

Mobile Payment

Feature Reference

Date: July 25, 2024



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 Site Controller.

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 Commander Site Controller.
- **Configuring** - This section contains information on how to configure the Mobile Payment feature on the Commander Site Controller.
- **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 Commander Site Controller.
- **Troubleshooting** - This section provides basic troubleshooting steps.

VeriFone, Inc.
2744 North University Drive
Coral Springs, FL 33065
Telephone: 800-837-4366
<http://www.verifone.com>

© 2024 VeriFone, Inc. All rights reserved.

No part of this publication covered by the copyrights herein may be reproduced or copied in any form or by any means - graphic, electronic, or mechanical, including photocopying, taping, or information storage and retrieval systems - without written permission of the publisher.

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. 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 Conexus V2 updates.
01/04/2022	Added the Mobile Payment (Collected by Host) Report.
02/01/2024	Updated document with branding changes.
07/25/2024	Updated to include that the Credit MOP soft key can be used for all network payment MOP types.

Contents

Overview	1
Feature Description	1
Hardware Requirements	1
Software Requirements	1
Configuring Mobile Payments	2
Prerequisites	2
Site Onboarding Information	2
Mobile Host Provided	2
Site Provided	2
Configuring User Roles for Mobile Configuration and Reports	3
Configure Mobile Method of Payment (MOP)	6
Mobile Payment Configuration	10
Site Mobile Configuration	12
Host Configuration	14
Configure Loyalty Key on DCR for Using Mobile Payment	18
Configure Loyalty Key “REWARDS” on Dispensers with Graphics DCR ..	18
Configure Loyalty Key on Dispensers with Non-Graphics DCR	20
Configure Site Address	20
Local Area Network Configuration	22
Configure Device Specific Routes	22
Enabling Mobile Payment to Appear on Day Close Report	24
Using Mobile Payments	28
Indoor Transactions	28
Pay at POS with Code Displayed on POP	28
Pay at POS with Code Displayed on Phone	29
Outdoor Transactions	31
Pay at Pump with Code Entry	31
Pay at Pump without Code Entry	32
Reporting	33
Mobile Settlement Report	34
Report Details	34
Header	34
Terminal and Host Totals	34
Payment Type Totals	34
Exception Transactions	34
Pending Transactions	35
Discounted Transactions	35
Mobile Terminal Batch Detail Report	35
Report Details	36
Header	36
Transaction Totals	36
Above Site Loyalty Reports	36
Terminal Batch Loyalty Summary Report	37
Loyalty Discount By Type Report	38
Loyalty Grade Totals Report	39

Loyalty Discount Detail Report	40
Above Site Mobile Report	41
Mobile Payment (Collected by Host) Report	41
Troubleshooting	42
Site Doesn't Display on Mobile Payment Application	42
Site Settlement Failed	42
Pump Reserved but Authorization Failed	42
Car Wash PLUs Not Displaying on Mobile Payment Application	43
Pump Can't Authorize Mobile Payment Application	44
Disabling the Mobile Host	45
Appendix A - Terms	47
Appendix B - Partner Links	49
FIS	49
Contact Information	49
Gas Buddy	49
Mailing Address	49
GasBuddy Mobile App	49
MShift, Inc.	49
Contact Information	49
Paydient	49
Contact Information	49
P97 Networks, Inc.	50
Contact Information	50
Documentation	50
ZipLine	50
Contact Information	50

Overview

Feature Description

The Mobile Payment feature reference provides information to setup a location to accept Mobile Payments at sites with a 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.

Hardware Requirements

- Commander Site Controller with C18
- Commander Site Controller with Topaz
- Commander Site Controller with Ruby2
- RubyCi with Topaz
- RubyCi with Ruby2
- Commander 16 with Topaz
- Commander 16 with Ruby2

Software Requirements

Commander Site Controller base 39 and higher.

Configuring Mobile Payments

Prerequisites

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 from 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)



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

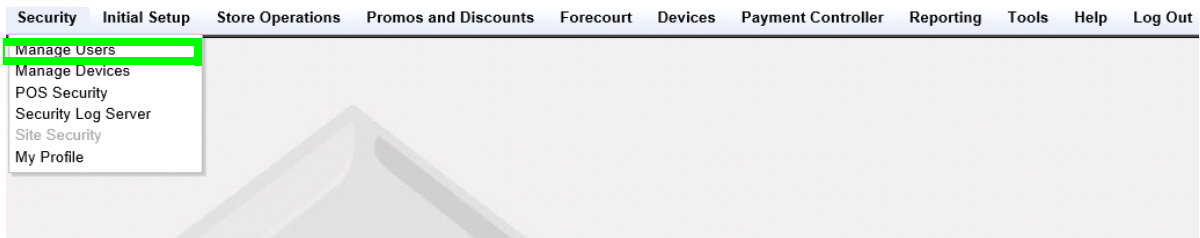
Configuring User Roles for Mobile Configuration and Reports

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



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)

Configure Users | **Configure Roles**

Select User

- manager
- Basic

Name: manager Disallow Login

Employee: Basic

Roles: basic, manager

Password Settings

Min. Length: 7 | New Password:

Max. Length: 40 | Confirm Password:

of Days to Expire: 90


Force change on next login:

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]**.

User Administration

 Edits require a one-time password (OTP)

Configure Users **Configure Roles**

Add Delete

Select Role

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

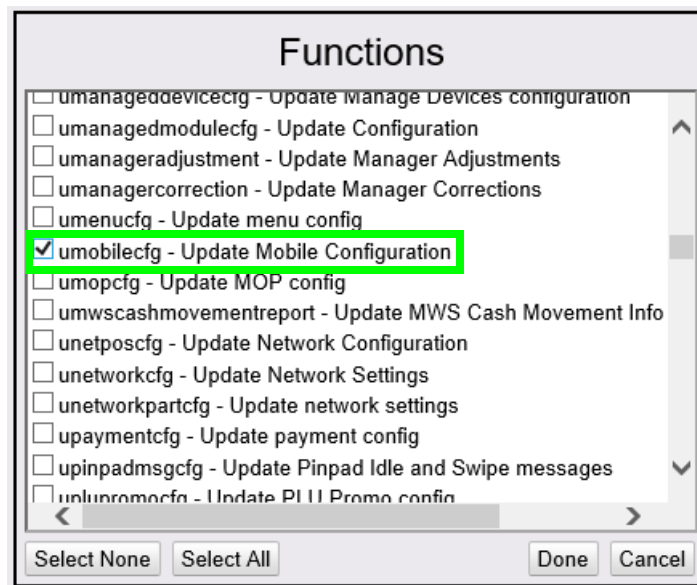
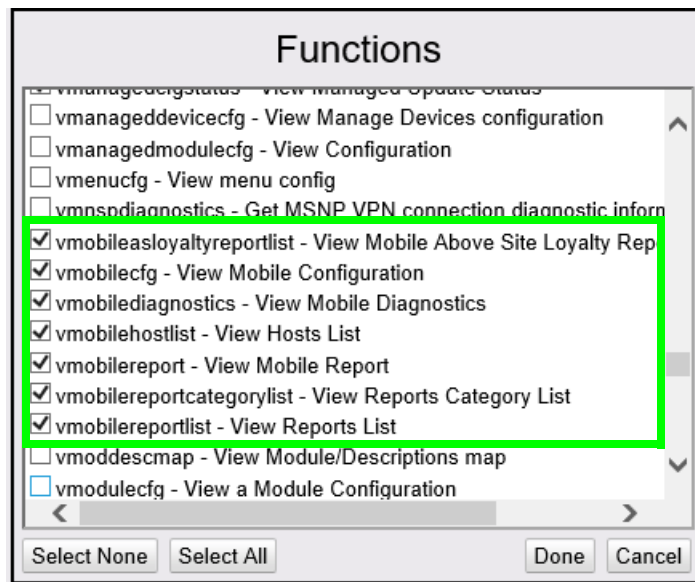
Name Secure Role

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
- ...

Edit

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



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)

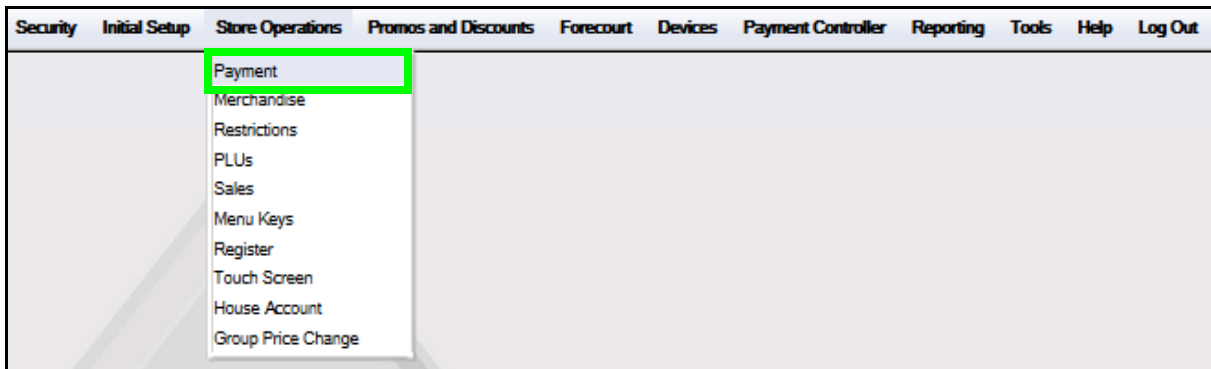


New installations have a default Method of Payment and Code configured in the system to accept mobile payments.

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.

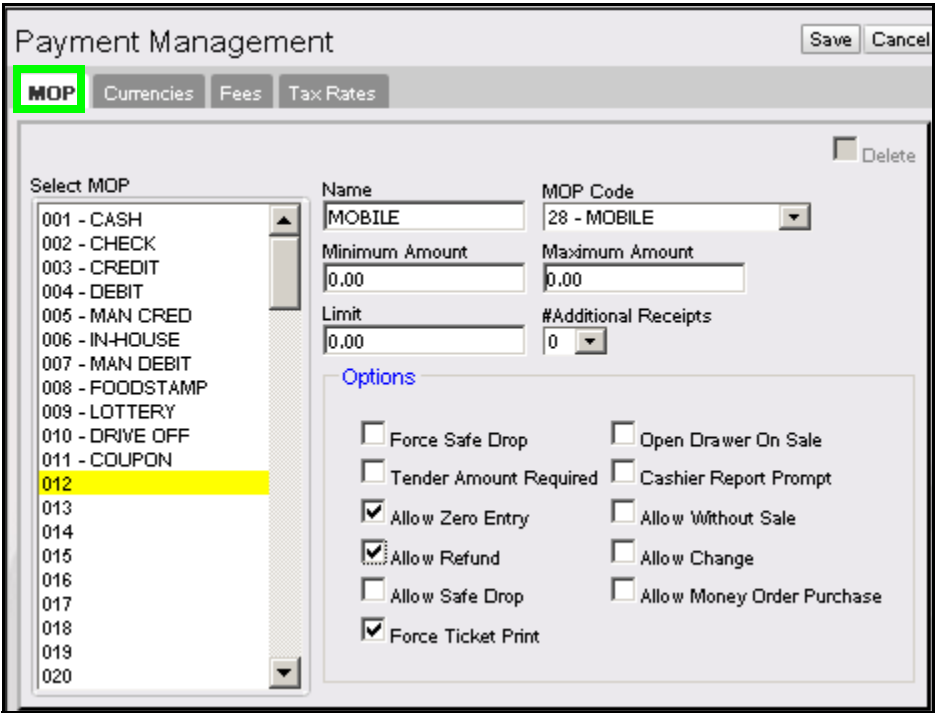


The Payment Management window displays.

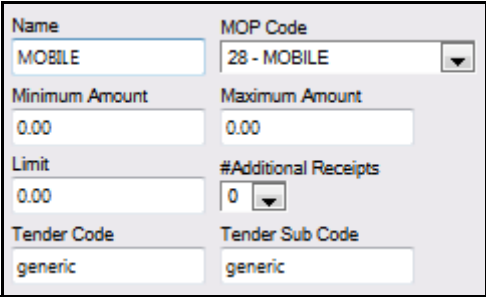
The screenshot shows the 'Payment Management' window. At the top, there are tabs for 'MOP', 'Currencies', 'Fees', and 'Tax Rates'. The 'MOP' tab is active. On the right side, there is a 'Delete' button. The main area is divided into several sections:

- Select MOP:** A list box containing MOP codes from 001 to 020. The list includes: 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, and 020.
- Name:** A text input field.
- MOP Code:** A dropdown menu currently showing '00 - CASH'.
- Minimum Amount:** A text input field.
- Maximum Amount:** A text input field.
- Limit:** A text input field.
- #Additional Receipts:** A dropdown menu currently showing '0'.
- Tender Code:** A text input field.
- Tender Sub Code:** A text input field.
- Options:** A section containing several checkboxes:
 - 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.



- 3. Scroll down the **<Select MOP>** pane to an unconfigured position.
- 4. Configure the Mobile MOP parameters.



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

<input type="checkbox"/> Force Safe Drop	<input type="checkbox"/> Open Drawer On Sale
<input type="checkbox"/> Tender Amount Required	<input type="checkbox"/> Cashier Report Prompt
<input checked="" type="checkbox"/> Allow Zero Entry	<input type="checkbox"/> Allow Without Sale
<input checked="" type="checkbox"/> Allow Refund	<input type="checkbox"/> Allow Change
<input type="checkbox"/> Allow Safe Drop	<input type="checkbox"/> Allow Money Order Purchase
<input checked="" type="checkbox"/> Force Ticket Print	

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

MOP Currencies Fees Tax Rates

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

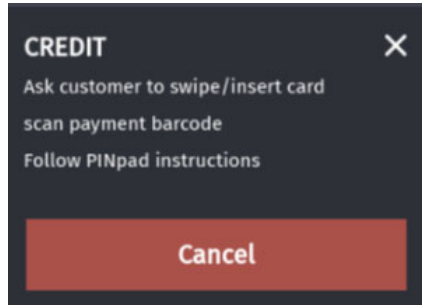
- Force Safe Drop
- Open Drawer On Sale
- Tender Amount Required
- Cashier Report Prompt
- Allow Zero Entry
- Allow Without Sale
- Allow Refund
- Allow Change
- Allow Safe Drop
- Allow Money Order Purchase
- Force Ticket Print

Delete



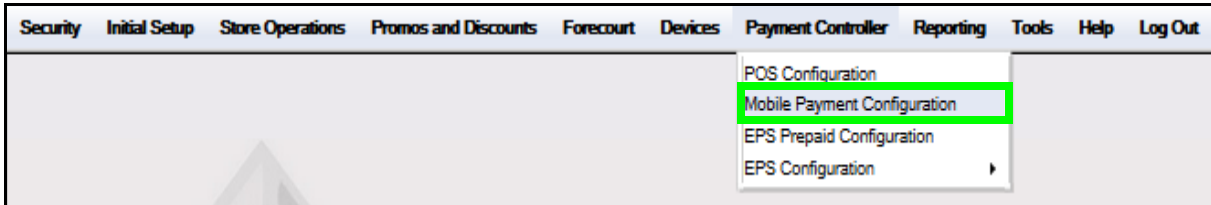
Log out and back in to all POS terminals after any setting modifications to allow these changes to take effect.

*From Verifone Commander Release 55.02, Credit MOP soft key can be used for all transactions using Credit, Debit, EBT, EBT Cash, Mobile Payment, Gift Card, or any other network payment methods. The following appears when cashier press **Total > Credit**:*




Mobile Payment Configuration

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



The Mobile Payment Configuration window displays.

Mobile Payment Configuration

 Edits require a one-time password (OTP)

Site Mobile Configuration | Host Configuration

Accept Mobile Payments

Site Configuration

Site Name

Welcome Message

Misc Configuration

Data Storage Time(In Days)

Site Address

Latitude

Longitude

Report 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

i Edits require a one-time password (OTP)

Site Mobile Configuration
Host Configuration

Accept Mobile Payments

Site Configuration

Site Name

Welcome Message

Misc Configuration

Data Storage Time(In Days)

Site Address

Latitude

Longitude

Report Format

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

Accept Mobile Payments

3. Configure the following Site Configuration parameters:

Site Configuration

Site Name

Welcome Message

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)

Site Address

Latitude

Longitude

Report 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	<p>The combination of these fields are used to set the format type for each report from the report drop-down.</p> <p>The values are “Standard” and “Extended Authorization”.</p> <p>The default format type would be “Standard” for all reports.</p> <p>In the Chevron distribution, the Mobile Terminal Batch Detail Report will default to Extended Authorization format.</p> <p>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.</p> <p>As of now this feature is applicable only for Mobile Terminal Batch Detail Report.</p>

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

Site Mobile Configuration **Host Configuration**

Enable Host

Host Configuration

Adapter: VF1 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: <ul style="list-style-type: none"> • FDC Mobile - ConnectorSwitch adapter or outdoor transactions. • VFIMobile V1 - for Conexus V1 standards • VFIMobile V2 - for Conexus V2 standards • Local MPPA - for Shell Distribution
Program Name	The Program Name
Merchant ID	The Merchant ID number provided by the Mobile Payment Host.

Variable	Value
<p>Authentication Type</p>	<p>The site Authentication Type:</p> <ul style="list-style-type: none"> • 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. <p>If the Adapter type is 'FDC Mobile', then the field 'Authentication type' is disabled. This adapter allows only outdoor transactions.</p>
<p>Site Terminal ID</p>	<p>ID number for the terminal received from the Mobile Payment Host.</p> <p> Note: For Conexus standards, <i>Site_terminal ID and Location ID are greyed out.</i></p>
<p>Location ID</p>	<p>The Location ID provided by the Mobile Payment Host; identifies the site during the on boarding process.</p> <p> Note: For Conexus standards, <i>Site_terminal ID and Location ID are greyed out.</i></p>
<p>Store ID</p>	<p>The site Store ID number.</p>
<p>Settlement Employee Number</p>	<p>The Settlement Employee Number provided by the Mobile Payment Host</p>
<p>Settlement Passcode</p>	<p>The Settlement Passcode.</p>

Variable	Value
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.



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 Commander Site Controller 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:

The screenshot shows a window titled "Misc Configuration". It contains two fields: "Outdoor PreAuthorization Timeout (In Secs)" which is an empty text input box, and "Site Initiated Loyalty" which is a dropdown menu currently set to "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: <ul style="list-style-type: none"> • 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

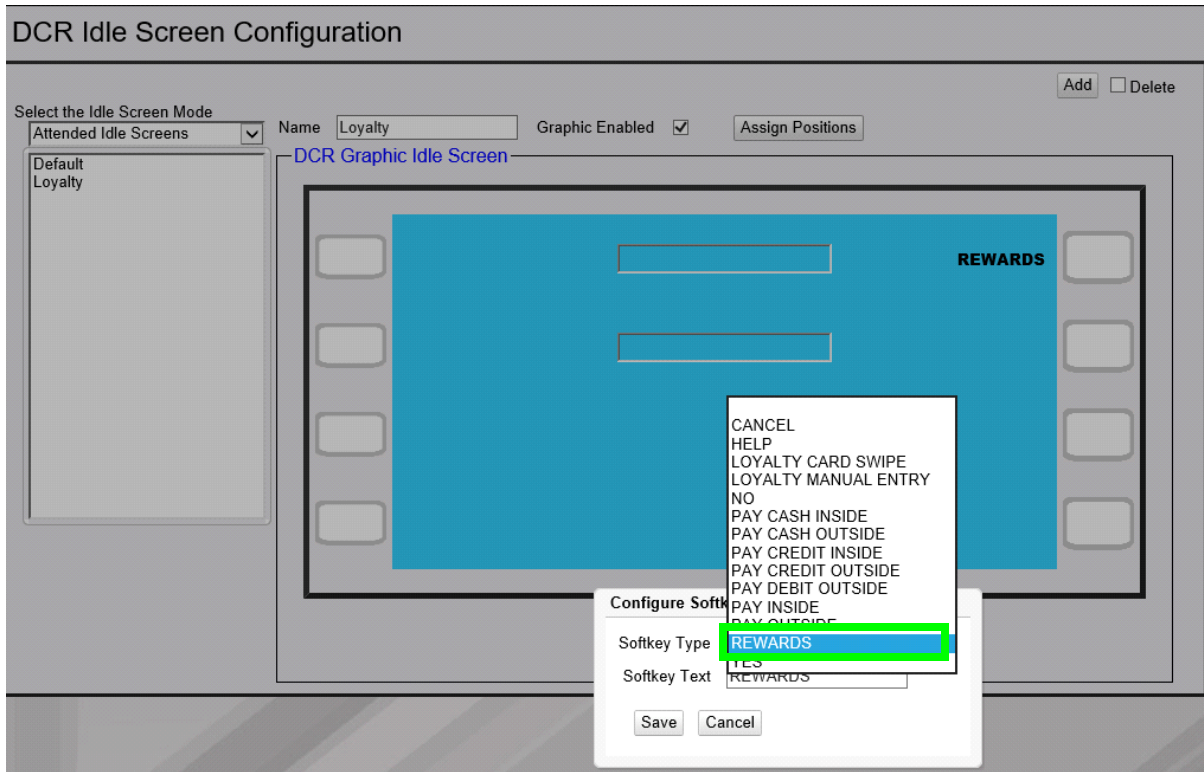
Following are the steps to configure loyalty for mobile payment if site has a loyalty program(s) enabled.

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 Commander 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.



*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.

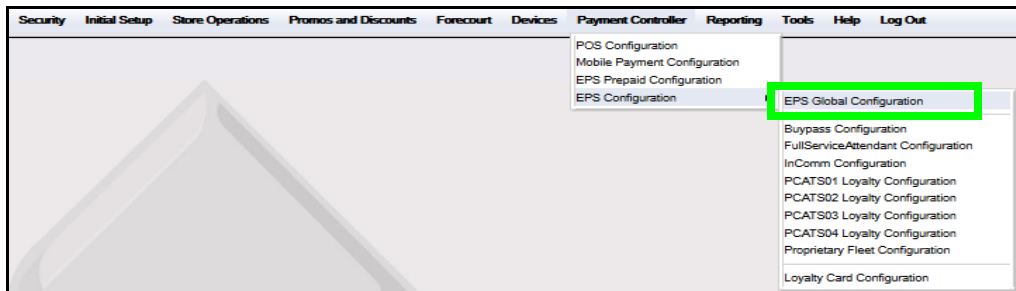


*Do a **Tools > Refresh Configuration** and **Forecourt > Initialization > DCR** after the configuration changes.*

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**.



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

EPS Global Configuration [Save] [Cancel]

EPS POP PINPAD Message Loyalty Trigger Pull Configuration EMV Configuration EMV Initialization

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

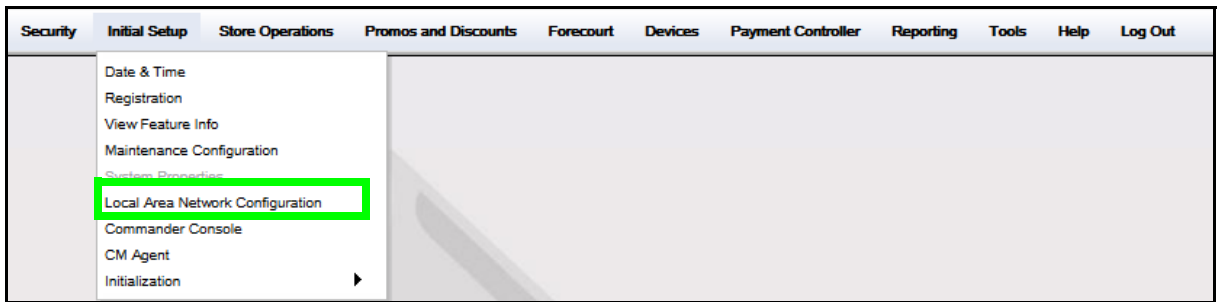
3. Select **[Save]** to accept, or **[Cancel]** to exit without saving changes.



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.

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

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

- Enter the Device Specific Host Route Destination address provided by the Mobile Payment Host.
- Enter the Gateway address; this will be the site's Payment Gateway address, as associated with the Isolated Payment NIC.

- Enter the Netmask = 255.255.255.255.
- Click **[Save]** in the New Route Configuration dialog box.

9. Click [**Save**] on the main form.
10. Reboot the Commander Site Controller to ensure proper network routing is used for all devices.

The screenshot shows the 'Local Area Network Configuration' window. At the top right, the 'Save' button is highlighted with a green box. The window is divided into several sections:

- Global Routes:** A table with columns 'Route Type', 'Destination', 'Gateway', and 'Netmask'. Below the table are 'New' and 'Delete' buttons.
- Device Specific IP Configuration:** A table with columns 'NIC Description', 'IP Address', 'Configure By DHCP', and 'Default Route'. It lists 'Isolated payment NIC' and 'Verifone Zone'.
- Device Specific Routes:** A table with columns 'Route Type', 'Destination', 'Gateway', and 'Netmask'. It lists a 'host' route.
- DNS:** Fields for 'Domain Name (Optional)', 'DNS 1', 'DNS 2', and 'DNS 3'.

Enabling Mobile Payment to Appear on Day Close Report

The Mobile Payment Report must be enabled to appear on the Daily Close Report print out.

1. From the Configuration Client, go to: **Reporting > Report Configuration**.

The screenshot shows the 'Report Configuration' window. At the top, there are tabs for 'Report Configuration', 'Auto End Of Day(AEOD)', and 'Manager Workstation'. The 'Report Configuration' tab is active.

The window is divided into three main sections:

- Period Configuration:** Includes a dropdown for '2 - Day', a 'Description' field with 'Day', 'Period Type' set to 'day', 'Delay Between Close' set to '0' with a 'DAYS' dropdown, 'Roll Up DB Reports' set to 'Yes', and 'Store T-Log Data' set to 'Yes'.
- Report Parameters:** Includes 'Reclose Security' (5), 'Force Close Pending Security' (5), and 'Override AEOD Security' (9). There are several checkboxes: 'Print Automatically' (unchecked), 'Force Cashier Closed' (checked), 'Cashier Span Shifts' (unchecked), 'Force Cashier To Print' (unchecked), 'Allow Close With No Activity' (unchecked), and 'Allow Suspended Sales' (unchecked).
- Configure Group List:** Includes a dropdown for '2 - Day' and a list of items: 'Summary By Register', 'Department', 'Tax', 'Fueling Position/ Product (Hose)', 'Fuel DCR Statistics', 'Fuel Cash Acceptor', and 'Network Card'. An 'Edit' button is next to the list.

At the bottom, there is a warning icon and text: 'Roll Up DB Reports' will take effect only after the next period close or after Commander reboot.

- 2. Make sure 2-DAY is selected from the drop-down box in the **Configure Group List** section.

The screenshot shows the 'Report Configuration' window with three tabs: 'Report Configuration', 'Auto End OF Day(AEOD)', and 'Manager Workstation'. The 'Report Configuration' tab is active. It is divided into three main sections: 'Period Configuration', 'Report Parameters', and 'Configure Group List'. In the 'Configure Group List' section, a dropdown menu is open, showing '2 - Day' selected and highlighted with a green box. The list of items includes: Summary By Register, Department, Tax, Fueling Position/ Product (Hose), Fuel DCR Statistics, Fuel Cash Acceptor, and Network Card. An 'Edit' button is visible to the right of the list. A warning icon and message are at the bottom: 'Roll Up DB Reports' will take effect only after the next period close or after Commander reboot.

- 3. Click **Edit** in the **Configure Group List** section.

This screenshot is identical to the one above, showing the 'Report Configuration' window. In this view, the 'Edit' button in the 'Configure Group List' section is highlighted with a green box, indicating the next step in the process. The '2 - Day' option remains selected in the dropdown menu. The rest of the interface, including the 'Report Parameters' and 'Period Configuration' sections, remains unchanged.

4. Scroll down the list and select the **Mobile Payment Report** option.

The screenshot shows the 'Report Configuration' window. The 'Period Configuration' section is set to '2 - Day' with a description of 'Day', period type of 'day', and a delay of 0 days. The 'Report Parameters' section includes security levels (Reclose: 5, Force Close Pending: 5, Override AEOD: 9) and various checkboxes, with 'Force Cashier Closed' checked. The 'Configure Group List' section shows a list of report names, with 'Mobile Payment Report' selected and highlighted by a green box. Other options include Fuel tank Reconciliation, Fuel Tier/ Product, POP Fuel Discount, POP Discount Definition Report, Network Card, Network Product, Carwash Pay Point, E-Safe Content Report, E-Safe End Of Day Report, and Proprietary Network Card. A warning message at the bottom states: 'Roll Up DB Reports' will take effect only after the next period close or after Commander reboot.

5. Click **DONE**.

This screenshot is identical to the previous one, but the 'Done' button at the bottom right of the 'Report Names' list is highlighted with a green box, indicating the final step in the configuration process.

6. Click **SAVE**.

Report Configuration [Save] [Cancel]

Report Configuration | Auto End OF Day(AEOD) | Manager Workstation

Period Configuration

2 - Day

Description: Day

Period Type: day

Delay Between Close: 0 DAYS

Roll Up DB Reports: Yes

Store T-Log Data: Yes

Report Parameters

Reclose Security: 5

Force Close Pending Security: 5

Override AEOD Security: 9

Print Automatically

Force Cashier Closed

Cashier Span Shifts

Force Cashier To Print

Allow Close With No Activity

Allow Suspended Sales

Configure Group List

2 - Day

- Summary By Register [Edit]
- Department
- Tax
- Fuel Cash Acceptor
- Fuel DCR Statistics
- Fueling Position/ Product (Hose)
- Network Card
- Mobile Payment Report

! 'Roll Up DB Reports' will take effect only after the next period close or after Commander reboot.

After this configuration, the Mobile Payment Report, will be available as part of the information printed on the Day Close Report.
The report is also available as a selectable option in Report Navigator.

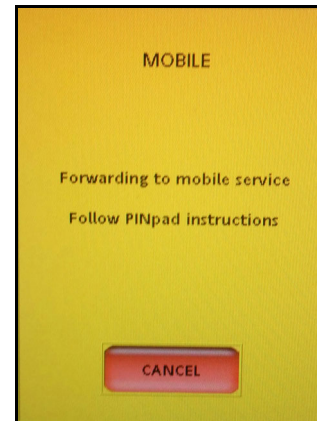
Using Mobile Payments

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.

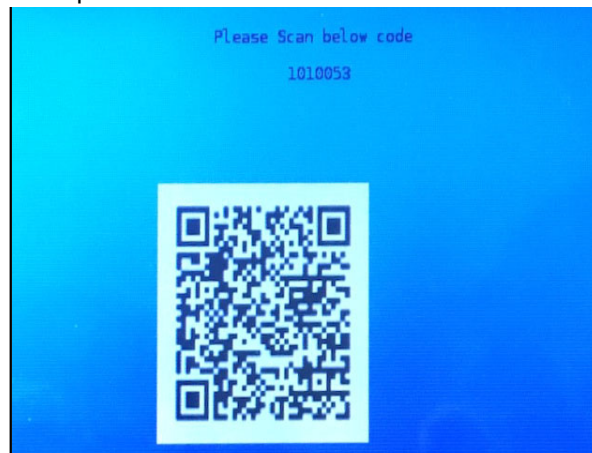


If multiple mobile hosts are configured at the site, then a host selection prompt appears on the POP device after Mobile MOP is selected.



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.



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.

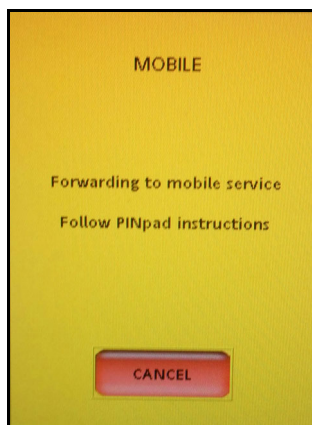


Receipt data sent to the MPPA is the same as the receipt being printed from the POS.

Pay at POS with Code Displayed on Phone

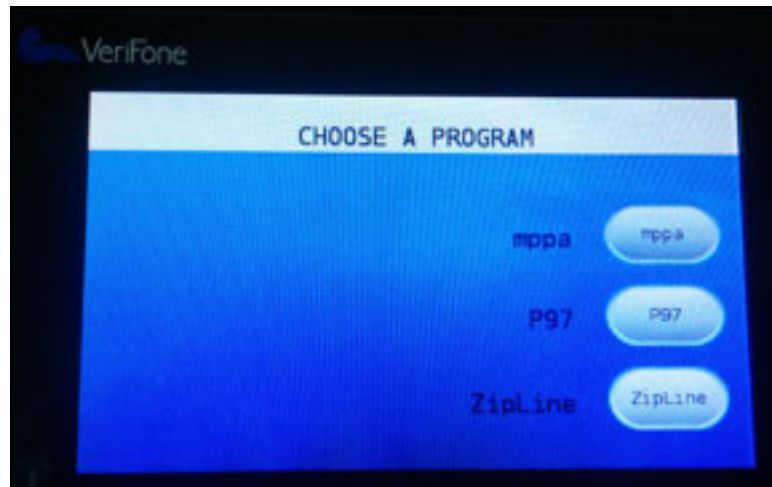
In this use case, the Customer initiates the mobile payment transaction request. The MPA initiates the transaction to obtain a dynamically generated pre-authorization token from the MPPA. The token is displayed on the phone and used to complete the transaction at the POS.

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.

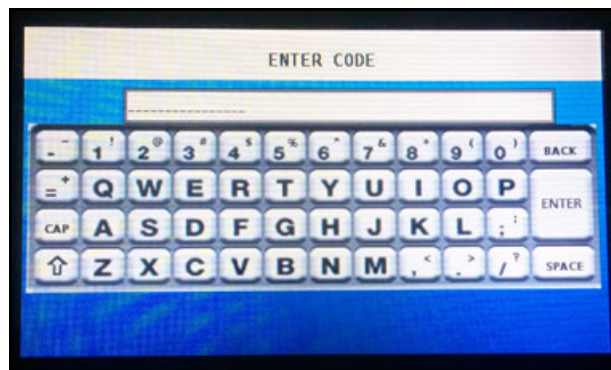


If multiple mobile hosts are configured at the site, then a host selection prompt appears on the POP device after Mobile MOP is selected.

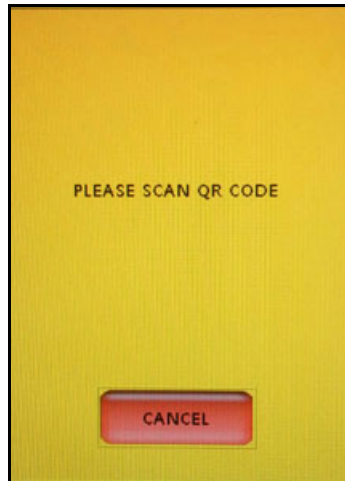
If a site has different Mobile Payment programs configured with Generate_Token authentication type for all, the customer is not prompted to select a mobile payment program during the transaction. After selecting mobile MOP, the PIN pad displays a QR Code instead of mobile payment program selection.



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.



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.



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

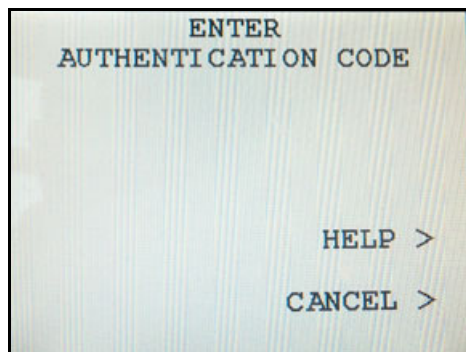
Outdoor Transactions

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.



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.

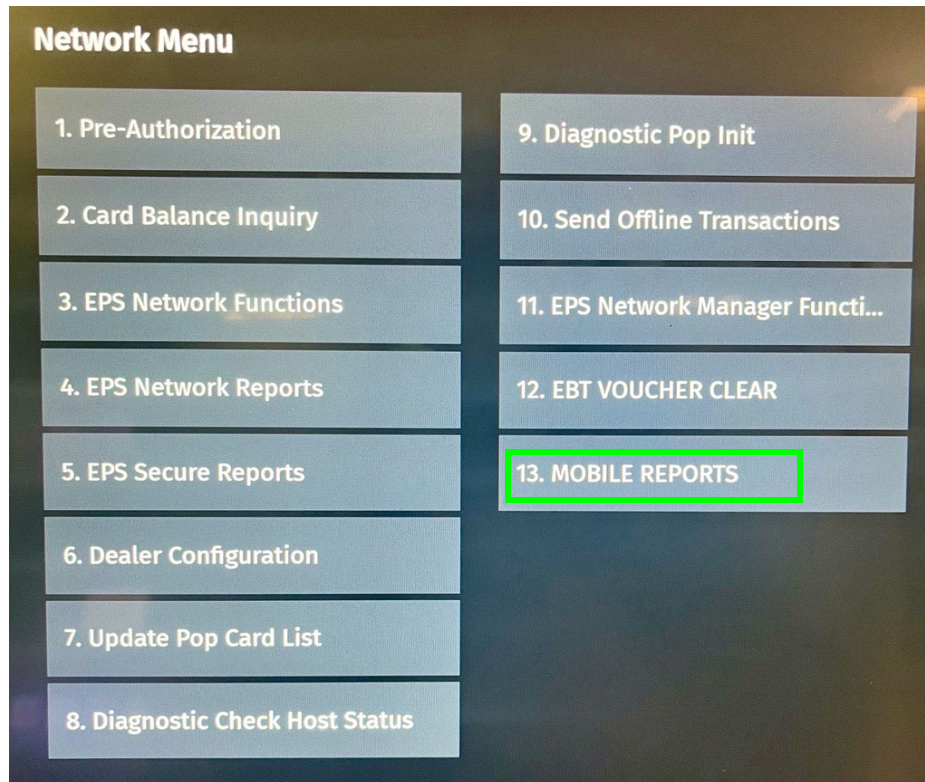
On completion, the DCR prints the receipt. The sales amount is transmitted to the MPPA, the customer's card is charged, and a receipt copy is sent to the registered MPA account for transaction history.

Reporting

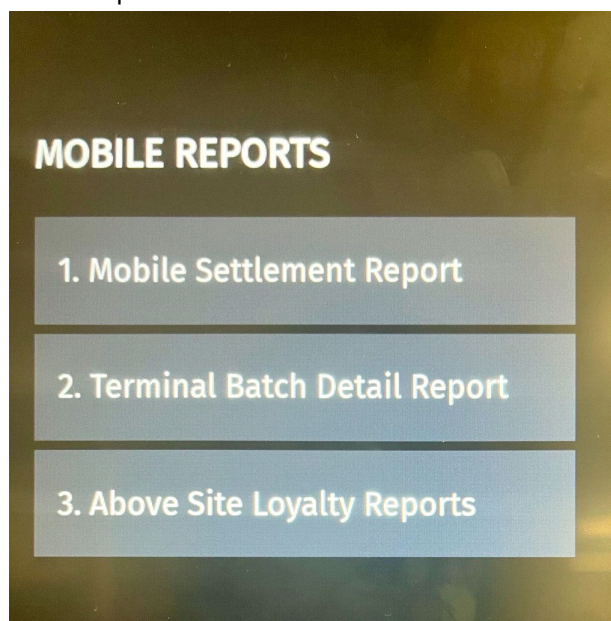
Reports and reporting options are provided by and will vary with the associated Host provider. Sample reports are provided for example purposes only.

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 Settlement Report

Report Details

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.

Settlement Report		
Host : VFIMobile		
Print Date : 04/09/14 01:53:38		
Period : 03-03-2014 To 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

- 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

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					

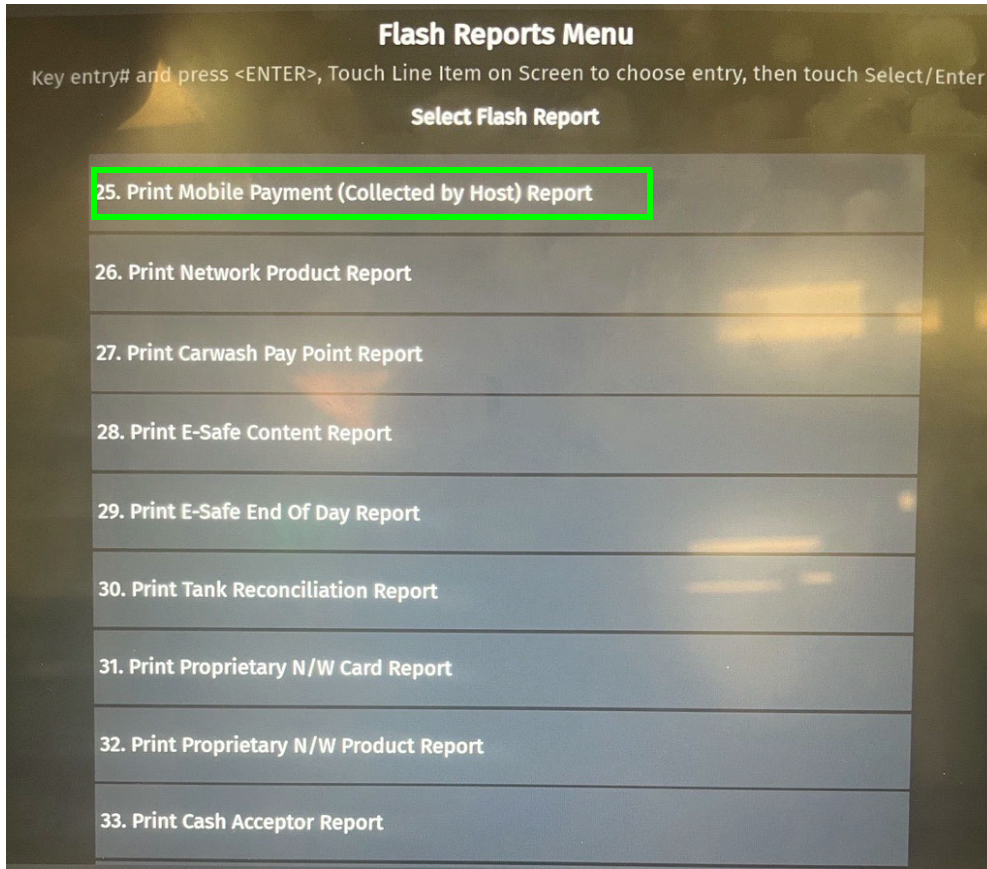
Mobile Host: mppa2					
Merchant ID: mppa2-mer					
Date	Time	Transaction	Item	Original Price	Final Price
			Discount	Quantity	Total Discount
07-31-2019	19:15:24	9010027			
		UNLD1		\$1.12	\$1.09
			\$0.01	4.673	\$0.05
			\$0.02	4.673	\$0.09
		904		\$0.00	-\$0.01
			\$0.01	1	\$0.01
		904		\$0.00	-\$0.02
			\$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**.



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 Commander Site Controller 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 Commander Site Controller 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.



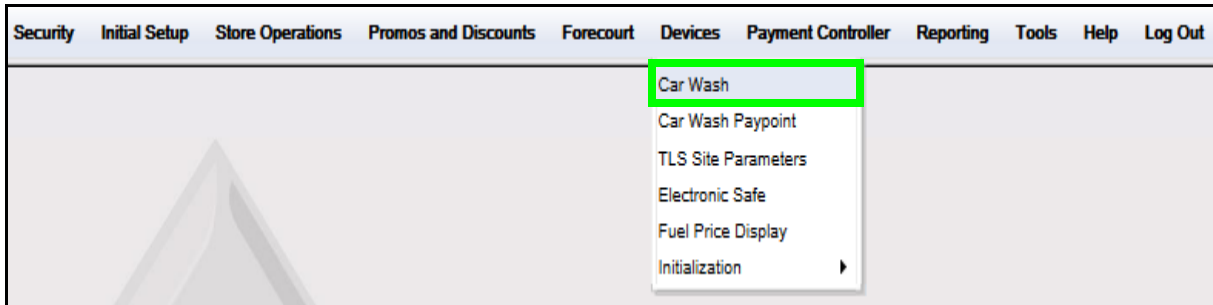
These attributes are specific to FDC Mobile and are not used by the VFIMobile adapter.

Pump Reserved but Authorization Failed

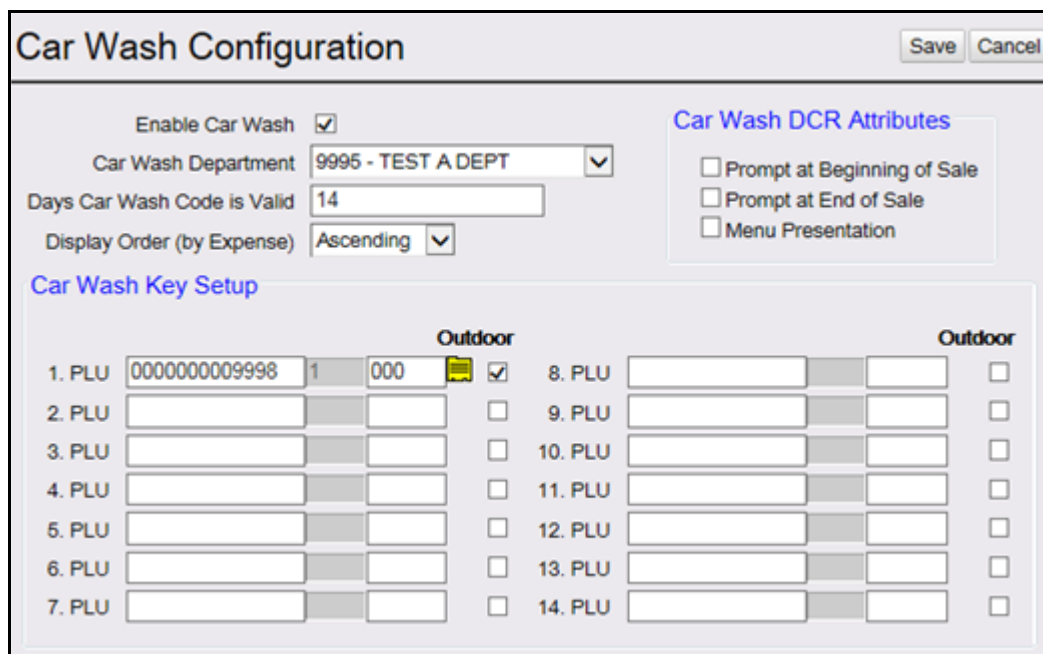
- The pump reservations are released after 3 minutes.

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.

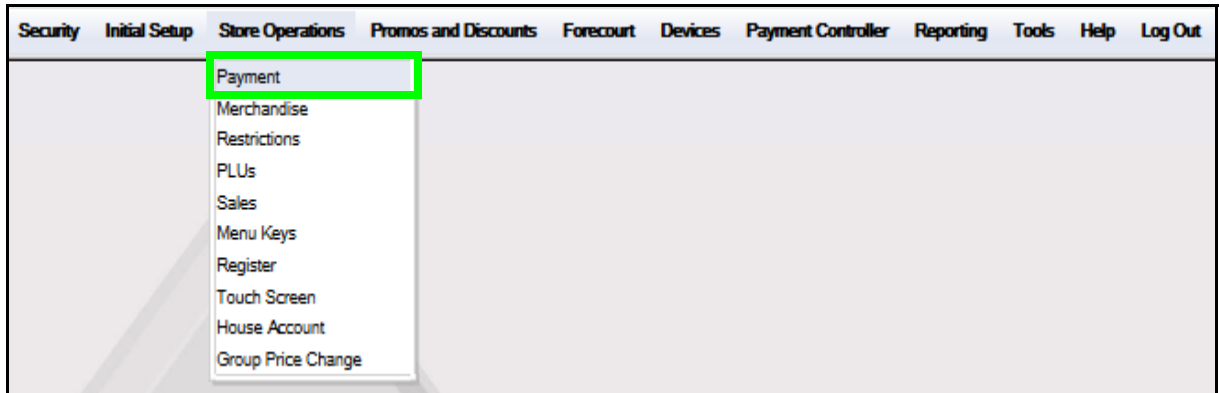
A screenshot of the 'Car Wash Configuration' window. The window has a title bar with 'Car Wash Configuration' and 'Save' and 'Cancel' buttons. The main content area is divided into several sections:

- Enable Car Wash:** A checkbox is checked.
- Car Wash Department:** A dropdown menu shows '9995 - TEST A DEPT'.
- Days Car Wash Code is Valid:** A text input field contains '14'.
- Display Order (by Expense):** A dropdown menu shows 'Ascending'.
- Car Wash DCR Attributes:** A section with three unchecked checkboxes: 'Prompt at Beginning of Sale', 'Prompt at End of Sale', and 'Menu Presentation'.
- Car Wash Key Setup:** A table with 14 rows, each representing a PLU. The first row is for PLU '0000000009998' and is marked as 'Outdoor' with a checked checkbox. The other 13 rows are empty and marked as 'Outdoor' with unchecked checkboxes.

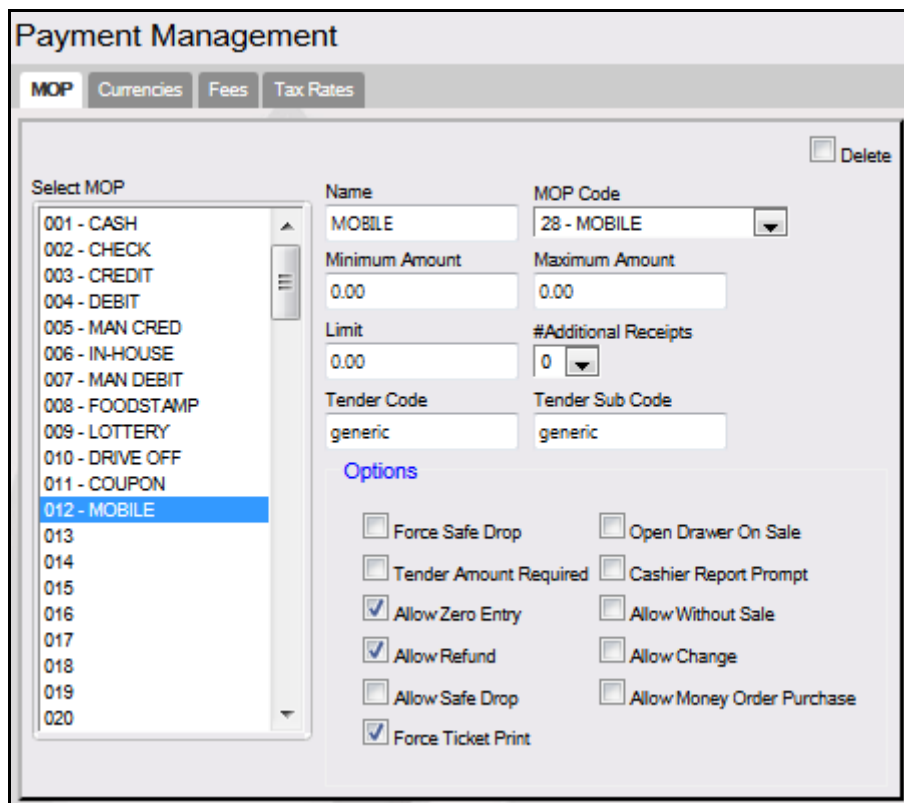
2. Verify that all Car Wash PLUs are configured and enabled for Outdoor.

Pump Can't Authorize Mobile Payment Application

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



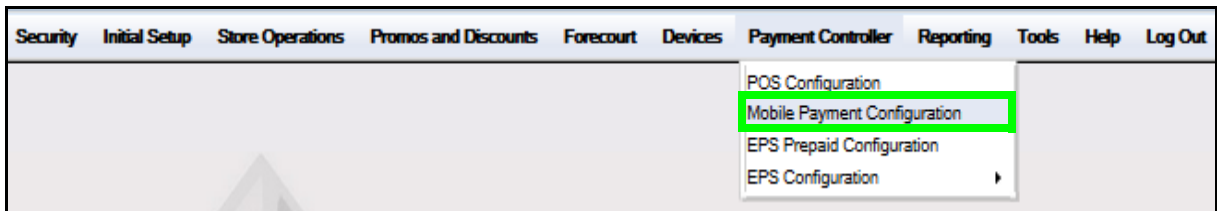
The Payment Management window displays.

A screenshot of the 'Payment Management' window. At the top, there are tabs for 'MOP', 'Currencies', 'Fees', and 'Tax Rates'. Below the tabs is a 'Select MOP' list box containing items from '001 - CASH' to '020'. '012 - MOBILE' is selected and highlighted in blue. To the right of the list box are several input fields: 'Name' (MOBILE), 'MOP Code' (28 - MOBILE), 'Minimum Amount' (0.00), 'Maximum Amount' (0.00), 'Limit' (0.00), '#Additional Receipts' (0), 'Tender Code' (generic), and 'Tender Sub Code' (generic). There is a 'Delete' checkbox in the top right corner. Below these fields is an 'Options' section with several checkboxes: 'Force Safe Drop' (unchecked), 'Open Drawer On Sale' (unchecked), 'Tender Amount Required' (unchecked), 'Cashier Report Prompt' (unchecked), 'Allow Zero Entry' (checked), 'Allow Without Sale' (unchecked), 'Allow Refund' (checked), 'Allow Change' (unchecked), 'Allow Safe Drop' (unchecked), 'Allow Money Order Purchase' (unchecked), and 'Force Ticket Print' (checked).

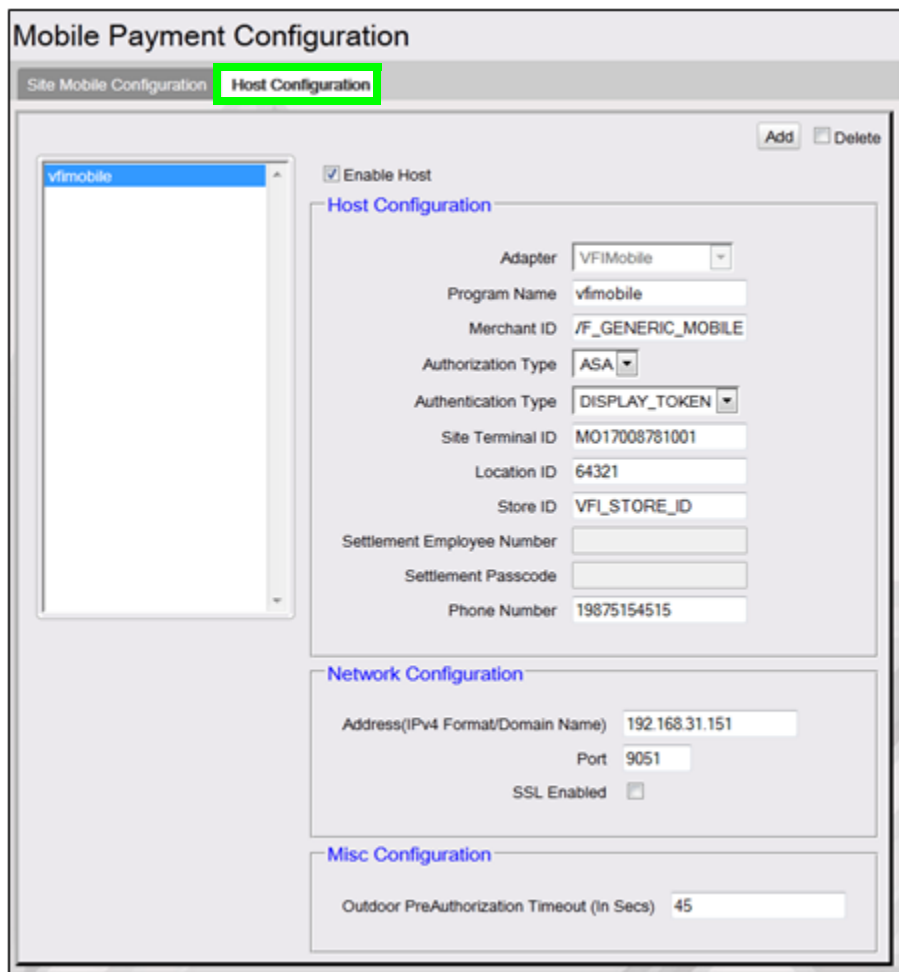
2. Verify that the Mobile MOP is configured.

Disabling the Mobile Host

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



The Mobile Payment Configuration window displays.

A screenshot of the 'Mobile Payment Configuration' window. The window has two tabs: 'Site Mobile Configuration' and 'Host Configuration' (the latter is highlighted with a green box). The 'Host Configuration' tab is active and contains the following fields:

- 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: [empty]
 - Settlement Passcode: [empty]
 - 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

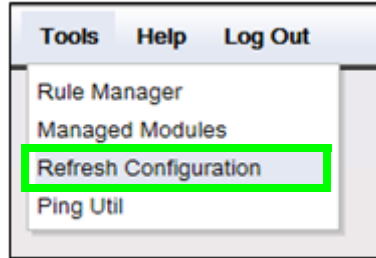
Buttons for 'Add' and 'Delete' are located in the top right corner of the configuration area.

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 Commander Site Controller 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.



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.

Term	Definition
MPA	Mobile Payments Application - a software application downloaded by a customer to a mobile device to facilitate mobile payment transactions.
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