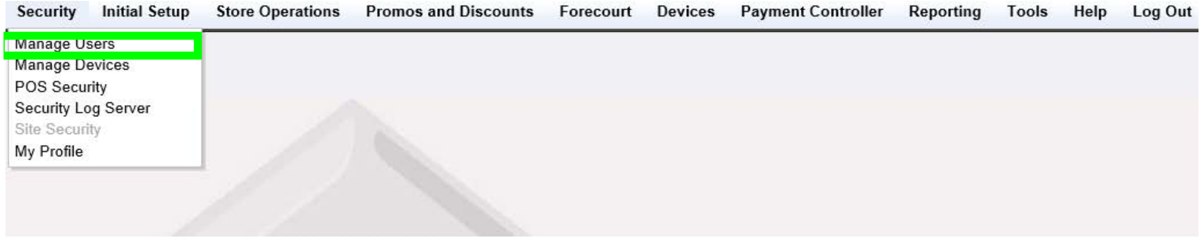
The protocol has changed from SSL to TLS for better encryption and security.

Configuring User Roles for Mobile Configuration and Reports

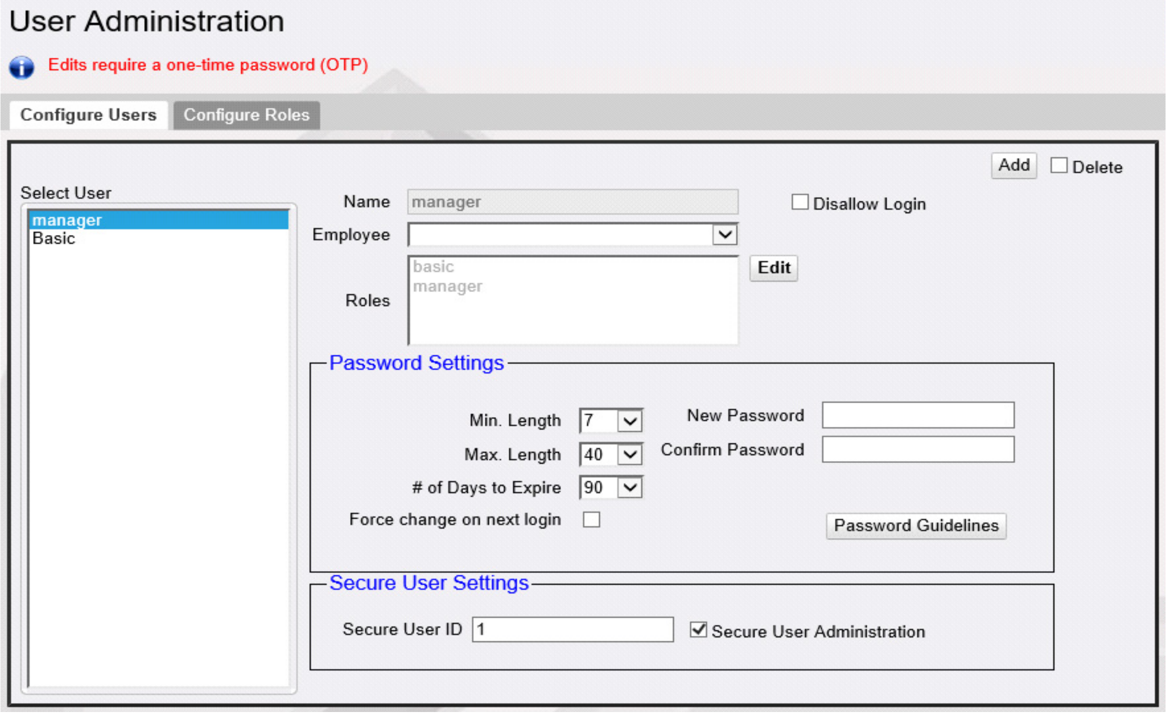
New installations will have default roles configured with all Mobile functions enabled, however, system upgrades will require additional user role setup.

NOTE *Any configuration import after a new install will require manually editing user roles for Mobile Payment function access.*

1. From the Configuration Client, go to: **Security > Manage Users**.



The User Administration window displays.


User Administration

Edits require a one-time password (OTP)

Name: manager

Employee:

Roles: basic, manager

Password Settings

Min. Length: 7

Max. Length: 40

# of Days to Expire: 90

Force change on next login: □

New Password:

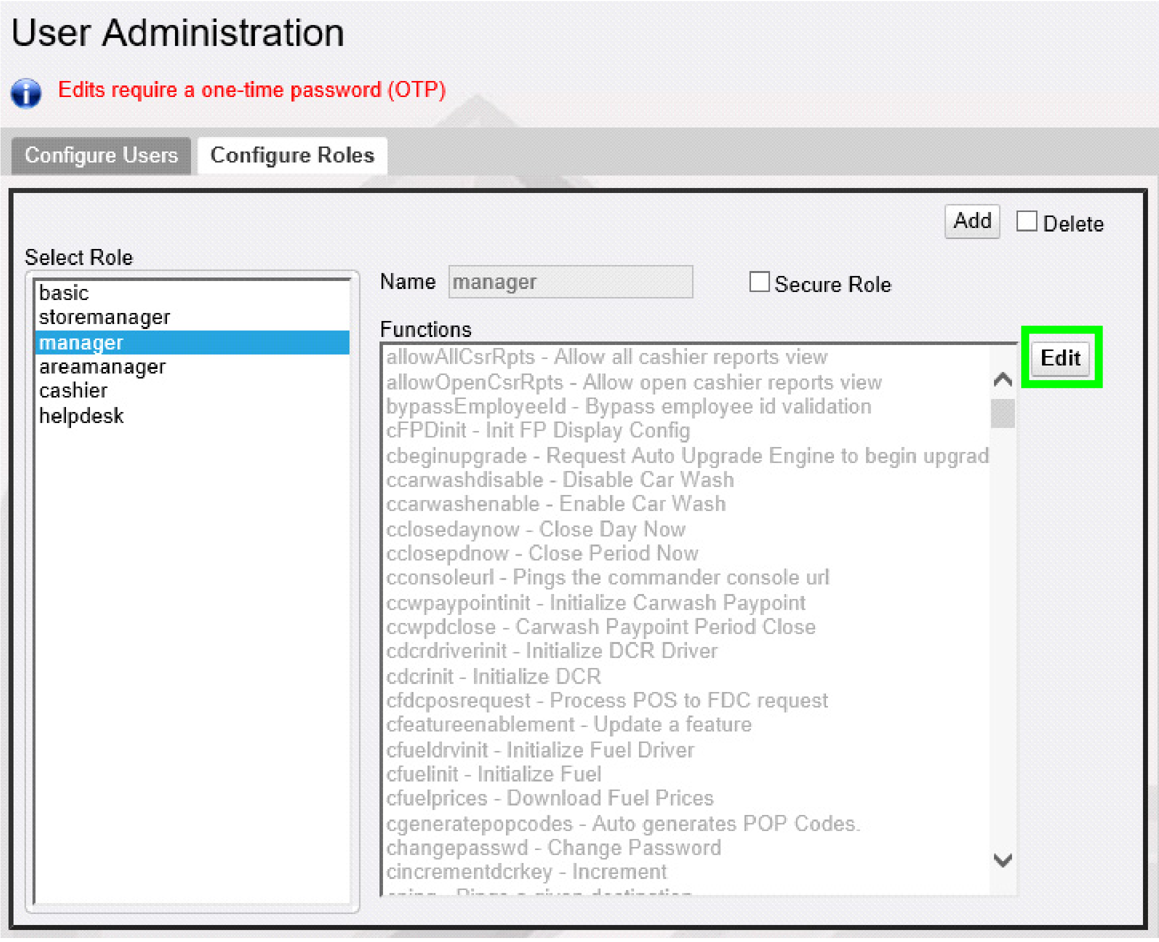
Confirm Password:

Secure User Settings

Secure User ID: 1

☑ Secure User Administration

2. From the User Administration window, select the **[Configure Roles]** tab.
3. In the Select Role pane, click to select the **<role>** to configure.
4. Select **[Edit]**.



Edits require a one-time password (OTP)

Select Role

- basic
- storemanager
- manager
- areamanager
- cashier
- helpdesk

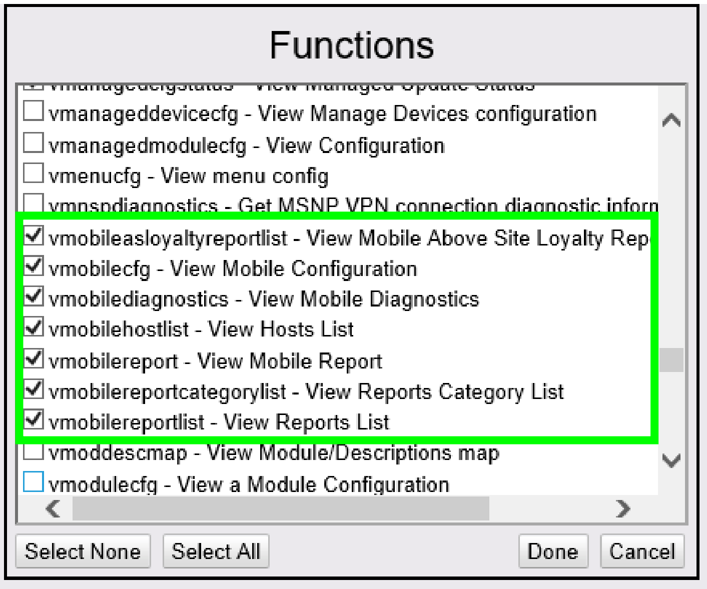
Name: manager

□ Secure Role

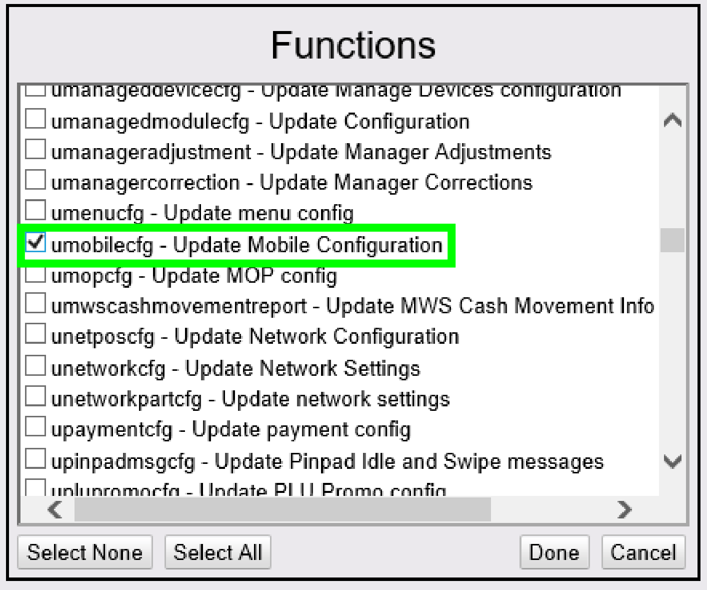
Functions

- allowAllCsrRpts - Allow all cashier reports view
- allowOpenCsrRpts - Allow open cashier reports view
- bypassEmployeeId - Bypass employee id validation
- cFPDinit - Init FP Display Config
- cbeginupgrade - Request Auto Upgrade Engine to begin upgrad
- ccarwashdisable - Disable Car Wash
- ccarwashenable - Enable Car Wash
- cclosedaynow - Close Day Now
- cclosepdnow - Close Period Now
- cconsoleurl - Pings the commander console url
- ccwpaypointinit - Initialize Carwash Paypoint
- ccwpdclose - Carwash Paypoint Period Close
- cdcrdriverinit - Initialize DCR Driver
- cdcrinit - Initialize DCR
- cfdcposrequest - Process POS to FDC request
- cfeatureenablement - Update a feature
- cfueldrvinit - Initialize Fuel Driver
- cfuelinit - Initialize Fuel
- cfuelprices - Download Fuel Prices
- cgeneratepopcodes - Auto generates POP Codes.
- changepasswd - Change Password
- cincrementdcrkey - Increment

5. Scroll the Functions List, locate and click to select and enable the following functions:
   - **umobilecfg** - Update Mobile Configuration
   - vmobileasloyaltyreport - View Mobile Above Site Loyalty Report
   - **vmobilecfg** - View Mobile Configuration
   - vmobilediagnostics - View Mobile Diagnostics
   - **vmobilehostlist** - View Hosts List
   - vmobilereportcategorylist - View Report’s Category List
   - **vmobilereport** - View Mobile Report
   - **vmobilereportlist** - View Reports List



☑ vmanagedcfgstatus - View Managed Update Status
□ vmanageddevicecfg - View Manage Devices configuration
□ vmanagedmodulecfg - View Configuration
□ vmenucfg - View menu config
□ vmnspdiagnostics - Get MSNP VPN connection diagnostic inforn
☑ vmobileasloyaltyreportlist - View Mobile Above Site Loyalty Rep
☑ vmobilecfg - View Mobile Configuration
☑ vmobilediagnostics - View Mobile Diagnostics
☑ vmobilehostlist - View Hosts List
☑ vmobilereport - View Mobile Report
☑ vmobilereportcategorylist - View Reports Category List
☑ vmobilereportlist - View Reports List
□ vmoddescmap - View Module/Descriptions map
□ vmodulecfg - View a Module Configuration



□ umanageddevicecfg - Update Manage Devices configuration
□ umanagedmodulecfg - Update Configuration
□ umanageradjustment - Update Manager Adjustments
□ umanagercorrection - Update Manager Corrections
□ umenucfg - Update menu config
☑ umobilecfg - Update Mobile Configuration
□ umopcfg - Update MOP config
□ umwscashmovementreport - Update MWS Cash Movement Info
□ unetposcfg - Update Network Configuration
□ unetworkcfg - Update Network Settings
□ unetworkpartcfg - Update network settings
□ upaymentcfg - Update payment config
□ upinpadmsgcfg - Update Pinpad Idle and Swipe messages
□ uplupromocfg - Update PLU Promo config

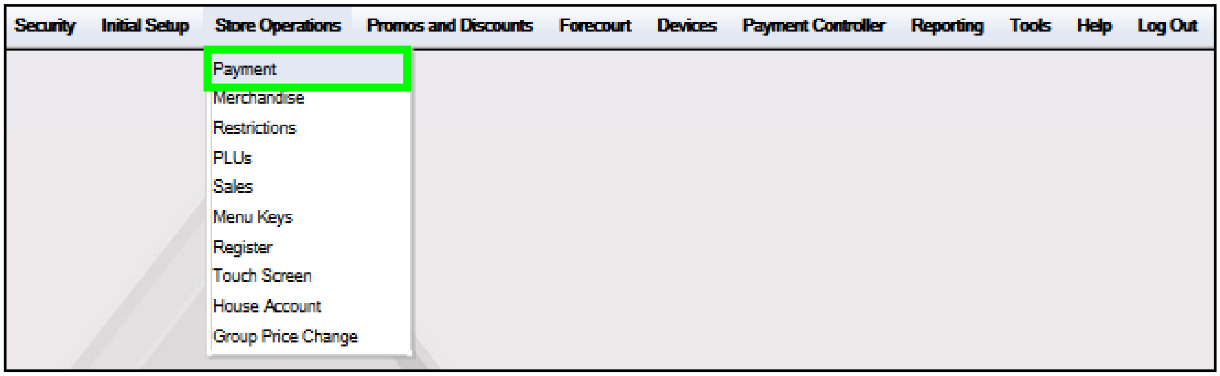
6. Click **[Done]**.
7. Select **[Save]** to accept, or **[Cancel]** to exit without saving changes.
8. Log out and log back into the Configuration Client for changes to take effect.

Configure Mobile Method of Payment (MOP)

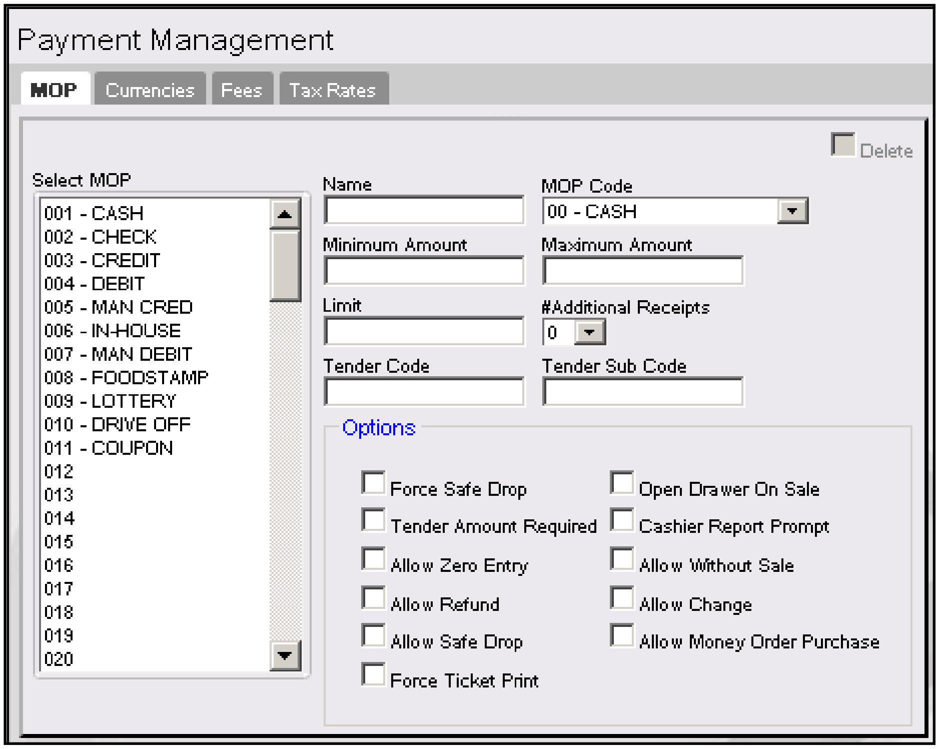
NOTE

New installations have a default Method of Payment and Code configured in the system to accept mobile payments.
If however, the system is upgraded, then the MOP and MOP Code must be configured.
If the site imported the mobile configuration using the ***Import and Export*** utility, either on a new install or upgrade, the Mobile MOP and Code will need to be configured manually.

1. From the Configuration Client, go to: Store Operations > Payment.



The Payment Management window displays.



Select MOP

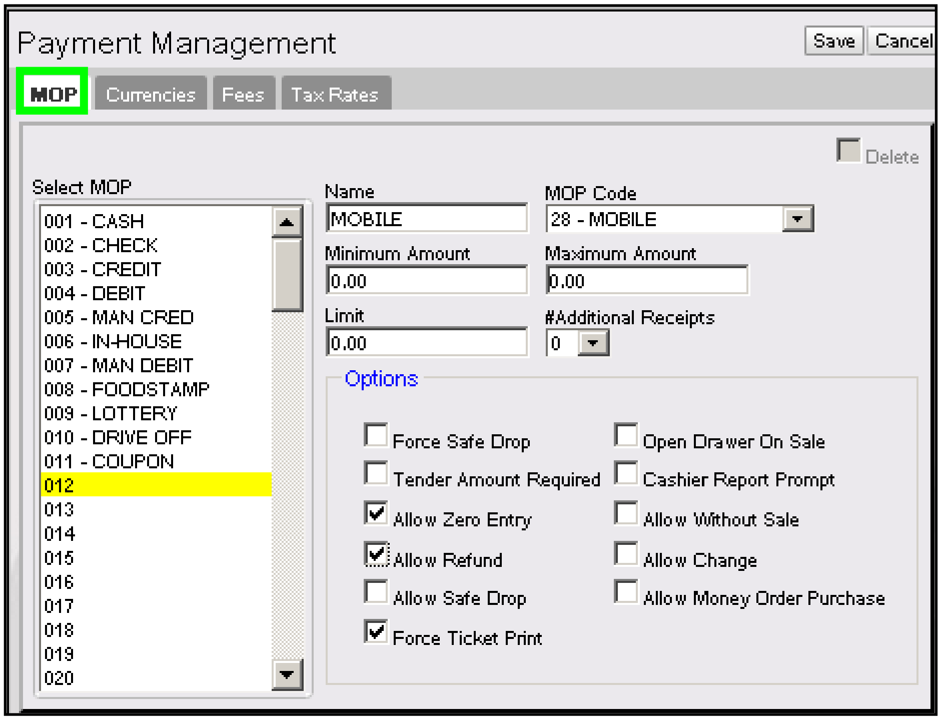
001 - CASH
002 - CHECK
003 - CREDIT
004 - DEBIT
005 - MAN CRED
006 - IN-HOUSE
007 - MAN DEBIT
008 - FOODSTAMP
009 - LOTTERY
010 - DRIVE OFF
011 - COUPON
012
013
014
015
016
017
018
019
020

Name:
MOP Code: 00 - CASH
Minimum Amount:
Maximum Amount:
Limit:
#Additional Receipts: 0
Tender Code:
Tender Sub Code:

Options

□ Force Safe Drop
□ Open Drawer On Sale
□ Tender Amount Required
□ Cashier Report Prompt
□ Allow Zero Entry
□ Allow Without Sale
□ Allow Refund
□ Allow Change
□ Allow Safe Drop
□ Allow Money Order Purchase
□ Force Ticket Print

2. From the Payment Management window, select the **[MOP]** tab.



□ Delete

Select MOP

001 - CASH
002 - CHECK
003 - CREDIT
004 - DEBIT
005 - MAN CRED
006 - IN-HOUSE
007 - MAN DEBIT
008 - FOODSTAMP
009 - LOTTERY
010 - DRIVE OFF
011 - COUPON
012
013
014
015
016
017
018
019
020

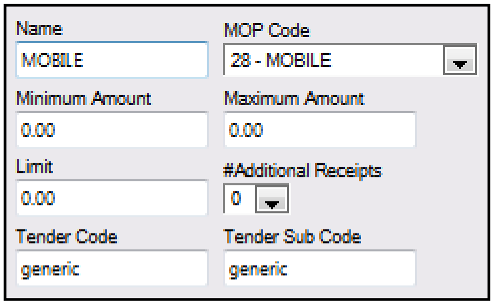
Name: MOBILE
MOP Code: 28 - MOBILE
Minimum Amount: 0.00
Maximum Amount: 0.00
Limit: 0.00
#Additional Receipts: 0

Options

□ Force Safe Drop
□ Open Drawer On Sale
□ Tender Amount Required
□ Cashier Report Prompt
☑ Allow Zero Entry
□ Allow Without Sale
☑ Allow Refund
□ Allow Change
□ Allow Safe Drop
□ Allow Money Order Purchase
☑ Force Ticket Print

3. Scroll down the **<Select MOP>** pane to an unused position.

4. Configure the Mobile MOP parameters.

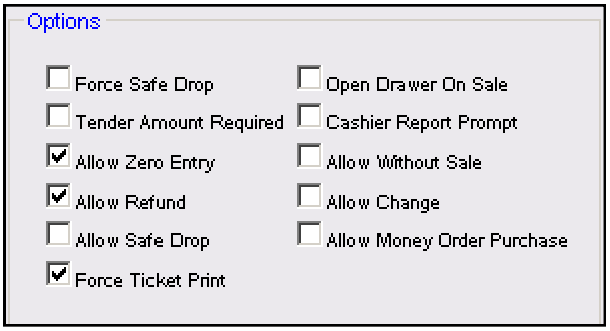


Name: MOBILE
MOP Code: 28 - MOBILE
Minimum Amount: 0.00
Maximum Amount: 0.00
Limit: 0.00
#Additional Receipts: 0
Tender Code: generic
Tender Sub Code: generic

Variable	Value
Name	Enter: **MOBILE**
MOP Code	Select: **28 - MOBILE**
Minimum Amount	Indicates the minimum amount accepted <$0.00-9999.99>.
Maximum Amount	Indicates the maximum amount accepted <$0.00-9999.99>.

Variable	Value
Limit	Alerts the cashier to the Mobile MOP limit <$0.00-9999.99>.
#Additional Receipts	Indicates how many additional receipts are required <0-3>.
Tender Code	Generic.
Tender Sub Code	Generic.

5. Select to enable additional Options parameters.



Options

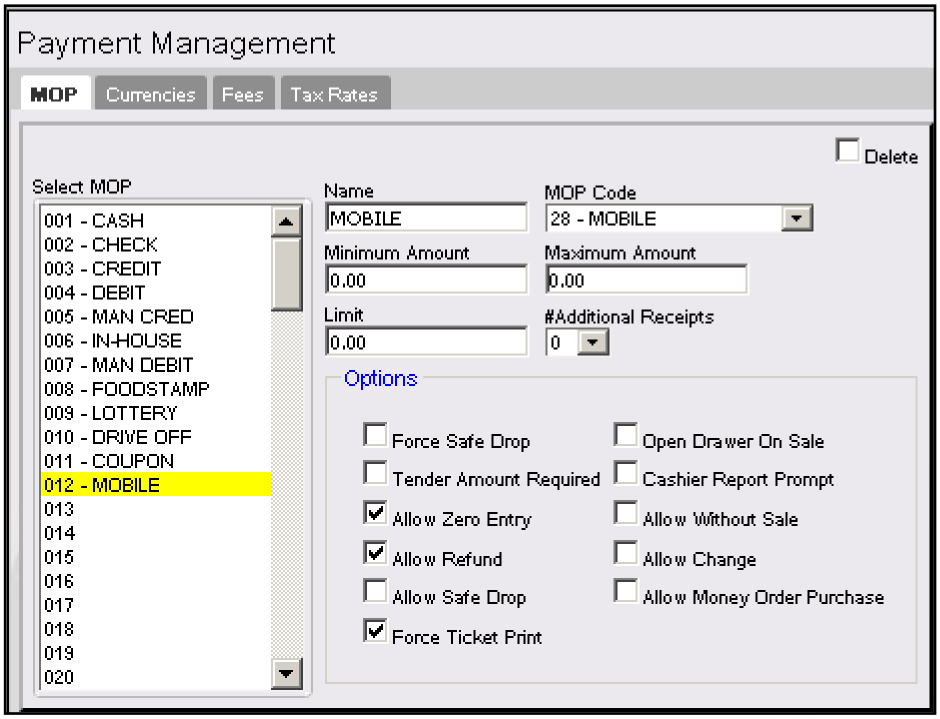
☐ Force Safe Drop
☐ Tender Amount Required
☑ Allow Zero Entry
☑ Allow Refund
☐ Allow Safe Drop
☑ Force Ticket Print
☐ Open Drawer On Sale
☐ Cashier Report Prompt
☐ Allow Without Sale
☐ Allow Change
☐ Allow Money Order Purchase

Variable	Value
Force Safe Drop	Enables a safe drop message (if the Limit value is not 0.00).
Tender Amount Required	Requires the clerk to enter an actual (counted) drawer amount before selecting this MOP.
Allow Zero Entry	Indicates a zero entry is allowed when entering a drawer amount.
Allow Refund	Permits a Refund transaction to be tendered.
Allow Safe Drop	Allows a safe drop.
Force Ticket Print	Forces a receipt to be printed for transactions that includes this MOP.
Open Drawer On Sale	Forces the cash drawer to open when a transaction includes this payment type.
Cashier Report Prompt	Prompts a cashier to enter the actual (counted) drawer amount when printing cashier report.

Variable	Value
Allow Without Sale	Permits acceptance without purchase. For example, cashing in a winning lottery ticket or permitting a check to be cashed without a purchase.
Allow Change	Allows the cashier to make change when “amount > amount due” is selected. For example, if a check can be written for more than the purchase amount.
Allow Money Order Purchase	Permits a money order sale.

6. Select **[Save]** to accept, or **[Cancel]** to exit without saving changes.

The setup of the Mobile Method of Payment is complete.



Payment Management

□ Delete

Select MOP

001 - CASH
002 - CHECK
003 - CREDIT
004 - DEBIT
005 - MAN CRED
006 - IN-HOUSE
007 - MAN DEBIT
008 - FOODSTAMP
009 - LOTTERY
010 - DRIVE OFF
011 - COUPON
012 - MOBILE
013
014
015
016
017
018
019
020

Name: MOBILE

MOP Code: 28 - MOBILE

Minimum Amount: 0.00

Maximum Amount: 0.00

Limit: 0.00

#Additional Receipts: 0

Options

□ Force Safe Drop
□ Tender Amount Required
☑ Allow Zero Entry
☑ Allow Refund
□ Allow Safe Drop
☑ Force Ticket Print
□ Open Drawer On Sale
□ Cashier Report Prompt
□ Allow Without Sale
□ Allow Change
□ Allow Money Order Purchase

NOTE

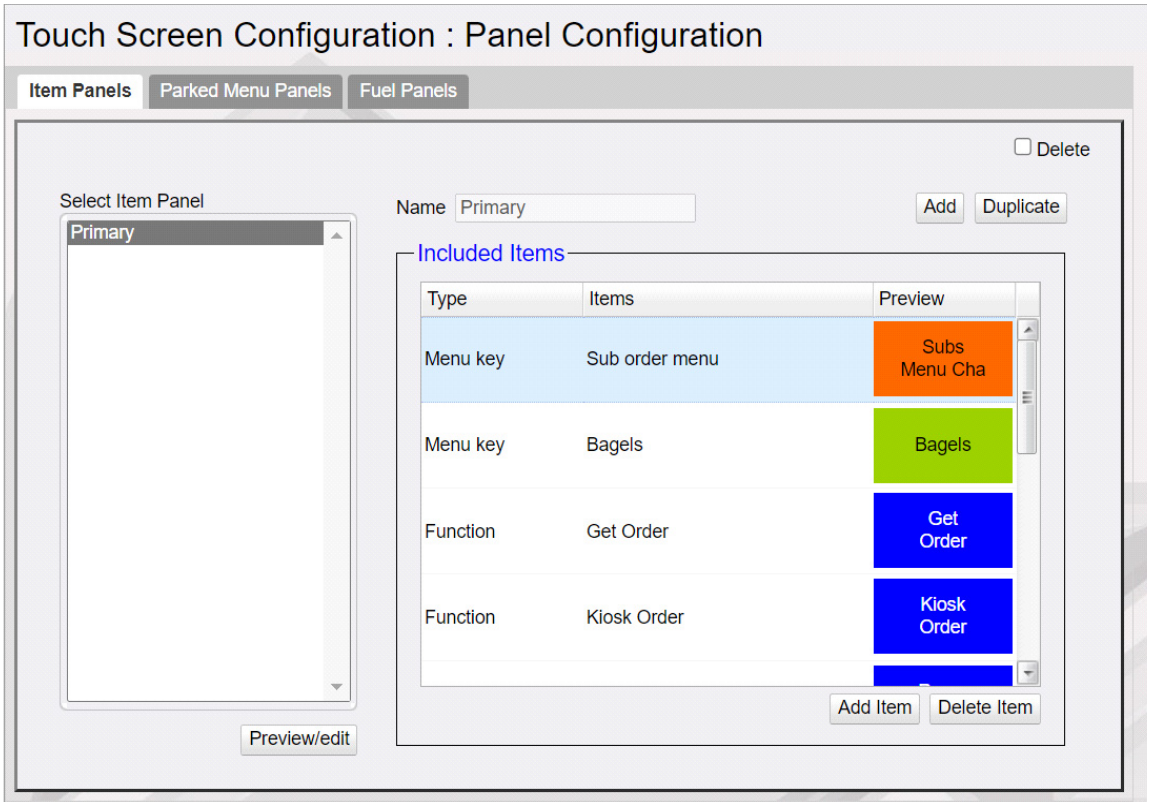
The Mobile Method of Payment must be assigned to a button on the POS touchscreen to be used. See the next section for details on how to add the button to the screen.

Mobile Payment Touchscreen Configuration

The Method of Payment created for Mobile Payment will need to be added to the POS touchscreen. The following instructions will discuss how to add the MOP to the touchscreen button to Verifone Commander software base 53+.

*For details on how to add the button on older software, please refer to the **Commander User Reference Guides** located on the Support.Verifone.com website under Support Articles > Petro & Convenience > Commander & RubyCi > Manuals & User Guides > Commander User References.*

1. From Configuration Client navigate to **Store Operations > Touchscreen > Panel Configuration > Item Panel Tab**.



Touch Screen Configuration : Panel Configuration

Select Item Panel: Primary

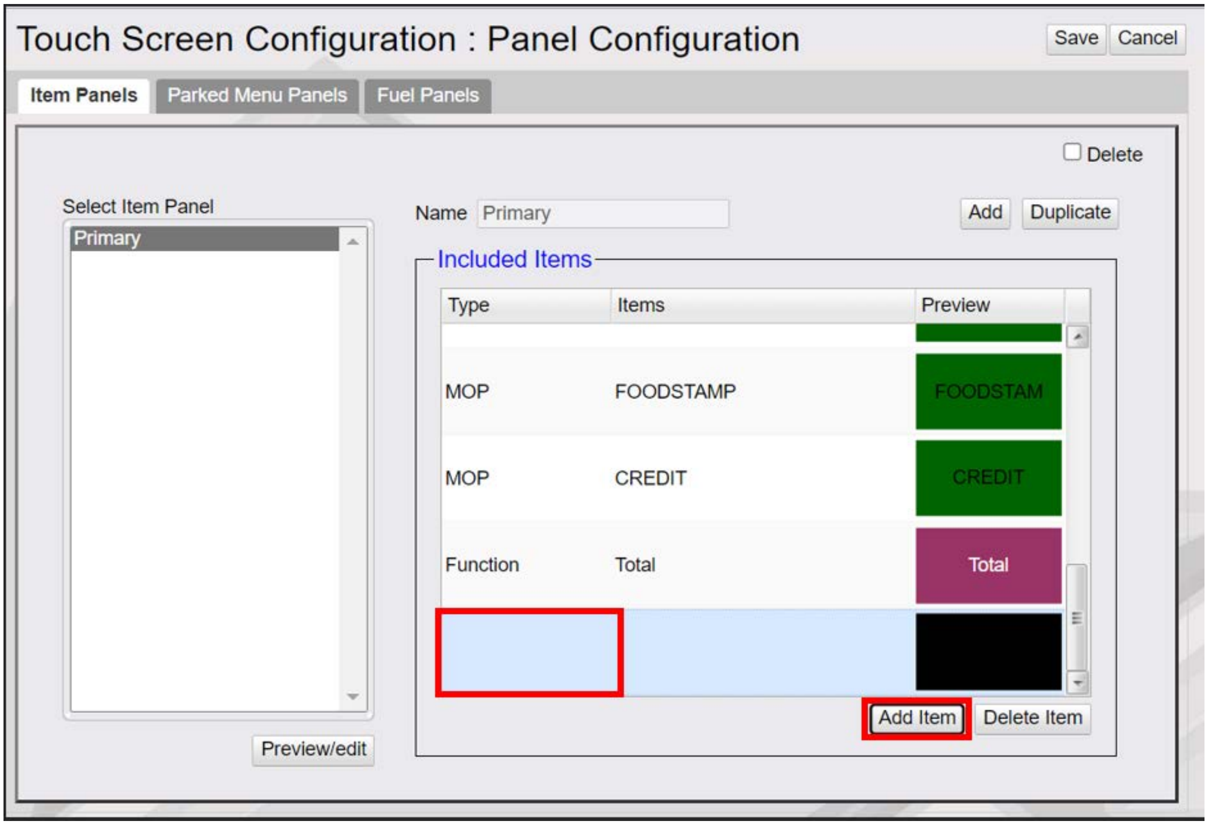
Name: Primary

Included Items

Type	Items	Preview
Menu key	Sub order menu	Subs Menu Cha
Menu key	Bagels	Bagels
Function	Get Order	Get Order
Function	Kiosk Order	Kiosk Order

2. Select the item panel on the left column that the Mobile Payment button will be configured.

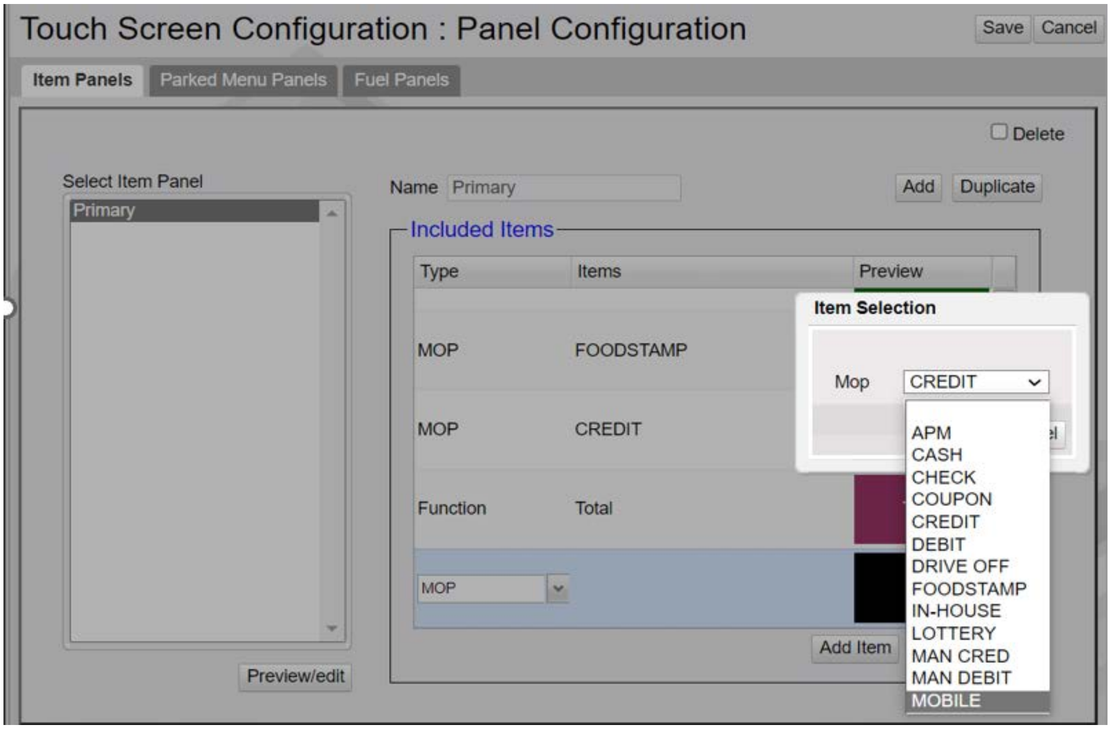
3. Select the Add Item button under the Included Items list.
4. A new row will appear. Click the first column and select MOP from the drop down.



Name: Primary

Type	Items	Preview
		🟩
MOP	FOODSTAMP	FOODSTAM
MOP	CREDIT	CREDIT
Function	Total	Total
		■

5. Select the Items column in the center of the row. Locate and click the Mobile method of payment from the list.



Touch Screen Configuration : Panel Configuration

Select Item Panel: Primary

Name: Primary

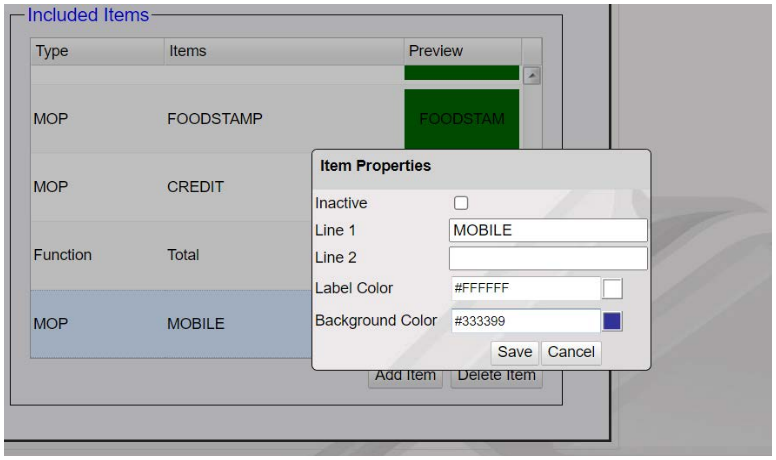
Included Items

Type	Items	Preview
MOP	FOODSTAMP	
MOP	CREDIT	
Function	Total	
MOP		

Item Selection

Mop: CREDIT

6. Under the Preview column, set the button color to the desired format.



Included Items

Type	Items	Preview
MOP	FOODSTAMP	FOODSTAM
MOP	CREDIT	
Function	Total	
MOP	MOBILE	

Item Properties

Inactive	□
Line 1	MOBILE
Line 2	
Label Color	#FFFFFF
Background Color	#333399

7. Select Save on the top of the page.

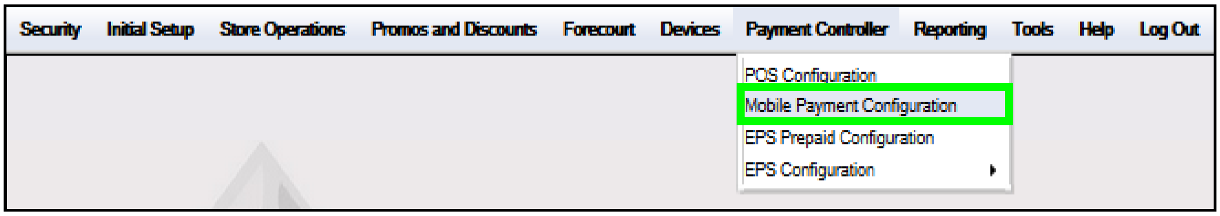
8. To see the changes on the POS, log out of sales mode and back in to update the screens.

NOTE

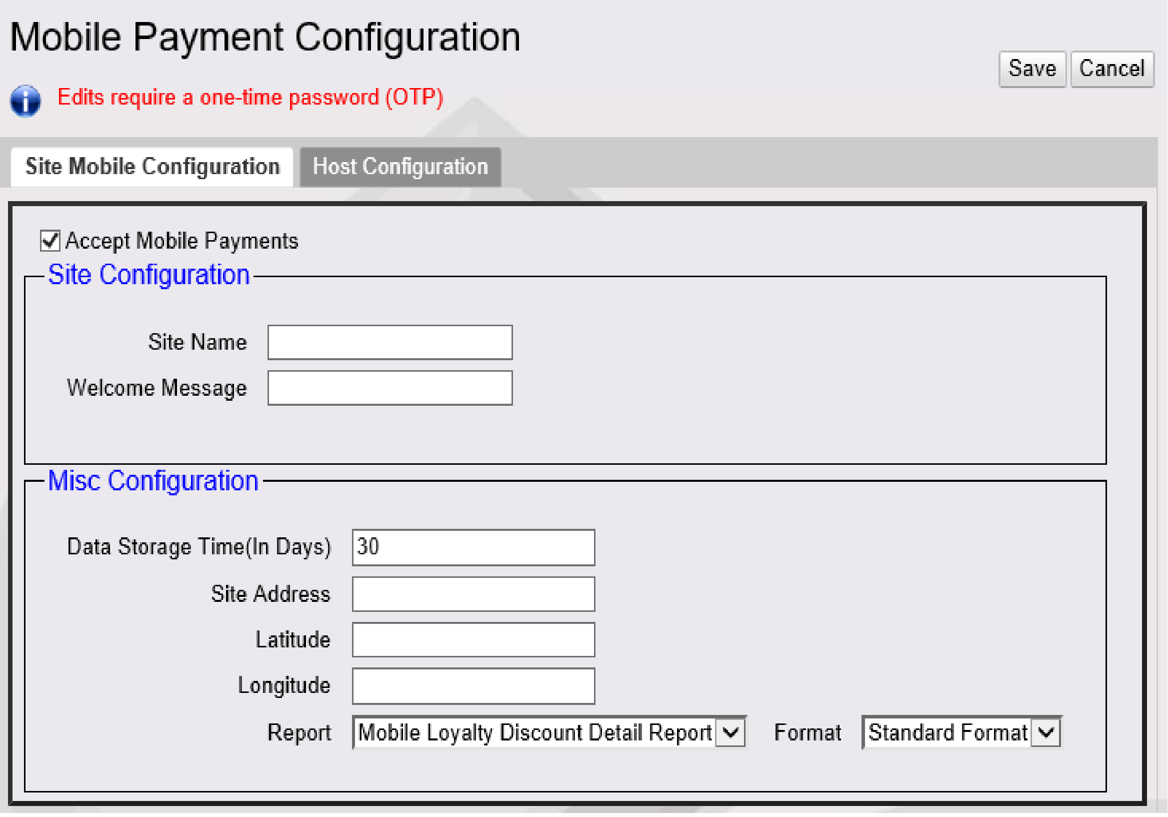
The Preview/edit button under the Select Item Panel section can be used to Preview the screen changes and can also be used to add a button to the touchscreen.

Mobile Payment Configuration

From the Configuration Client, go to: **Payment Controller > Mobile Payment Configuration.**



The Mobile Payment Configuration window displays.



Edits require a one-time password (OTP)

☑ Accept Mobile Payments

Site Name

Welcome Message

Data Storage Time(In Days) 30

Site Address

Latitude

Longitude

Report: Mobile Loyalty Discount Detail Report

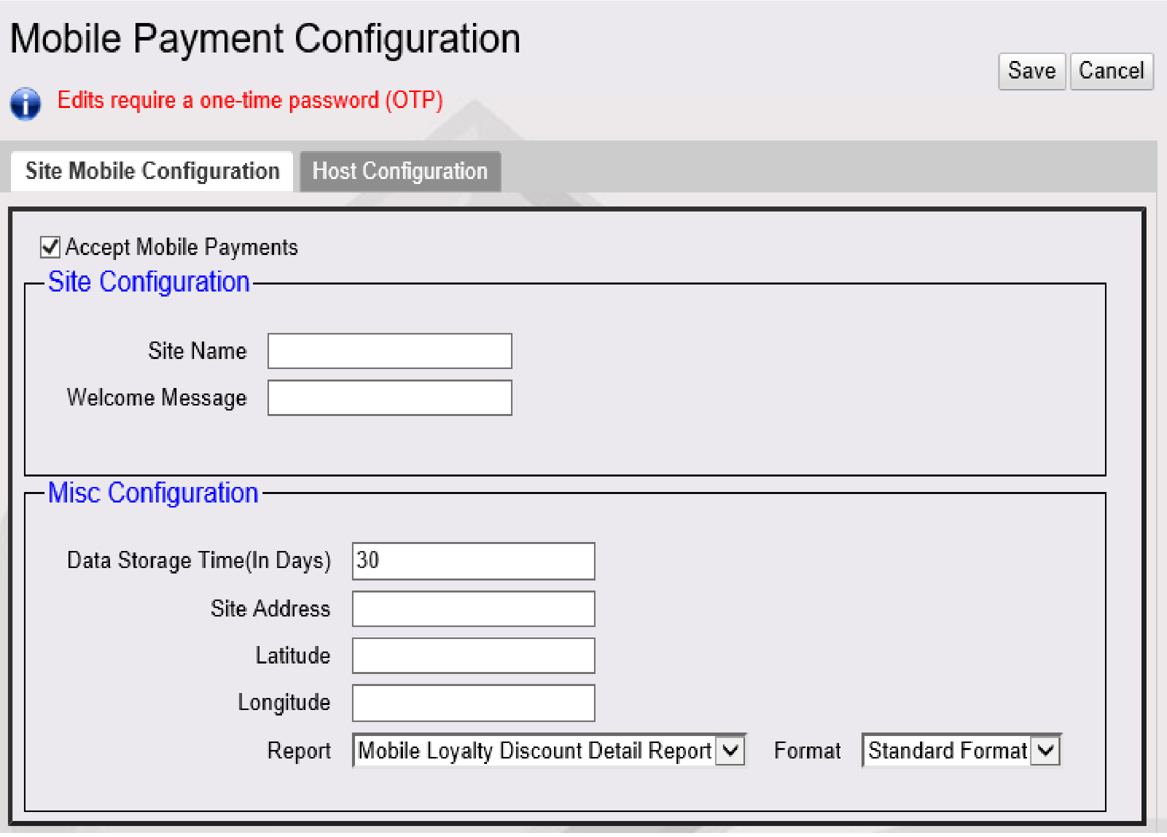
Format: Standard Format

The following tabs are available for selection:

- Site Mobile Configuration
- Host Configuration

Site Mobile Configuration

1. From the Mobile Configuration form, select the **[Site Mobile Configuration]** tab.



Mobile Payment Configuration

Edits require a one-time password (OTP)

☑ Accept Mobile Payments

Site Configuration

Site Name:

Welcome Message:

Misc Configuration

Data Storage Time(In Days): 30

Site Address:

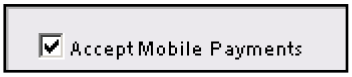
Latitude:

Longitude:

Report: Mobile Loyalty Discount Detail Report

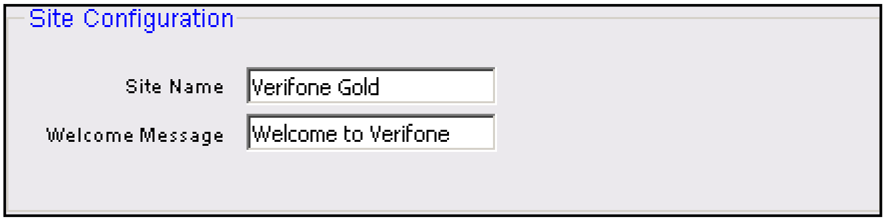
Format: Standard Format

2. Select **[Accept Mobile Payments]** to enable Mobile Payments.



☑ Accept Mobile Payments

3. Configure the following Site Configuration parameters:



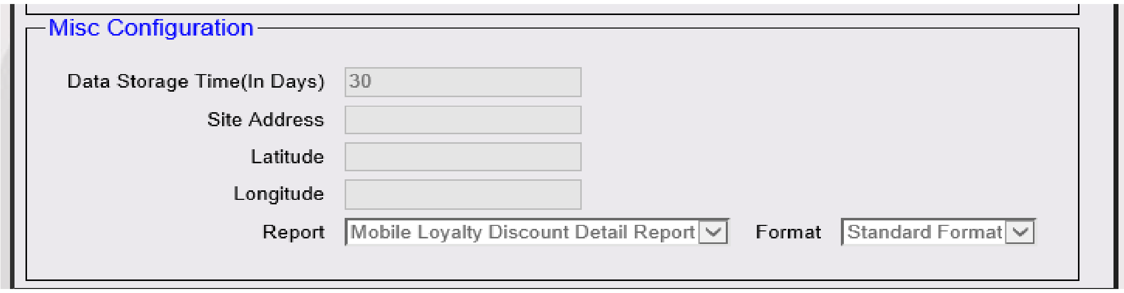
Site Configuration

Site Name: Verifone Gold

Welcome Message: Welcome to Verifone

Variable	Value
Site Name	The name of the site <20 characters>.
Welcome Message	The site's welcome message <100 characters>.

4. Configure the following Miscellaneous Configuration parameters:



Misc Configuration

Data Storage Time(In Days) 30

Site Address

Latitude

Longitude

Report: Mobile Loyalty Discount Detail Report

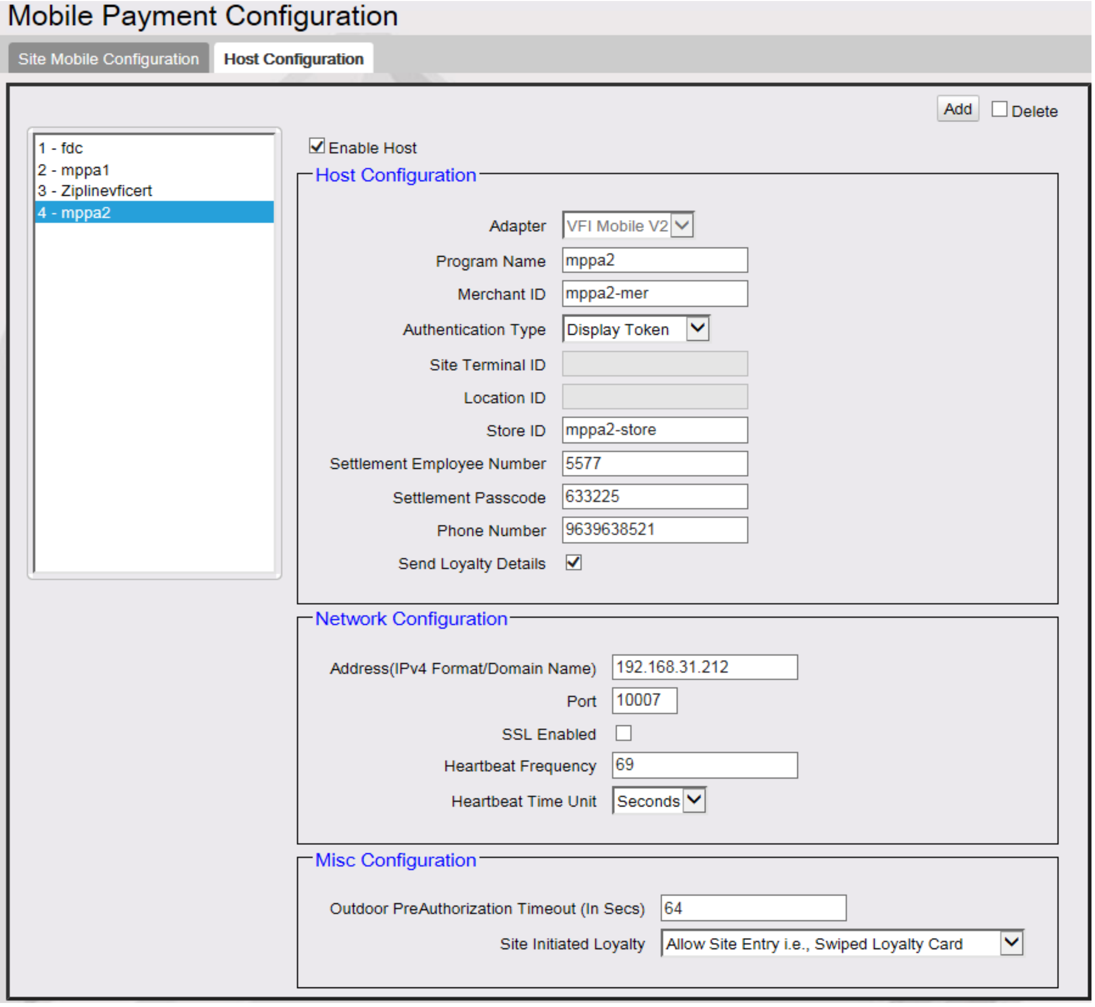
Format: Standard Format

Variable	Value
Data Storage Time	The Data Storage Time for retention <0-30 days>.
Site Address	The site street address.
Latitude/Longitude	The site GPS coordinates.
Report / Format	The combination of these fields are used to set the format type for each report from the report drop-down. The values are "Standard" and "Extended Authorization". The default format type would be "Standard" for all reports. In the Chevron distribution, the Mobile Terminal Batch Detail Report will default to Extended Authorization format. Standard: In this format max limit for authorization number is 14 digits and first 14 digits gets printed. Extended Authorization Format: Min limit for authorization number is 1; no upper limit. As of now this feature is applicable only for Mobile Terminal Batch Detail Report.

5. Select **[Save]** to accept, or **[Cancel]** to exit without saving changes.

Host Configuration

1. From the Mobile Payment Configuration window, select the **[Host Configuration]** tab.



Mobile Payment Configuration

☑ Enable Host

Host Configuration

Adapter: VFI Mobile V2
Program Name: mppa2
Merchant ID: mppa2-mer
Authentication Type: Display Token
Site Terminal ID:
Location ID:
Store ID: mppa2-store
Settlement Employee Number: 5577
Settlement Passcode: 633225
Phone Number: 9639638521
Send Loyalty Details: ☑

Network Configuration

Address(IPv4 Format/Domain Name): 192.168.31.212
Port: 10007
SSL Enabled: □
Heartbeat Frequency: 69
Heartbeat Time Unit: Seconds

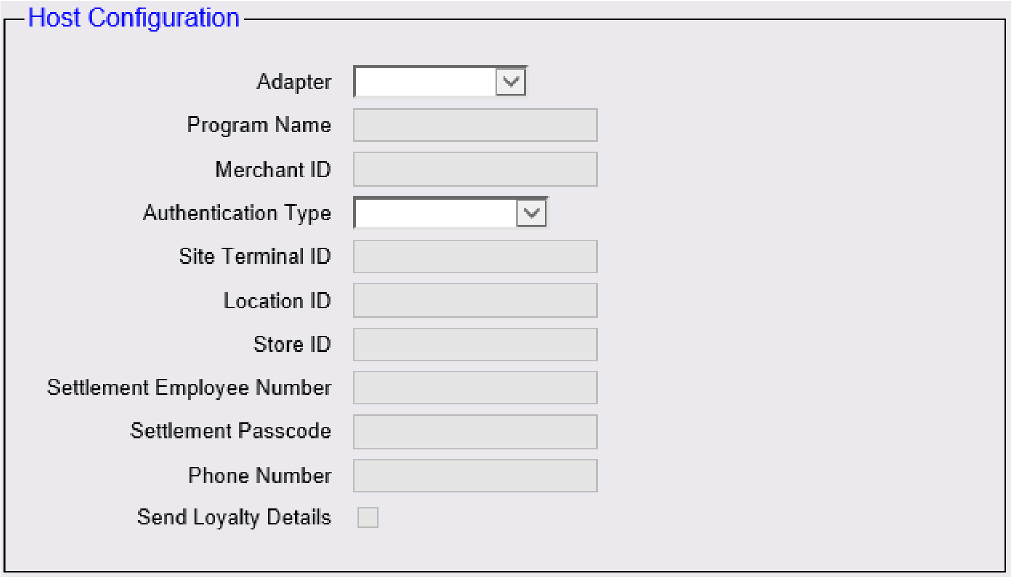
Misc Configuration

Outdoor PreAuthorization Timeout (In Secs): 64
Site Initiated Loyalty: Allow Site Entry i.e., Swiped Loyalty Card

2. Click **[Add]**.
3. Click to select **[Enable Host]**.

☑ Enable Host

4. Configure the Host Configuration parameters.



Host Configuration

Adapter	
Program Name	
Merchant ID	
Authentication Type	
Site Terminal ID	
Location ID	
Store ID	
Settlement Employee Number	
Settlement Passcode	
Phone Number	
Send Loyalty Details	□

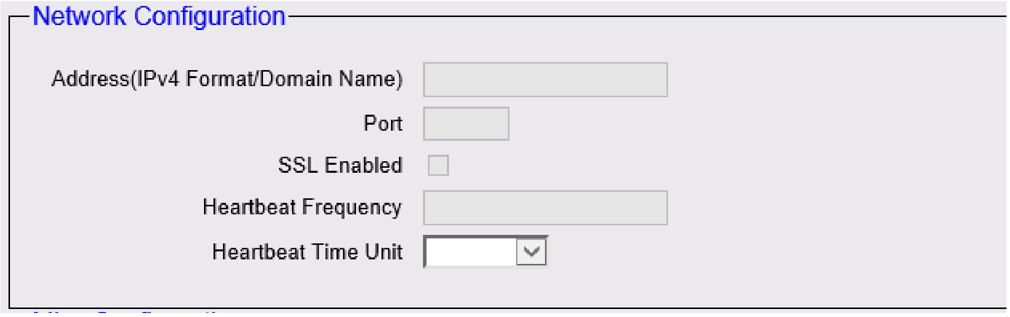
Variable	Value
Adapter	The site Adapter Type: • **FDC Mobile -** Connector Switch adapter *or outdoor transactions. Not supported in Verifone C-Site Management.* • **VFIMobile V1 -** *Conexxus V1 standards* • **VFIMobile V2 -** *Conexxus V2 standards* • **Local MPPA -** *for Shell Distribution. Not supported in Verifone C-Site Management.*
Program Name	The Program Name **must** be specific to the Mobile Payment Host. As of base 53.41, any Verifone Commander that is configured to connect to the Verifone C-Site Management application may receive Mobile Payment configuration updates remotely. The Program Name determines what updates will be sent. Work with the Verifone C-Site administrator for the site if you're unsure which naming convention to use and the site is connected to the cloud.
Merchant ID	The Merchant ID (MID) number provided by the Mobile Payment Host.

Variable	Value
Authentication Type	The site Authentication Type: • **SCAN_TOKEN:** QR Code generated on the MPA is scanned using the POS scanner. • **ENTER_TOKEN**: Customer or cashier enters token on the PIN pad. • **DISPLAY_TOKEN**: Token for customer to enter is displayed on the PIN pad. • **GENERATE_TOKEN**: Both Display_Token and Generate_Token display a token on the PIN pad to be scanned or entered for authenticating the transaction. If a site has different Mobile Payment programs configured with Generate_Token authentication type for all, the customer is not prompted to select a mobile payment program during the transaction. After selecting mobile MOP, the PIN pad displays a QR Code instead of mobile payment program selection. *If the Adapter type is 'FDC Mobile', then the field 'Authentication type' is disabled. This adapter allows only outdoor transactions.*
Site Terminal ID	ID number for the terminal received from the Mobile Payment Host. **Note: For Conexxus standards, Site_terminal ID and Location ID are greyed out.**
Location ID	The Location ID provided by the Mobile Payment Host; identifies the site during the on boarding process. **Note: For Conexxus standards, Site_terminal ID and Location ID are greyed out**
Store ID	The site Store ID number.
Settlement Employee Number	The Settlement Employee Number provided by the Mobile Payment Host
Settlement Passcode	The Settlement Passcode.
Phone Number	The Site Phone Number.
Send Loyalty Details	Enabling this flag will sends SLA/EPS loyalty program details to MPPA under Mobile Site Data Request.

NOTE

If Scan Token is selected as the Authentication Type, the scanner must be programmed with a prefix "P01"to correctly identify QR Codes.

5. Configure the Network Configuration parameters.



Network Configuration

Address(IPv4 Format/Domain Name)

Port

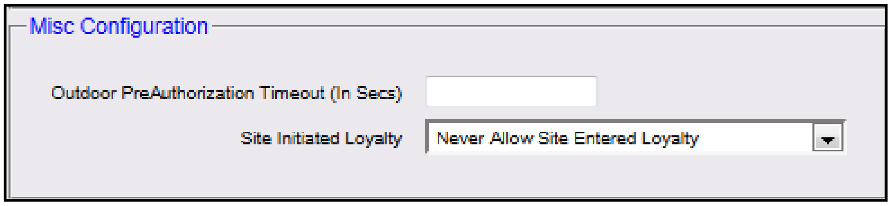
SSL Enabled □

Heartbeat Frequency

Heartbeat Time Unit

Variable	Value
Address	The Host IP or URL. (IPv4 format or http domain name).
Port	The communications port number.
SSL Enabled	Enables Secure Socket Layer (SSL) for client/ host communications.
Heartbeat Frequency / Unit	The time after which the Verifone Commander pings the mobile program host to check connection. If the host is offline, the mobile host offline alarm appears on the POS.

6. Configure the following Miscellaneous Configuration parameters:



Misc Configuration

Outdoor PreAuthorization Timeout (In Secs)

Site Initiated Loyalty: Never Allow Site Entered Loyalty

Variable	Value
Outdoor PreAuthorization Timeout	The DCR Pre-Authorization timeout (in seconds).
Site Initiated Loyalty	The Site Initiated Loyalty setting for outdoor transactions: • Never Allow Site Entered Loyalty - Allow only mobile loyalty. • Allow Site Entry i.e. Swiped Loyalty Card - Both swiped and mobile loyalties are honored. • Allow Site Entered Loyalty if no Mobile Loyalty - Allow swiped loyalty if there is no mobile loyalty.

7. Select **[Save]** to accept, or **[Cancel]** to exit without saving changes.

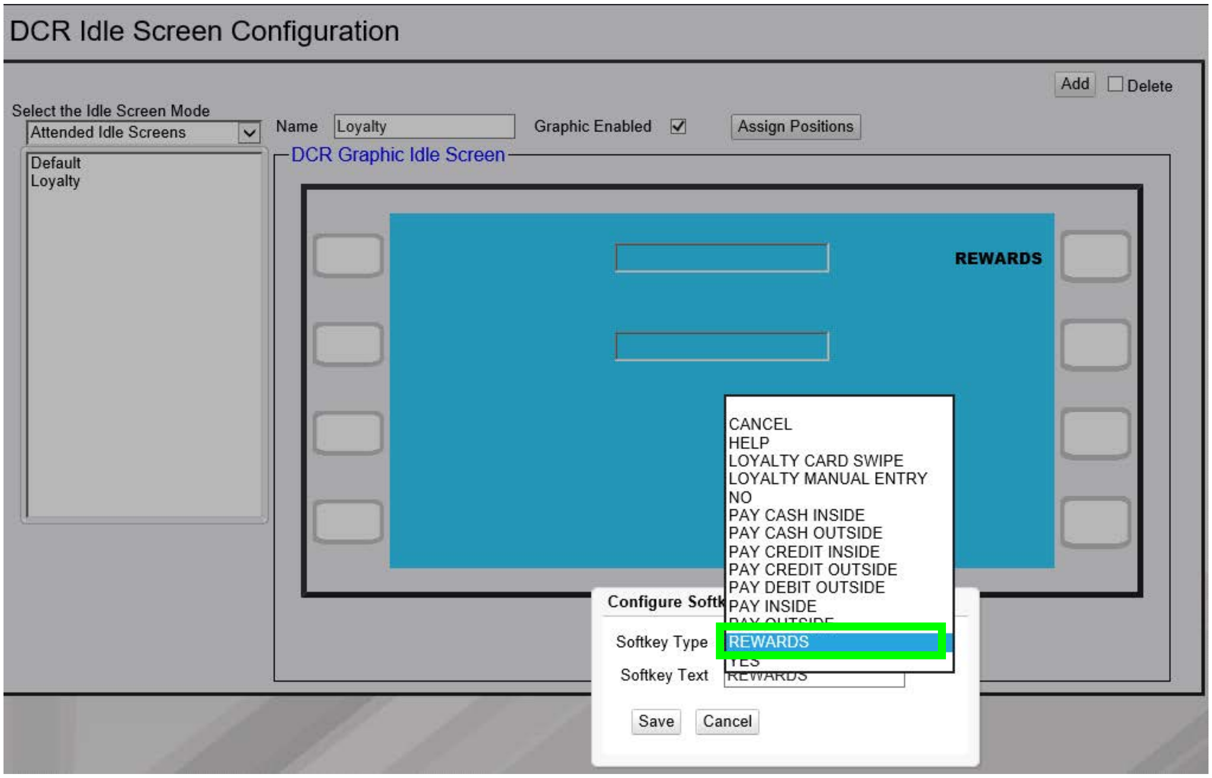
Configure Loyalty Key on DCR for Using Mobile Payment

Following are the steps to configure loyalty for mobile payment if site has a loyalty program(s) enabled.

Configure Loyalty Key “REWARDS” on Dispensers with Graphics DCR

If site has already configured "Loyalty" soft key, replace it with "REWARDS" soft key type. This soft key has the functionalities of the "Loyalty" soft key type and also links mobile payment with loyalty. The soft key text can remain as “Loyalty”.
On Configuration Client, go to **Forecourt > DCR Idle Screen**.

Configure a soft key to **“REWARDS”** soft key type and not LOYALTY_CARD_SWIPE or LOYALTY_MANUAL_ENTRY. For more information on configuring soft keys, refer to the Commander Site Controller User Reference.



DCR Idle Screen Configuration

Select the Idle Screen Mode: Attended Idle Screens

Name: Loyalty

Graphic Enabled ☑

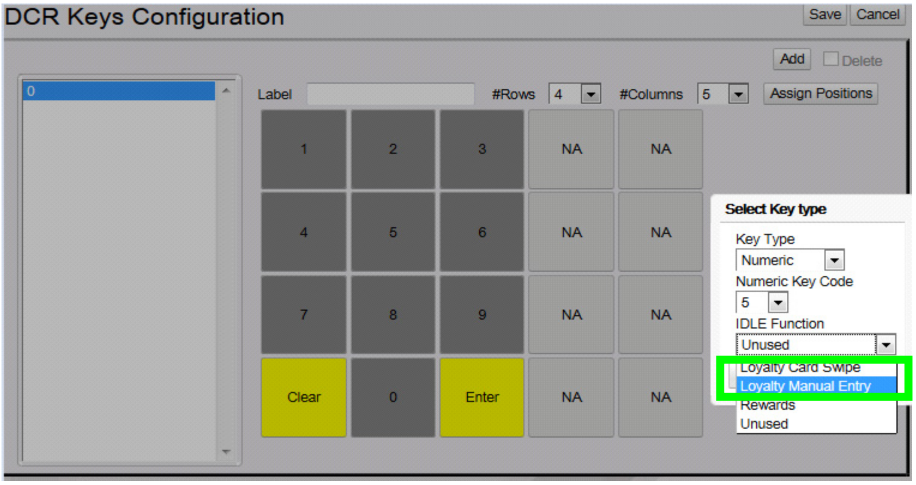
Softkey Type: REWARDS

Softkey Text: REWARDS

> NOTE
>
> *Do a **Tools** > **Refresh Configuration** and **Forecourt** > **Initialization** > **DCR** after the configuration changes.*

Configure Loyalty Key on Dispensers with Non-Graphics DCR

On Configuration Client, go to **Forecourt > DCR Keys**. Select a numeric key which should work as loyalty key when dispenser is idle as shown below. In the example below numeric key 5 is used as loyalty key.



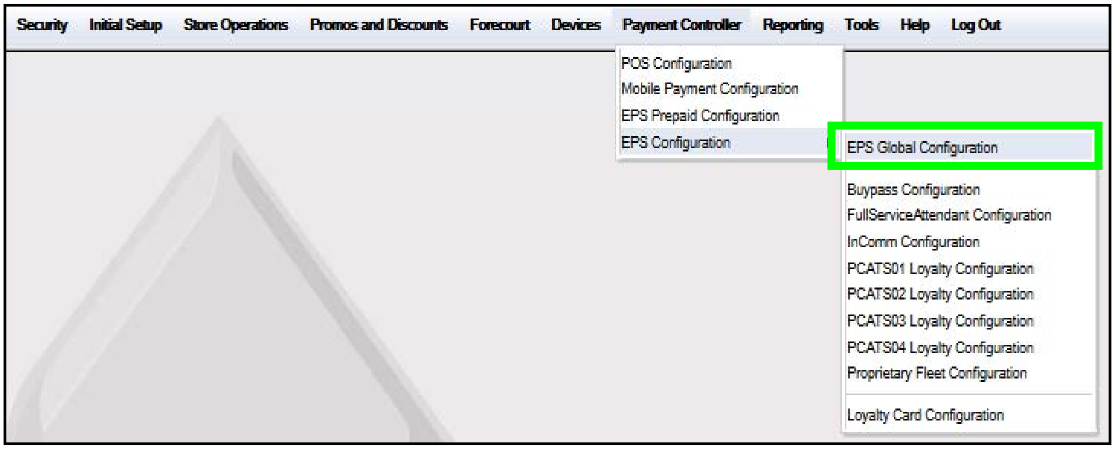
Label
#Rows 4
#Columns 5
Key Type: Numeric
Numeric Key Code: 5
IDLE Function: Unused

> *Do a **Tools > Refresh Configuration** and **Forecourt > Initialization > DCR** after the configuration changes.*

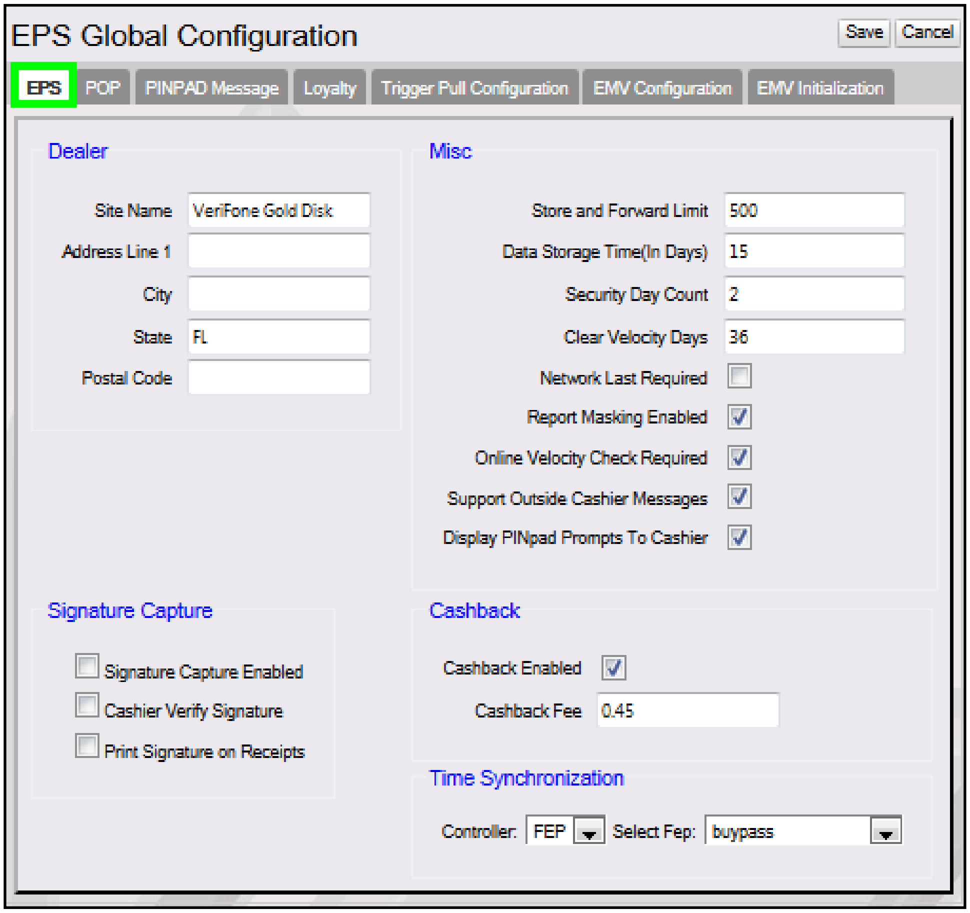
Configure Site Address

The Dealer address details are used for displaying site information on the mobile application when a customer does a check-in through the mobile application.

From Configuration Client, go to: **Payment Controller > EPS Configuration > EPS Global Configuration.**


Security
Initial Setup
Store Operations
Promos and Discounts
Forecourt
Devices
Payment Controller
Reporting
Tools
Help
Log Out
POS Configuration
Mobile Payment Configuration
EPS Prepaid Configuration
EPS Configuration
EPS Global Configuration
Buypass Configuration
FullServiceAttendant Configuration
InComm Configuration
PCATS01 Loyalty Configuration
PCATS02 Loyalty Configuration
PCATS03 Loyalty Configuration
PCATS04 Loyalty Configuration
Proprietary Fleet Configuration
Loyalty Card Configuration

1. From the EPS Global Configuration window, select the **[EPS]** tab.



EPS Global Configuration

Dealer

Site Name: VeriFone Gold Disk
Address Line 1:
City:
State: FL
Postal Code:

Misc

Store and Forward Limit: 500
Data Storage Time(In Days): 15
Security Day Count: 2
Clear Velocity Days: 36
Network Last Required ☐
Report Masking Enabled ☑
Online Velocity Check Required ☑
Support Outside Cashier Messages ☑
Display PINpad Prompts To Cashier ☑

Signature Capture

☐ Signature Capture Enabled
☐ Cashier Verify Signature
☐ Print Signature on Receipts

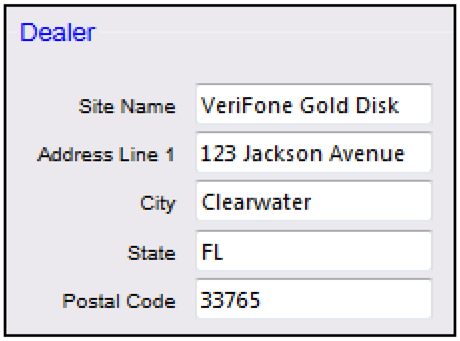
Cashback

Cashback Enabled ☑
Cashback Fee: 0.45

Time Synchronization

Controller: FEP Select Fep: buypass

2. Configure the Dealer parameters.



Dealer

Site Name: VeriFone Gold Disk
Address Line 1: 123 Jackson Avenue
City: Clearwater
State: FL
Postal Code: 33765

Variable	Value
Site Name	Dealer Name
Address Line1	Dealer Street
City	Dealer City

Variable	Value
State	Dealer State
Postal Code	Dealer Zip Code

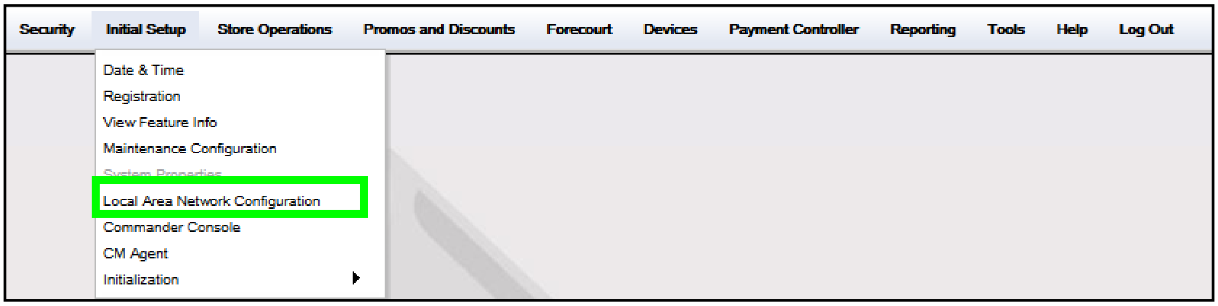
3. Select **[Save]** to accept, or **[Cancel]** to exit without saving changes.

NOTE

Log out and back in to all POS terminals after any setting modifications to allow these changes to take affect.

Local Area Network Configuration

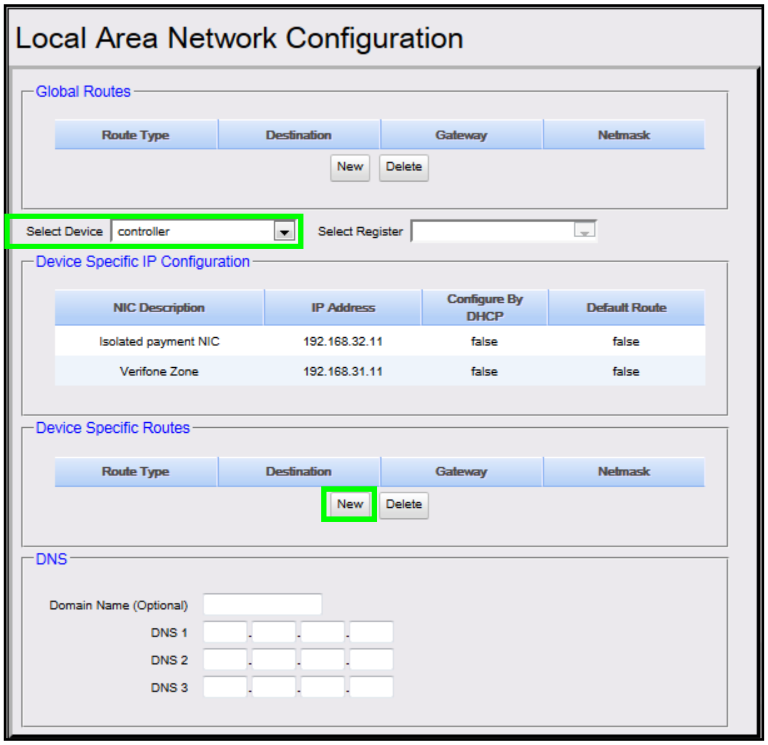
1. From the Configuration Client, go to: **Initial Setup > Local Area Network Configuration.**



Configure Device Specific Routes

2. Confirm the Controller is the device selected to configure.

3. Click **[New]** in Device Specific Routes.



Local Area Network Configuration

Global Routes

Route Type	Destination	Gateway	Netmask

New Delete

Select Device: controller

Select Register:

Device Specific IP Configuration

NIC Description	IP Address	Configure By DHCP	Default Route
Isolated payment NIC	192.168.32.11	false	false
Verifone Zone	192.168.31.11	false	false

Device Specific Routes

Route Type	Destination	Gateway	Netmask

New Delete

DNS

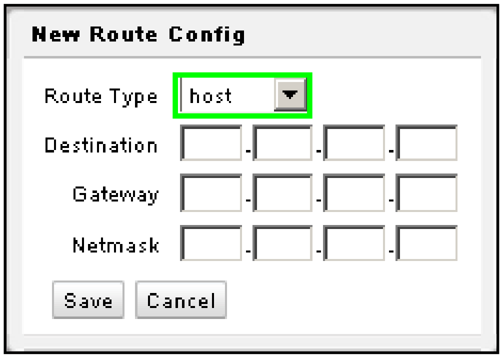
Domain Name (Optional)

DNS 1 . . .

DNS 2 . . .

DNS 3 . . .

4. Select the New Route Config Route Type: **Host**.



New Route Config

Route Type: host

Destination . . .

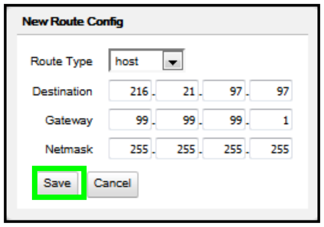
Gateway . . .

Netmask . . .

Save Cancel

5. Enter the Device Specific Host Route Destination address provided by the Mobile Payment Host.

6. Enter the Gateway address; this will be the site’s Payment Gateway address, as associated with the Isolated Payment NIC.



New Route Config

Route Type: host

Destination: 216 . 21 . 97 . 97

Gateway: 99 . 99 . 99 . 1

Netmask: 255 . 255 . 255 . 255

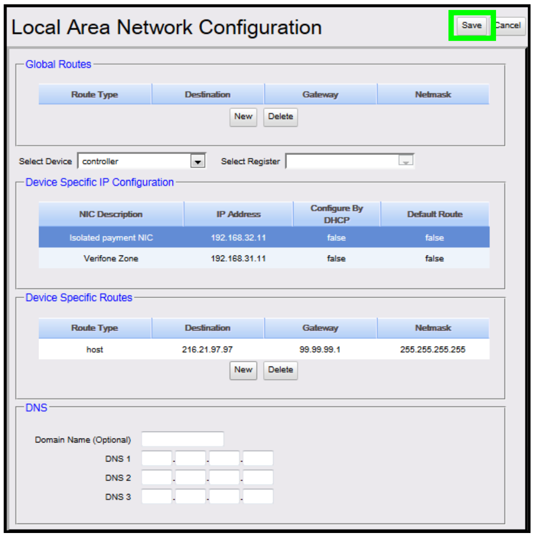
Save Cancel

7. Enter the Netmask = 255.255.255.255.

8. Click **[Save]** in the New Route Configuration dialog box.

9. Click **[Save]** on the main form.

10. Reboot the Verifone Commander to ensure proper network routing is uses for all devices.



Local Area Network Configuration

Global Routes

Route Type	Destination	Gateway	Netmask

Select Device: controller

Select Register:

Device Specific IP Configuration

NIC Description	IP Address	Configure By DHCP	Default Route
Isolated payment NIC	192.168.32.11	false	false
Verifone Zone	192.168.31.11	false	false

Device Specific Routes

Route Type	Destination	Gateway	Netmask
host	216.21.97.97	99.99.99.1	255.255.255.255

DNS

Domain Name (Optional)

DNS 1 . . .

DNS 2 . . .

DNS 3 . . .

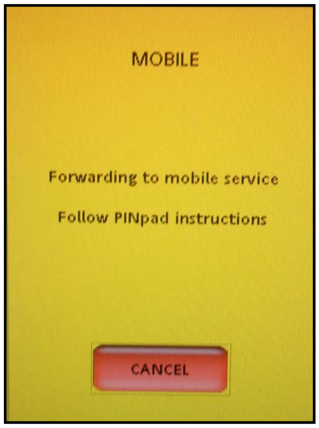
Using Mobile Payments

Indoor Transactions

Pay at POS with Code Displayed on POP

In this use case, the Cashier initiates the payment transaction by requesting a dynamically generated token from the MPPA. The Customer is provided a transaction code to enter into the mobile application, thereby connecting to the transaction.

1. Customer makes a purchase and tells the cashier that he wants to pay using his mobile app.
2. The cashier selects “Mobile” MOP on the POS.
3. The Site Controller submits a request to the MPPA host for a transaction code.



MOBILE

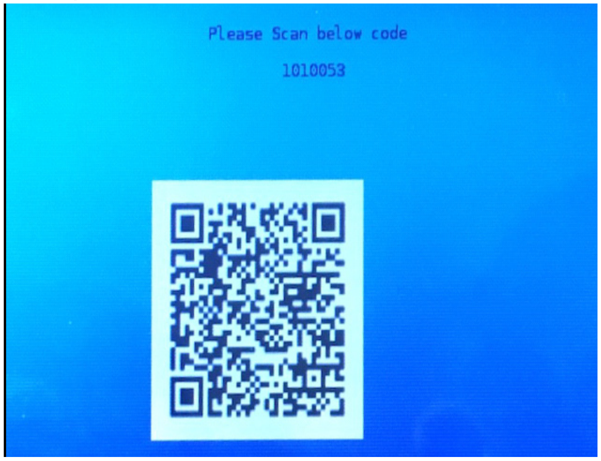
Forwarding to mobile service

Follow PINpad instructions

NOTE

> *If multiple mobile hosts are configured at the site, then a host selection prompt appears on the POP device after Mobile MOP is selected.*
>
> *If multiple mobile hosts are configured at the site, the Authentication Type should be Generate_Token so that a host selection prompt does not appear on the POP device after Mobile MOP is selected.*

4. The host responds with a transaction code which is displayed on the POP.



Please Scan below code

1010053

5. The customer opens the mobile payment app on their phone, enters or scans the transaction code, which links to the transaction at the POS.

6. After successful code verification, the host authorizes the transaction.
7. On completion of the transaction, receipt details are sent to the MPPA and will be available for the customer to view on the mobile application.

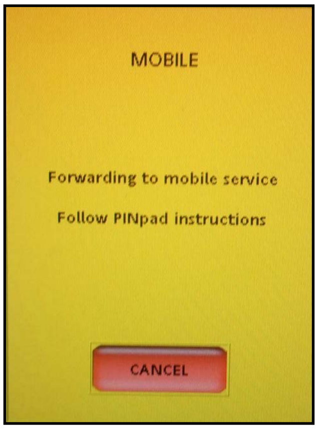
NOTE

Receipt data sent to the MPPA is the same as the receipt being printed from the POS.

Pay at POS with Code Displayed on Phone

In this use case, the Customer initiates the mobile payment transaction request. The MPA initiates the transaction to obtain a dynamically generated pre-authorization token from the MPPA The token is displayed on the phone and used to complete the transaction at the POS.

1. Customer makes a purchase and tells the cashier that he wants to pay using his mobile app.
2. The cashier selects “Mobile” MOP on the POS.


MOBILE

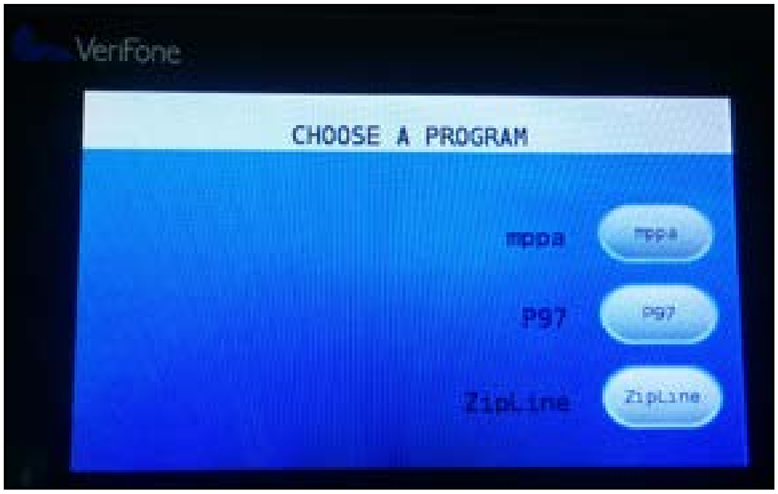
Forwarding to mobile service

Follow PINpad instructions

NOTE

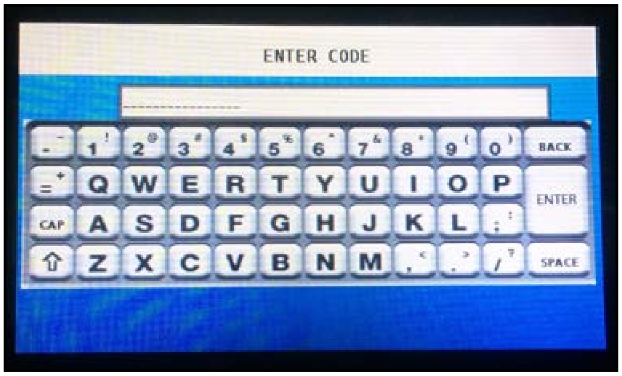
If multiple mobile hosts are configured at the site, then a host selection prompt appears on the POP device after Mobile MOP is selected.

If a site has different Mobile Payment programs configured with Generate_Token authentication type for all, the customer is not prompted to select a mobile payment program during the transaction. After selecting mobile MOP, the PIN pad displays a QR Code instead of mobile payment program selection.

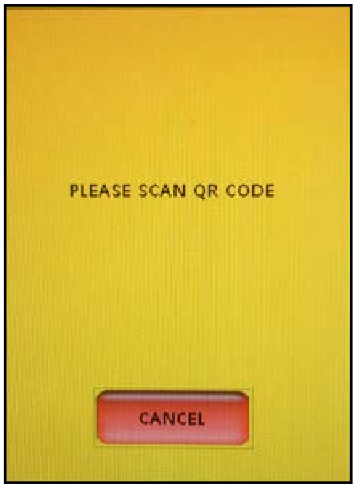


3. The Customer initiates the mobile payment transaction request, and depending on the system host configuration, the mobile application will display either an alphanumeric string code or a QR code.

   If the MPA displays a string code, the customer enters the code on the POP.


ENTER CODE
- 1 2 3 4 5 6 7 8 9 0 BACK
= Q W E R T Y U I O P ENTER
CAP A S D F G H J K L ;
⇧ Z X C V B N M , . / SPACE

If the MPA displays a QR code, the cashier scans the QR code.



4. After successful code verification, the host authorizes the transaction.
5. On completion of the transaction, receipt details are sent to the MPPA and will be available for the customer to view on the mobile application.

NOTE *Receipt data sent to the MPPA is the same as the receipt being printed from the POS.*

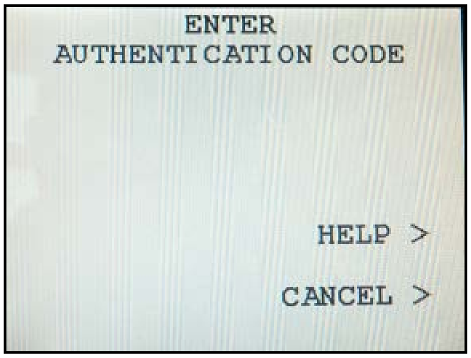
Outdoor Transactions

Pay at Pump with Code Entry

In this use case, the customer initiates the transaction through the MPA by selecting an available pump at the site. The pump is reserved, and the customer is prompted to enter an authorization code at the DCR. The authorization code will be sent to customer's phone. After fueling, the sales amount is charged to the MPA's registered card.

1. The Customer opens the MPA and selects the PUMP to reserve.
2. An authorization code is sent to the customer's phone.

3. The DCR prompts the customer to enter the authorization code.On successful code validation, the PUMP will be armed.



ENTER
AUTHENTICATION CODE

HELP >

CANCEL >

The pump is authorized only on code validation success. Authorization will fail if maximum retries are exhausted or if the Validation Code Prompt times out.

4. The Customer dispenses the fuel. Depending on the MPA, the customer is notified on their phone of the fueling start and stop.
5. On completion, the DCR prints the receipt. The sales amount is transmitted to the MPPA, the customer’s card is charged, and a receipt copy is sent to the registered MPA account for transaction history.

Pay at Pump without Code Entry

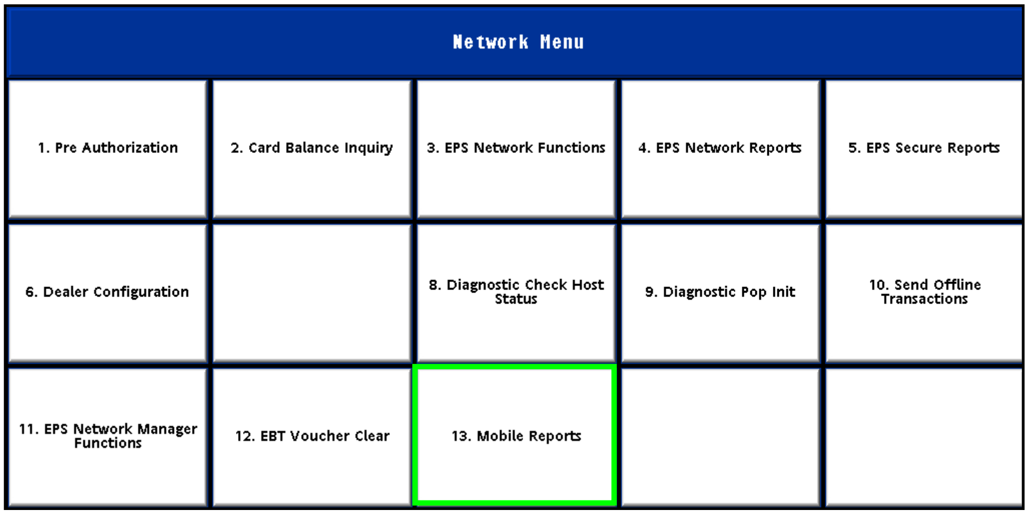
In this use case, the customer initiates the transaction through the MPA by selecting an available pump at the site. The pump is reserved and pre-authorized. After fueling, the sales amount is charged to the MPA’s registered card.

1. The Customer opens the MPA and selects the PUMP to reserve and authorize.
2. The Customer dispenses the fuel. Depending on the MPA, the customer is notified on their phone of the fueling start and stop.

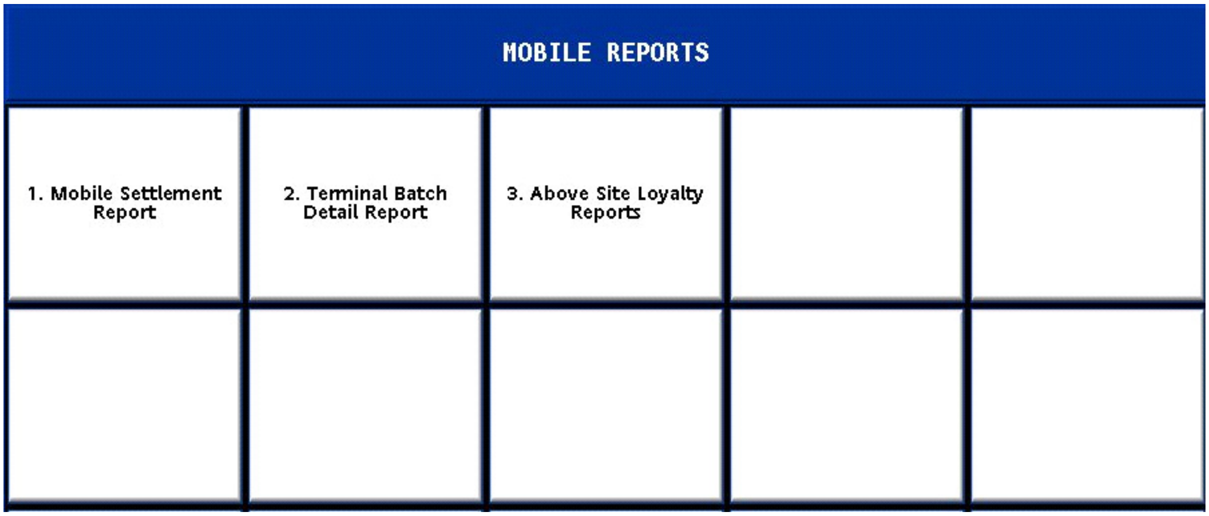
On completion, the DCR prints the receipt. The sales amount is transmitted to the MPPA, the customer’s card is charged, and a receipt copy is sent to the registered MPA account for transaction history.

Reporting

Reports and reporting options are provided by and will vary with the associated Host provider. Sample reports are provided for example purposes only.
Mobile Reports are located on the POS terminal **CSR Functions > Network Menu**.
Select **[Mobile Reports]** from the POS Network Menu.

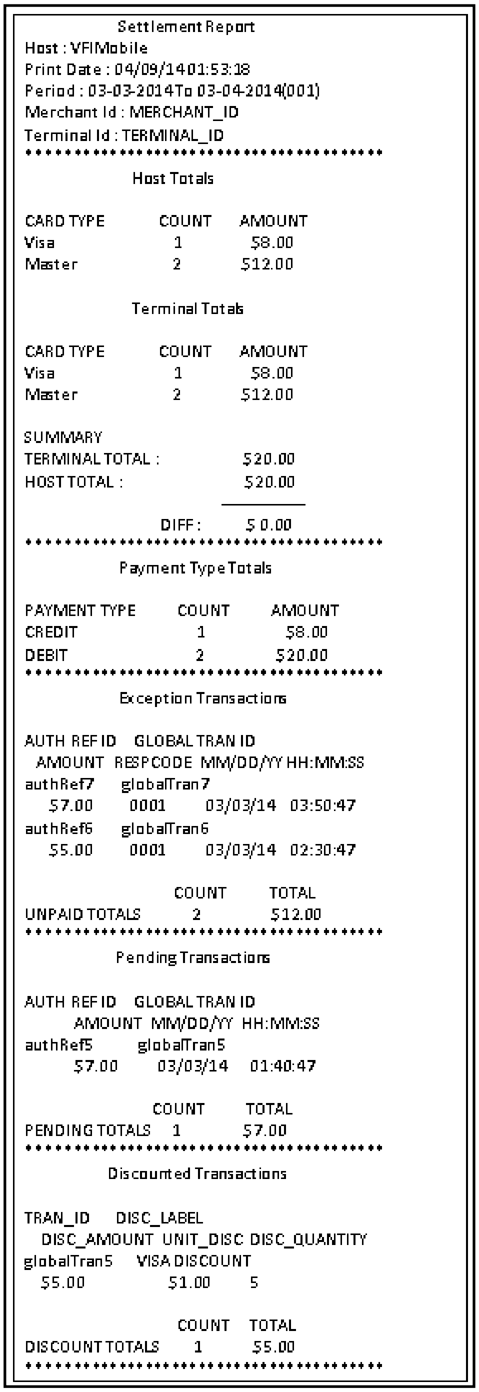


Select an available Mobile Reports option, then follow the instructions on the Report screen to select from the provided reports.


MOBILE REPORTS
1. Mobile Settlement Report
2. Terminal Batch Detail Report
3. Above Site Loyalty Reports

Mobile Settlement Report

Report Details



```
              Settlement Report
Host : VFIMobile
Print Date : 04/09/1401:53:18
Period : 03-03-2014To 03-04-2014(001)
Merchant Id : MERCHANT_ID
Terminal Id : TERMINAL_ID
***************************************
                Host Totals

CARD TYPE          COUNT     AMOUNT
Visa                 1          $8.00
Master               2         $12.00

                Terminal Totals

CARD TYPE          COUNT     AMOUNT
Visa                 1          $8.00
Master               2         $12.00

SUMMARY
TERMINAL TOTAL :               $20.00
HOST TOTAL :                   $20.00
                            ________
                   DIFF :      $ 0.00
***************************************
              Payment Type Totals

PAYMENT TYPE        COUNT       AMOUNT
CREDIT                1           $8.00
DEBIT                 2          $20.00
***************************************
              Exception Transactions

AUTH REF ID   GLOBAL TRAN ID
  AMOUNT  RESPCODE  MM/DD/YY HH:MM:SS
authRef7     globalTran7
   $7.00      0001      03/03/14  03:50:47
authRef6     globalTran6
   $5.00      0001      03/03/14  02:30:47

                    COUNT       TOTAL
UNPAID TOTALS         2          $12.00
***************************************
             Pending Transactions

AUTH REF ID   GLOBAL TRAN ID
       AMOUNT  MM/DD/YY  HH:MM:SS
authRef5        globalTran5
       $7.00      03/03/14    01:40:47

                  COUNT       TOTAL
PENDING TOTALS    1          $7.00
***************************************
            Discounted Transactions

TRAN_ID     DISC_LABEL
   DISC_AMOUNT  UNIT_DISC DISC_QUANTITY
globalTran5     VISA DISCOUNT
   $5.00             $1.00       5

                     COUNT    TOTAL
DISCOUNT TOTALS       1        $5.00
***************************************
```

Header

- **HOST:** Host name.
- **Print Date:** Date/Time of report.
- **Period:** Reporting Period.
- **Merchant ID:** Configured Merchant ID.
- **Terminal ID:** Configured Terminal ID.

Terminal and Host Totals

- **CARD TYPE**: Type of card used in the transaction (e.g., VISA, MASTERCARD).
- **COUNT**: The total number of sales for a card type.
- **AMOUNT:** The total sale amount for a card type.
- **TERMINAL TOTAL:** The Terminal Total of all card types.
- **HOST TOTAL:** The Host total for all card types.
- **DIFF**: The difference between terminal and host totals.

Payment Type Totals

- **PAYMENT TYPE:** Type of payment (e.g., CREDIT, DEBIT).
- **COUNT:** The total number of a payment type.
- **AMOUNT:** The total payment amount for a payment type.

Exception Transactions

Transactions that were pre-authorized by the host but later rejected during completion. These transactions need to be manually settled with the host.

- **AUTH REF ID:** The authorization reference id.
- **GLOBAL TRAN ID:** The transaction id.
- **AMOUNT:** The transaction amount.

- **RESPCODE:** Transaction decline response code.
- **DATE/TIME:** The transaction date and time.

Pending Transactions

Transactions that were pre-authorized by the host but are not yet completed.

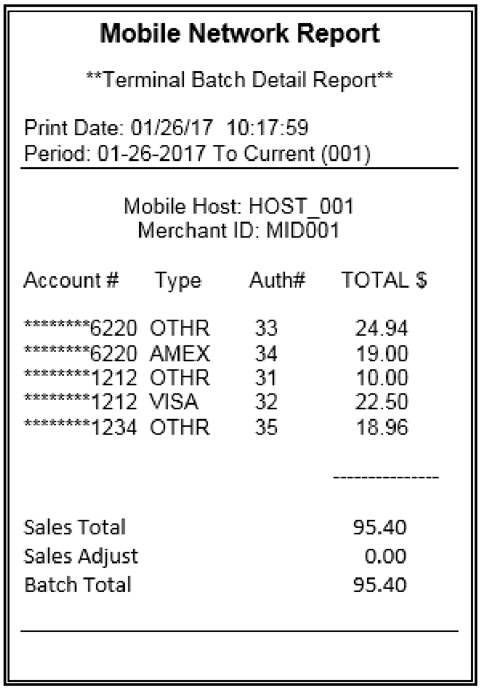
- **AUTH REF ID:** The authorization reference id.
- **GLOBAL TRAN ID:** The transaction id.
- **AMOUNT:** The transaction amount.
- **DATE/TIME:** The transaction date and time.

Discounted Transactions

Some transactions are given host discounts based on the card type used in the transaction. These discounts are not reported as part of any POS or EPS reports.

- **TRAN_ID:** Unique number given by the host to identify a transaction.
- **DISC_LABEL:** Reason/description of the given discount.
- **DISC_AMOUNT:** Total discount amount applied on the transaction.
- **UNIT_DISC:** PPG discount qualified for the selected grade.
- **DISC_QUANTITY:** Quantity of grade fuel dispensed by the customer which qualified for a discount

Mobile Terminal Batch Detail Report



```
              Mobile Network Report

          **Terminal Batch Detail Report**

Print Date: 01/26/17  10:17:59
Period: 01-26-2017 To Current (001)
__________________________________________

            Mobile Host: HOST_001
            Merchant ID: MID001

Account #     Type     Auth#    TOTAL $

********6220  OTHR     33        24.94
********6220  AMEX     34        19.00
********1212  OTHR     31        10.00
********1212  VISA     32        22.50
********1234  OTHR     35        18.96

                               ---------------

Sales Total                      95.40
Sales Adjust                      0.00
Batch Total                      95.40
__________________________________________
```

Report Details

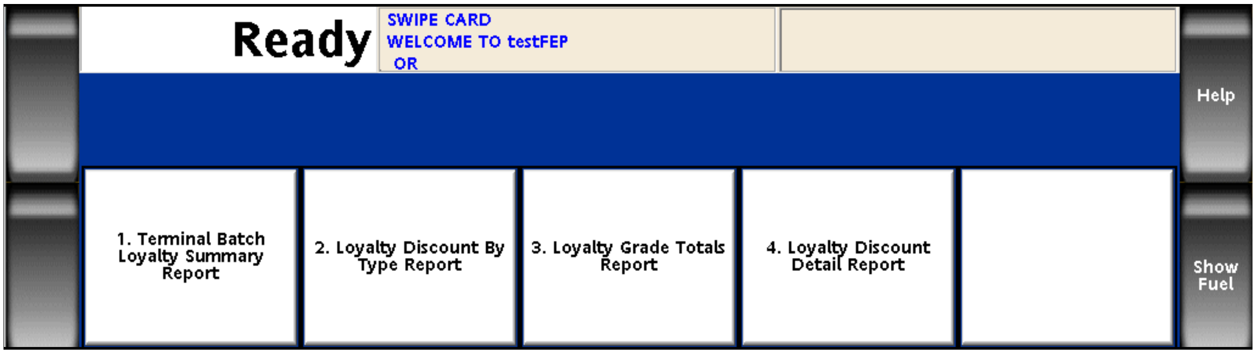
Header

- **Print Date:** Date/Time of report
- **Period:** Reporting Period
- **Mobile Host:** Mobile Payment Host
- Merchant ID: Configured Merchant ID

Transaction Totals

- **Account #**: Masked card number.
- **Type**: OTHER.
- **Auth #:** Transaction authorization number.
- **TOTAL:** Transaction amount total.
- **Sales Total:** Summary total of all transaction amounts.
- **Sales Adjust:** Summary total of any adjusted transaction amounts.
- **Batch Total:** Adjusted sales amount.

Above Site Loyalty Reports



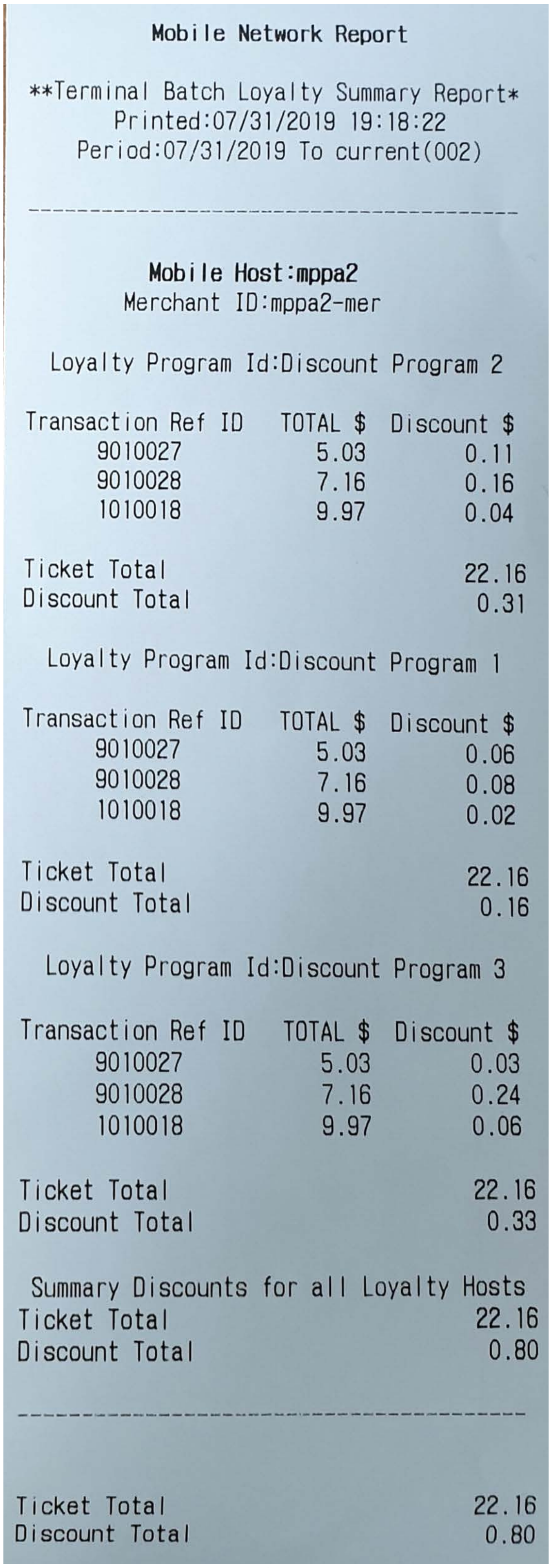
Ready

SWIPE CARD
WELCOME TO testFEP
OR

Help
1. Terminal Batch Loyalty Summary Report
2. Loyalty Discount By Type Report
3. Loyalty Grade Totals Report
4. Loyalty Discount Detail Report
Show Fuel

Terminal Batch Loyalty Summary Report

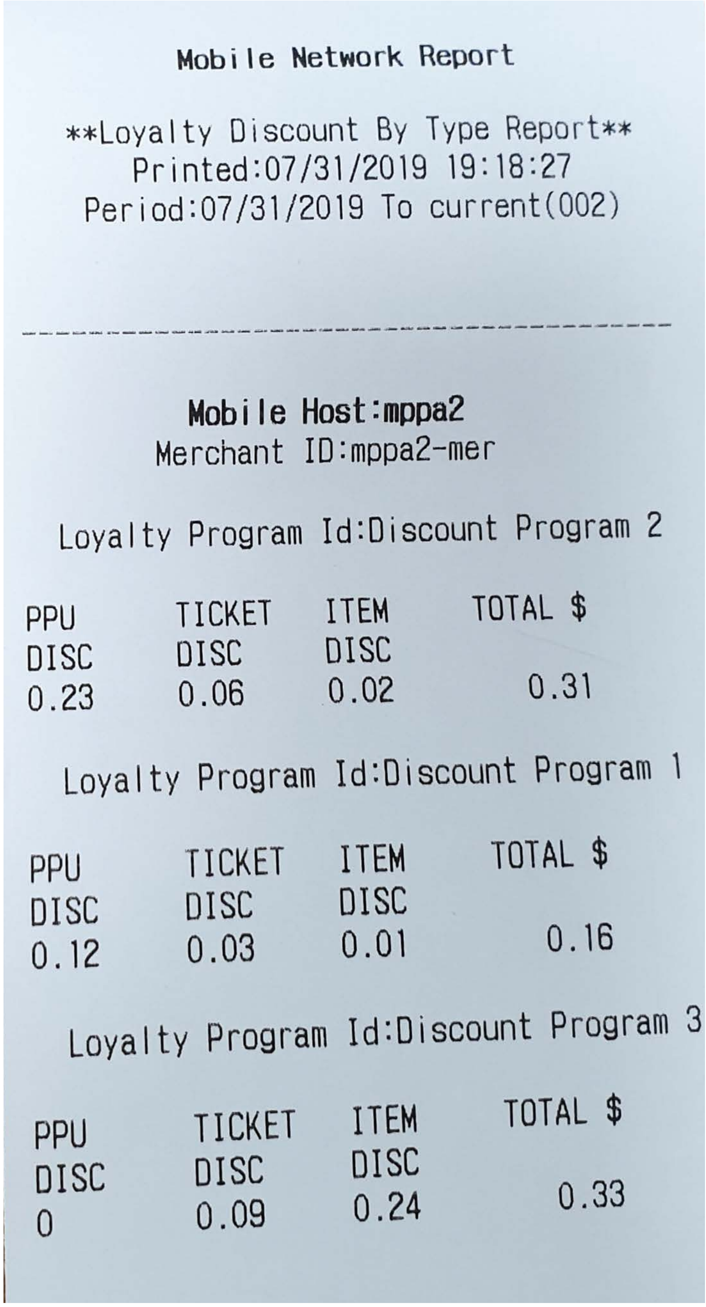
Terminal Batch Loyalty Summary Report gives a summary of ASA loyalty discounts applied on Mobile transactions.



```
           Mobile Network Report

  **Terminal Batch Loyalty Summary Report*
         Printed:07/31/2019 19:18:22
      Period:07/31/2019 To current(002)

------------------------------------------

             Mobile Host:mppa2
           Merchant ID:mppa2-mer

   Loyalty Program Id:Discount Program 2

Transaction Ref ID   TOTAL $  Discount $
      9010027          5.03         0.11
      9010028          7.16         0.16
      1010018          9.97         0.04

Ticket Total                       22.16
Discount Total                      0.31

   Loyalty Program Id:Discount Program 1

Transaction Ref ID   TOTAL $  Discount $
      9010027          5.03         0.06
      9010028          7.16         0.08
      1010018          9.97         0.02

Ticket Total                       22.16
Discount Total                      0.16

   Loyalty Program Id:Discount Program 3

Transaction Ref ID   TOTAL $  Discount $
      9010027          5.03         0.03
      9010028          7.16         0.24
      1010018          9.97         0.06

Ticket Total                       22.16
Discount Total                      0.33

 Summary Discounts for all Loyalty Hosts
Ticket Total                       22.16
Discount Total                      0.80

------------------------------------------


Ticket Total                       22.16
Discount Total                      0.80
```

Loyalty Discount By Type Report

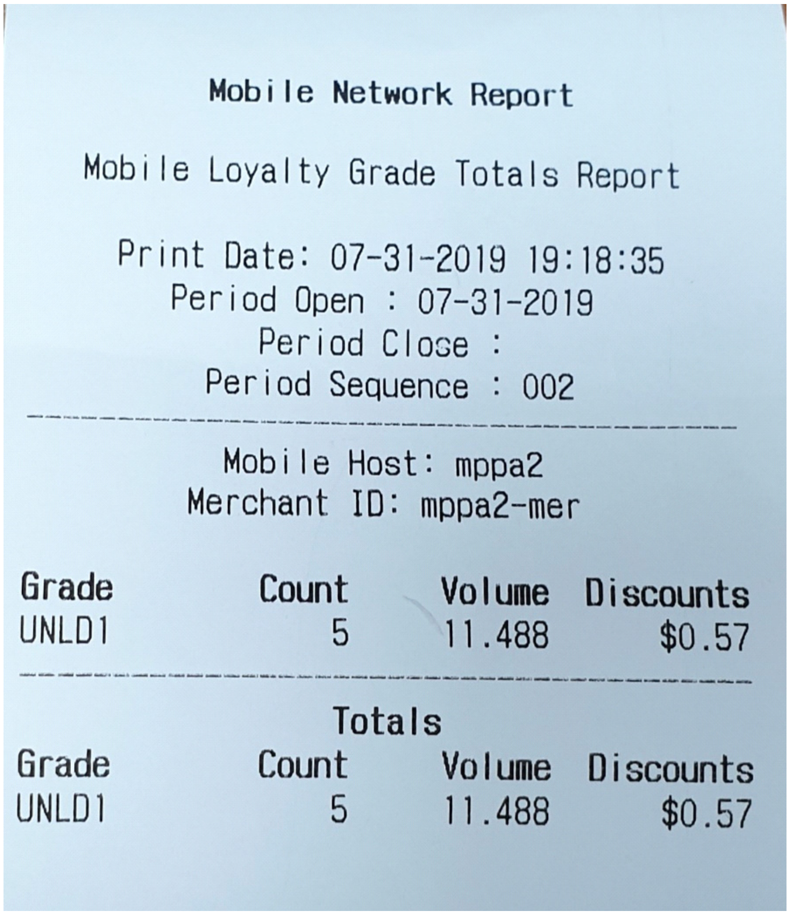
Loyalty Discount by Type Report gives details about PPG, Ticket, Line items loyalty discounts given by MPPA.



```
          Mobile Network Report

     **Loyalty Discount By Type Report**
         Printed:07/31/2019 19:18:27
     Period:07/31/2019 To current(002)


-------------------------------------------

             Mobile Host:mppa2
           Merchant ID:mppa2-mer

   Loyalty Program Id:Discount Program 2

PPU       TICKET    ITEM      TOTAL $
DISC      DISC      DISC
0.23      0.06      0.02         0.31

   Loyalty Program Id:Discount Program 1

PPU       TICKET    ITEM      TOTAL $
DISC      DISC      DISC
0.12      0.03      0.01         0.16

   Loyalty Program Id:Discount Program 3

PPU       TICKET    ITEM      TOTAL $
DISC      DISC      DISC
0         0.09      0.24         0.33
```

Loyalty Grade Totals Report

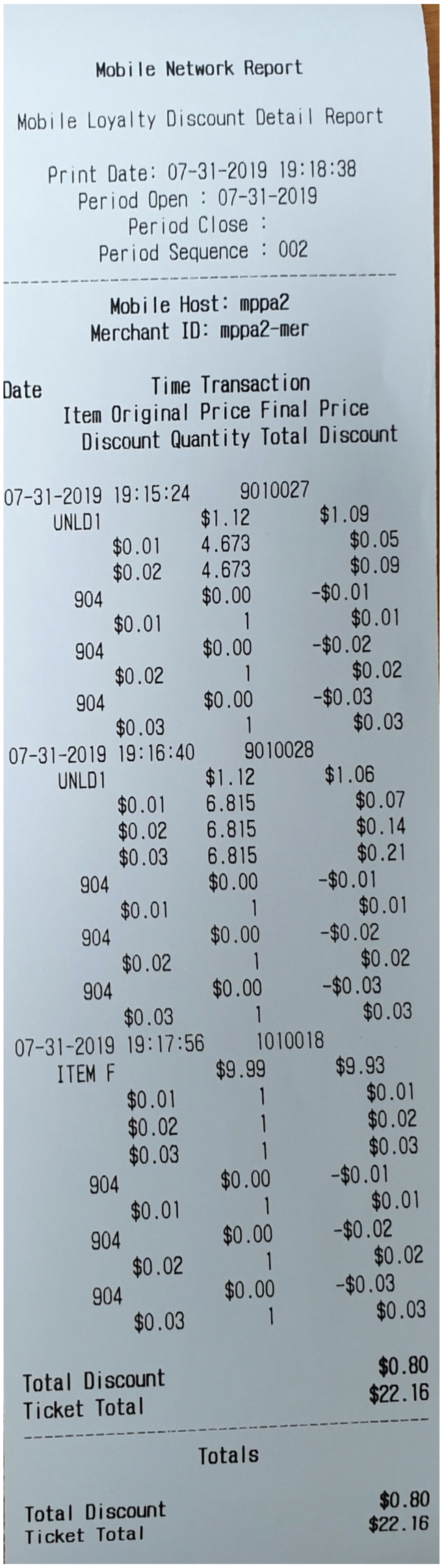
Loyalty Grade Totals Report gives details about all ASA PPG discounts given by all configured mobile host programs.



```
            Mobile Network Report

     Mobile Loyalty Grade Totals Report

       Print Date: 07-31-2019 19:18:35
          Period Open : 07-31-2019
              Period Close :
          Period Sequence : 002
--------------------------------------------
            Mobile Host: mppa2
          Merchant ID: mppa2-mer

Grade          Count     Volume  Discounts
UNLD1              5     11.488      $0.57
--------------------------------------------
                     Totals
Grade          Count     Volume  Discounts
UNLD1              5     11.488      $0.57
```

Loyalty Discount Detail Report

Loyalty Discount Detail Report gives you detail about all ASA discounts given by all configured mobile host programs.

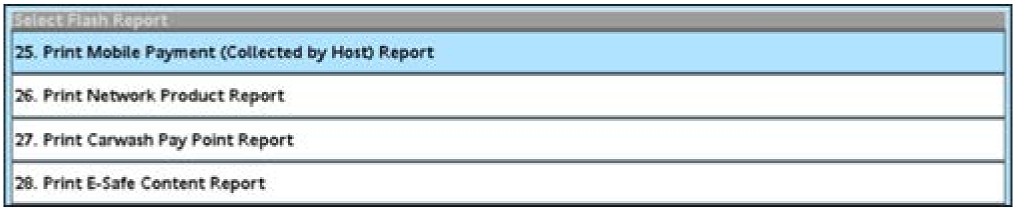


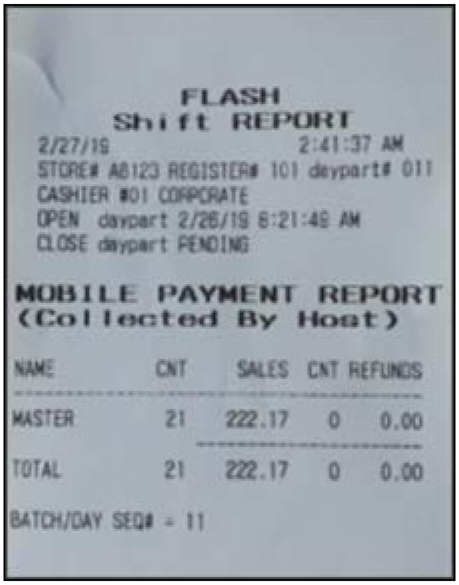
```
              Mobile Network Report

       Mobile Loyalty Discount Detail Report

          Print Date: 07-31-2019 19:18:38
            Period Open : 07-31-2019
              Period Close :
           Period Sequence : 002
-----------------------------------------------
              Mobile Host: mppa2
            Merchant ID: mppa2-mer

Date             Time Transaction
       Item Original Price Final Price
         Discount Quantity Total Discount

07-31-2019 19:15:24     9010027
     UNLD1          $1.12        $1.09
          $0.01     4.673           $0.05
          $0.02     4.673           $0.09
       904          $0.00       -$0.01
          $0.01         1           $0.01
       904          $0.00       -$0.02
          $0.02         1           $0.02
       904          $0.00       -$0.03
          $0.03         1           $0.03
07-31-2019 19:16:40     9010028
     UNLD1          $1.12        $1.06
          $0.01     6.815           $0.07
          $0.02     6.815           $0.14
          $0.03     6.815           $0.21
       904          $0.00       -$0.01
          $0.01         1           $0.01
       904          $0.00       -$0.02
          $0.02         1           $0.02
       904          $0.00       -$0.03
          $0.03         1           $0.03
07-31-2019 19:17:56     1010018
     ITEM F         $9.99        $9.93
          $0.01         1           $0.01
          $0.02         1           $0.02
          $0.03         1           $0.03
       904          $0.00       -$0.01
          $0.01         1           $0.01
       904          $0.00       -$0.02
          $0.02         1           $0.02
       904          $0.00       -$0.03
          $0.03         1           $0.03

 Total Discount                     $0.80
 Ticket Total                      $22.16
-----------------------------------------------
                  Totals

 Total Discount                     $0.80
 Ticket Total                      $22.16
```

Above Site Mobile Report

Mobile Payment (Collected by Host) Report

The Mobile Payment (Collected by Host) Report gives details about all ASA Mobile Payments based on card type collected by the Host. This report is printed from the **CSR Functions > Reporting > Flash Reports Menu**.


Select Flash Report
25. Print Mobile Payment (Collected by Host) Report
26. Print Network Product Report
27. Print Carwash Pay Point Report
28. Print E-Safe Content Report



```
            FLASH
        Shift REPORT
  2/27/19                2:41:37 AM
  STORE# AB123 REGISTER# 101 daypart# 011
  CASHIER #01 CORPORATE
  OPEN  daypart 2/26/19 6:21:46 AM
  CLOSE daypart PENDING

MOBILE PAYMENT REPORT
(Collected By Host)

NAME           CNT     SALES  CNT REFUNDS
------------------------------------------
MASTER          21    222.17    0    0.00
                    ----------------------
TOTAL           21    222.17    0    0.00

BATCH/DAY SEQ# = 11
```

Troubleshooting

Site Doesn’t Display on Mobile Payment Application

1. Verify that site has Mobile Host connectivity.
   - Ping the host from: POS Main Menu > Maintenance > Ping Test (site level)
   - Ping the host from Verifone Commander as the VASC-level user MAINT using: Ping < Mobile Host IP Address>.
2. If the site has connectivity, but does not appear on the mobile application, verify connectivity to the Mobile Host.
   - Check the logs (/var/log/messages) to verify a site update request from the Verifone Commander to the Mobile Host was successful
   - If needed, contact mobile host provider.
3. Confirm the Mobile Host Provide onboarding details were configured properly.

Site Settlement Failed

1. Verify that the settlement details (e.g., settlement employee number and settlement password) were entered in Mobile Host Configuration.

   The settlement details must be the same as what was received from the Mobile Host Provider during the site onboarding process for Mobile Payment.
2. Contact the mobile host provider if the entered configuration details are correct.

NOTE

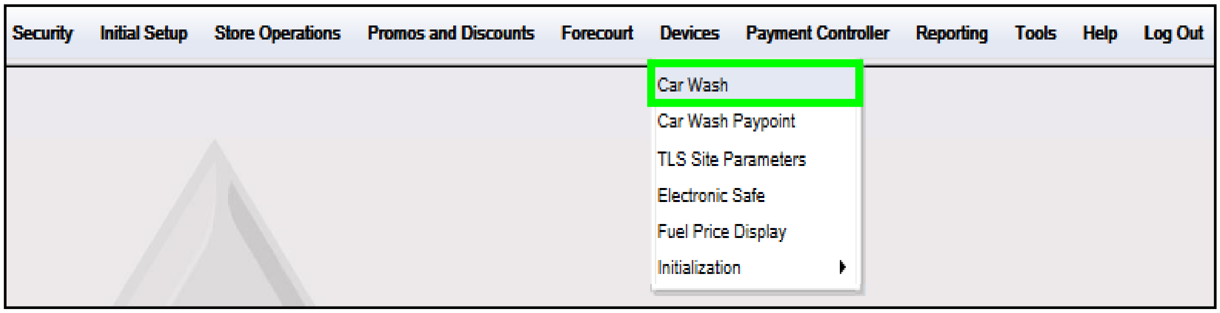
These attributes are specific to FDC Mobile and are not used by the VFIMobile adapter.

Pump Reserved but Authorization Failed

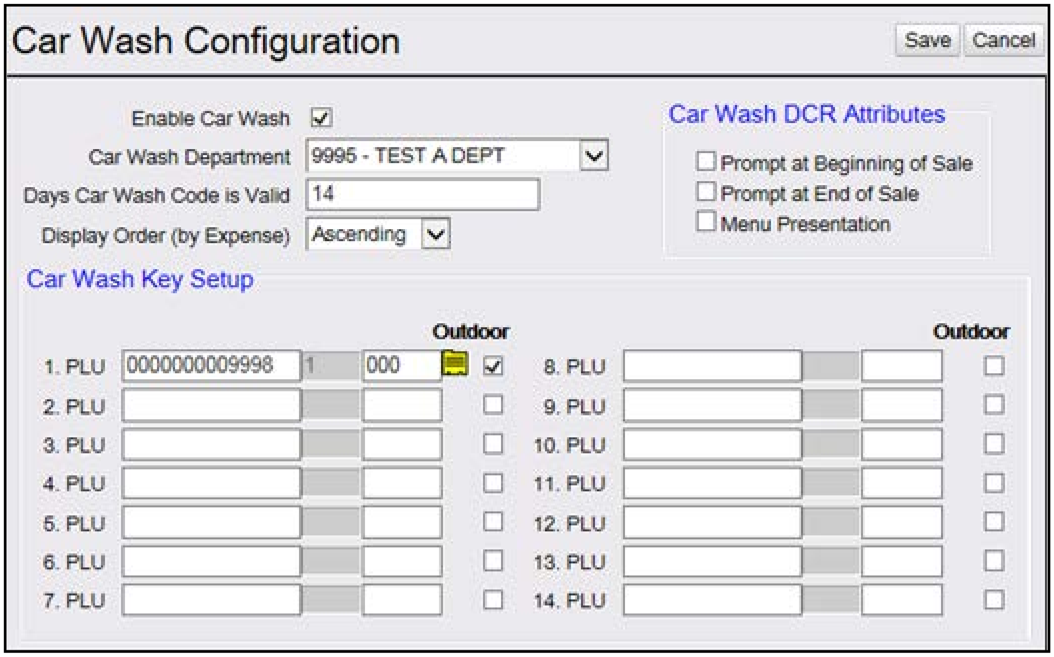
- The pump reservations are released after 3 minutes.

Car Wash PLUs Not Displaying on Mobile Payment Application

1. From the Configuration Client, go to: Devices > Car Wash.



The Car Wash Configuration window displays.



Enable Car Wash ☑

Car Wash Department 9995 - TEST A DEPT

Days Car Wash Code is Valid 14

Display Order (by Expense) Ascending

Car Wash DCR Attributes

□ Prompt at Beginning of Sale

□ Prompt at End of Sale

□ Menu Presentation

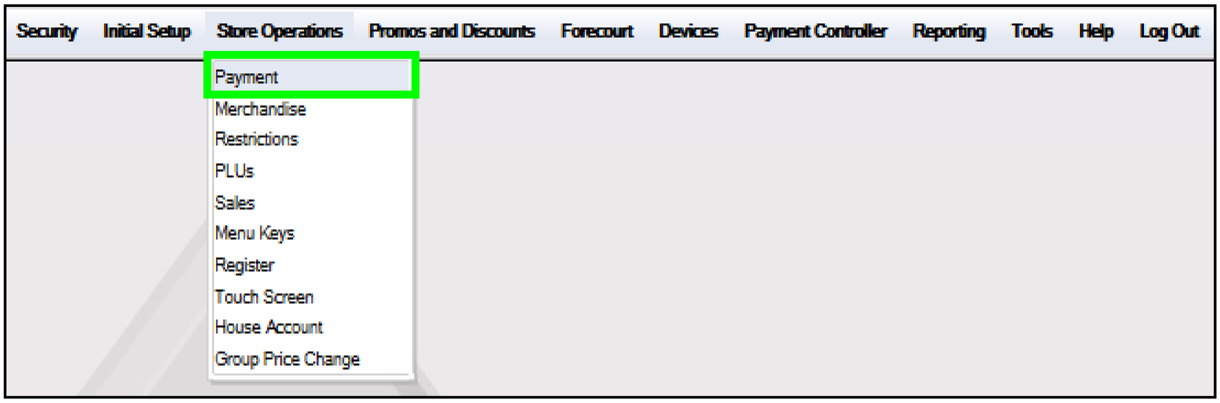
Car Wash Key Setup

				Outdoor					Outdoor
1. PLU	0000000009998	1	000	☑	8. PLU				□
2. PLU				□	9. PLU				□
3. PLU				□	10. PLU				□
4. PLU				□	11. PLU				□
5. PLU				□	12. PLU				□
6. PLU				□	13. PLU				□
7. PLU				□	14. PLU				□

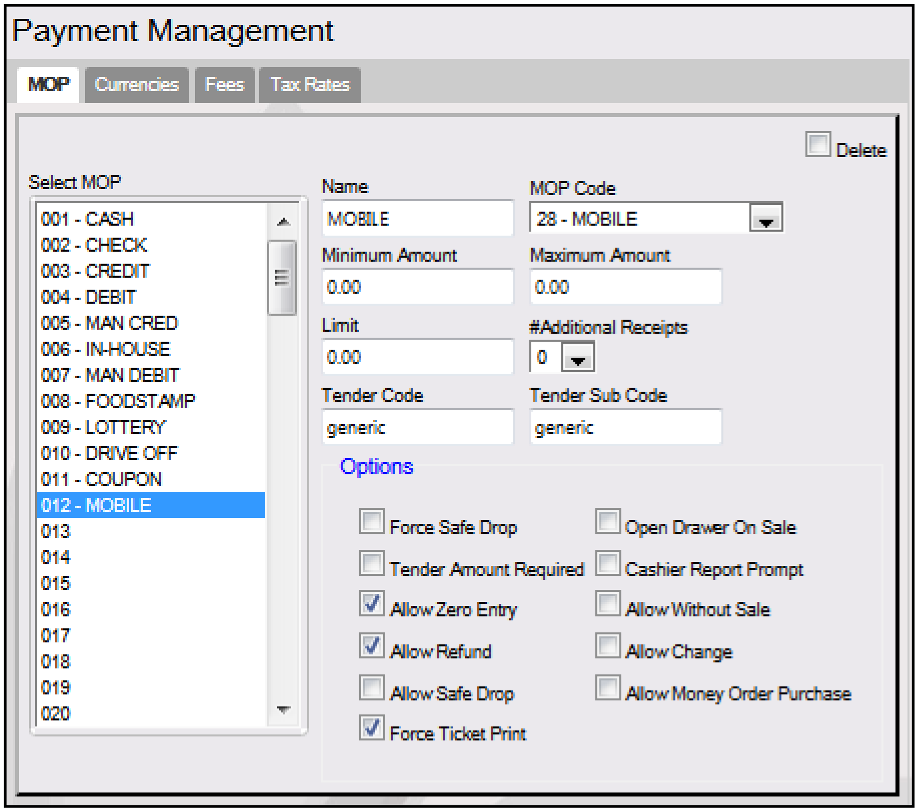
2. Verify that all Car Wash PLUs are configured and enabled for Outdoor.

Pump Can’t Authorize Mobile Payment Application

1. From the Configuration Client, go to: Store Operations > Payment.



The Payment Management window displays.



Payment Management

MOP | Currencies | Fees | Tax Rates

□ Delete

Select MOP

001 - CASH
002 - CHECK
003 - CREDIT
004 - DEBIT
005 - MAN CRED
006 - IN-HOUSE
007 - MAN DEBIT
008 - FOODSTAMP
009 - LOTTERY
010 - DRIVE OFF
011 - COUPON
012 - MOBILE
013
014
015
016
017
018
019
020

Name: MOBILE

MOP Code: 28 - MOBILE

Minimum Amount: 0.00

Maximum Amount: 0.00

Limit: 0.00

#Additional Receipts: 0

Tender Code: generic

Tender Sub Code: generic

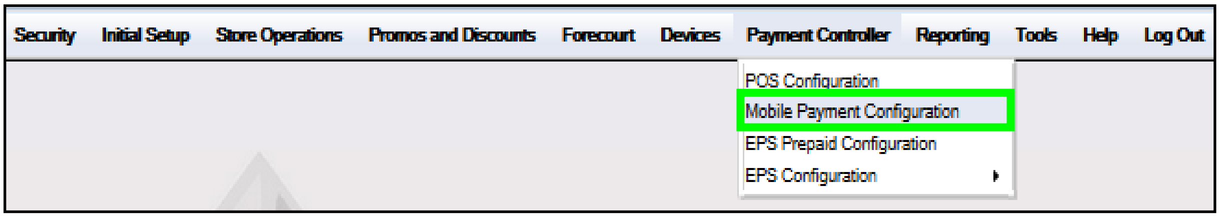
Options

□ Force Safe Drop
□ Open Drawer On Sale
□ Tender Amount Required
□ Cashier Report Prompt
☑ Allow Zero Entry
□ Allow Without Sale
☑ Allow Refund
□ Allow Change
□ Allow Safe Drop
□ Allow Money Order Purchase
☑ Force Ticket Print

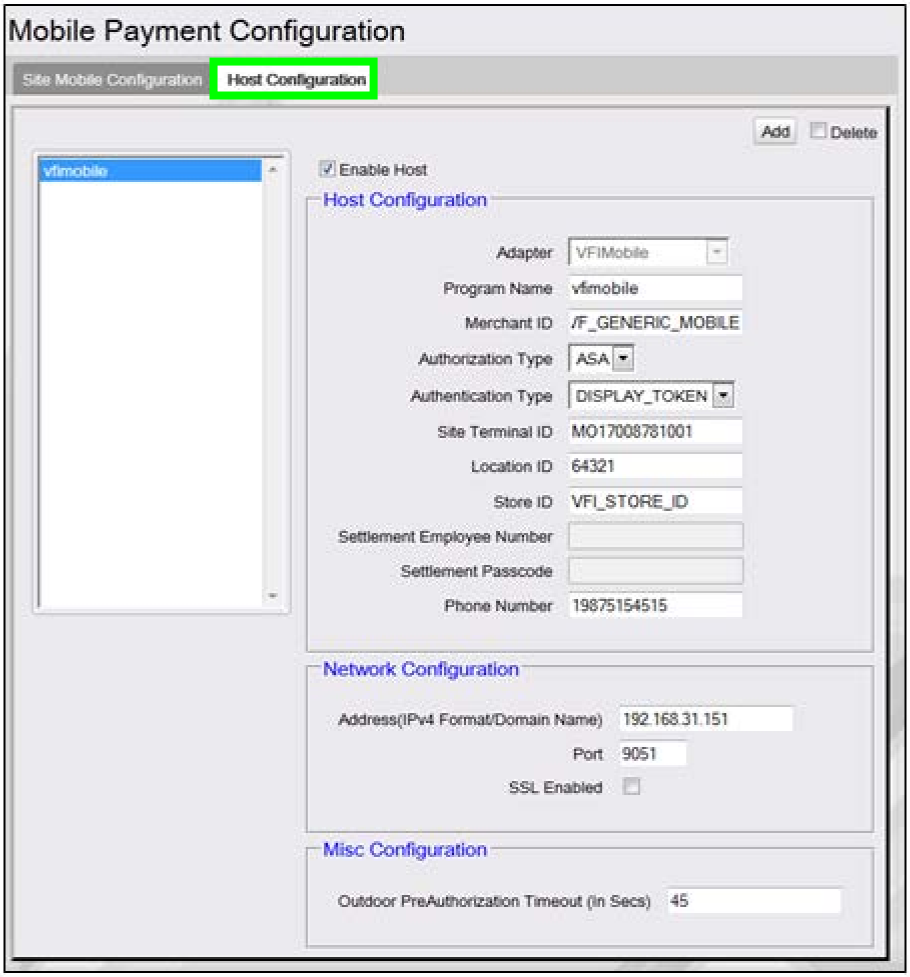
2. Verify that the Mobile MOP is configured.

Disabling the Mobile Host

1. From the Configuration Client, go to: Payment Controller > Mobile Payment Configuration.



The Mobile Payment Configuration window displays.



Mobile Payment Configuration

vfimobile

☑ Enable Host

Host Configuration

Adapter: VFIMobile
Program Name: vfimobile
Merchant ID: /F_GENERIC_MOBILE
Authorization Type: ASA
Authentication Type: DISPLAY_TOKEN
Site Terminal ID: MO17008781001
Location ID: 64321
Store ID: VFI_STORE_ID
Settlement Employee Number:
Settlement Passcode:
Phone Number: 19875154515

Network Configuration

Address(IPv4 Format/Domain Name): 192.168.31.151
Port: 9051
SSL Enabled: □

Misc Configuration

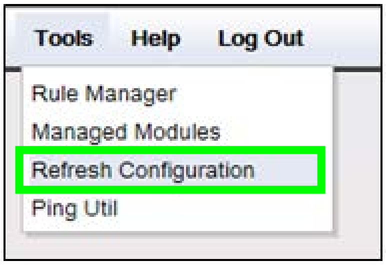
Outdoor PreAuthorization Timeout (In Secs): 45

2. Select the **[Host Configuration]** tab.
3. Deselect **[Enable Host]**.

4. Select **[Save]** to accept, or **[Cancel]** to exit without saving changes.

⚠ *After disabling the host, the POS displays an alarm “**Host Disable in Progress**.” The Verifone Commander will not accept new transactions until the Host Disabled alarm is cleared, once the settlement with MPPA completes.*

5. To apply new settings, go to: Configuration Client > Tools > Refresh Configuration.



NOTE *Log out and back in to all POS terminals after any setting modifications to allow these changes to take affect.*

Appendix A - Terms

Term	Definition
API	Application Programming Interface.
ASA	Above Site Authorization - above site authorization is the scenario when MPPA talks to the PFEP to obtain an authorization outside of the Site System. The POS does not engage the EPS or PFEP for payment. The mobile authorization request is an unsolicited message from MPPA to the site system Mobile Service.
DCR	Dispenser Card Reader.
EPS	Electronic Payments System – a hardware/software application that processes payments thru a payment host or series of payment hosts.
FCC	Forecourt Controller – the controller that handles pump processing at the site.
FEP	Front End Processor - software process that resides on the EPS. The FEP is the front-end process for a particular host.
OPT	Outdoor Payment Terminal - a device installed at a retail petroleum site to enable payment outdoors without direct intervention from a site operator.
POP	Point of Payment.
POS	Point of Sale.
PPG	Price Per Gallon.
PFEP	Payment Front End Processor - the application or institution that the Site or MPPA uses for the processing of payments.
MD	Mobile Device - the mobile device (e.g., smart phone) used by the customer to interface with the Mobile Payments Processing Application (host).
Mobile Service	Mobile Service – a software program at the Site that facilitates the communication between the MPPA, the Site's System, the POS, and in some cases the PFEP.
MPA	Mobile Payments Application - a software application downloaded by a customer to a mobile device to facilitate mobile payment transactions.

Term	Definition
MPPA	Mobile Payments Processing Application - the application/ host that facilitates the communication between the MPA on the mobile device, Site System, and at times the PFEP for purposes of mobile payments.
SLA	Site Level Authorization - is the scenario when MPPA provide necessary details (Payment instrument) to site system so Mobile Service makes a card/payment request to EPS with those details to get authorization. EPS component will communicate with PFEP processor for authorization. MPPA does not engage PFEP for this use case. Authorization request is an unsolicited message from MPPA to the site system Mobile Service.
SSL	Secure Socket Layer - is a standard security technology for establishing an encrypted link between a server and a client.
UMTI	Unique Mobile Transaction Identifier - serves as a transaction identifier. It is expected that the UMTI will remain the same for all the messages exchanged for a single transaction.
VPN	Virtual Private Network.

Appendix B - Partner Links

FIS

www.FISglobal.com

Contact Information

601 Riverside Avenue, Jacksonville, FL 32204
904-438-6000
E-Mail: moreinfo@fisglobal.com

Gas Buddy

www.GasBuddy.com

Mailing Address

60 Canal St, Boston, MA 02109

GasBuddy Mobile App

www.gasbuddy.com/App

MShift, Inc.

www.MShift.com

Contact Information

39899 Balentine Drive, Suite 235, Newark, CA 94560
510-933-5901
E-Mail: info@mshift.com

Paydient

www.Paydient.com

Contact Information

275 Grove St, Auburndale, MA 02466
617-219-4200
E-Mail: info@paydiant.com

P97 Networks, Inc.

www.P97.com

Contact Information

10333 Richmond Avenue #250, Houston, TX 77042
713-588-4200 (8:00 AM – 5:00 PM CST, Monday-Friday)
E-mail: support@p97.com

Documentation

PetroZone Functions Supported by Mobile API: http://p97.com/dox/PZE-UC006.pdf
PetroZone Installation Reference for Mobile API: http://p97.com/dox/DEL-INREF016.pdf

ZipLine

www.ZipLine.biz

Contact Information

4171 West Hillsboro Boulevard, Suite 5, Coconut Creek, FL 33073
954-449-9540
E-mail: Info@zipline.biz