Outside EMV

Feature Reference

Date: February 16, 2022

Verifone®

Outside EMV

Using This Feature Reference

This Feature Reference provides detailed information on how to configure and use the Outside Contact and Contactless EMV feature on Commander and Gilbarco, Wayne, Bennett, and Invenco Automated Fuel Dispensers (AFD).

All references to EMV in this document mean Outside Contact and Contactless EMV.

This feature document contains the subsections listed below:

- **Overview** - This chapter contains a brief description, requirements and the supported hardware configurations for the EMV feature on the related Site Controller.
- **Configuring Gilbarco** - This chapter contains information on how to configure Gilbarco dispensers terminals the EMV feature on the related Site Controller.
- **Configuring Wayne** - This chapter contains information on how to configure Wayne dispensers the EMV feature on the related Site Controller.
- **Configuring Bennett** - This chapter contains information on how to configure Bennett dispensers the EMV feature on the related Site Controller.
- **Configuring Invenco** - This chapter contains information on how to configure Invenco the EMV feature on the related Site Controller.
- **Troubleshooting** - This chapter provides basic troubleshooting steps if EMV transactions are not performing as expected with Gilbarco.
- **Appendices** - These appendices provide additional information.

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

© 2022 Verifone, Inc. All rights reserved.

No part of this publication covered by the copyrights hereon 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.

Verifone, Ruby SuperSystem, and Secure PumpPAY are registered trademarks of Verifone, Inc. Ruby Card, iOrder, and Commander Site Controller are trademarks of Verifone. All other brand names and trademarks mentioned in this document are the properties of their respective holders.

Revision History

Date	Description
03/22/2019	Initial Documentation Release.
03/29/2019	Updated the Acumera phone number.
06/05/2019	Updated Appendix B with Wayne/Dover phone number.
07/16/2019	Updated Hardware and Software sections. Updated Gilbarco, Secure PumpPAY, Wayne, and Troubleshooting chapters.
08/06/2019	Added references to Appendix A in the Overview section and added Shell notes to the Gilbarco and Wayne sections.
08/13/2019	Updated Appendix B > MNSP Availability sections.
11/06/2019	Updated the Gilbarco and Wayne EMV Configuration tabs.
11/12/2019	Updated Gilbarco and Wayne Dispenser Requirements section.
02/03/2020	Updated contact address, changed notes about Wayne DCR IP addresses.
04/08/2020	Added note to the introduction regarding upgrading PIN pad software to be used with the new EMV Kernel.
04/14/2020	Added a note to the Local Area Network Configuration section in the Wayne Chapter.
05/07/2020	Added a STOP note to the Supported Software section regarding Quick Chip.
05/14/2020	Added a Shell note to the STOP note in the Supported Software section regarding Quick Chip.
05/15/2020	Updated AvaLAN MNSP support information.
10/20/2020	Added informational note about NFC Readers for Gilbarco and Wayne dispensers, and added “RFID” entry to the Glossary of Terms.
01/18/2021	Updated the Isolated NIC Payment sections in the Gilbarco and Wayne chapters and added Appendix D.
01/27/2022	Removed SPP. Added Contactless settings. Added Invenco and Bennett.
02/16/2022	Updated the diagram chapter and system requirements section.

Contents

Outside Contact and Contactless EMV 1
Overview 1
Network Services Outdoor EMV Support 2
MNSP Support Phone Numbers 2
System Requirements 3
Supported Hardware 3
Supported Software 4
EMV Network Communication 6
Verifone Gilbarco FlexPay™ CRIND 6
Wayne iX Pay™ CAT 6
Bennett Simply Secure Payment (SSP) 6
Invenco G6 OPT 6
Pre-Install Checklist for EMV Readiness 7
Order of Upgrade/Install Checklist 9
Network Topology Configuration 10
Configuring Gilbarco 11
Configuring EMV in Configuration Client 11
Configuration Client Access 12
Accessing EMV Configuration 12
Outdoor EMV Configuration for Gilbarco CRIND 13
Managed Modules 13
DCR Configuration 15
DCR Keys Configuration 16
Local Area Network Configuration 19
EPS Global Configuration 21
Fuel and DCR Initialization 22
EMV Initialization 25
Verification of Forecourt Status 27
Configuring Wayne 28
Configuring EMV in Configuration Client 28
Configuration Client Access 29
Accessing EMV Configuration 29
Outdoor EMV Configuration for Wayne iX Pay CAT 30
Managed Modules 30
DCR Configuration 32
DCR Keys Configuration 33
Local Area Network Configuration 35
EPS Global Configuration 37
Fuel and DCR Initialization 38
EMV Initialization 41
Verification of Forecourt Status 43
Configuring Bennett 44
Configuring EMV in Configuration Client 44
Configuration Client Access 45
Accessing EMV Configuration 45

Outdoor EMV Configuration for Bennett SSP 46
Managed Modules 46
DCR Configuration 48
DCR Keys Configuration 49
Local Area Network Configuration 51
EPS Global Configuration 53
Fuel and DCR Initialization 54
EMV Initialization 56
Verification of Forecourt Status 58
Configuring Invenco 59
Configuring EMV in Configuration Client 59
Configuration Client Access 60
Accessing EMV Configuration 60
Outdoor EMV Configuration for Invenco OPT 61
Managed Modules 61
DCR Configuration 63
DCR Keys Configuration 64
Local Area Network Configuration 66
Isolated Payment NIC 66
EPS Global Configuration 68
Fuel and DCR Initialization 69
EMV Initialization 71
Verification of Forecourt Status 73
Troubleshooting Gilbarco Dispensers 74
Gilbarco FlexPay II CRIND 75
Verification of TLS Certification 75
Gilbarco FlexPay II CRIND 77
Verification of Single-Auth TLS Mode 77
Gilbarco FlexPay II CRIND 79
POS COMM set to IP 79
Gilbarco FlexPay IV CRIND 82
Verification of Single-Authorization TLS Mode 82
Gilbarco FlexPay IV CRIND 84
Verify IP Interface 84
Wayne iX CAT Firmware 86
Client/Server Configuration 86
Glossary of Terms 87

Appendices

Documentation 91
Documentation 91
Support 92
Contact Information 92
Diagrams 94
Gilbarco FlexPay with MNSP (AOR) 95

Wayne iX Pay with MNSP (AOR) 96
Bennett SSP with MNSP 97
Invenco G6 OPT with MNSP 98
Shell Branded Sites. 99
Gilbarco Local Area Network Configuration 99
Isolated Payment NIC 99
Verifone Zone (Shell - Two router MNSP LAN Settings) 101
Wayne Local Area Network Configuration 102
Verifone Zone (Shell - Two router MNSP LAN Settings) 104

1 Outside Contact and Contactless EMV

Overview

EMV is the new standard for credit card processing. It describes a transaction between a chip card and an EMV-enabled terminal. EMV transactions are more secure than magnetic stripe card transactions.

This feature reference guide provides details on how to configure and use the Outside Contact and Contactless EMV on Commander Site Controller. All EMV communications are TCP/IP. This document is intended to provide guidance and topology recommendations for Gilbarco, Wayne, Bennett, and Invenco EMV DCRs and locations using the Commander Site Controller with a Managed Network Service Provider (MNSP).

Indoor EMV must be configured and operational prior to implementing Outdoor EMV.

It is required for the PIN pad software to be upgraded to use the new EMV kernel. See the ViperPAY Application table at the Verifone Premier Portal > PIN Pads > MX 900 section to find the correct ViperPAY version number.

For the EVPAY (Engage) Certified Versions for M400 and P400, see the Current VRSD Software List at the Support.Verifone.com > Technical Support > Support Articles > Petro and Convenience > Products and Services > Software Updates (VRSD) > VRSD FAQs.

See the Inside EMV Feature Reference for steps on how to configure Indoor EMV on the Premier Portal at Petro Downloads > Feature References and application specific documentation on the Premier Portal under Petro Downloads > Commander > Commander Software Suites, Release Notes and Documentation.

A Glossary of Terms is provided to assist with understanding content and terminology presented in this Feature Reference.

Prior to initiating Outside EMV configuration, read the Network Services Outdoor EMV Support section below.

Network Services Outdoor EMV Support

The advantage of the Managed Network Service Provider (MNSP) program is that each provider has access to their own device including the ability to determine if connected devices are communicating with their solution. For this reason, each MNSP is responsible for supporting their solution. Outdoor EMV will rely on the MNSP and Verifone products being configured correctly and working in harmony.

Prior to contacting Verifone support, technicians must verify that the MNSP is able to see the EMV traffic occurring in the forecourt system. Issues related to the MNSP are supported by the MNSP. Verifone supports the Verifone equipment within the Verifone Zone.

It is important for technicians to be prepared with the necessary site information prior to contacting support for outdoor EMV sites. Verifone will advise technicians to gather the following information and call/chat again after it has been gathered.

1. Site Information: Service ID, Brand, Major Oil flag.
2. Site Equipment: MNSP solution information, all network and routing equipment, dispenser and DCR brand and firmware versions, Verifone equipment installed with software versions.
3. Configuration: Site topology must be in drawing form or technician must be able to clearly articulate each device and connection.

MNSP Support Phone Numbers

MNSP Network	Phone Number
Acumera	512-687-7401
AvaLAN	603-644-1461, Option 1
ControlScan	800-393-3246
Cybera	866-429-2372, Option 1
Transaction Network Services (TNS)	866-523-0661

MNSP Network	Phone Number
Mako Networks	844-807-0307
Omega	610-639-7996
SageNet	866-480-2263
Hughes	866-350-8786

System Requirements

Supported Hardware

Contact the dispenser manufacturer regarding required hardware and compatibility (e.g. BRCM/DCM compatibility).

Verifone POS System Requirements

- Commander Site Controller
- Commander16
- RubyCi

Managed Network Service Provider (MNSP)

- Verifone Certified MNSP for providing site network connectivity
- Get the latest MNSP documentations at the Premier Portal and then navigate to Manage > Petro Download > PC Utilities & Routers > MNSP Documentation

Gilbarco® Dispenser Requirements

- FlexPay™ II with HCR2
- FlexPay™ IV with UX 300
- 2-wire twisted pair for BRCM with DCM or Direct Ethernet cable to dispenser

Wayne Dispenser Requirements

- Single and Dual iX Pay™ boards with EMV Supported Hardware (iX Pay II is currently not supported)
- 2-wire twisted pair for Wayne Connect IP-485S or Direct Ethernet cable to dispenser

Bennett Dispenser Requirements

- Simply Secure Payment (SSP)
- 2-wire twisted pair for Bennett 901 or Direct Ethernet cable to dispenser

Invenco Dispenser Requirements

- G6 OPT
- 2-wire twisted pair for Invenco Link or Direct Ethernet cable to dispenser

Supported Software

Verifone POS System Requirements

- Production Software Base 49.05+ (Auto Upgrade Preferred)

Gilbarco® Dispenser Card Reader Requirements (Minimum)

- FlexPay™ II CRIND® US EMV 3.2.24 (or Higher)
- FlexPay™ IV CRIND® US EMV 42.06.12(or Higher)

Wayne Dispenser Card Reader Requirements (Minimum)

- iX Pay™ Serial version 2.8.102.80 (Prior to upgrading to Wayne EMV software)
- iX Pay™ EMV version 2.8.105.20(or Higher)

Bennett Dispenser Card Reader Requirements (Minimum)

- XXXXXX.10.10.01

The "XXXXXX" number is based on hardware revision.

Invenco Dispenser Card Reader Requirements (Minimum)

- 3.2.20

Verifone MX 9xx PIN Pad (Minimum)

- ViperPAY 4.05.03.03 (or Higher)
- OS 30251000
- Contactless 1.30.01A6
- VHQ Agent Version 2.13.2-276

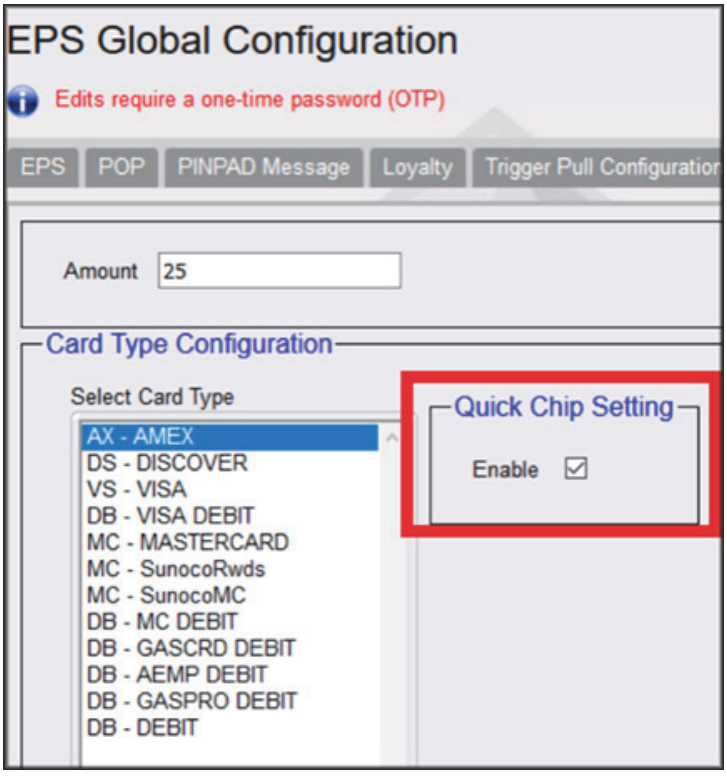
*Outdoor EMV transactions **must** utilize Quick Chip. Quick Chip is automatically enabled within the software configuration once the supported Base software (Base 51) has been loaded. Quick Chip changes the flow of transactions inside the store, prompting the customer to remove their card prior to selecting OK for the total.*

As part of the installation, prior to leaving the store, notify the store personnel that the transaction flow on the PIN pad has changed. Failure to complete the transaction on the PIN pad will result in the card not being charged for the transaction.

Do not disable quick chip for outdoor EMV locations!

Shell Vantage sites do not need to have the Quick Chip feature enabled in the Commander software.

The screenshot below shows where to enable Quick Chip in Configuration Manager.



EMV Network Communication

Verifone Gilbarco FlexPay™ CRIND

The Verifone Commander Site Controller establishes outbound connections to the Gilbarco FlexPay™ CRIND. Verifone Commander is the TCP client and the Gilbarco dispenser are the listening server.

EMV port 4871 is used for TLS communications with the Gilbarco FlexPay™ CRINDs.

The network communication between the Verifone zone and the outdoor EMV VLAN is controlled by the Managed Network Service Provider (MNSP).

Wayne iX Pay™ CAT

The Wayne iX Pay CAT establishes outbound connections to the Verifone Commander. Wayne dispenser is the TCP client and the Verifone Commander is the listening server.

EMV port 9700 is used for TLS communications with Wayne iX Pay CAT.

The network communication between the Verifone zone and the outdoor EMV VLAN is controlled by the Managed Network Service Provider (MNSP).

Bennett Simply Secure Payment (SSP)

The Bennett SSP establishes outbound connections to the Verifone Commander. Bennett SSP is the TCP client and the Verifone Commander is the listening server.

EMV port 9700 is used for TLS communications with Bennett SSP.

The network communication between the Verifone zone and the outdoor EMV VLAN is controlled by the Managed Network Service Provider (MNSP).

Invenco G6 OPT

The Invenco G6 OPT establishes outbound connections to the Verifone Commander. Invenco G6 OPT is the TCP client and the Verifone Commander is the listening server.

EMV port 9700 is used for TLS communications with Invenco G6 OPT.

The network communication between the Verifone zone and the outdoor EMV VLAN is controlled by the Managed Network Service Provider (MNSP).

Pre-Install Checklist for EMV Readiness

The following steps are expected to be configured prior to setting up Outdoor EMV on Commander. It is the responsibility of the pump technician to complete this configuration.

*IP Address for the Gilbarco CRIND and Wayne CAT **CANNOT** be on Verifone subnet. Consult IP scheme recommended by the dispenser manufacturer if it has not been pre-identified by the site.*

☑	**Managed Network Service Provider (MNSP)**
	Acquire/Install MNSP solution (See Appendix A)

☑	**Gilbarco® Dispenser**
	Verify with the Network if Gilbarco dispensers are EMV Contact certified and EMV Contactless certified. Make sure to configure accordingly as Noted in the DCR Configuration section. Also, see Outdoor EMV Implementation Status.
	Verify EMV ready card reader hardware (HCR/UX 300)
	Hardware needed for IP connectivity to CRIND (BRCM/DCM)
	CRIND IP Addresses
	Pump Router IP Address (Check with MNSP if required)
	Install required EMV CRIND software
	Install TLS Certification (Required for FlexPay II)
	Set Single-Auth setting
	Change POS COM from SERIAL to IP

☑	Wayne Dispenser Requirements
	Verify with the Network if Wayne dispensers are EMV Contact certified and EMV Contactless certified. Make sure to configure accordingly as Noted in the DCR Configuration section. Also, see Outdoor EMV Implementation Status.
	Verify iX Pay card reader (iX Pay II currently not supported)
	Load Minimum CAT software prior to IP software
	Using Wayne iX Configuration Tool, build/load Minimum EMV CAT software
	Hardware needed for IP connectivity to dispenser (Wayne Connect IP-485S)
	CAT IP Addresses
	Pump Router IP Address (Check with MNSP if required)

☑	Bennett Dispenser Requirements
	Verify with the Network if Bennett SSPs are EMV Contact certified and EMV Contactless certified. Make sure to configure accordingly as Noted in the DCR Configuration section. Also, see Outdoor EMV Implementation Status.
	Verify EMV ready card reader hardware
	Install required EMV DCR software

☑	Invenco Dispenser Requirements
	Verify with the Network if Invenco OPTs are EMV Contact certified and EMV Contactless certified. Make sure to configure accordingly as Noted in the DCR Configuration section. Also, see Outdoor EMV Implementation Status.
	Verify EMV ready card reader hardware
	Hardware needed for IP connectivity to DCR
	DCR IP Addresses

	Pump Router IP Address (Check with MNSP if required)
	Install required EMV DCR software

Order of Upgrade/Install Checklist

The general steps for the implementation of Outdoor EMV is outlined below. Do not proceed with the installation if the site is experiencing other issues such as not being able to process cards.

#	☑	Order of Upgrade/Install Checklist
1.		Verify site is functional and Indoor EMV is operational
2.		Perform any site backups and close daily. Ensure the site's transactions are received by the network before completing any software reloads or upgrades.
3.		Upgrade POS/PIN Pad software (Auto-Upgrade recommended)
		If an Auto Upgrade is being completed, see the Auto Upgrade Feature Reference Manual.
4.		Verify Payment Network Communication for indoor (EMV) and outdoor (Swipe) card transactions after upgrading the software.
5.		Verify that Pre-install Checklist for EMV Readiness has been completed.
6.		Configure hardware wiring (i.e. Re-wiring Ethernet cables, replacing routers with MNSP, etc.)
		DO NOT rewire the Gilbarco BRCM or Wayne Connect from the existing 2-wire loops media connection. Outdoor EMV TCP/IP packets will be sent on the existing 2-wires and converted back in the dispenser same as the media.
7.		LAN Configuration in POS for site specific outdoor EMV topology (i.e. Adding routes)
8.		Enable/Configure POS for outdoor EMV DCR.
9.		Verify Payment Network Communication for EMV indoor/ outdoor card transactions.

Network Topology Configuration

It is important that the site networking and routing changes have been completed prior to making changes to the Configuration Client. Contact the site MNSP for the outdoor EMV network topology.

Also, for more information regarding Network Topology Configurations, see the following Appendices:

- Appendix A - Documentation
- Appendix B - Support
- Appendix C - Diagrams

The Customer/Site area is owned, managed and configured by the MNSP network administrator. Installer should ensure there is a bi-directional communication to and from the Forecourt between the VFI network and CRIND/CAT network before beginning installation. Failure to do so will result in issues during setup.

2 CONFIGURING GILBARCO

The following steps are for configuring POS for Gilbarco CRIND.

Before starting the conversion of the outdoor EMV, make sure that Pre-Install Checklist for EMV Readiness has been completed.

Before configuring Commander Configuration Client, follow the steps in setting up the networking communication that is identified for the site by the MNSP.

Configuring EMV in Configuration Client

By default, the Commander is installed with EMV disabled. The following section provides instructions on how to enable Outside EMV for the Commander Site Controller.

The following section provides instructions on how to enable Outside EMV for the Commander Site Controller.

Configuration Client Access

***For Shell branded sites**, the EPS controls the configuration of roles below.*

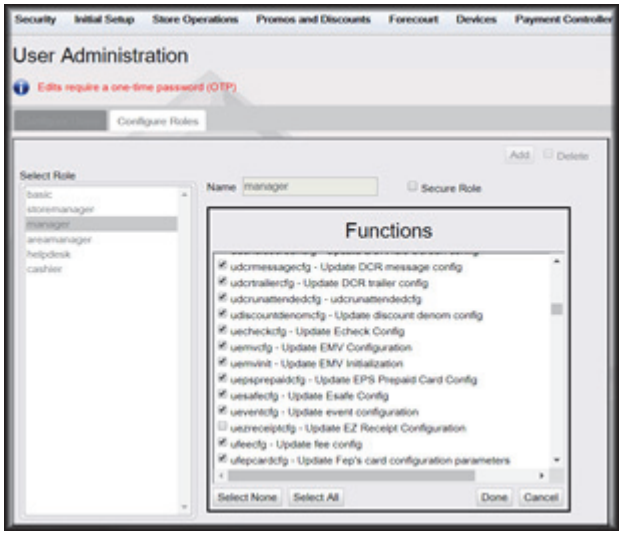
Accessing EMV Configuration

If this is a new Production Signed software installation, all menu selections to configure the system for EMV transaction processing are immediately visible and available.

If the software is being updated for EMV-readiness from a prior installation, user permissions must be updated to allow access to the EMV menu selections.

If accessing the Configuration Client from the POS and the EMV Configuration and Initialization tabs are grayed out, then this indicates the logged in user account does not have the correct functions added to the associated role. Activate the following roles for the user accessing Configuration Client at https://192.168.31.11/ConfigClient.html.

1. Navigate to Security > Manage Users > Configure Roles.
2. Select Role (i.e. Manager).
3. Select Edit.
4. Check the following Functions:
   - uemvcfg - Update EMV Configuration
   - uemvinit - Update EMV Initialization
   - vemvcfg - View EMV Configuration
   - vemvinit - View EMV Initialization
5. Logout of the Configuration Client and log back in for the Role changes to take effect.



Outdoor EMV Configuration for Gilbarco CRIND

Managed Modules

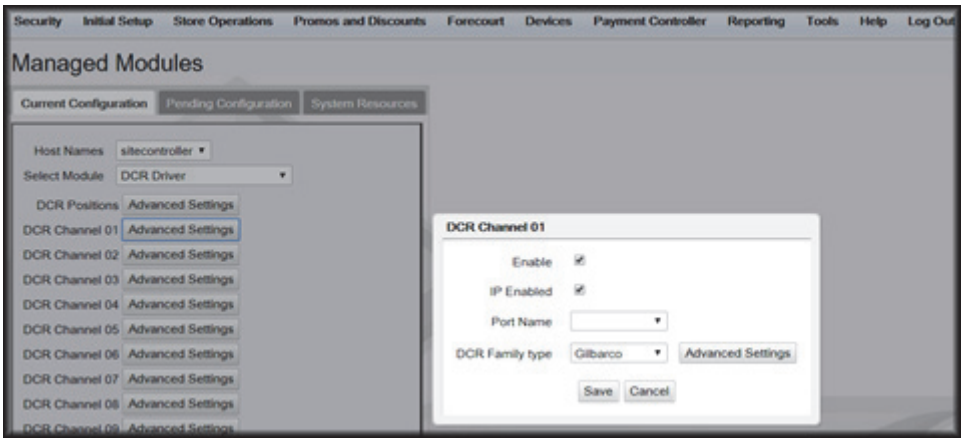
1. Navigate to Tools > Managed Modules > Current Configuration.
2. **At Host Names**, select sitecontroller.
3. **At Select Module,** choose the **DCR Driver** option.
4. Select the DCR Channel to set up.

All IP enabled DCR, the DCR should be placed on the same channel (i.e. DCR Channel 01). There is no advantage to splitting up the channels.

5. For each DCR Channel for EMV, select:
   a. **Enable** option must be checked.
   b. **IP Enabled** option must be checked.
   c. **Port Name** option must remain empty.

EMV communications is done via the Ethernet port on the Commander, therefore the DCR Channel Port Name will be left blank.
There will be no LED lights for DCR on the front of the Commander since the communications is via the Ethernet port.

   d. **DCR Family type** selection is Gilbarco.

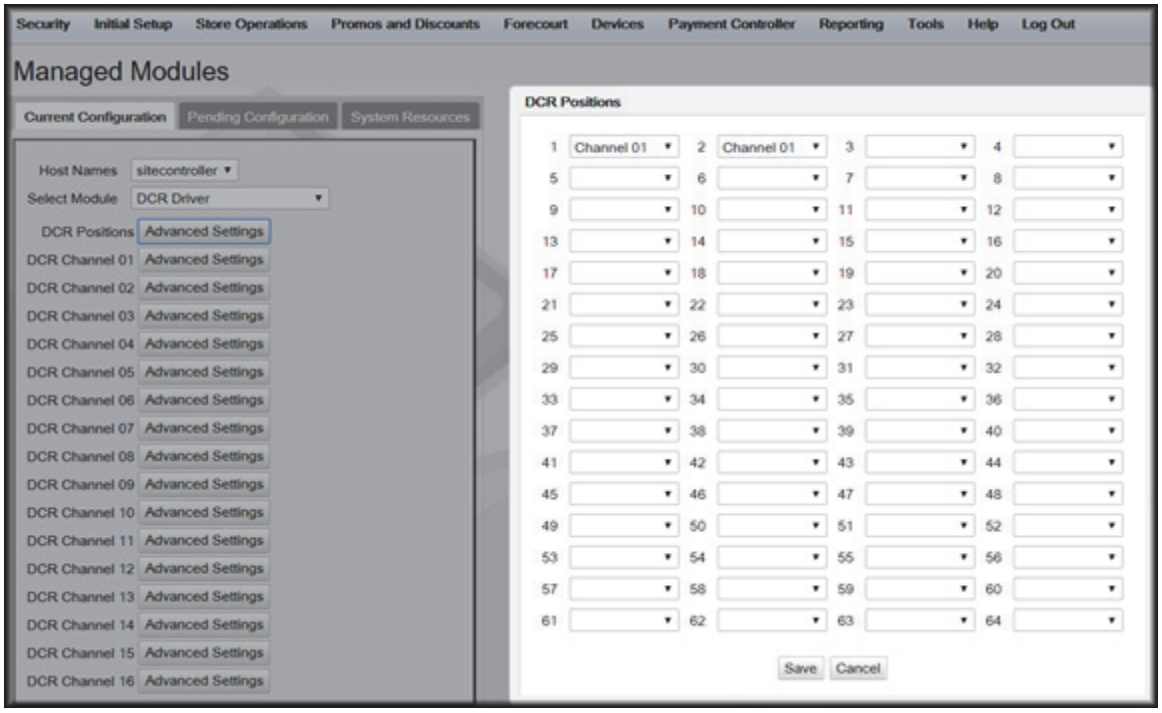


   e. Save DCR Driver changes.

If both IP Enabled and Port Name parameters are selected, an error displays when attempting to save the configuration changes.

6. After completing the DCR Channel set-up, select **DCR Positions** option and assign CRIND positions to their respective DCR.

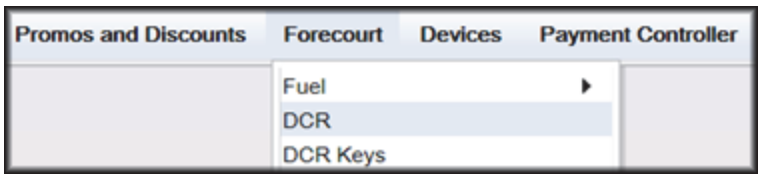
If the site is an Auto-Upgrade and has multiple channels configured, reconfigure all the DCR Positions on a single channel (i.e. Channel 01).



DCR Configuration

The following EMV specific parameters are required for each EMV DCR/CRIND position:

1. Navigate to Configuration Client > Forecourt > DCR.



NOTE

*In order for NFC Readers to accept mobile device payments, make sure Contactless is not disabled at **Configuration Client > Forecourt > DCR > DCR Configuration > DCR Position Attributes > NFC Mode**.*

2. Select DCR Position Attributes.
3. Under EMV Parameters section for each of the Selected EMV DCR Position:
   a. **Enable EMV** must be checked.
   b. **IP Address** must be entered.

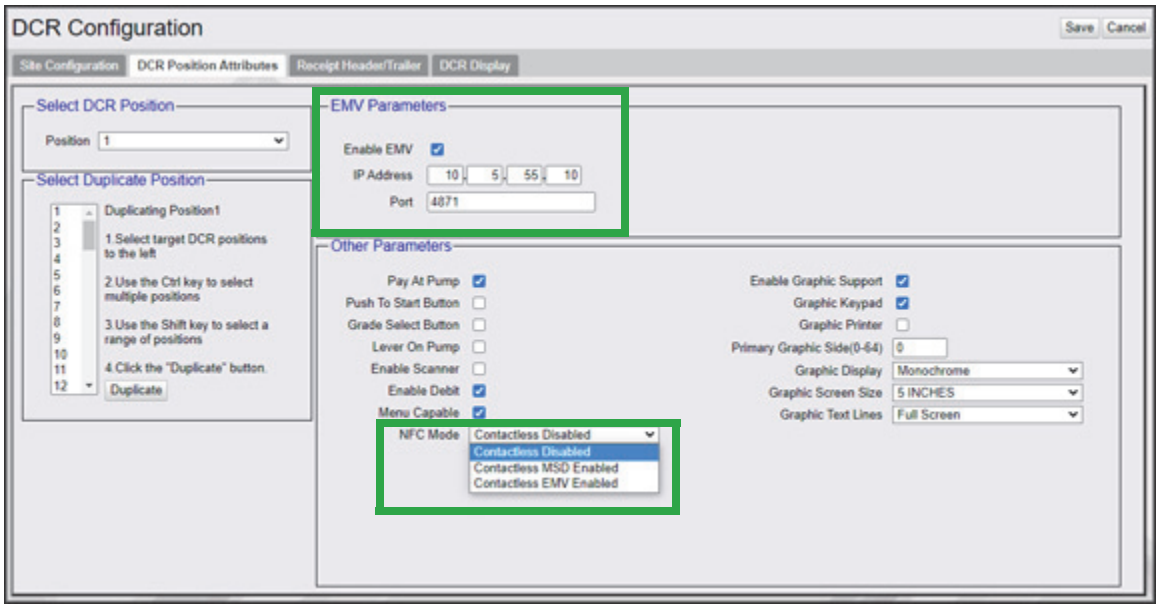
STOP

IP Address for the EMV CRIND CANNOT be on a Verifone subnet.

NOTE

Consult IP scheme recommended by Gilbarco if it has not been pre-identified by the site.

   c. **Port** value is 4871.
   d. For **NFC Mode**, select one of the following:
      - Contactless Disabled — Contactless (including Mobile Payments) is not being used at the DCR.
      - Contactless MSD Enabled — Use only if Contactless EMV is not supported or not certified for Gilbarco dispensers. This mode uses the Mag-Stripe Data (MSD).
      - Contactless EMV Enabled — Use if Contactless EMV is supported and network certified for Gilbarco dispensers. This mode uses the chip data on the card.

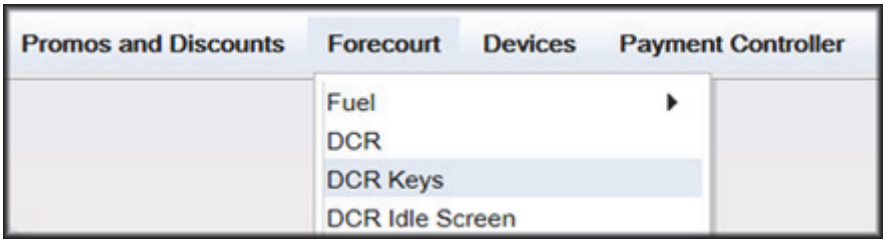


4. In the Other Parameters section, select the appropriate parameter configurations and click Save.

DCR Keys Configuration

DCR key mapping is necessary for the PIN pad to respond correctly to customer key presses.

1. Navigate to Configuration Client > Forecourt > DCR Keys.



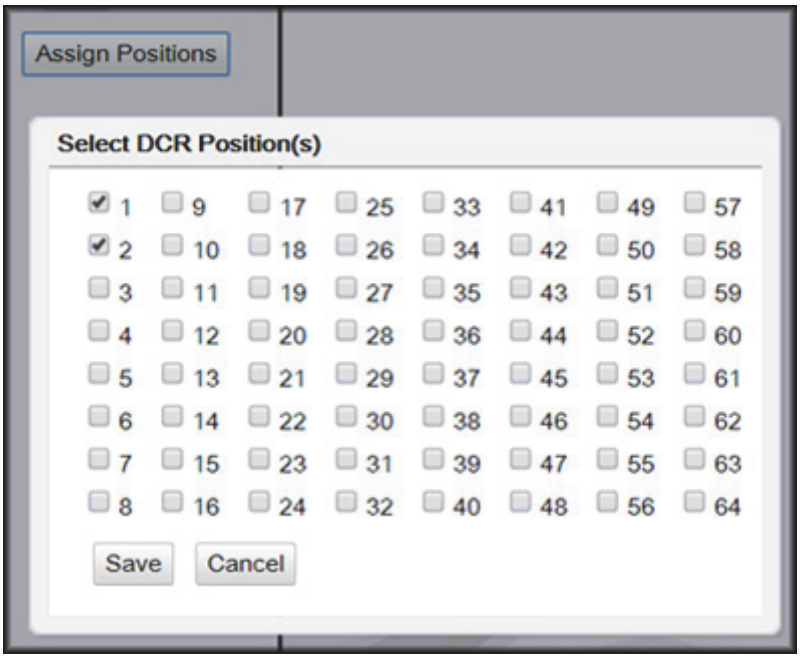
2. Create a DCR Keys layout by clicking on **Add** for Gilbarco DCRs below.

Gilbarco DCRs:

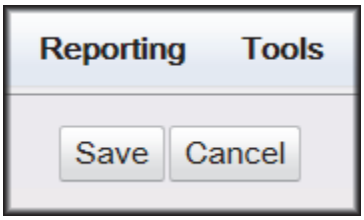
a. **Label**: Gilbarco EMV
b. **#Rows**: 4
c. **#Columns**: 6

3. Select a (NA) square and configure the Key type for the DCR:
   a. Key Type: Function
   b. Function Key Code: (As shown in the images above for the site EMV key pads)

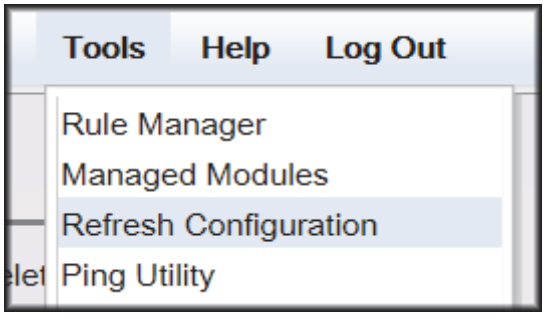
4. Select Assign Positions and Select DCR Position(s) to all the DCRs and click **Save**.



5. Click **Save** at DCR Keys Configuration.



6. Navigate to Configuration Client > Tools > Refresh Configuration.



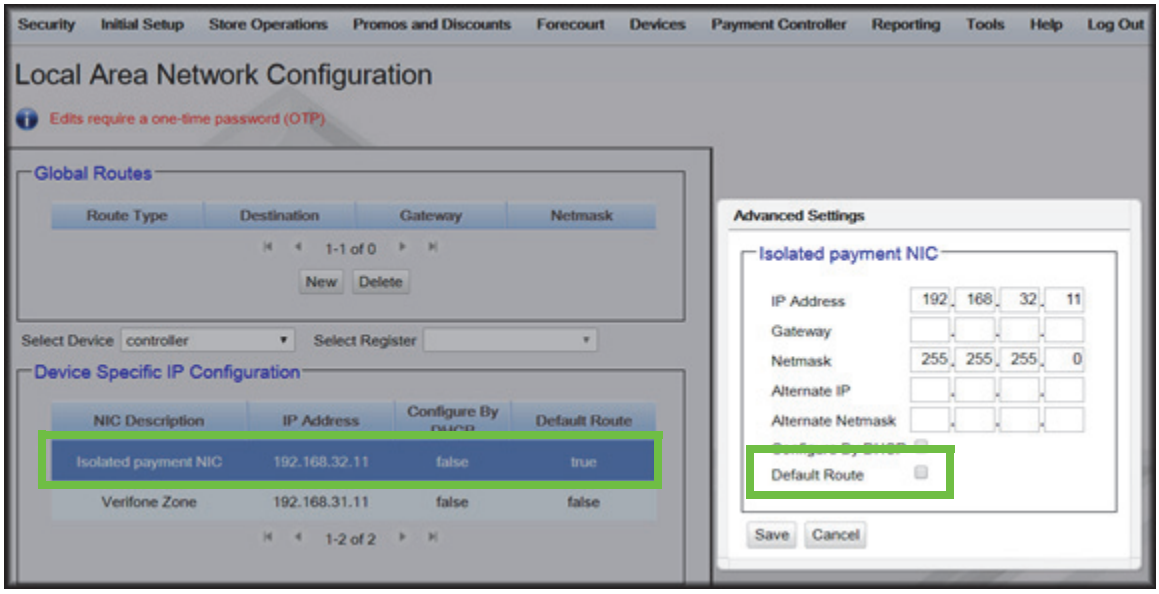
Local Area Network Configuration

The LAN needs to be configured for Gilbarco CRIND. In the Gilbarco configuration, the Commander is the CLIENT and the Gilbarco CRIND is the SERVER. The Outdoor EMV DCR IP traffic must be routed from Commander through the network IP of 192.168.31.31. Depending on which device specific IP configuration is selected for the site. Device Specific network routes might need to be added.

***For Shell branded sites**, see **Appendix D** at the back of the document for Shell Verifone Zone settings.*

Isolated Payment NIC

1. In Configuration Client, navigate to Initial Setup > Local Area Network Configuration.
2. Click on Isolated Payment NIC in the Device Specific IP Configuration.
3. Verify with your network provider if the "Default Route" parameter needs to be checked. If the parameter is checked, then continue with the next steps. If not checked, then skip to the EPS Global Configuration Section.



Using the IP address entered in the EMV Parameter in DCR configuration, add a network destination route with the 4th octet (last) set to ZERO. i.e. 10.5.55.0. This should cover all the IP ranges from 10.5.55.1 through10.5.55.255.

If Default Route is checked, then add New Route Config to the Device Specific Routes per site.

- **Route Type**: Network
- EMV Parameter IP Address (Forecourt > DCR > DCR Position Attributes) with the 4th octet set to 0.
- **Gateway**: 192.168.31.31
- **Netmask**: 255.255.255.0

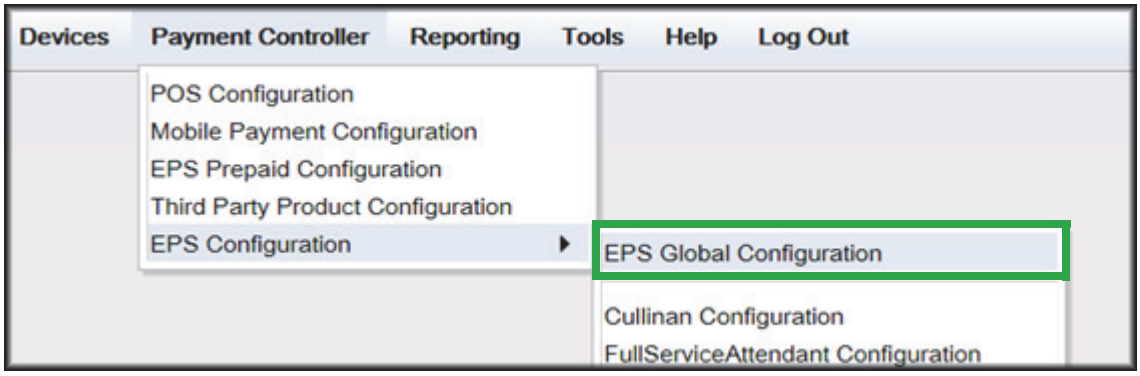
4. Save the configuration changes and reboot the site controller.

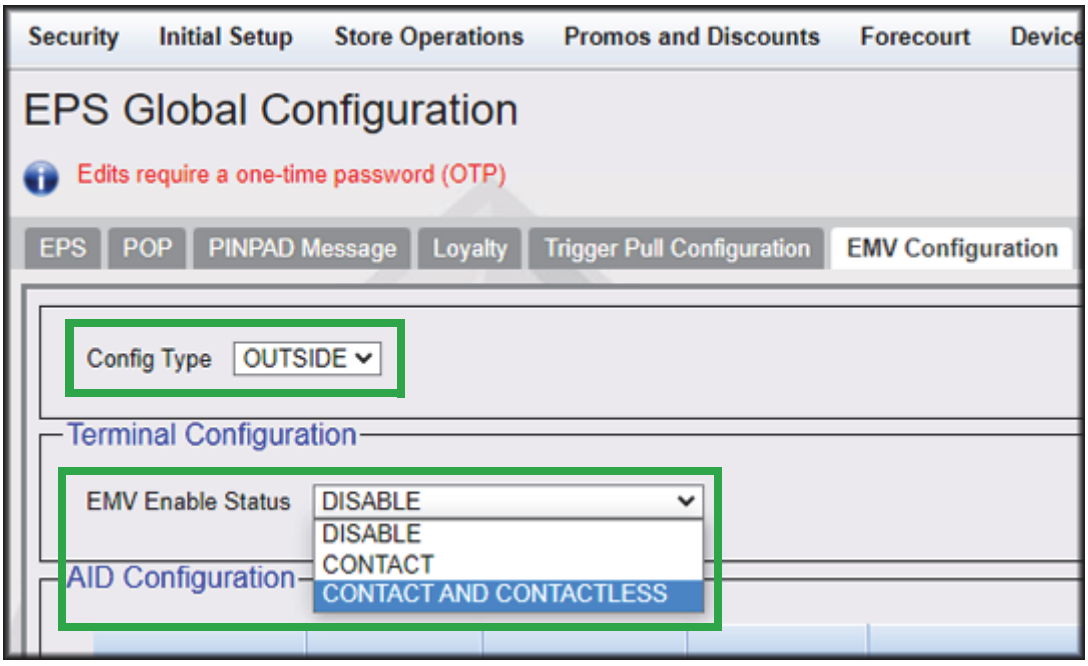
EPS Global Configuration

For Shell branded sites, EPS Global Configuration is controlled by Wincor. This should be pre-configured and enabled prior to converting the site for outdoor EMV. No changes are needed in EPS Global Configuration. Proceed to Fuel and DCR Initialization.

The EMV Configuration tab of the EPS Global Configuration screen contains options for both inside and outside EMV use.

1. Navigate to Configuration Client > Payment Controller > EPS Global Configuration > EMV Configuration.

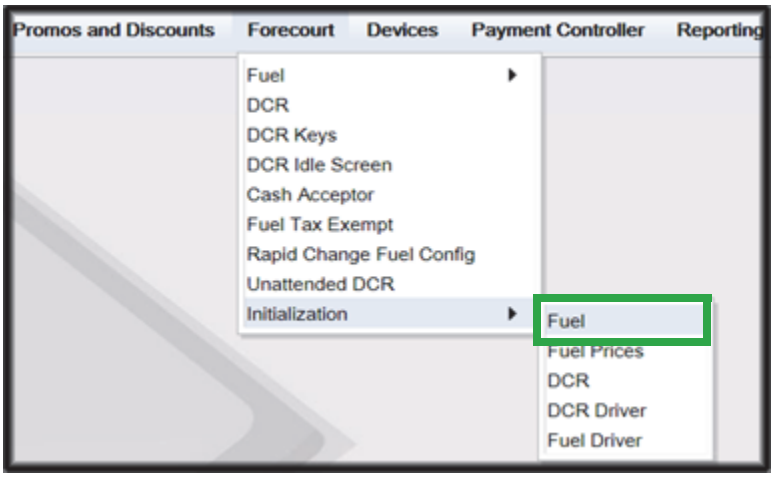




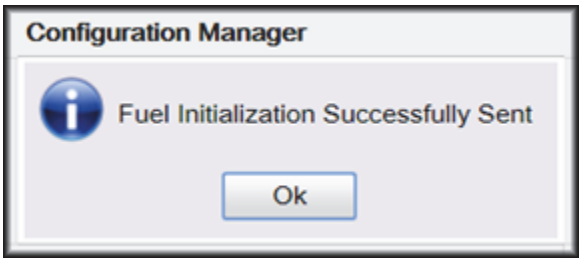
2. From the Config Type drop down menu, select **OUTSIDE**.
3. In the Terminal Configuration section and from the EMV Enable Status drop down menu, select the parameter **CONTACT** or **CONTACT AND CONTACTLESS**.
4. Select Save.

Fuel and DCR Initialization

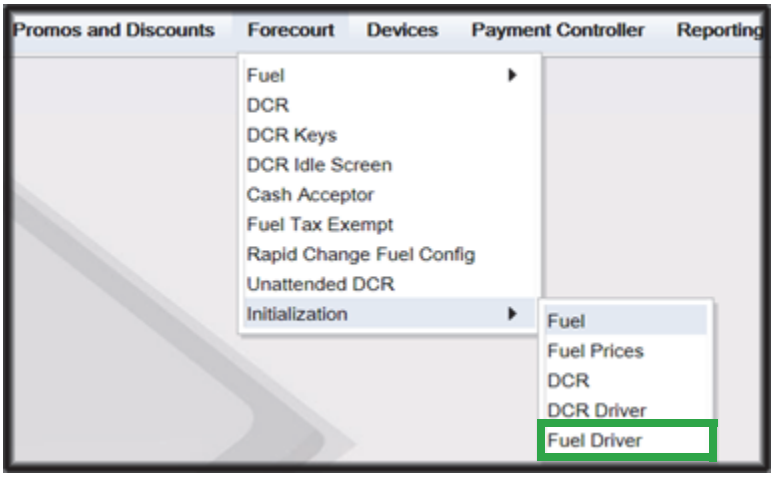
1. After configuring Managed Modules for Fuel and DCR, perform a Fuel and DCR initialization.
2. Navigate to Configuration Client > Tools > Refresh Configuration.
3. To initialize Fuel, navigate to Configuration Client > Forecourt > Initialization and then select Fuel.



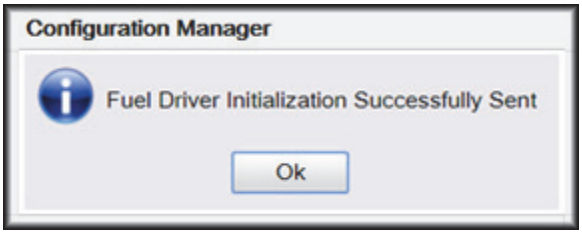
4. A message stating Fuel Initialization Successfully Sent displayed. Select Ok.



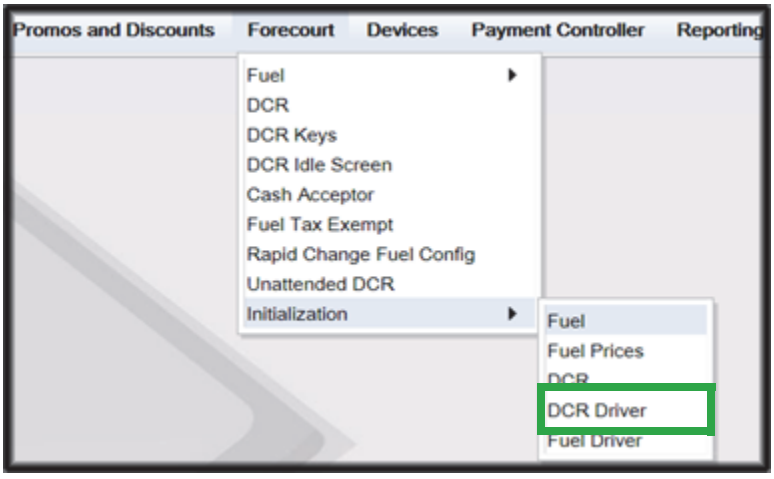
5. To initialize the Fuel Driver, navigate to Configuration Client > Forecourt > Initialization and then select Fuel Driver.



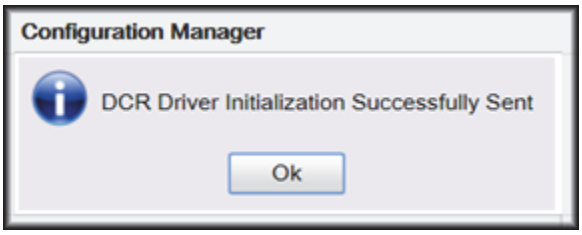
6. A message stating Fuel Driver Initialization Successfully Sent displayed. Select Ok



7. To initialize DCR Driver, navigate to Configuration Client > Forecourt > Initialization and then select DCR Driver



8. A message stating DCR Driver Initialization Successfully Sent displayed. Select Ok.



Check the dispensers to verify that they are loaded.

After the dispensers are all loaded, perform second DCR Driver initialization.

EMV Initialization

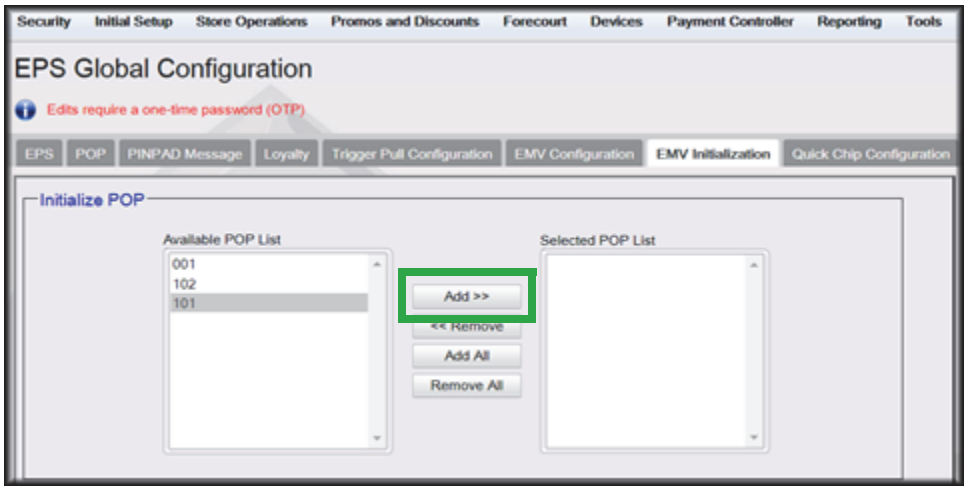
For Shell branded sites, Shell will enable Outdoor EMV on the Wincor device prior to the EMV installation. EMV Initialization is controlled by Wincor. This should take place when Wincor and Commander sync and exchange information.

After Commander has established communications with the Gilbarco FlexPay™ CRIND positions, it will require an EMV Initialization to be performed. This action sends required Gilbarco EMV resource files to the selected CRIND positions.

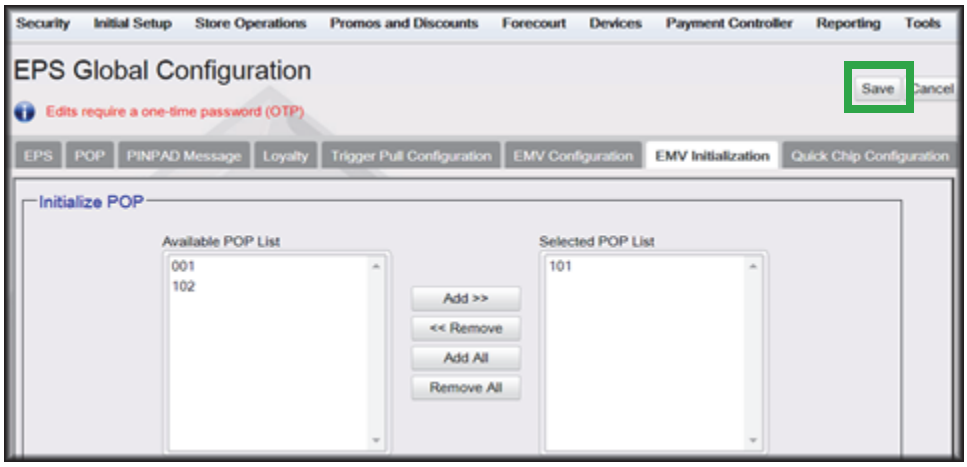
A DCR Driver Initialization must have been performed before starting the following steps. This will add DCR IDs to the Available POP List which can then be selected to receive the EMV Initialization.
An EMV Initialization does not perform a DCR Driver Initialization or a DCR Initialization.

1. Navigate to the Configuration Client > Payment Controller > EPS Global Configuration > EMV Initialization.
2. From the Initialize POP section locate the **Available POP List**.
3. For the CRIND(s) requiring initialization, select the required CRIND ID and click the **Add >>** button to move it to the **Selected POP List**.

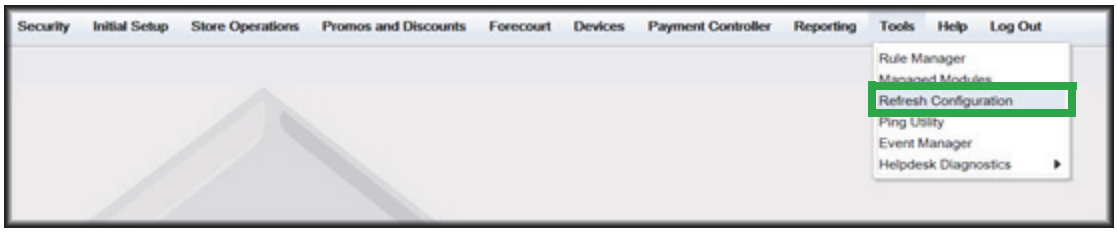
Outdoor card readers will be identified as POP 101, 102, 103, etc.



4. Repeat steps 2 and 3 for any additional CRIND IDs.



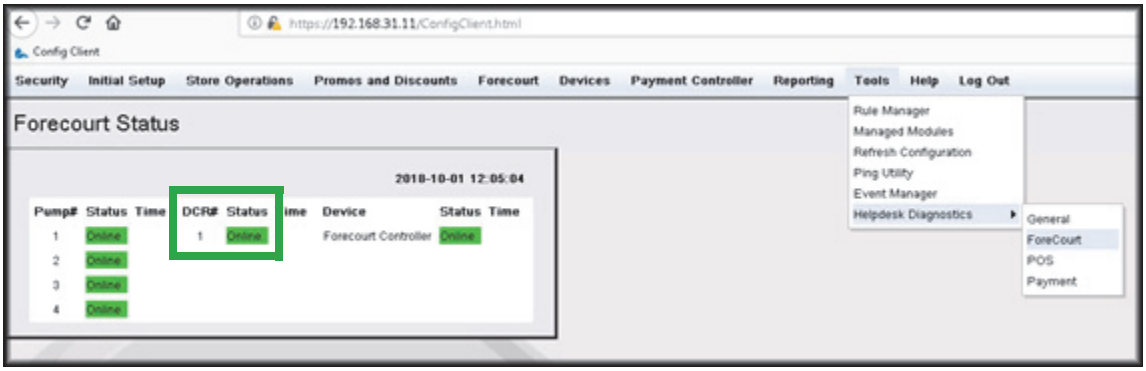
5. When finished selecting POP positions to be initialized, click Save. This performs an EMV POP initialization of the selected CRIND positions.
6. If another EMV Initialization is required, first perform a Refresh Configuration.
7. Navigate to Configuration Client > Tools > Refresh Configuration. This updates the Available POP List contents. Repeat the EMV Initialization steps 1 through 5 above.



Verification of Forecourt Status

Use the following steps to verify IP based communications to the DCRs.

Navigate to Configuration Client > Tools > Helpdesk Diagnostics > Forecourt. The DCR Status should appear as “Online.” If they are offline, then communications to the DCRs have not been established. Recheck the connections and verify TCP/IP connectivity.



3 CONFIGURING WAYNE

The following steps are for configuring POS for Wayne iX Pay CAT.

Before starting the conversion of the outdoor EMV, make sure that Pre-Install Checklist for EMV Readiness has been completed.

Before configuring Commander Configuration Client, follow the steps in setting up the networking communication that is identified for the site by the MNSP.

Configuring EMV in Configuration Client

By default, the Commander is installed with EMV disabled. The following section provides instructions on how to enable Outside EMV for the Commander Site Controller.

The following section provides instructions on how to enable Outside EMV for the Commander Site Controller.

Configuration Client Access

***For Shell branded sites**, the EPS controls the configuration of roles below.*

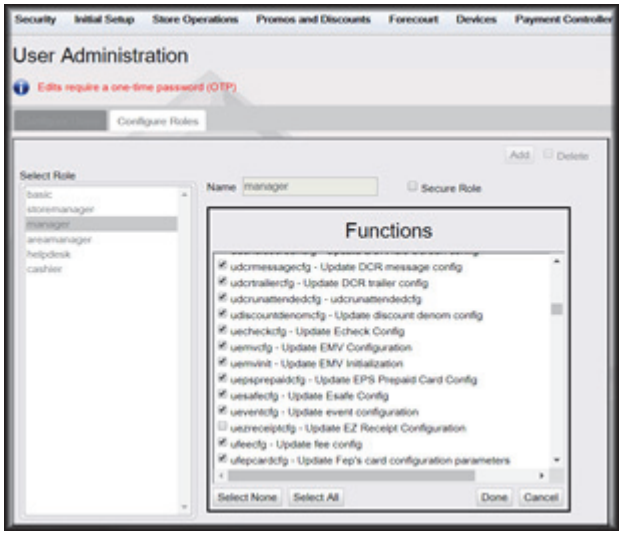
Accessing EMV Configuration

If this is a new Production Signed software installation, all menu selections to configure the system for EMV transaction processing are immediately visible and available.

If the software is being updated for EMV-readiness from a prior installation, user permissions must be updated to allow access to the EMV menu selections.

If accessing the Configuration Client from the POS and the EMV Configuration and Initialization tabs are grayed out, then this indicates the logged in user account does not have the correct functions added to the associated role. Activate the following roles for the user accessing Configuration Client at https://192.168.31.11/ConfigClient.html.

1. Navigate to Security > Manage Users > Configure Roles.
2. Select Role (i.e. Manager).
3. Select Edit.
4. Check the following Functions:
   - uemvcfg - Update EMV Configuration
   - uemvinit - Update EMV Initialization
   - vemvcfg - View EMV Configuration
   - vemvinit - View EMV Initialization
5. Logout of the Configuration Client and log back in for the Role changes to take effect.



Outdoor EMV Configuration for Wayne iX Pay CAT

Managed Modules

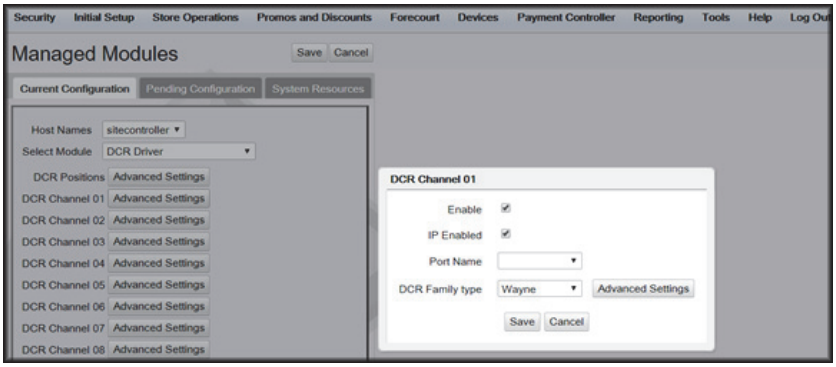
1. Navigate to Tools > Managed Modules > Current Configuration.
2. **At Host Names**, select sitecontroller.
3. **At Select Module,** choose the **DCR Driver** option.
4. Select the DCR Channel to set up.

All IP enabled DCR, the DCR should be placed on the same channel (i.e. DCR Channel 01). There is no advantage to splitting up the channels.

5. For each DCR Channel for EMV, select:
   a. **Enable** option must be checked.
   b. **IP Enabled** option must be checked.
   c. **Port Name** option must remain empty.

EMV communications is done via the Ethernet port on the Commander, therefore the DCR Channel Port Name will be left blank.
There will be no LED lights for DCR on the front of the Commander since the communications is via the Ethernet port.

   d. **DCR Family type** selection is Wayne.



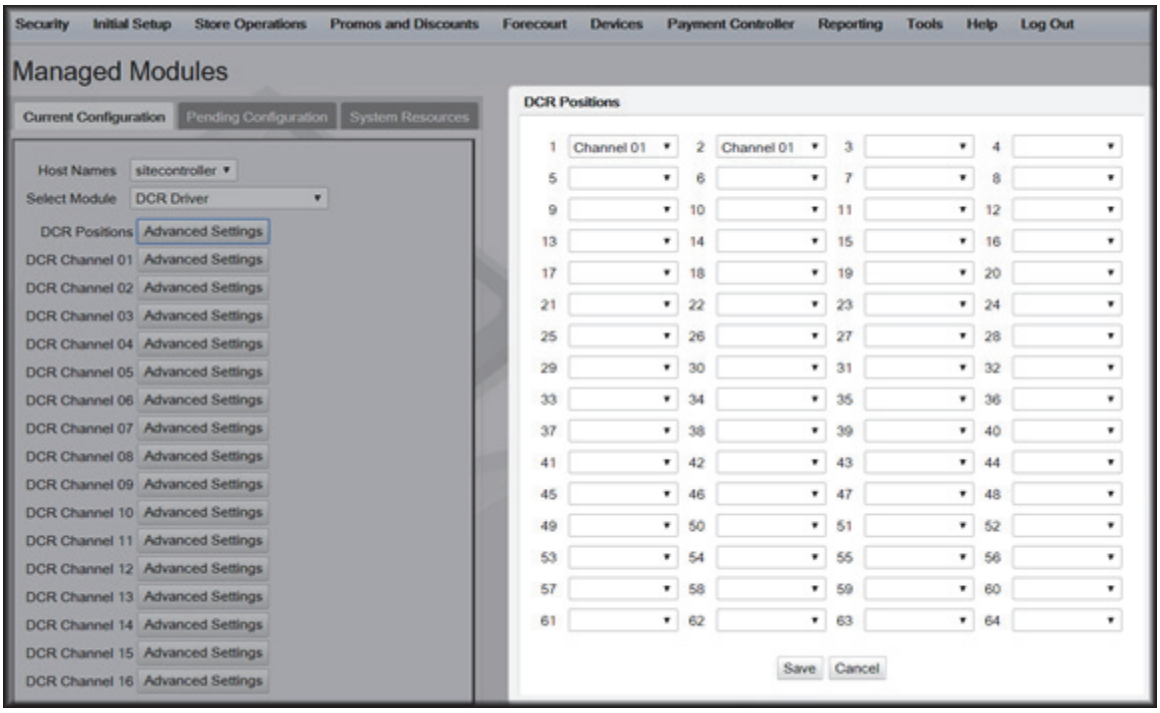
   e. Save DCR Driver changes.

If both IP Enabled and Port Name parameters are selected, an error displays when attempting to save the configuration changes.

6. After completing the DCR Channel set-up, select **DCR Positions** option and assign CRIND positions to their respective DCR.

NOTE

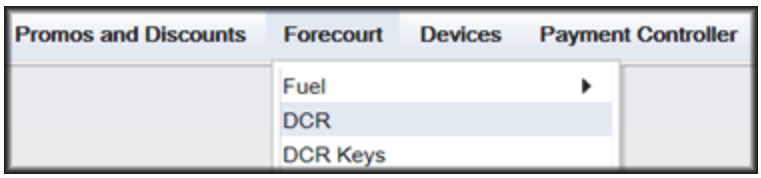
If the site is an Auto-Upgrade and has multiple channels configured, reconfigure all the DCR Positions on a single channel (i.e. Channel 01).



DCR Configuration

The following EMV specific parameters are required for each EMV DCR position:

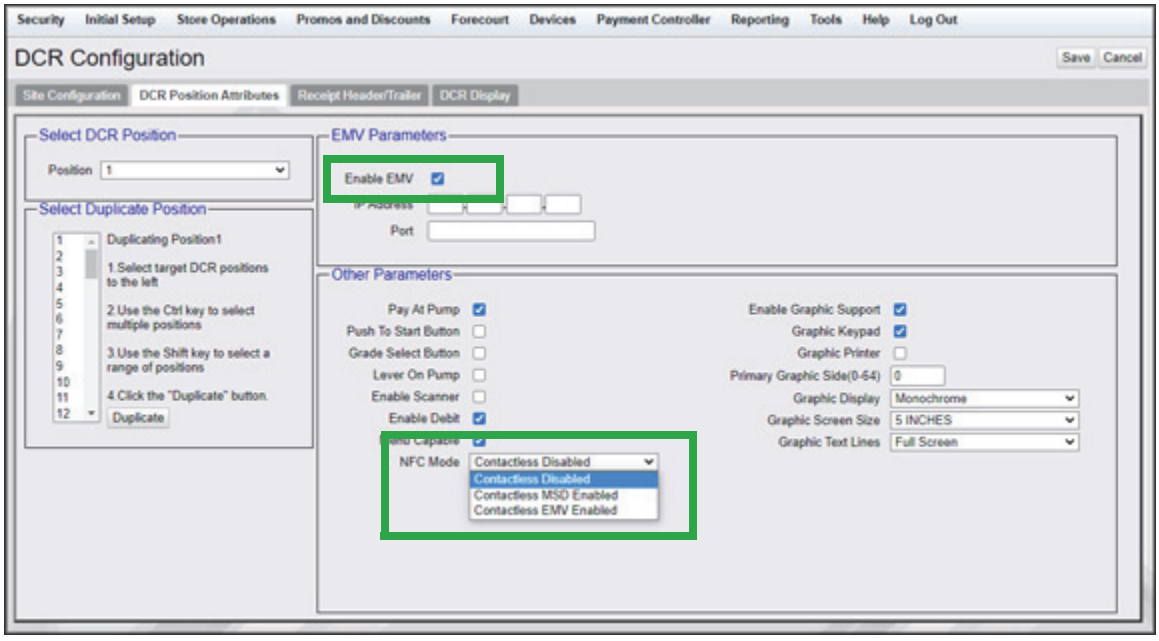
1. Navigate to Configuration Client > Forecourt > DCR.



NOTE

In order for NFC Readers to accept mobile device payments, make sure Contactless is not disabled at ***Configuration Client > Forecourt > DCR > DCR Configuration > DCR Position Attributes > NFC Mode****.*

2. Select DCR Position Attributes.
3. Under EMV Parameters section for each of the Selected EMV DCR Position:
   a. **Enable EMV** must be checked.
   b. **IP Address** must be left blank.
   c. **Port** must be left blank.
   d. For **NFC Mode**, select one of the following:
      - Contactless Disabled — Contactless (including Mobile Payments) is not being used at the DCR.
      - Contactless MSD Enabled — Use only if Contactless EMV is not supported or not certified for Wayne dispensers. This mode uses the Mag-Stripe Data (MSD).
      - Contactless EMV Enabled — Use if Contactless EMV is supported and network certified for Wayne dispensers. This mode uses the chip data on the card.



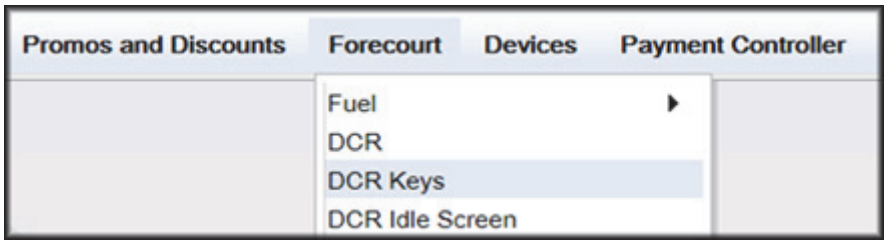
4. In the Other Parameters section, select the appropriate parameter configurations and click Save.

IP Address and Port should be left blank for Wayne Configuration.

DCR Keys Configuration

DCR key mapping is necessary for the PIN pad to respond correctly to customer key presses.

1. Navigate to Configuration Client > Forecourt > DCR Keys.

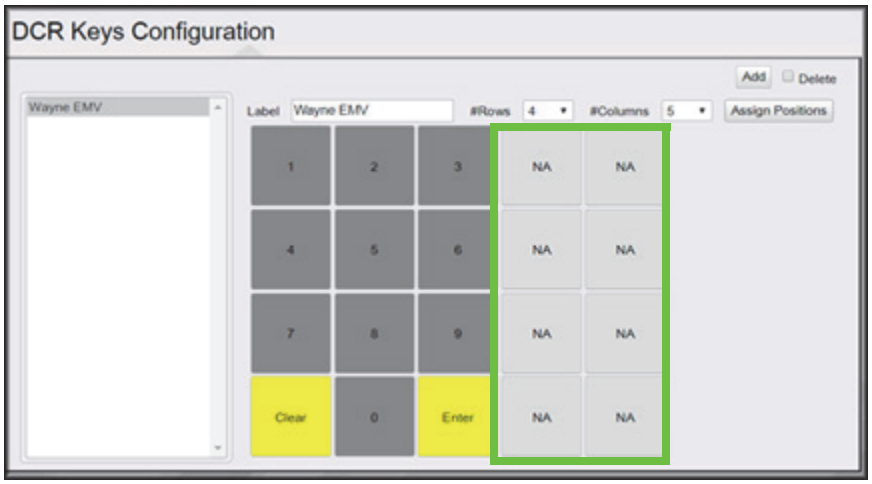


2. Create a DCR Keys layout by clicking on **Add** for Wayne DCRs below

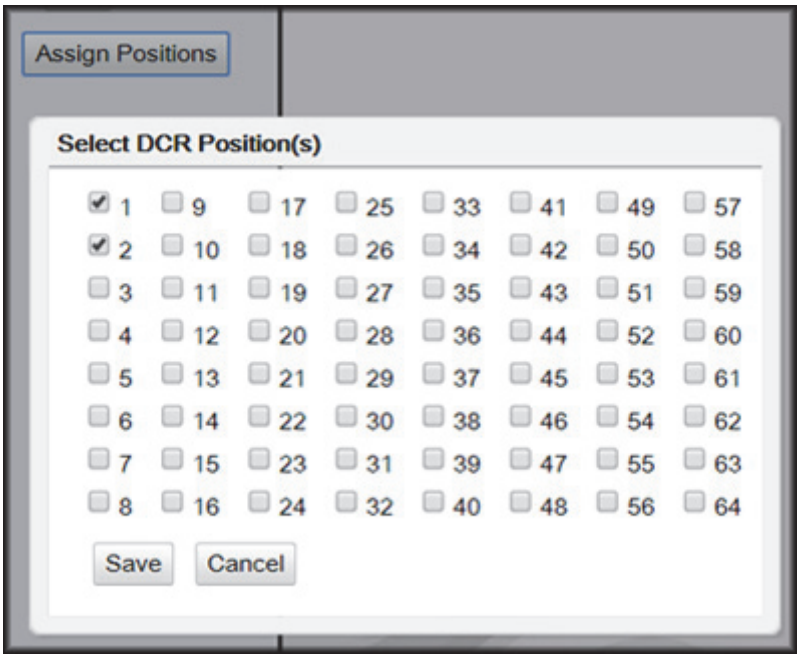
Wayne DCRs:

a. **Label**: Wayne EMV
b. **#Rows**: 4
c. **#Columns**: 5

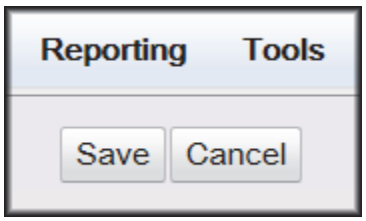
The two right-hand columns, outlined in green below, are left blank. They are programmed internally in the Commander software.



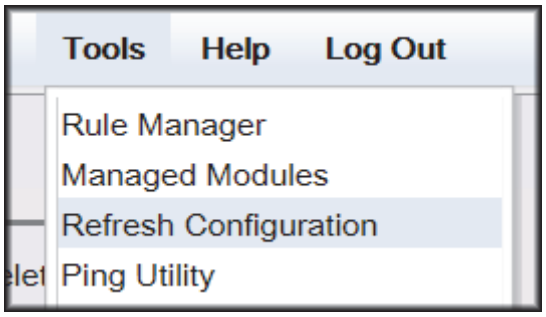
3. Select Assign Positions and Select DCR Position(s) to all the DCRs and click **Save**.



4. Click **Save** at DCR Keys Configuration.



5. Navigate to Configuration Client > Tools > Refresh Configuration.



Local Area Network Configuration

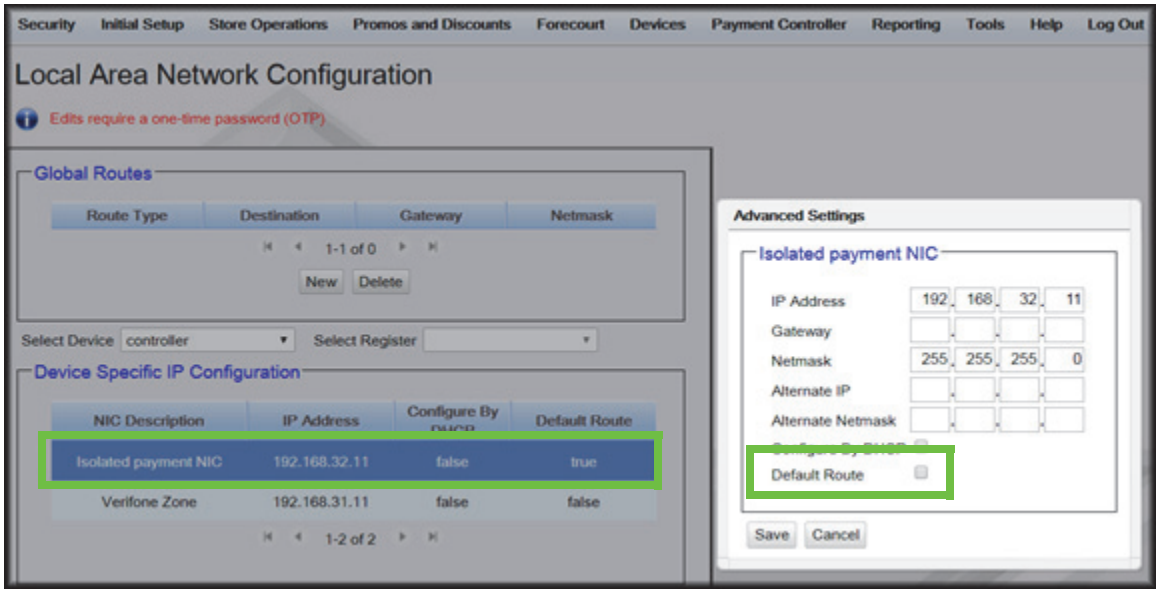
Verify Gateway IP addresses have been setup for EMV and the MNSP (Switch) Vendor has pushed the correct rules and polices.

The LAN is required to be configured for Wayne CAT. In the Wayne configuration, the Commander is the SERVER and the Wayne CAT is the CLIENT. The Outdoor EMV DCR IP traffic must be routed from the Commander through the Network IP Address 192.168.31.31. Depending on which Device Specific IP Configuration is selected for the site, Device Specific Network Routes may need to be added.

***For Shell branded sites**, see Appendix D at the back of the document for Shell Verifone Zone settings.*

Isolated Payment NIC

1. In Configuration Client, navigate to Initial Setup > Local Area Network Configuration.
2. Click on Isolated Payment NIC in the Device Specific IP Configuration.
3. Verify with your network provider if the “Default Route” parameter needs to be checked. If the parameter is checked, then continue with the next steps. If not checked, then skip to the EPS Global Configuration Section.



Using the Wayne DCR IP addresses, add a Network Destination Route with the 4th octet (last) set to ZERO. i.e. if the DCR IP addresses were 172.29.1.1. to 172.29.1.10, then the IP address used for this route would be 172.29.1.0.

4. If the Default Route is checked, then add New Route Config to the Device Specific Routes per site.
   a. **Route Type**: Network
   b. Enter in the IP address used for the DCRs with the last octet set to 0. See the note above for more details.
   c. **Gateway**: 192.168.31.31
   d. **Netmask**: 255.255.255.0

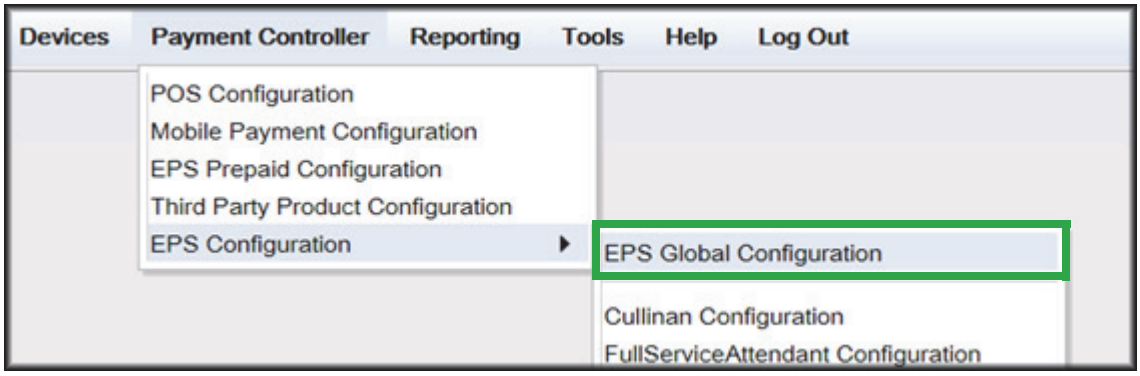
5. Click **Save** and then reboot the Commander.

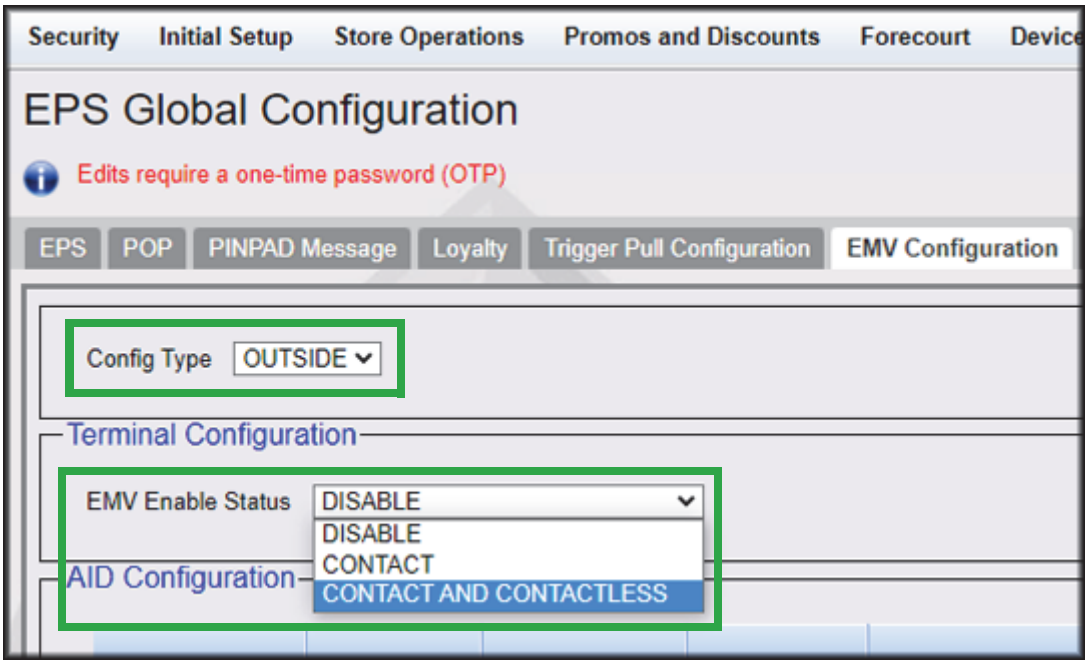
EPS Global Configuration

For Shell branded sites, EPS Global Configuration is controlled by Wincor. This should be pre-configured and enabled prior to converting the site for outdoor EMV. No changes are needed in EPS Global Configuration. Proceed to Fuel and DCR Initialization.

The EMV Configuration tab of the EPS Global Configuration screen contains options for both inside and outside EMV use.

1. Navigate to Configuration Client > Payment Controller > EPS Global Configuration > EMV Configuration.

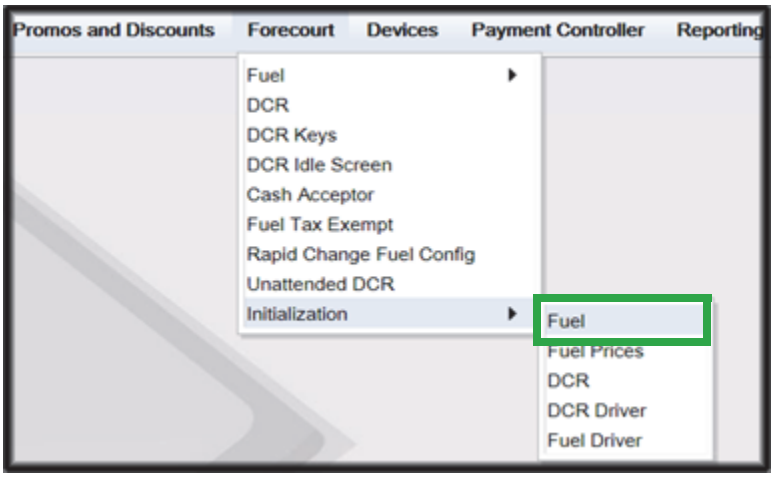




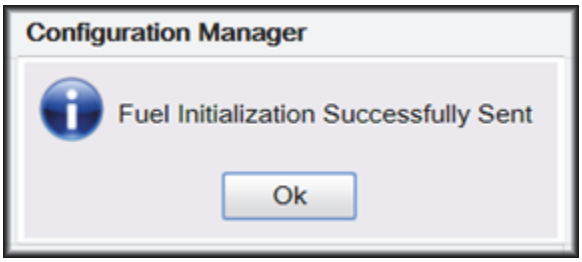
2. From the Config Type drop down menu, select **OUTSIDE**.
3. In the Terminal Configuration section and from the EMV Enable Status drop down menu, select the parameter **CONTACT** or **CONTACT AND CONTACTLESS**.
4. Select Save.

Fuel and DCR Initialization

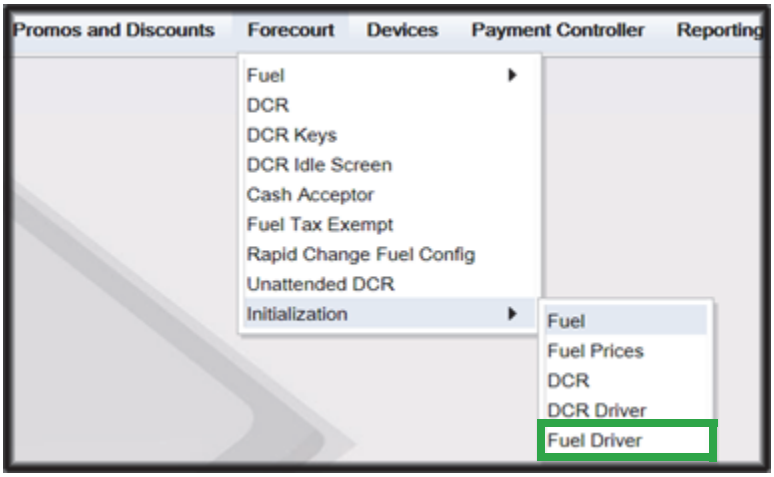
1. After configuring Managed Modules for Fuel and DCR, perform a Fuel and DCR initialization.
2. Navigate to Configuration Client > Tools > Refresh Configuration.
3. To initialize Fuel, navigate to Configuration Client > Forecourt > Initialization and then select Fuel.



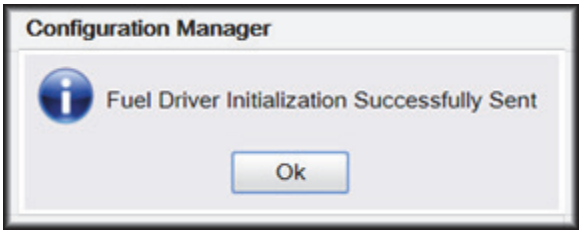
4. A message stating Fuel Initialization Successfully Sent displayed. Select Ok.



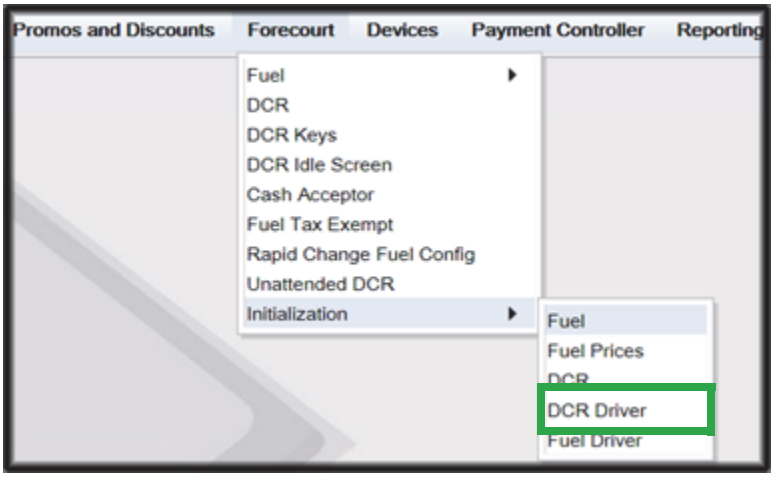
5. To initialize the Fuel Driver, navigate to Configuration Client > Forecourt > Initialization and then select Fuel Driver.



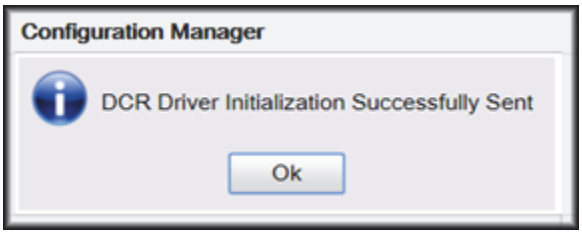
6. A message stating Fuel Driver Initialization Successfully Sent displayed. Select Ok



7. To initialize DCR Driver, navigate to Configuration Client > Forecourt > Initialization and then select DCR Driver



8. A message stating DCR Driver Initialization Successfully Sent displayed. Select Ok.



Check the dispensers to verify that they are loaded.

After they are all loaded, perform second DCR Driver initialization.

Again, check the dispensers to verify that they are loaded. Perform EMV transaction. If loaded and unable to perform an Outdoor EMV transactions, then go to next step.

EMV Initialization

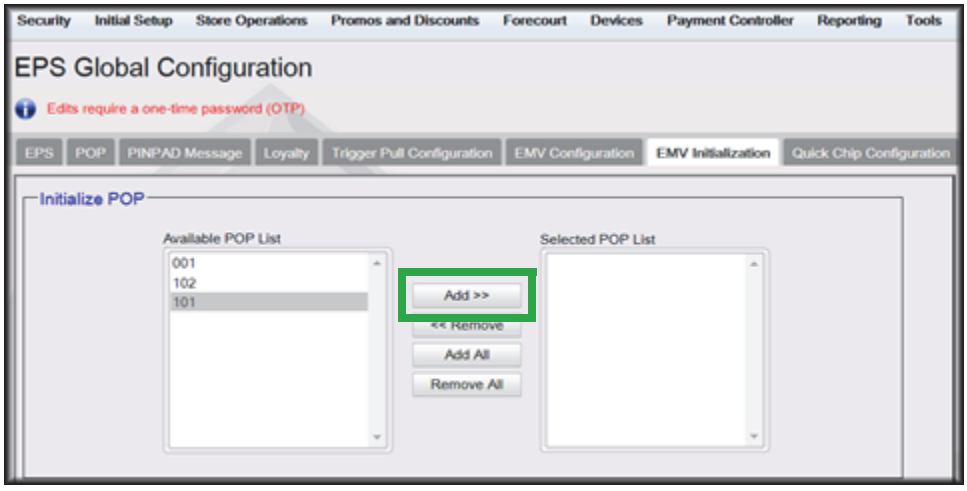
For Shell branded sites, EMV Initialization is controlled by Wincor. This should take place when Wincor and Commander sync and exchange information. No need to perform EMV initialization. Proceed to Verification of Forecourt Status.

After the Commander has established communications with the Wayne DCR positions, it is required to perform an EMV Initialization.

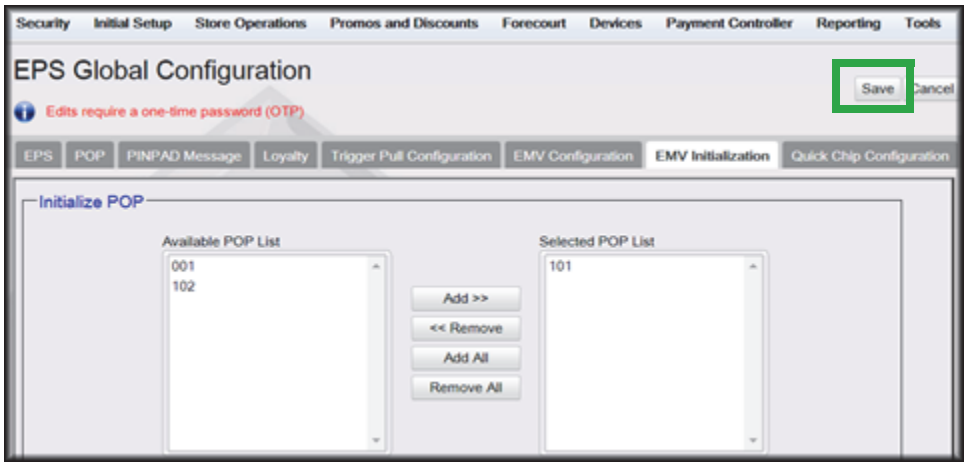
A DCR Driver Initialization must have been performed before starting the following steps. This will add DCR IDs to the Available POP List which can then be selected to receive the EMV Initialization.
An EMV Initialization does not perform a DCR Driver Initialization or a DCR Initialization.

1. Navigate to the Configuration Client > Payment Controller > EPS Global Configuration > EMV Initialization.
2. From the Initialize POP section locate the **Available POP List**.
3. For the DCR(s) requiring initialization, select the required DCR ID and click the **Add >** button to move it to the **Selected POP List**.

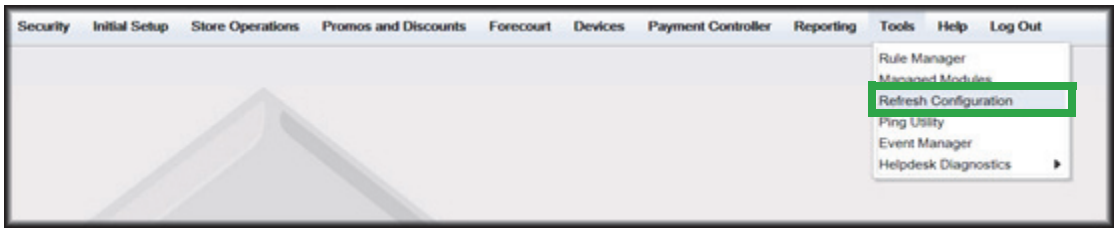
Outdoor card readers will be identified as POP 101, 102, 103, etc.



4. Repeat steps 2 and 3 for any additional DCR IDs.



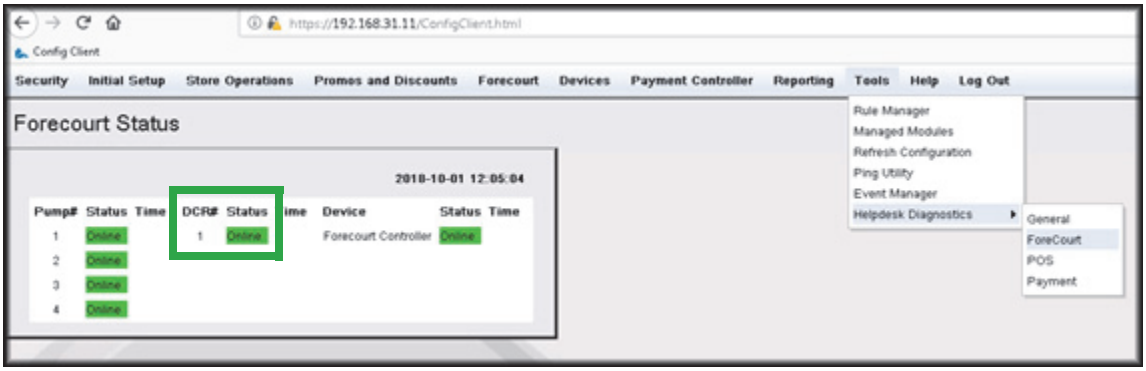
5. When finished selecting POP positions to be initialized, click Save. This performs an EMV POP initialization of the selected DCR positions.
6. If another EMV Initialization is required, first perform a Refresh Configuration.
7. Navigate to Configuration Client > Tools > Refresh Configuration. This updates the Available POP List contents. Repeat the EMV Initialization steps 1 through 5 above.



Verification of Forecourt Status

Use the following steps to verify IP based communications to the DCRs.

Navigate to Configuration Client > Tools > Helpdesk Diagnostics > Forecourt. The DCR Status should appear as “Online.” If they are offline, then communications to the DCRs have not been established. Recheck the connections and verify TCP/IP connectivity.



4 CONFIGURING BENNETT

The following steps are for configuring POS for Bennett SSP.

Before starting the conversion of the outdoor EMV, make sure that Pre-Install Checklist for EMV Readiness has been completed.

Before configuring Commander Configuration Client, follow the steps in setting up the networking communication that is identified for the site by the MNSP.

Configuring EMV in Configuration Client

By default, the Commander is installed with EMV disabled. The following section provides instructions on how to enable Outside EMV for the Commander Site Controller.

The following section provides instructions on how to enable Outside EMV for the Commander Site Controller.

Configuration Client Access

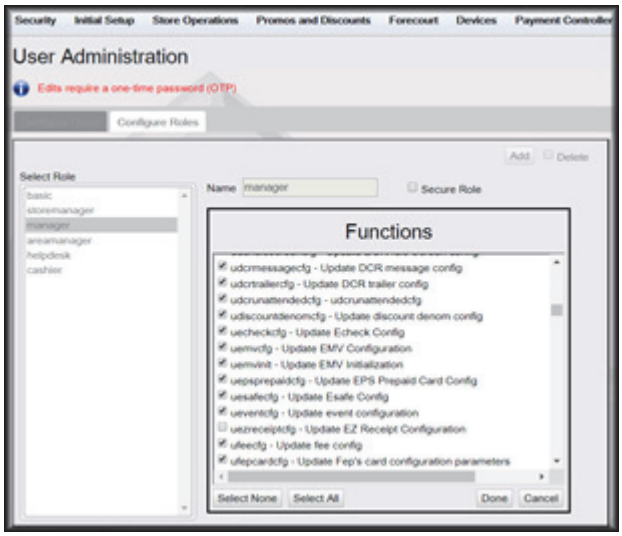
Accessing EMV Configuration

If this is a new Production Signed software installation, all menu selections to configure the system for EMV transaction processing are immediately visible and available.

If the software is being updated for EMV-readiness from a prior installation, user permissions must be updated to allow access to the EMV menu selections.

If accessing the Configuration Client from the POS and the EMV Configuration and Initialization tabs are grayed out, then this indicates the logged in user account does not have the correct functions added to the associated role. Activate the following roles for the user accessing Configuration Client at https://192.168.31.11/ConfigClient.html.

1. Navigate to Security > Manage Users > Configure Roles.
2. Select Role (i.e. Manager).
3. Select Edit.
4. Check the following Functions:
   - uemvcfg - Update EMV Configuration
   - uemvinit - Update EMV Initialization
   - vemvcfg - View EMV Configuration
   - vemvinit - View EMV Initialization
5. Logout of the Configuration Client and log back in for the Role changes to take effect.



Outdoor EMV Configuration for Bennett SSP

Managed Modules

1. Navigate to Tools > Managed Modules > Current Configuration.
2. **At Host Names**, select sitecontroller.
3. **At Select Module,** choose the **DCR Driver** option.
4. Select the DCR Channel to set up.

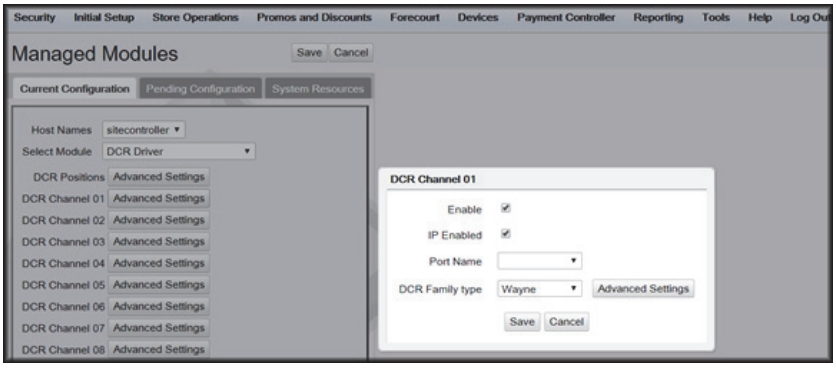
All IP enabled DCR, the DCR should be placed on the same channel (i.e. DCR Channel 01). There is no advantage to splitting up the channels.

5. For each DCR Channel for EMV, select:
   a. **Enable** option must be checked.
   b. **IP Enabled** option must be checked.
   c. **Port Name** option must remain empty.

EMV communications is done via the Ethernet port on the Commander, therefore the DCR Channel Port Name will be left blank.
There will be no LED lights for DCR on the front of the Commander since the communications is via the Ethernet port.

   d. **DCR Family type** selection is Wayne.

*Currently, the **Bennett** selection for DCR Family type is "Wayne."*

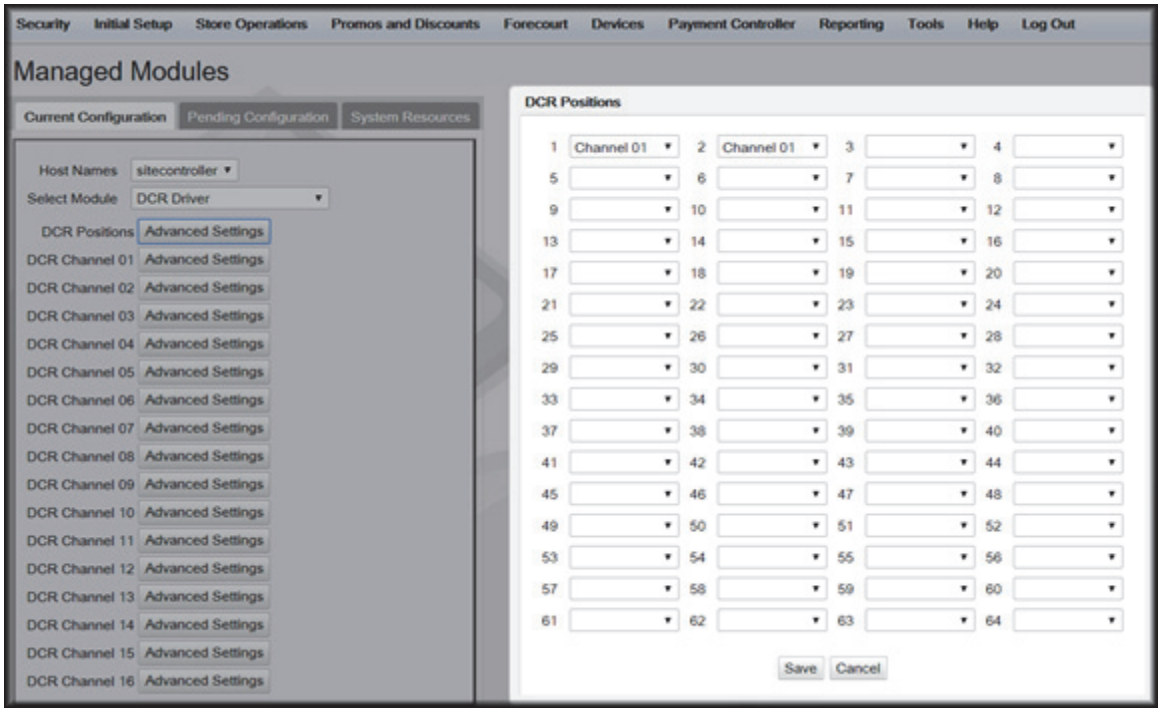


   e. Save DCR Driver changes.

If both IP Enabled and Port Name parameters are selected, an error displays when attempting to save the configuration changes.

6. After completing the DCR Channel set-up, select **DCR Positions** option and assign CRIND positions to their respective DCR.

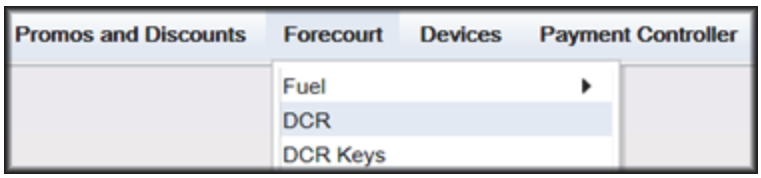
If the site is an Auto-Upgrade and has multiple channels configured, reconfigure all the DCR Positions on a single channel (i.e. Channel 01).



DCR Configuration

The following EMV specific parameters are required for each EMV DCR position:

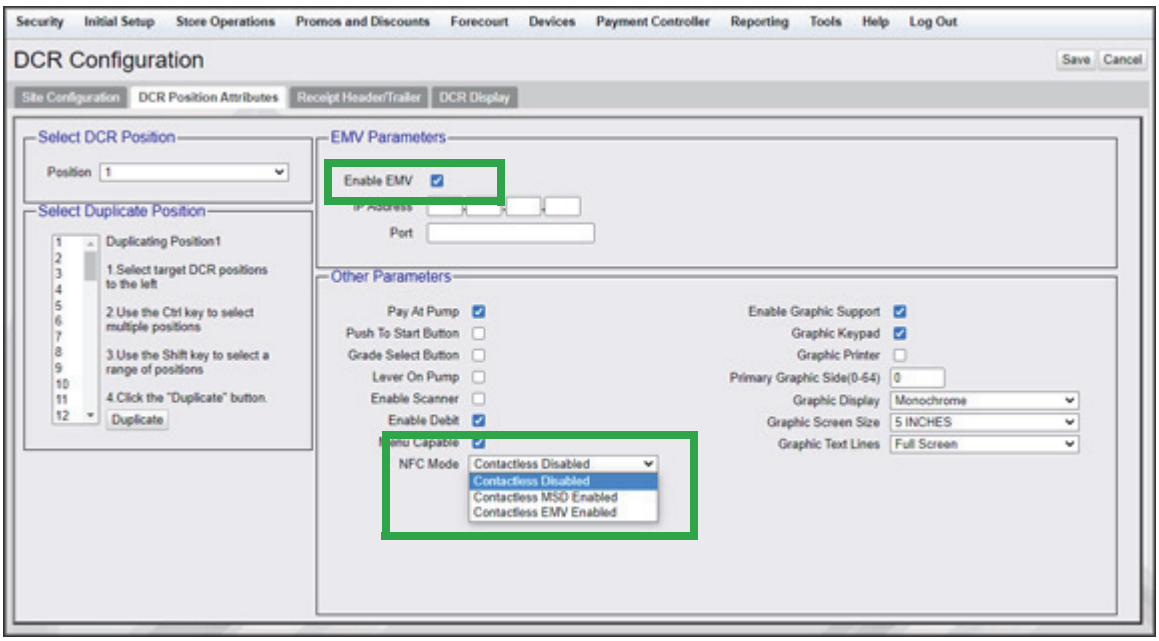
1. Navigate to Configuration Client > Forecourt > DCR.



NOTE

In order for NFC Readers to accept mobile device payments, make sure Contactless is not disabled at ***Configuration Client > Forecourt > DCR > DCR Configuration > DCR Position Attributes > NFC Mode****.*

2. Select DCR Position Attributes.
3. Under EMV Parameters section for each of the Selected EMV DCR Position:
   a. **Enable EMV** must be checked.
   b. **IP Address** must be left blank.
   c. **Port** must be left blank.
   d. For **NFC Mode**, select one of the following:
      - Contactless Disabled — Contactless (including Mobile Payments) is not being used at the DCR.
      - Contactless MSD Enabled — Use only if Contactless EMV is not supported or not certified for Bennett dispensers. This mode uses the Mag-Stripe Data (MSD).
      - Contactless EMV Enabled — Use if Contactless EMV is supported and network certified for Bennett dispensers. This mode uses the chip data on the card.



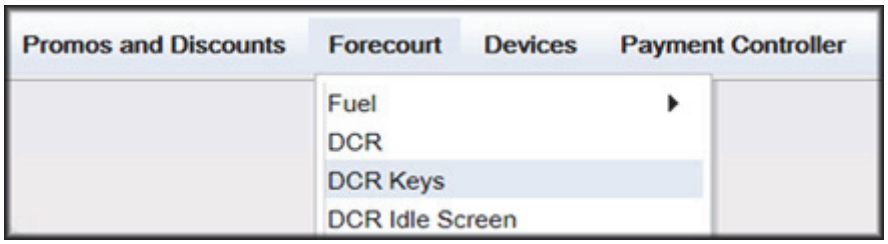
4. In the Other Parameters section, select the appropriate parameter configurations and click Save.

IP Address and Port should be left blank for Bennett Configuration.

DCR Keys Configuration

DCR key mapping is necessary for the PIN pad to respond correctly to customer key presses.

1. Navigate to Configuration Client > Forecourt > DCR Keys.

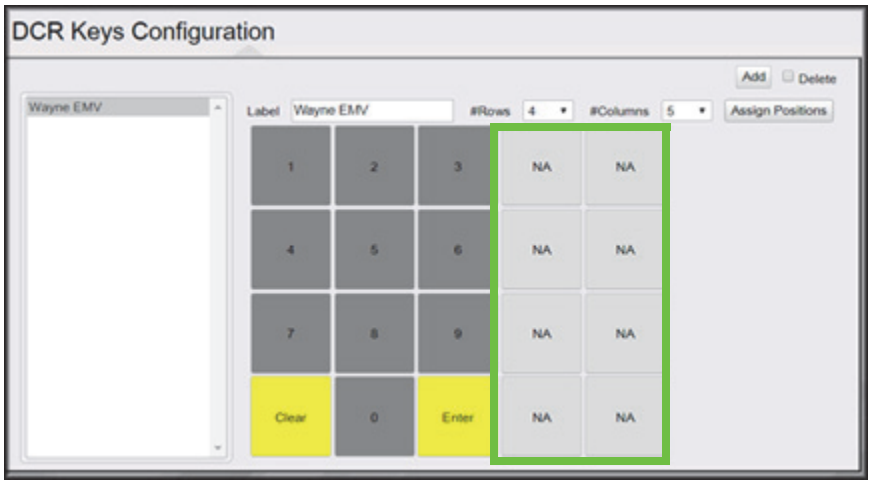


2. Create a DCR Keys layout by clicking on **Add** for Bennett SSPs below

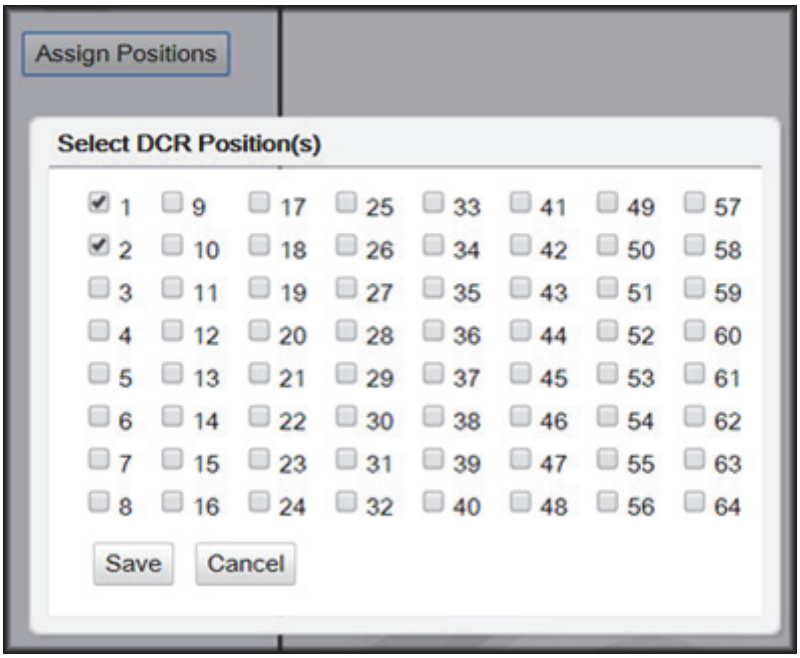
Bennett SSPs:

a. **Label**: Bennett EMV
b. **#Rows**: 4
c. **#Columns**: 5

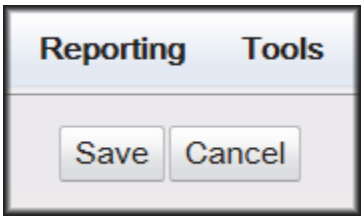
The two right-hand columns, outlined in green below, are left blank. They are programmed internally in the Commander software.



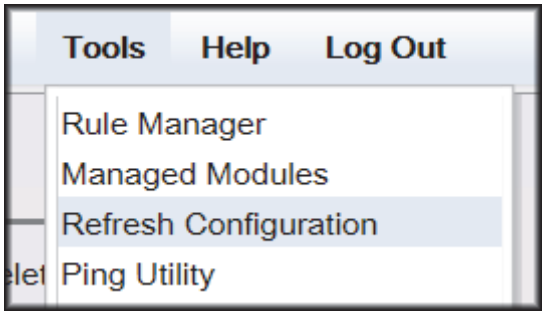
3. Select Assign Positions and Select DCR Position(s) to all the DCRs and click **Save**.



4. Click **Save** at DCR Keys Configuration.



5. Navigate to Configuration Client > Tools > Refresh Configuration.



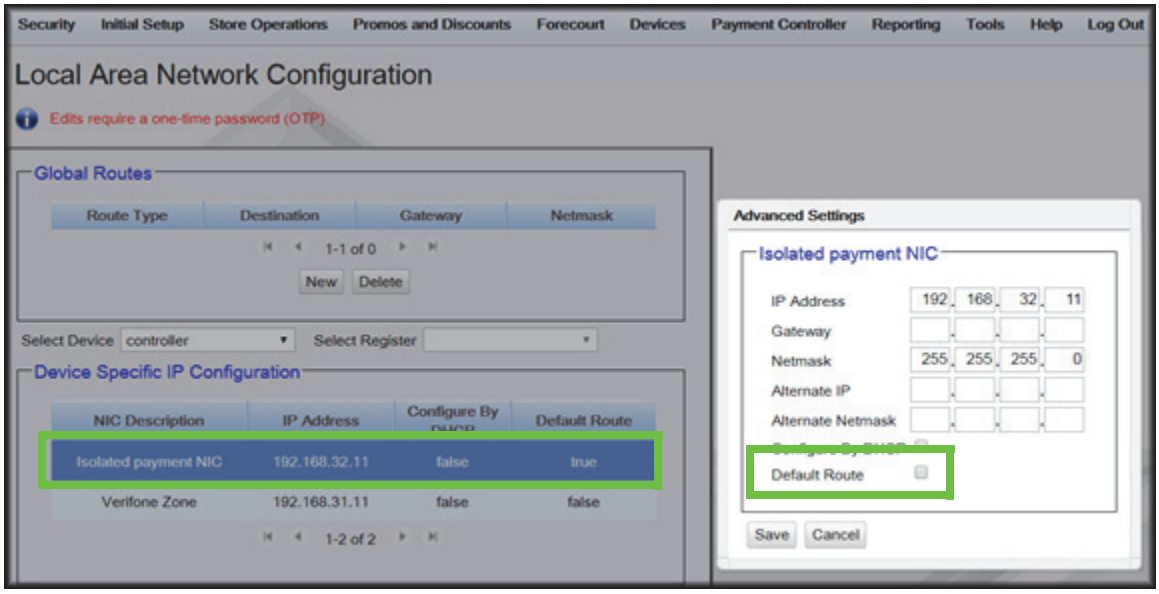
Local Area Network Configuration

Verify Gateway IP addresses have been setup for EMV and the MNSP (Switch) Vendor has pushed the correct rules and polices.

The LAN is required to be configured for Bennett SSP. In the Bennett configuration, the Commander is the SERVER and the Bennett SSP is the CLIENT. The Outdoor EMV DCR IP traffic must be routed from the Commander through the Network IP Address 192.168.31.31. Depending on which Device Specific IP Configuration is selected for the site, Device Specific Network Routes may need to be added.

Isolated Payment NIC

1. In Configuration Client, navigate to Initial Setup > Local Area Network Configuration.
2. Click on Isolated Payment NIC in the Device Specific IP Configuration.
3. Verify with your network provider if the “Default Route” parameter needs to be checked. If the parameter is checked, then continue with the next steps. If not checked, then skip to the EPS Global Configuration Section.



Using the Bennett SSP IP addresses, add a Network Destination Route with the 4th octet (last) set to ZERO. i.e. if the DCR IP addresses were 172.29.1.1. to 172.29.1.10, then the IP address used for this route would be 172.29.1.0.

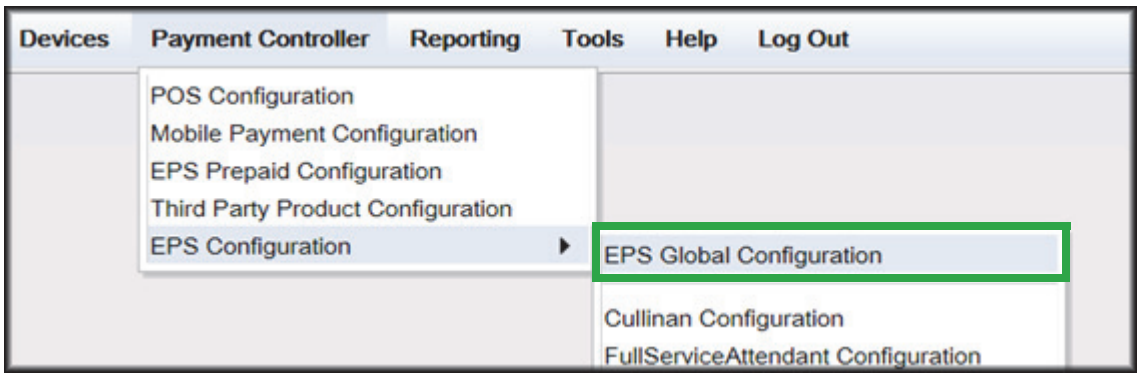
4. If the Default Route is checked, then add New Route Config to the Device Specific Routes per site.
   a. **Route Type**: Network
   b. Enter in the IP address used for the DCRs with the last octet set to 0. See the note above for more details.
   c. **Gateway**: 192.168.31.31
   d. **Netmask**: 255.255.255.0

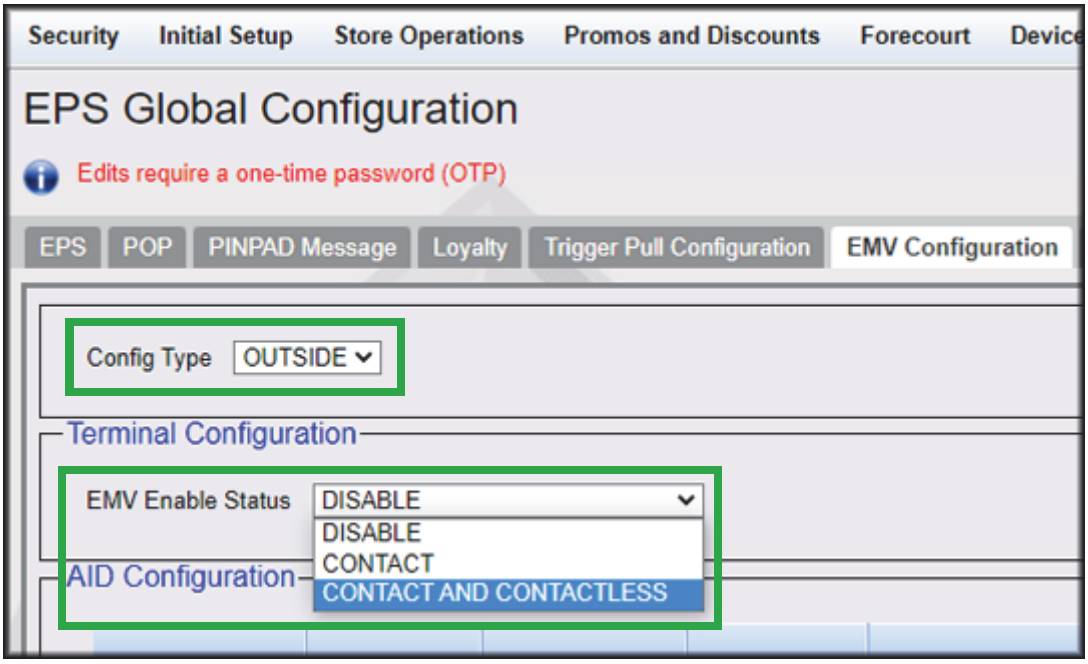
5. Click **Save** and then reboot the Commander.

EPS Global Configuration

The EMV Configuration tab of the EPS Global Configuration screen contains options for both inside and outside EMV use.

1. Navigate to Configuration Client > Payment Controller > EPS Global Configuration > EMV Configuration.

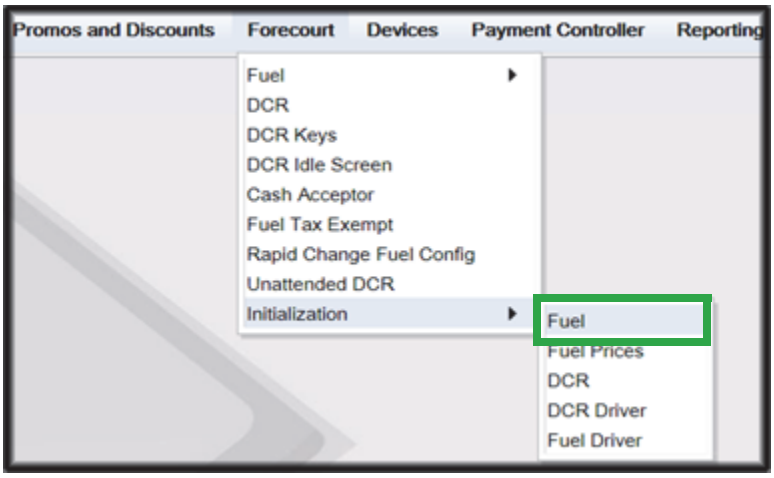




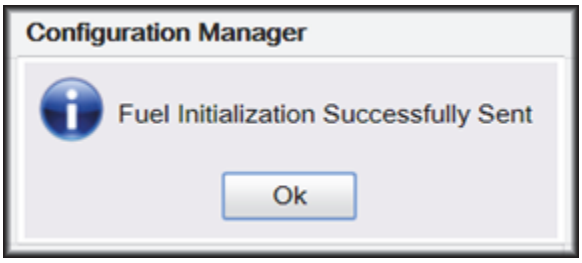
2. From the Config Type drop down menu, select **OUTSIDE**.
3. In the Terminal Configuration section and from the EMV Enable Status drop down menu, select the parameter **CONTACT** or **CONTACT AND CONTACTLESS**.
4. Select Save.

Fuel and DCR Initialization

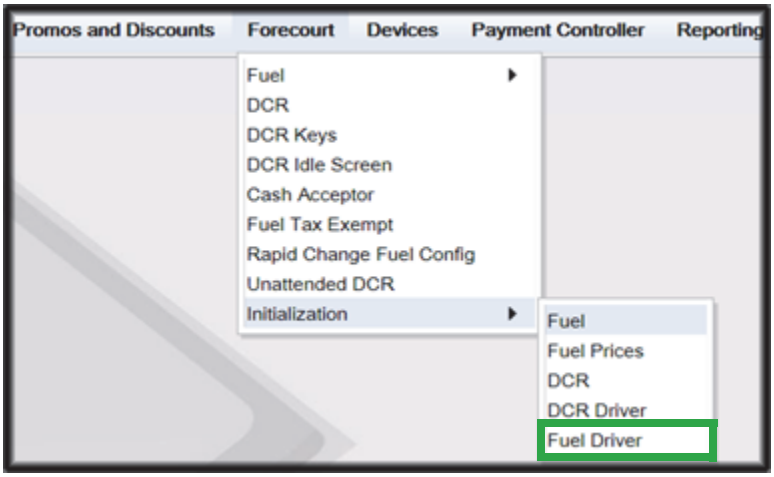
1. After configuring Managed Modules for Fuel and DCR, perform a Fuel and DCR initialization.
2. Navigate to Configuration Client > Tools > Refresh Configuration.
3. To initialize Fuel, navigate to Configuration Client > Forecourt > Initialization and then select Fuel.



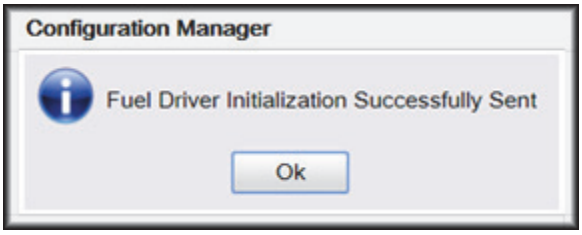
4. A message stating Fuel Initialization Successfully Sent displayed. Select Ok.



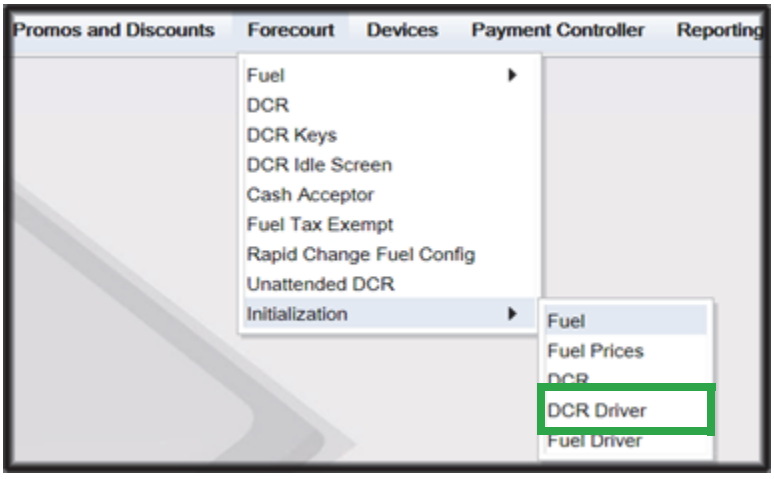
5. To initialize the Fuel Driver, navigate to Configuration Client > Forecourt > Initialization and then select Fuel Driver.



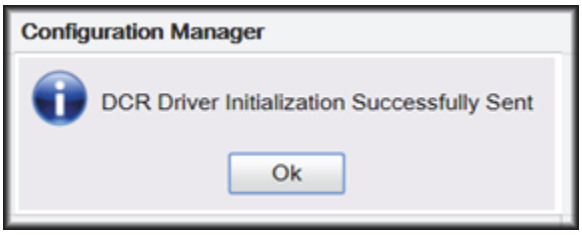
6. A message stating Fuel Driver Initialization Successfully Sent displayed. Select Ok



7. To initialize DCR Driver, navigate to Configuration Client > Forecourt > Initialization and then select DCR Driver



8. A message stating DCR Driver Initialization Successfully Sent displayed. Select Ok.



Check the dispensers to verify that they are loaded.

After they are all loaded, perform second DCR Driver initialization.

Again, check the dispensers to verify that they are loaded. Perform EMV transaction. If loaded and unable to perform an Outdoor EMV transactions, then go to next step.

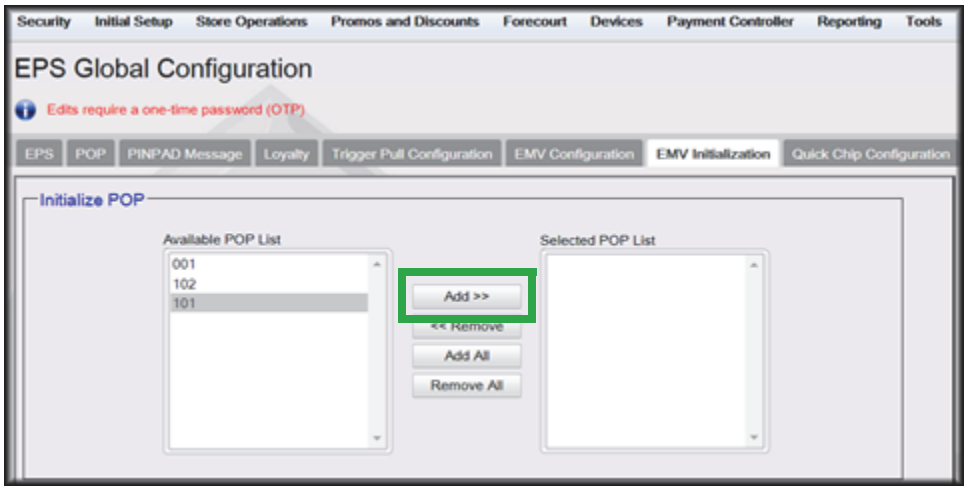
EMV Initialization

After the Commander has established communications with the Bennett SSP positions, it is required to perform an EMV Initialization.

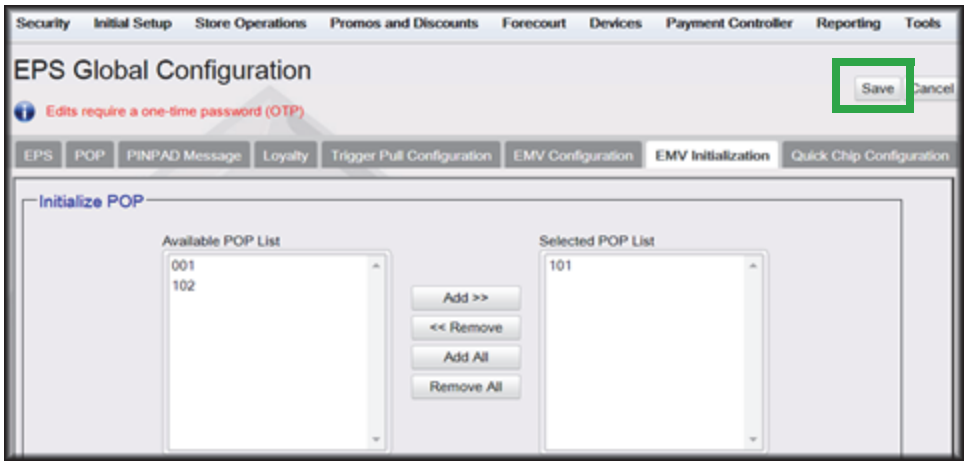
A DCR Driver Initialization must have been performed before starting the following steps. This will add DCR IDs to the Available POP List which can then be selected to receive the EMV Initialization.
An EMV Initialization does not perform a DCR Driver Initialization or a DCR Initialization.

1. Navigate to the Configuration Client > Payment Controller > EPS Global Configuration > EMV Initialization.
2. From the Initialize POP section locate the **Available POP List**.
3. For the DCR(s) requiring initialization, select the required DCR ID and click the **Add >** button to move it to the **Selected POP List**.

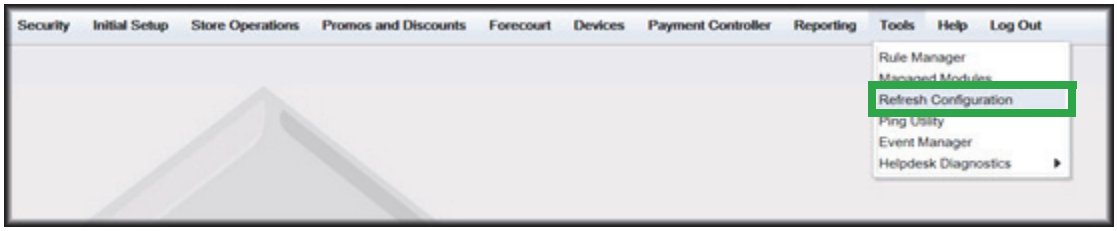
Outdoor card readers will be identified as POP 101, 102, 103, etc.



4. Repeat steps 2 and 3 for any additional DCR IDs.



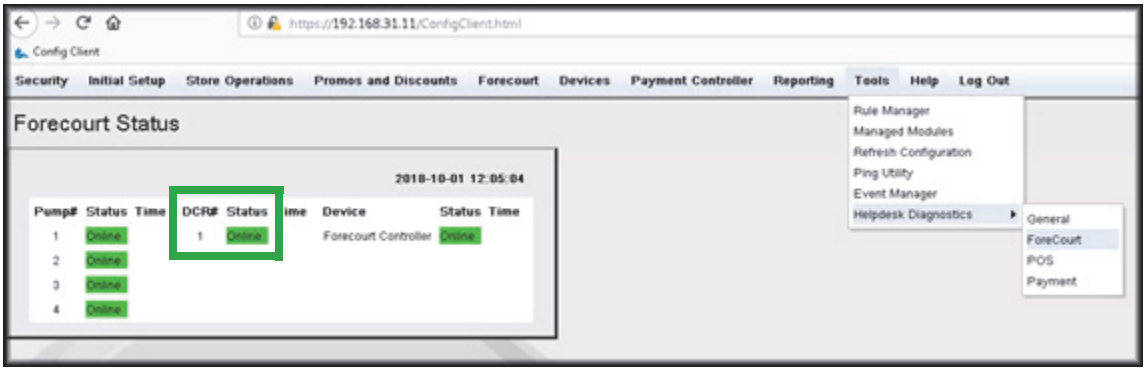
5. When finished selecting POP positions to be initialized, click Save. This performs an EMV POP initialization of the selected DCR positions.
6. If another EMV Initialization is required, first perform a Refresh Configuration.
7. Navigate to Configuration Client > Tools > Refresh Configuration. This updates the Available POP List contents. Repeat the EMV Initialization steps 1 through 5 above.



Verification of Forecourt Status

Use the following steps to verify IP based communications to the DCRs.

Navigate to Configuration Client > Tools > Helpdesk Diagnostics > Forecourt. The DCR Status should appear as “Online.” If they are offline, then communications to the DCRs have not been established. Recheck the connections and verify TCP/IP connectivity.



5 CONFIGURING INVENCO

The following steps are for configuring POS for Invenco OPT.

Before starting the conversion of the outdoor EMV, make sure that Pre-Install Checklist for EMV Readiness has been completed.

Before configuring Commander Configuration Client, follow the steps in setting up the networking communication that is identified for the site by the MNSP.

Configuring EMV in Configuration Client

By default, the Commander is installed with EMV disabled. The following section provides instructions on how to enable Outside EMV for the Commander Site Controller.

The following section provides instructions on how to enable Outside EMV for the Commander Site Controller.

Configuration Client Access

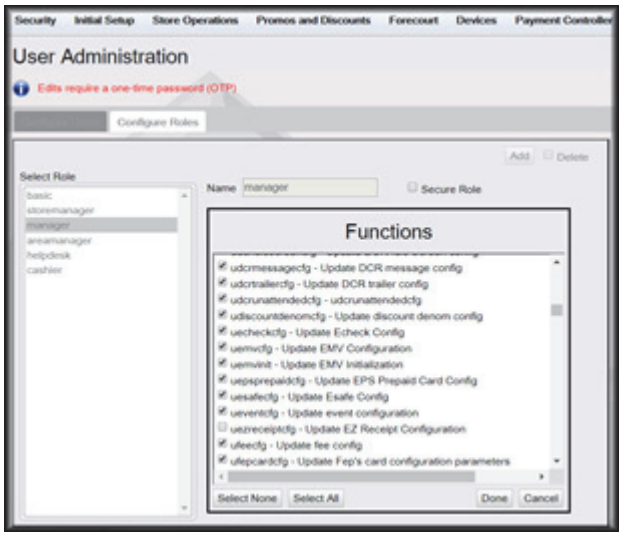
Accessing EMV Configuration

If this is a new Production Signed software installation, all menu selections to configure the system for EMV transaction processing are immediately visible and available.

If the software is being updated for EMV-readiness from a prior installation, user permissions must be updated to allow access to the EMV menu selections.

If accessing the Configuration Client from the POS and the EMV Configuration and Initialization tabs are grayed out, then this indicates the logged in user account does not have the correct functions added to the associated role. Activate the following roles for the user accessing Configuration Client at https://192.168.31.11/ConfigClient.html.

1. Navigate to Security > Manage Users > Configure Roles.
2. Select Role (i.e. Manager).
3. Select Edit.
4. Check the following Functions:
   - uemvcfg - Update EMV Configuration
   - uemvinit - Update EMV Initialization
   - vemvcfg - View EMV Configuration
   - vemvinit - View EMV Initialization
5. Logout of the Configuration Client and log back in for the Role changes to take effect.



Outdoor EMV Configuration for Invenco OPT

Managed Modules

1. Navigate to Tools > Managed Modules > Current Configuration.
2. **At Host Names**, select sitecontroller.
3. **At Select Module,** choose the **DCR Driver** option.
4. Select the DCR Channel to set up.

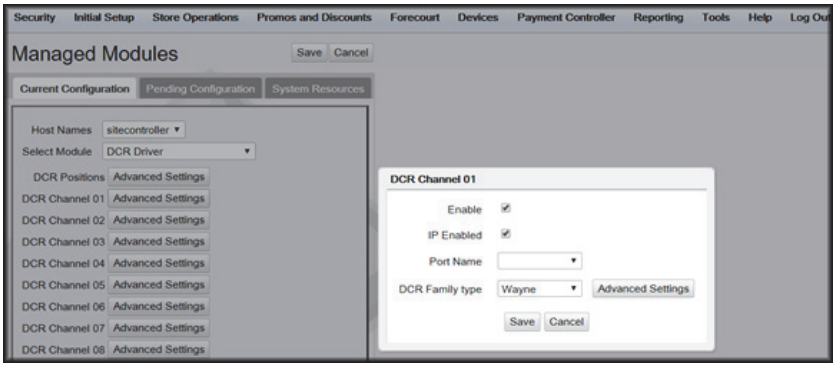
All IP enabled DCR, the DCR should be placed on the same channel (i.e. DCR Channel 01). There is no advantage to splitting up the channels.

5. For each DCR Channel for EMV, select:
   a. **Enable** option must be checked.
   b. **IP Enabled** option must be checked.
   c. **Port Name** option must remain empty.

EMV communications is done via the Ethernet port on the Commander, therefore the DCR Channel Port Name will be left blank.
There will be no LED lights for DCR on the front of the Commander since the communications is via the Ethernet port.

   d. **DCR Family type** selection is Wayne.

*Currently, the **Invenco** selection for DCR Family type is "Wayne."*

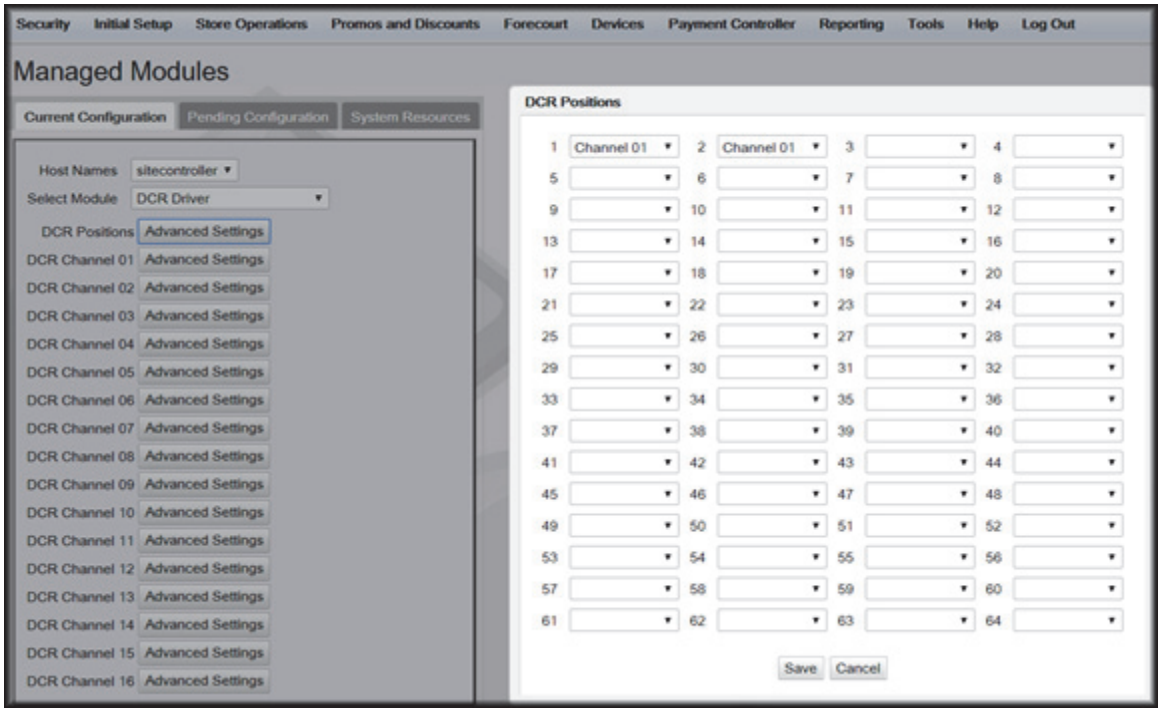


   e. Save DCR Driver changes.

If both IP Enabled and Port Name parameters are selected, an error displays when attempting to save the configuration changes.

6. After completing the DCR Channel set-up, select **DCR Positions** option and assign CRIND positions to their respective DCR.

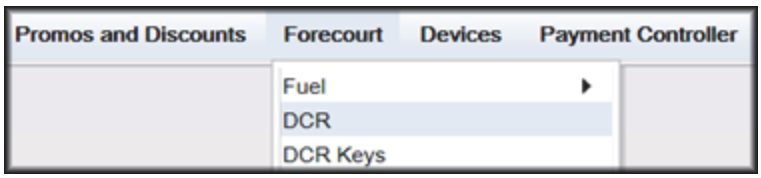
If the site is an Auto-Upgrade and has multiple channels configured, reconfigure all the DCR Positions on a single channel (i.e. Channel 01).



DCR Configuration

The following EMV specific parameters are required for each EMV DCR position:

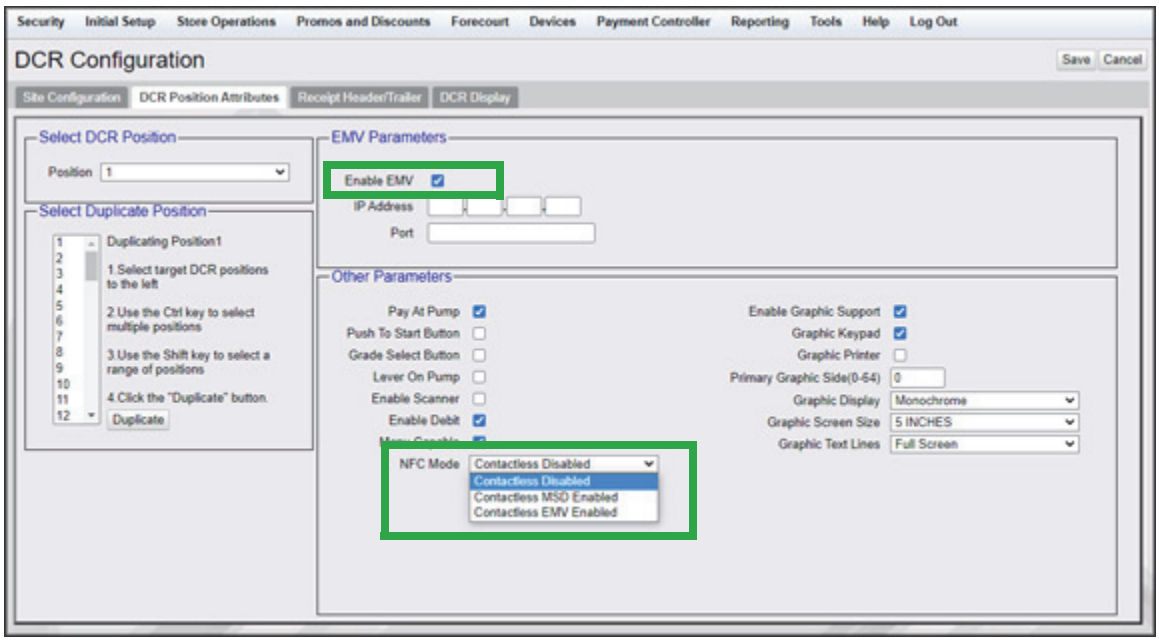
1. Navigate to Configuration Client > Forecourt > DCR.



NOTE

In order for NFC Readers to accept mobile device payments, make sure Contactless is not disabled at ***Configuration Client > Forecourt > DCR > DCR Configuration > DCR Position Attributes > NFC Mode****.*

2. Select DCR Position Attributes.
3. Under EMV Parameters section for each of the Selected EMV DCR Position:
   a. **Enable EMV** must be checked.
   b. **IP Address** must be left blank.
   c. **Port** must be left blank.
   d. For **NFC Mode**, select one of the following:
      - Contactless Disabled — Contactless (including Mobile Payments) is not being used at the DCR.
      - Contactless MSD Enabled — Use only if Contactless EMV is not supported or not certified for Invenco dispensers. This mode uses the Mag-Stripe Data (MSD).
      - Contactless EMV Enabled — Use if Contactless EMV is supported and network certified for Invenco dispensers. This mode uses the chip data on the card.



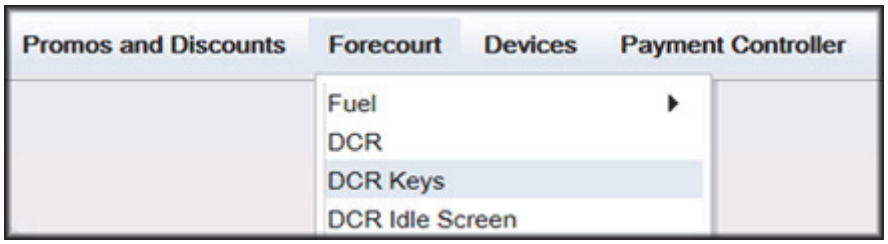
4. In the Other Parameters section, select the appropriate parameter configurations and click Save.

IP Address and Port should be left blank for Invenco Configuration.

DCR Keys Configuration

DCR key mapping is necessary for the PIN pad to respond correctly to customer key presses.

1. Navigate to Configuration Client > Forecourt > DCR Keys.

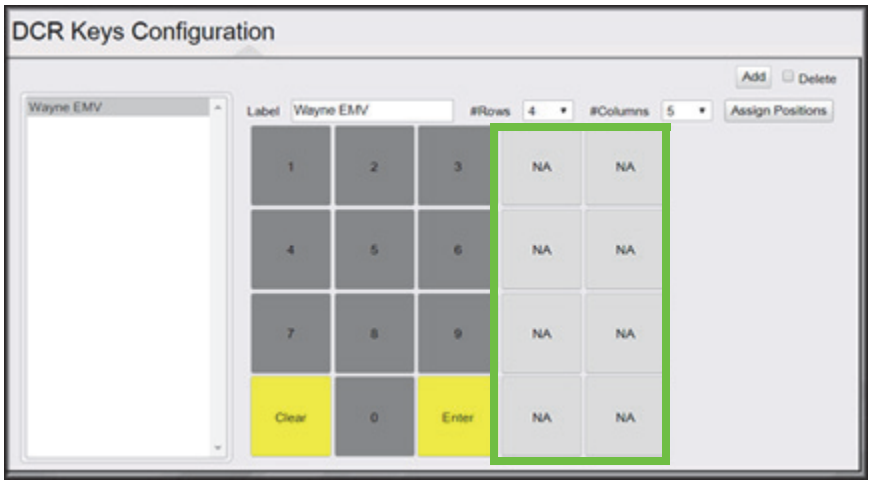


2. Create a DCR Keys layout by clicking on **Add** for Invenco OPTs below

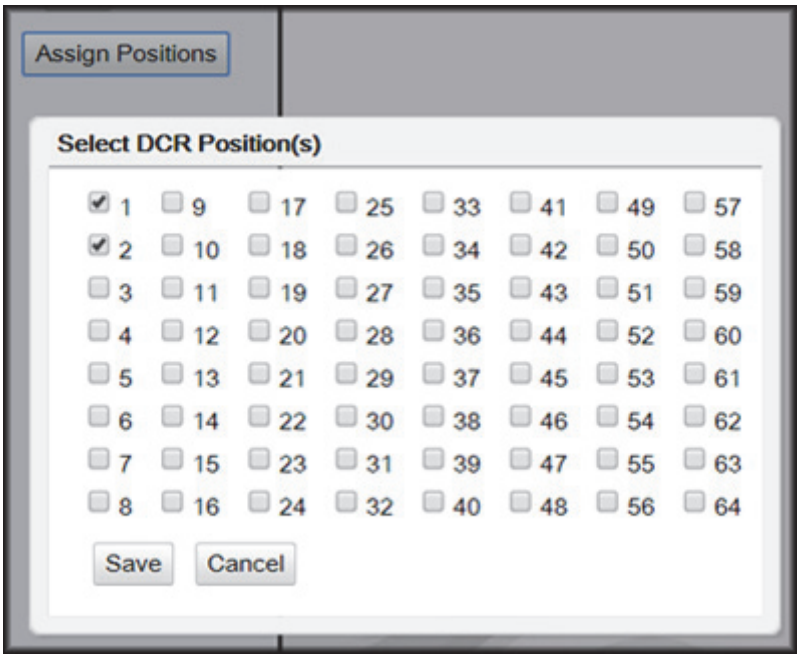
Invenco OPTs:

a. **Label**: Invenco EMV
b. **#Rows**: 4
c. **#Columns**: 5

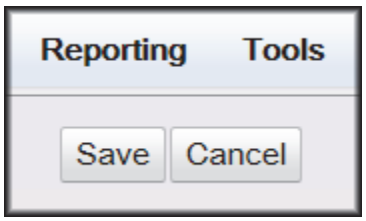
The two right-hand columns, outlined in green below, are left blank. They are programmed internally in the Commander software.



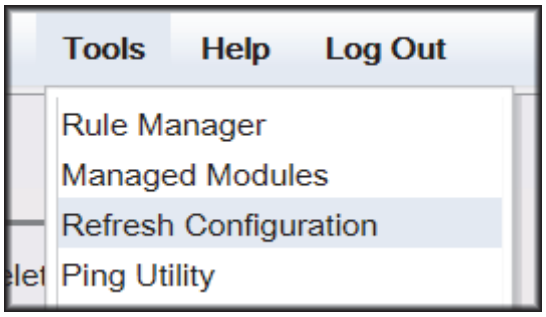
3. Select Assign Positions and Select DCR Position(s) to all the DCRs and click **Save**.



4. Click **Save** at DCR Keys Configuration.



5. Navigate to Configuration Client > Tools > Refresh Configuration.



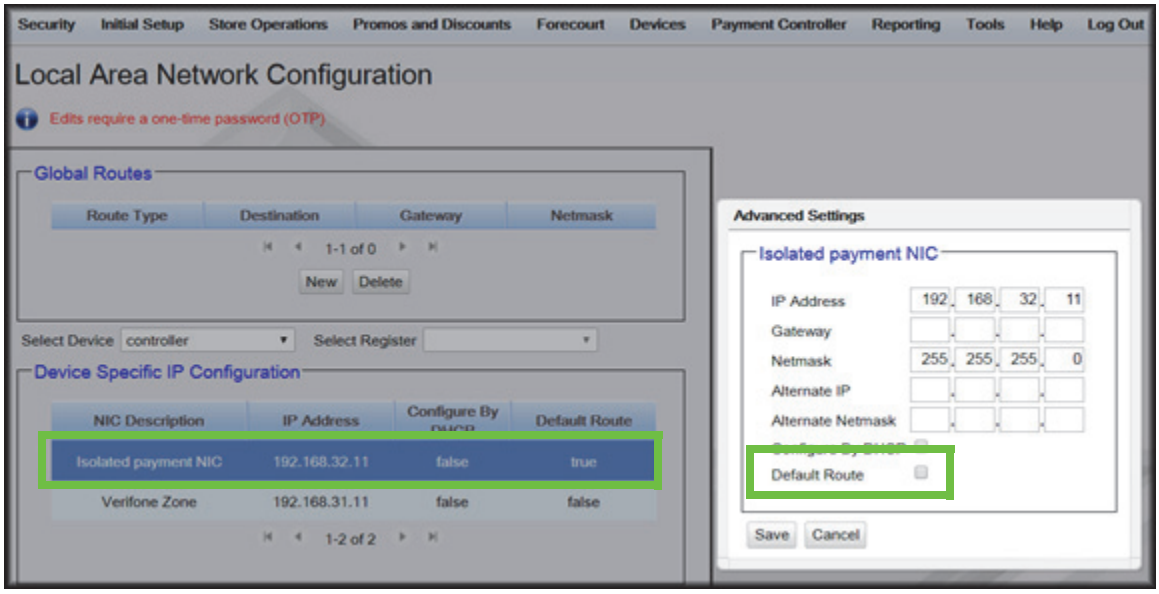
Local Area Network Configuration

Verify Gateway IP addresses have been setup for EMV and the MNSP (Switch) Vendor has pushed the correct rules and polices.

The LAN is required to be configured for Invenco OPT. In the Invenco configuration, the Commander is the SERVER and the Invenco OPT is the CLIENT. The Outdoor EMV DCR IP traffic must be routed from the Commander through the Network IP Address 192.168.31.31. Depending on which Device Specific IP Configuration is selected for the site, Device Specific Network Routes may need to be added.

Isolated Payment NIC

1. In Configuration Client, navigate to Initial Setup > Local Area Network Configuration.
2. Click on Isolated Payment NIC in the Device Specific IP Configuration.
3. Verify with your network provider if the “Default Route” parameter needs to be checked. If the parameter is checked, then continue with the next steps. If not checked, then skip to the EPS Global Configuration Section.



Using the Invenco DCR IP addresses, add a Network Destination Route with the 4th octet (last) set to ZERO. i.e. if the DCR IP addresses were 172.29.1.1. to 172.29.1.10, then the IP address used for this route would be 172.29.1.0.

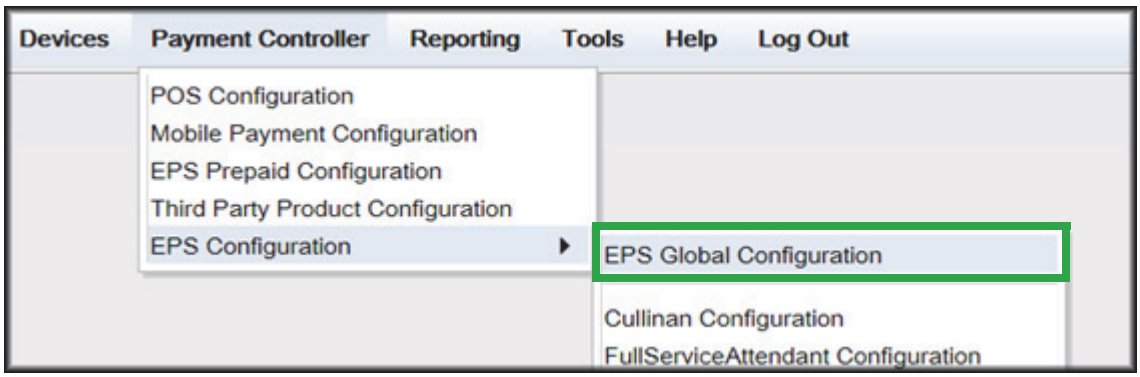
4. If the Default Route is checked, then add New Route Config to the Device Specific Routes per site.
   a. **Route Type**: Network
   b. Enter in the IP address used for the DCRs with the last octet set to 0. See the note above for more details.
   c. **Gateway**: 192.168.31.31
   d. **Netmask**: 255.255.255.0

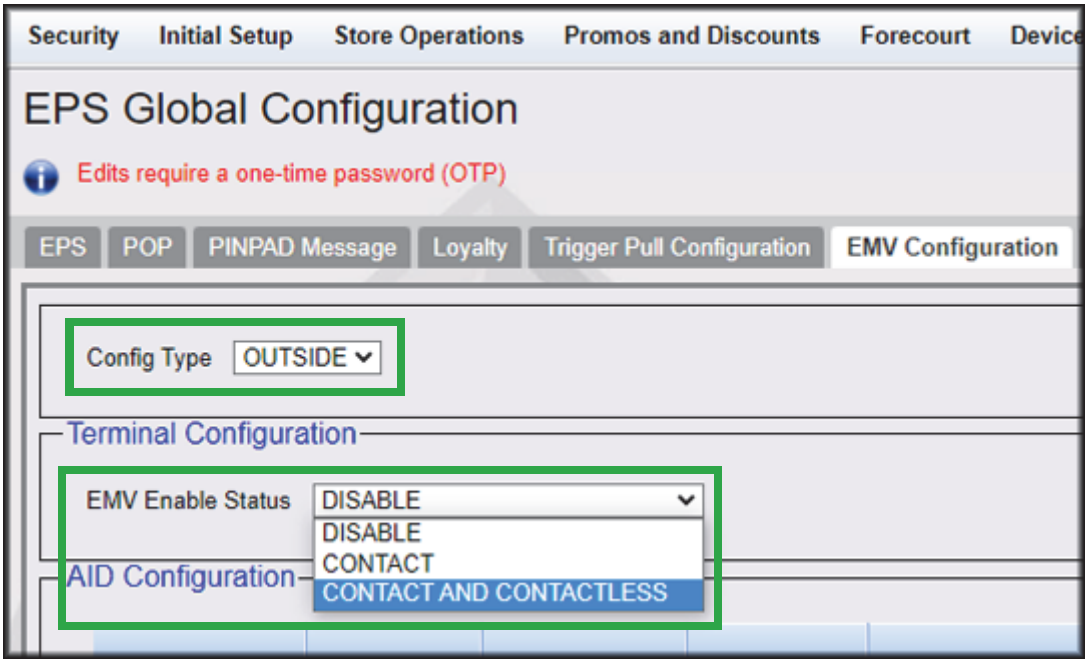
5. Click **Save** and then reboot the Commander.

EPS Global Configuration

The EMV Configuration tab of the EPS Global Configuration screen contains options for both inside and outside EMV use.

1. Navigate to Configuration Client > Payment Controller > EPS Global Configuration > EMV Configuration.

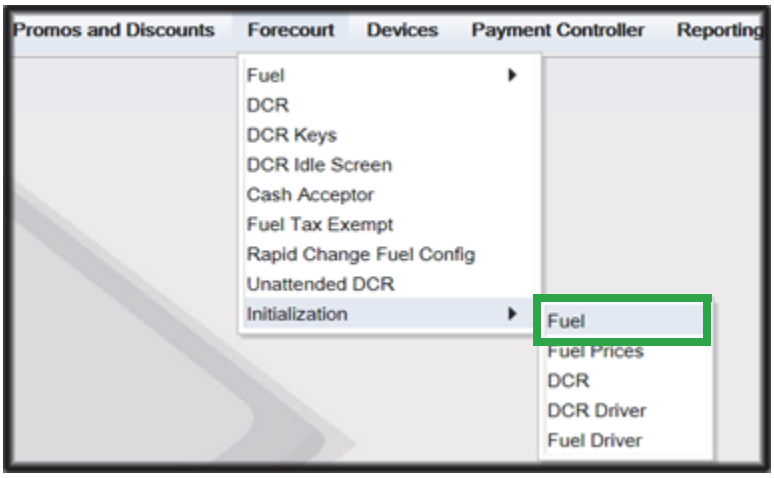




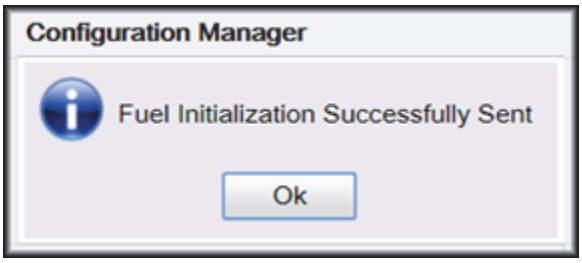
2. From the Config Type drop down menu, select **OUTSIDE**.
3. In the Terminal Configuration section and from the EMV Enable Status drop down menu, select the parameter **CONTACT** or **CONTACT AND CONTACTLESS**.
4. Select Save.

Fuel and DCR Initialization

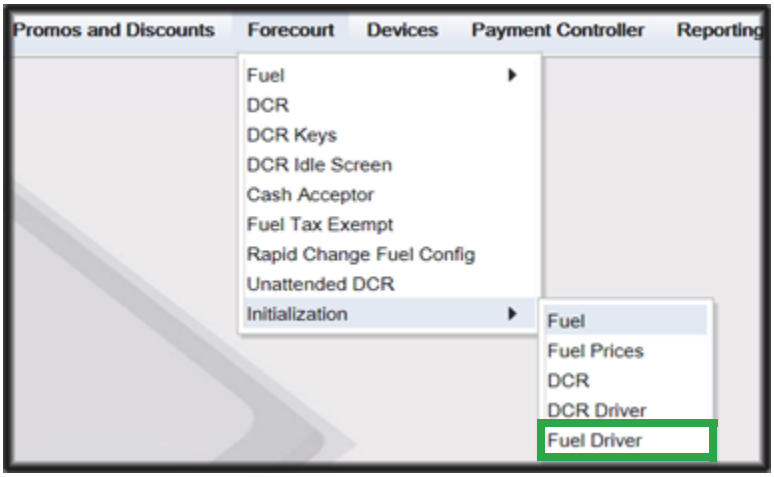
1. After configuring Managed Modules for Fuel and DCR, perform a Fuel and DCR initialization.
2. Navigate to Configuration Client > Tools > Refresh Configuration.
3. To initialize Fuel, navigate to Configuration Client > Forecourt > Initialization and then select Fuel.



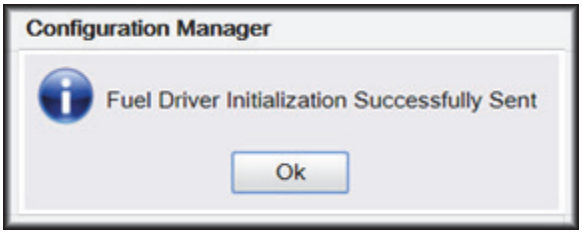
4. A message stating Fuel Initialization Successfully Sent displayed. Select Ok.



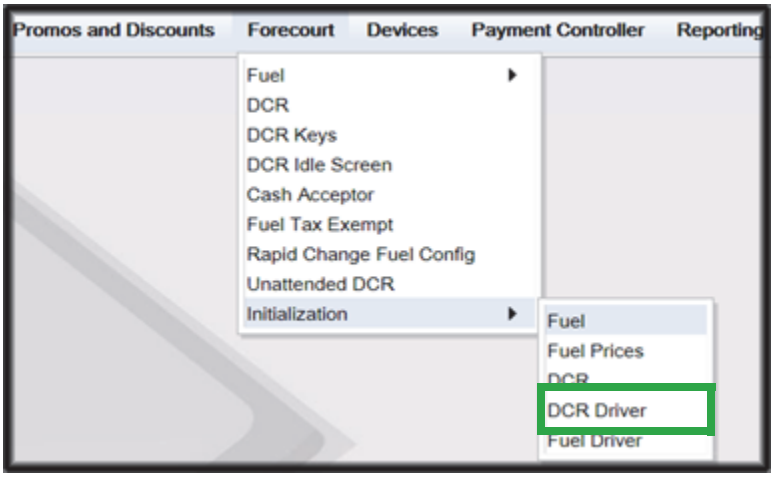
5. To initialize the Fuel Driver, navigate to Configuration Client > Forecourt > Initialization and then select Fuel Driver.



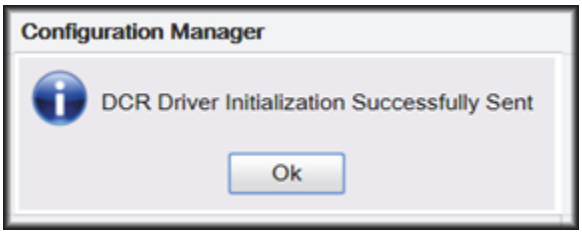
6. A message stating Fuel Driver Initialization Successfully Sent displayed. Select Ok



7. To initialize DCR Driver, navigate to Configuration Client > Forecourt > Initialization and then select DCR Driver



8. A message stating DCR Driver Initialization Successfully Sent displayed. Select Ok.



Check the dispensers to verify that they are loaded.

After they are all loaded, perform second DCR Driver initialization.

Again, check the dispensers to verify that they are loaded. Perform EMV transaction. If loaded and unable to perform an Outdoor EMV transactions, then go to next step.

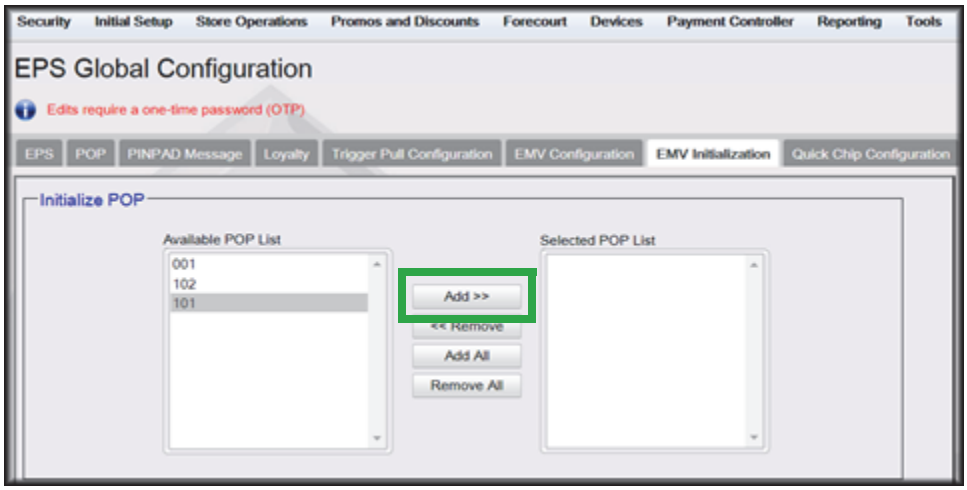
EMV Initialization

After the Commander has established communications with the Invenco DCR positions, it is required to perform an EMV Initialization.

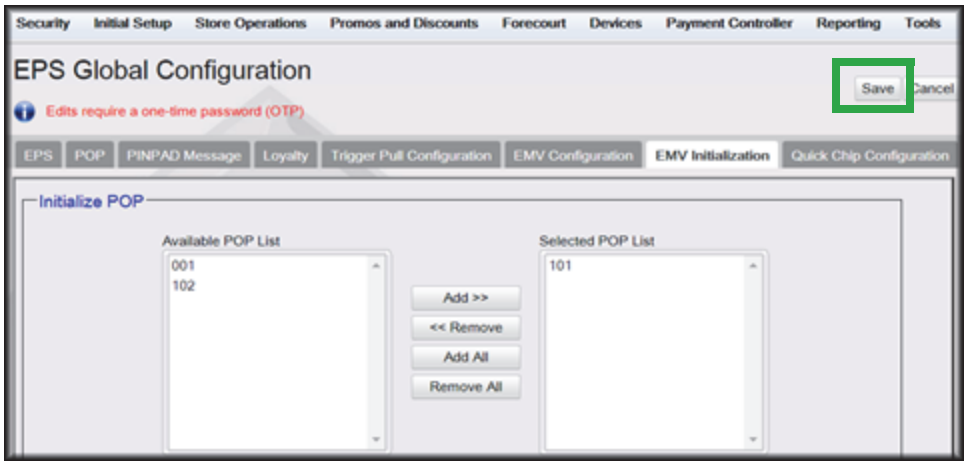
A DCR Driver Initialization must have been performed before starting the following steps. This will add DCR IDs to the Available POP List which can then be selected to receive the EMV Initialization.
An EMV Initialization does not perform a DCR Driver Initialization or a DCR Initialization.

1. Navigate to the Configuration Client > Payment Controller > EPS Global Configuration > EMV Initialization.
2. From the Initialize POP section locate the **Available POP List**.
3. For the DCR(s) requiring initialization, select the required DCR ID and click the **Add >** button to move it to the **Selected POP List**.

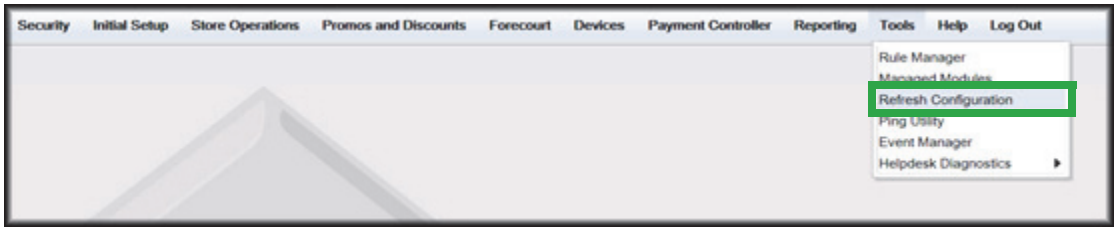
Outdoor card readers will be identified as POP 101, 102, 103, etc.



4. Repeat steps 2 and 3 for any additional DCR IDs.



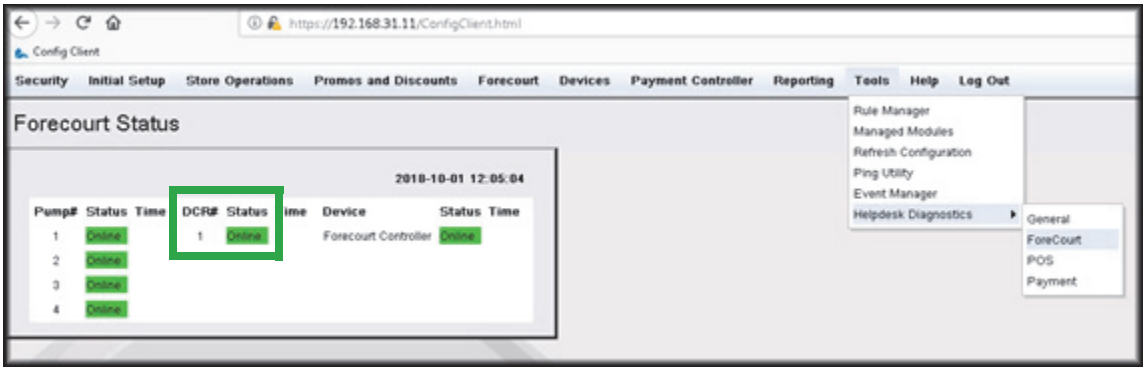
5. When finished selecting POP positions to be initialized, click Save. This performs an EMV POP initialization of the selected DCR positions.
6. If another EMV Initialization is required, first perform a Refresh Configuration.
7. Navigate to Configuration Client > Tools > Refresh Configuration. This updates the Available POP List contents. Repeat the EMV Initialization steps 1 through 5 above.



Verification of Forecourt Status

Use the following steps to verify IP based communications to the DCRs.

Navigate to Configuration Client > Tools > Helpdesk Diagnostics > Forecourt. The DCR Status should appear as “Online.” If they are offline, then communications to the DCRs have not been established. Recheck the connections and verify TCP/IP connectivity.



6 TROUBLESHOOTING GILBARCO DISPENSERS

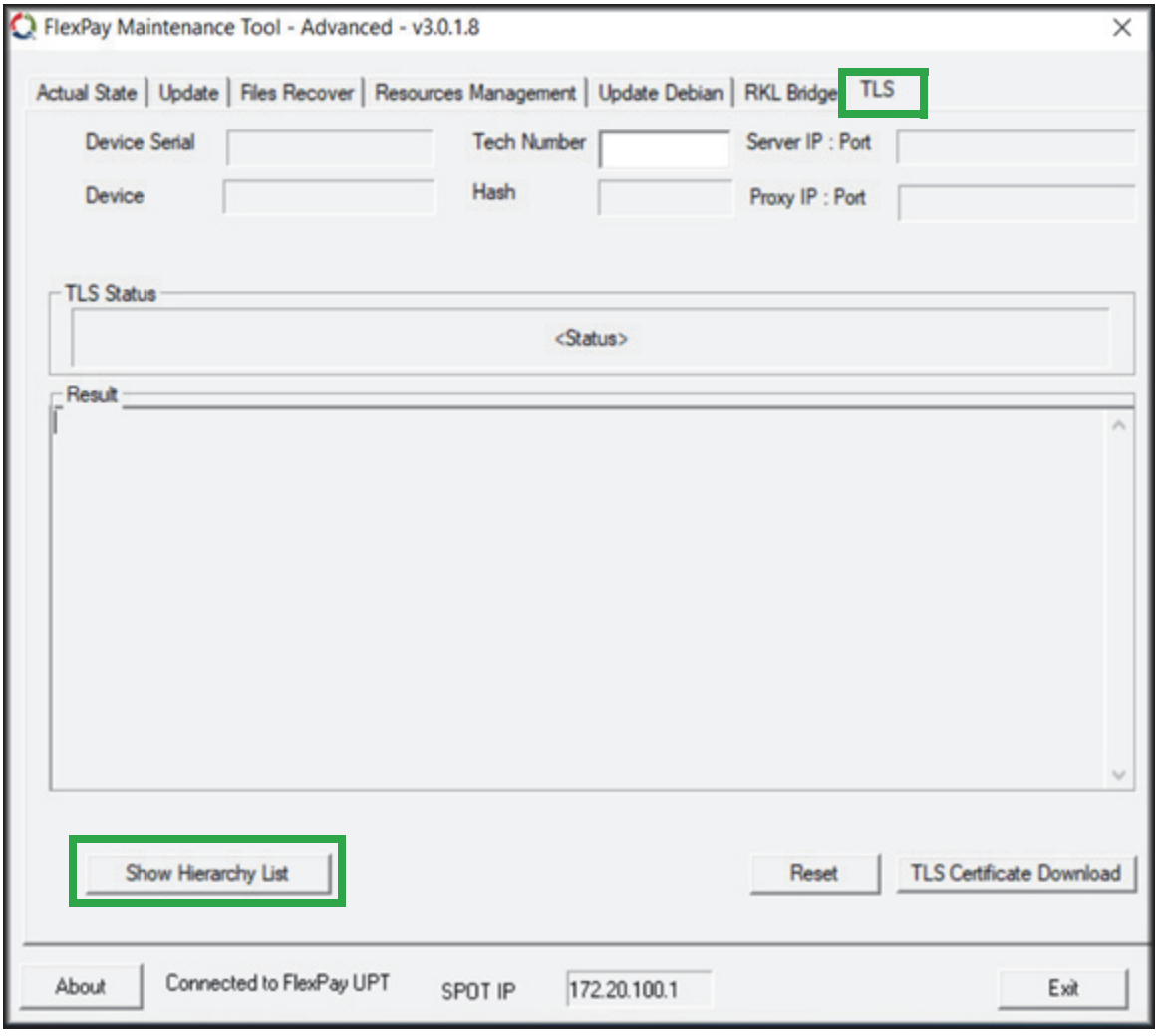
The information in this chapter is for reference only. Contact the Area of Responsibility (AOR) parties for up-to-date information.

Gilbarco FlexPay II CRIND

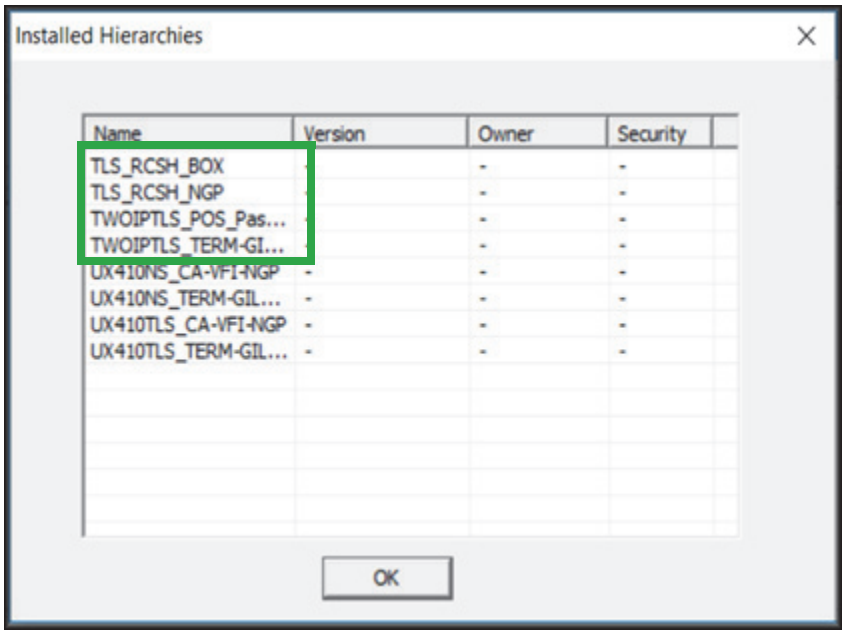
Verification of TLS Certification

The TLS Certification enhances a secure communication between the Gilbarco CRIND and Verifone Commander. Gilbarco FlexPay II CRIND does not always come loaded with a TLS Certification. Using the Advanced FlexPay Maintenance Tool, the TLS Certification can be verified and loaded if necessary.

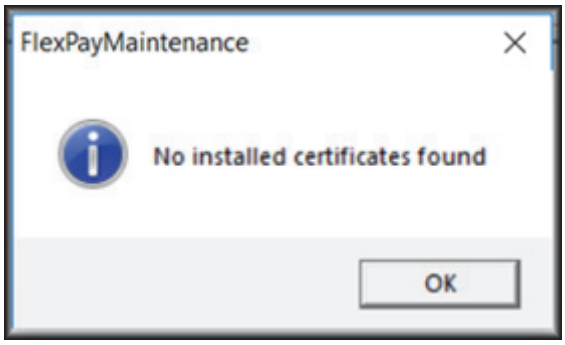
1. Open the FlexPay Tool and connect to the FlexPay Control Board.
2. Select the TLS tab.
3. Select Show Hierarchy List button.



4.If the TLS Certification is installed, the TLS files will be listed.



4. If the Certification is not installed, then the error window below displays. Contact Gilbarco for steps and instructions on how to install the TLS Certification in the Gilbarco CRIND.



Gilbarco FlexPay II CRIND

Verification of Single-Auth TLS Mode

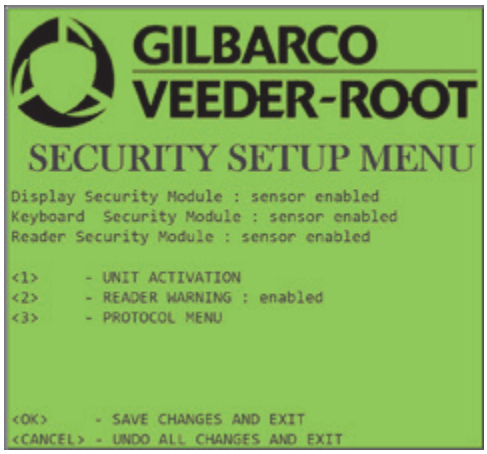
The TLS Certification enhances the secure communication between the Gilbarco CRIND and Verifone Commander. Gilbarco FlexPay II CRIND does not always come loaded with TLS Certification. Using the Advanced FlexPay Maintenance Tool, the TLS Certification can be verified and loaded if necessary.

1. Reboot the CRIND and enter Service Menu with dispenser password.

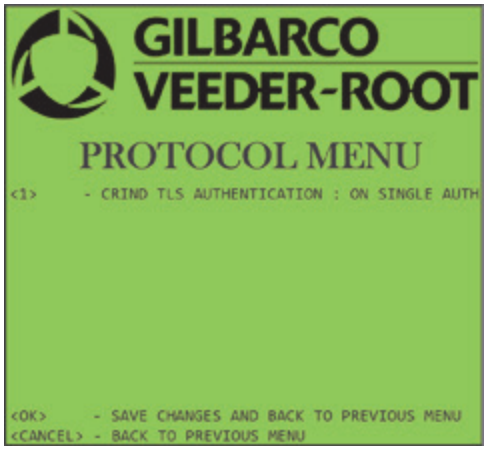
2. From the Service Menu, select option <3> Security Setup Menu.

3. Enter Matching Password. This requires a call to Gilbarco TAC.

4. After entering the Security Setup Menu, select <3> Protocol Menu.



5. Verify that option <1> CRIND TLS Authentication is set: ON SINGLE AUTH.

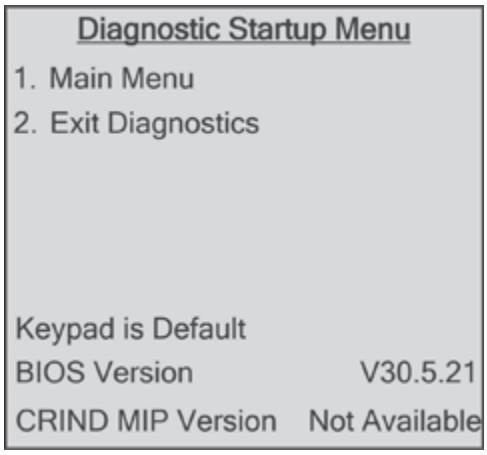


Gilbarco FlexPay II CRIND

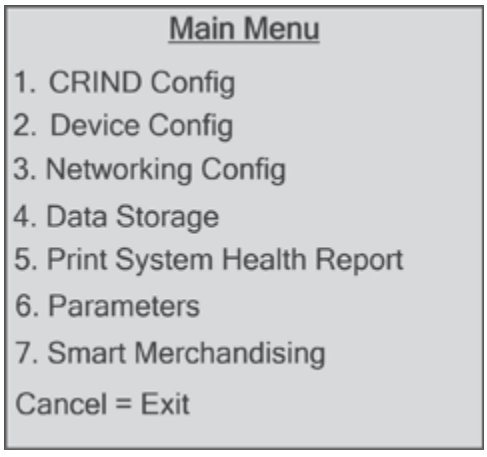
POS COMM set to IP

The outdoor EMV communication from the Verifone Commander to the CRIND is in the TCP/IP protocol. Previously Verifone Commander communicated in a SERIAL protocol. For the CRINDS to accept the TCP/IP protocol, the settings on the CRINDs needs to be changed.

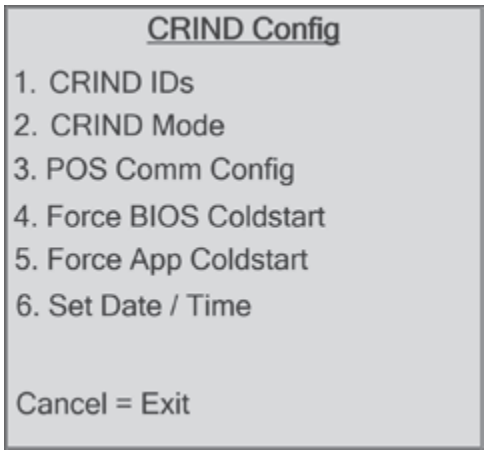
1. Using the Gilbarco Diagnostic, enter into Diagnostic Startup Menu.



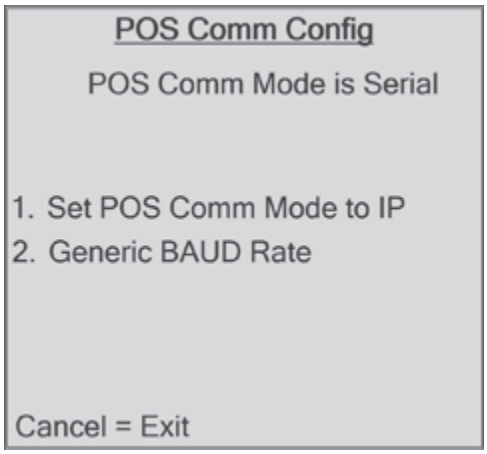
2. Press ‘1’ and Enter for Main Menu.



3. Press ‘1’ and Enter for CRIND Config.

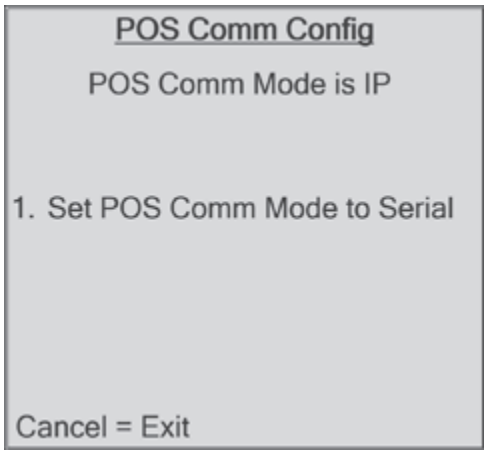


4. Press ‘3’ and Enter for POS Comm Config.

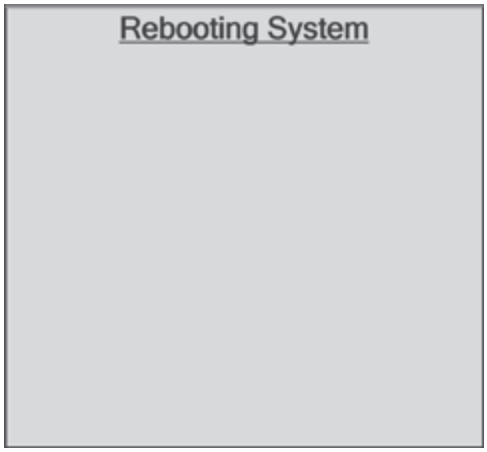


5. Press ‘1’ and Enter to Set POS COMM Mode to IP.

If the POS Comm Mode is already set to IP, then Cancel out of the POS Comm Config settings.



6. After the POS Comm Mode is set to IP, press the Cancel key until back at the Diagnostic Startup Menu.
7. Press ‘2’ and Enter to Exit the Diagnostics. This will warm reboot the CRINDS.

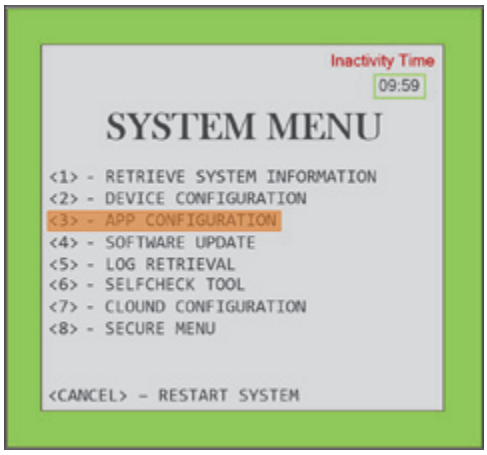


Gilbarco FlexPay IV CRIND

Verification of Single-Authorization TLS Mode

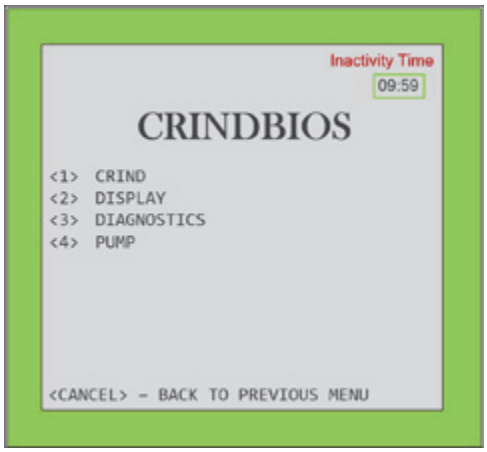
The TLS Certification enhances the secure communication between the Gilbarco CRIND and Verifone Commander. Gilbarco FlexPay II CRIND does not always come loaded with TLS Certification. Using the Advanced FlexPay Maintenance Tool, the TLS Certification can be verified and loaded if necessary.

1. Reboot the CRIND and enter the System Menu.

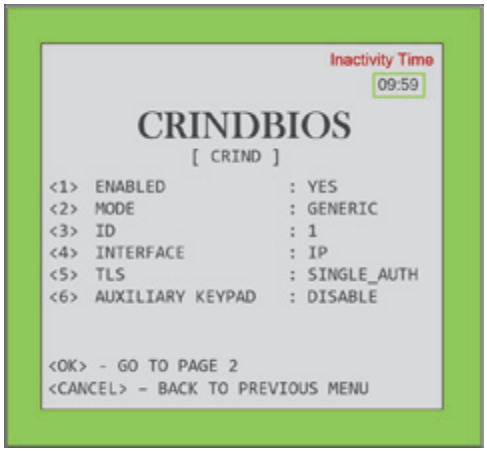


2. Select <3> App Configuration.

3. Select <1> CRINDBIOS.



4. Select <1> CRIND.



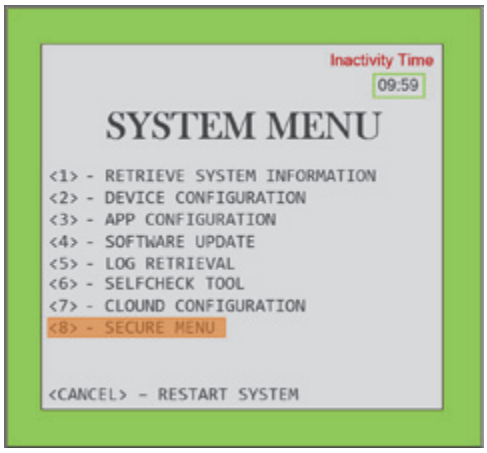
5. Verify the following two CRIND Settings:
   a. Option <4> INTERFACE: IP
   b. Option <5> TLS Mode: SINGLE_AUTH
6. If they are set, then Press <Cancel> all the way back to the System Menu.

Gilbarco FlexPay IV CRIND

Verify IP Interface

The outdoor EMV communication from the Verifone Commander to the CRIND is in the TCP/IP protocol. The previously Verifone Commander communicated in a SERIAL protocol. For the CRINDS to accept the TCP/IP protocol, the settings on the CRINDs needs to be changed

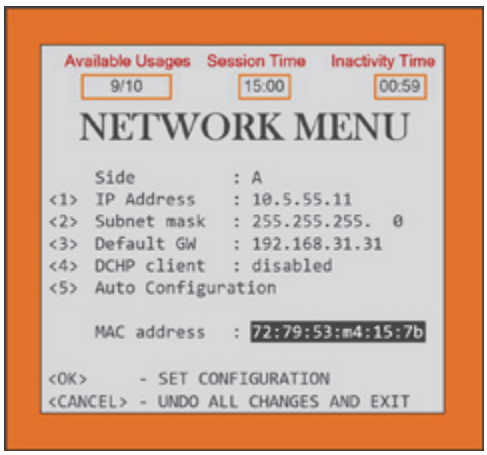
1. From the System Menu, select Secure Menu.



2. Call Gilbarco TAC and provide the CHALLENGE ## displayed on the screen for the unit and get the VERIFICATION CODE to enter SECURE MENU.

3. After entering Secure Menu, select <2> Network Menu.

4. Set all the TCP/IP info for the dispenser.



IP Address for the EMV CRIND CANNOT be on Verifone subnet.

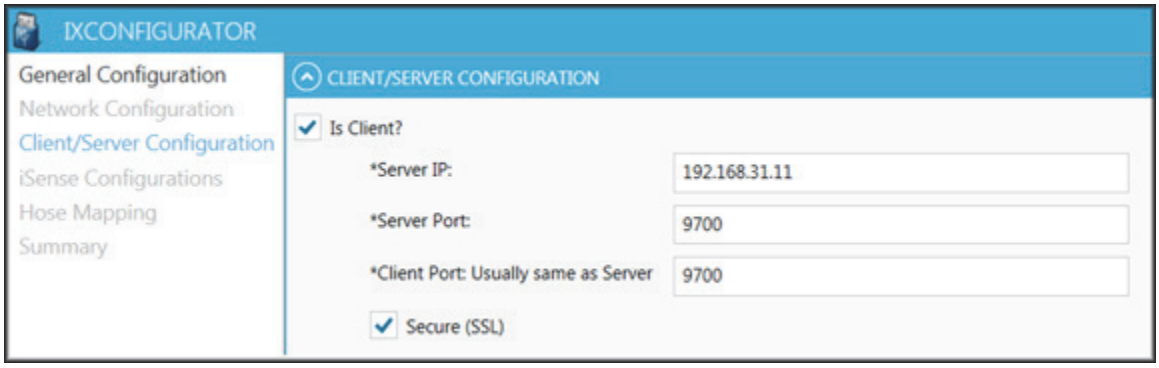
Consult IP scheme recommended by Gilbarco if it has not been pre-identified by the site.

5. Press <OK> to set configuration.

Wayne iX CAT Firmware

Client/Server Configuration

In the Wayne iX CAT Outdoor EMV Configuration, the Verifone POS is the SERVER and the Wayne iX CAT is the CLIENT. The Wayne iX CAT needs to communicate to the Verifone POS on Server PORT 9700. Using the Wayne iXConfigurator tool, set the Client/Server Configuration.



7 GLOSSARY OF TERMS

The following terms and definitions will assist with understanding the contents of the Feature Reference.

Term	Definition
AAC	Application Authentication Cryptogram. Generated whenever a card declines a transaction. This may be generated at the 1st or 2nd GenAC step.
AID	Application Identifier, specified by the acquiring host and used to identify the EMV applications that a system can support. Cards and terminals use AIDs to determine which applications are mutually supported, as both the card and the terminal must support the same AID to initiate a transaction. Both cards and terminals may support multiple AIDs.
ARC	Authorization Response Code indicates the transaction disposition of the transaction received from the issuer for online authorizations.
ARQC	Authorization Request Cryptogram. Generated by the card when it instructs the system to go online for an approval. An ARQC is generated at the 1st Gen AC step.
CAPK	Certificate Authority Public Key. The list of keys created by the card issuers used to support EMV cryptographic functions. Each card brand has CAPKs. These keys are loaded into the PIN Pad's during system startup and kept up to date by the system based on data exchanges from the acquiring host.
Contact EMV	An EMV transaction where the EMV card data is read by inserting a chipped card into the card reader slot on the PIN pad. The card remains inserted in the PIN pad for the duration of the transaction. The PIN pad and the card communicate several times during the course of a transaction.
Contactless EMV	See NFC, Near Field Communications.

Term	Definition
CVM	Cardholder Verification Method. The method that the card instructs the terminal to use in order to validate the cardholder. Consists of online PIN, offline PIN, Signature, and No CVM.
EMV	Europay, MasterCard, and Visa. The implementation-oriented global specifications regarding the use of chip card technology for the payments industry; established to ensure interoperability and acceptance of payment system Integrated Circuit Cards on a worldwide basis; the acronym refers to the three organizations that initially collaborated on the specification, now maintained by EMVCo. EMV is now analogous with payment cards with embedded security microchips. Within this document EMV is assumed to mean “Inside Contact EMV”.
EMV Kernel	A layer of software, specific to the hardware it is running on that handles the actual communication with the EMV chip on the card. It is versioned, it has an expiration date, and is certified by EMVCo.
EMV Tag	An EMV identifier. EMV data is maintained in tags – for example 8A and 9F12 are tags representing Authorization Response Code and Application Preferred Name respectively.
EPS	Electronic Payment Server
Fallback	Fallback in EMV terms means allowing a magnetic stripe swipe if the chip read fails. See Technical Fallback.
FEP	Front-End Processor
First Generate AC or 1st Gen AC	At a high level this is the stage in an EMV transaction where an approval is first requested from the card. Responses can be a TC (approved by the card), ARQC (request to go online for approval) or an AAC (decline).
Global AID	An AID that is owned by the global/international payment network whose logo is on the card. Global Payment Networks include American Express, Discover, MasterCard and Visa.
IAD	The Issuer Application Data (IAD) contains proprietary application data for transmission to the issuer in an online transaction.
ICC	Integrated Chip Card, or Integrated Circuit Card.

Term	Definition
Magnetic Stripe Fallback	See Technical Fallback.
MSA	Merchant Services Account.
MSD	Magnetic Stripe Data – The term is used to describe the legacy card entry method requiring a swipe of the card to read the magnetic stripe.
MSP	A merchant services provider (MSP) is an umbrella term that covers banks, third-party processors or any other entity that provides businesses and individuals with the products and services necessary to accept credit cards, debit cards and other forms of electronic payment.
MSR	Magnetic Swipe Read.
NFC	Near Field Communications is used to describe an EMV transaction where the EMV card data is read by tapping or waving the card above the PIN pad within the zone, allowing the card and the PIN pad to interact. The card is then removed from the zone and the transaction proceeds with no further Card to PINpad interaction.
PDL	Parameter Download. Some acquiring hosts supply configuration and other processing data via a PDL.
PIN	Personal Identification Number.
POP	Point of Purchase hardware, referring to MX800 Series and MX900 Series PINpads used to read EMV cards.
POS System	Includes the POS (Point of Sale) terminal(s), site controller and the electronic payment system (EPS).
Rapid Connect	Rapid Connect is a new payment interface that provides single point integration to all First Data payment platforms including Buypass.
RCI	Remote Configuration Interface.
RFID	Radio-Frequency Identification, a process where a transponder chip uses radio waves to communicate between a reader device and the chip. An RFID reader device (in this case, the DCR) transmits a radio pulse to the chip (in a mobile device), which responds with the payment information.

Term	Definition
RID	Registered Application Provider Identifier. The RID is a fixed length unique identifier allocated to each card scheme to identify EMV applications provided by that scheme. The schemes may then suffix this with an optional PIX to further differentiate between multiple products supported by the scheme, and together they form the AID.
STAN	The System Trace Audit Number which identifies the transaction number processed through the merchant account.
Stand-in	A process whereby a transaction may be approved locally according to specific transaction criteria even if the system cannot approve a transaction online.
Table Owner	The entity responsible for maintaining the VIPER tables. Depending on the FEP and the brand, this may be the major oil brand, the processor, Verifone, or a combination of Verifone and brand/processor.
TC	Transaction Certificate. Generated at the 2nd Gen AC step for approved transactions.
Technical Fallback	This is the exception process whereby the magnetic stripe, rather than the chip data, is read by an EMV-capable device.
Terminal ID	The PINpad terminal identifier.
TPP ID	Third Party Processor ID. This is an ID that uniquely identifies a particular version of a payment application and which also functions as the Project ID during the certification process. It is assigned when the project is created and follows the application through to the production environment.
TSI	Transaction Status Information.
TVR	Terminal Verification Results.
UMF	Universal Message Format. This is the XML based message format specification for the Rapid Connect application.
U.S. Common Debit AID	An AID that is owned by a global card brand, but can be licensed by a debit network. Discover, MasterCard, and Visa all provide a U.S. Common Debit AID.
VAP	Value Added Platform.
VIPER	Verifone's EPS payment processing application.

A DOCUMENTATION

Documentation

Any additional documentation required for the installation of outdoor EMV may be found on the Verifone Premier Portal (https://premier.verifone.com).

Documentation for updating the dispenser equipment can be obtained by the dispenser manufacturer.

Managed Network Service Provider documentation may be obtained through the Premier Portal under Manage > Petro Downloads > PC Utilities & Routers. If additional information is needed for the MNSP configuration, please contact the MNSP for this information.

B SUPPORT

Contact Information

*The Area of Responsibility (AOR) for customer/site area is owned, managed and configured by the **Managed Network Service Provider (MNSP) network administrator**. Installer should ensure there is bi-directional communication to and from the Forecourt between the VFI network and Dispenser network before beginning installation. Failure to do so will result in issues during setup*

For installations support, contact appropriate Area of Responsibility (AOR) via listed contact information. The following contact info may be needed during installation:

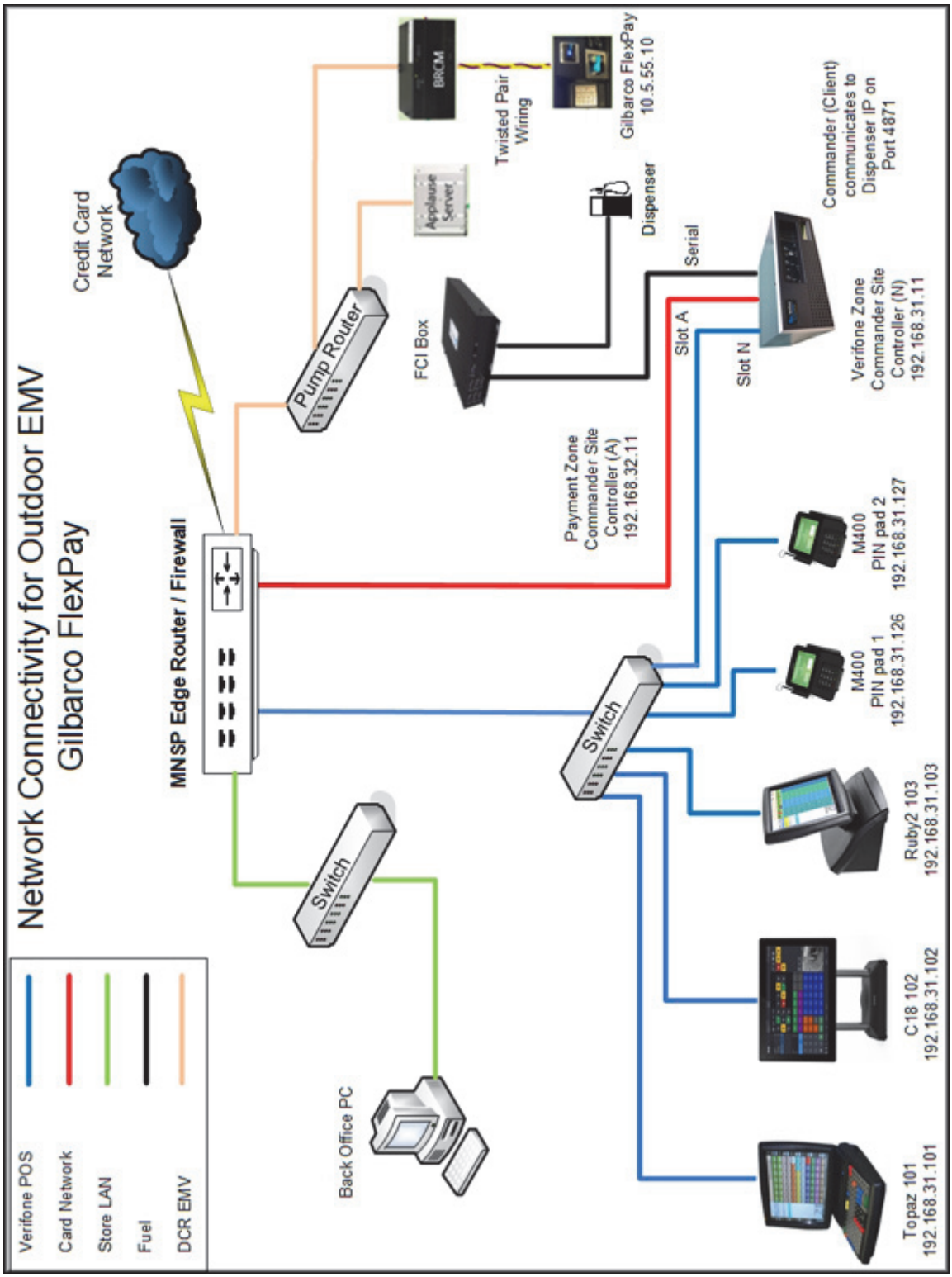
Verifone POS (AOR)	Phone number	Availability
Verifone VASC Helpdesk	888-777-3536	24/7

Dispenser (AOR)	Phone number	Availability
Gilbarco (TAC)	800-743-7501	24/7
Wayne/Dover	800-289-2963 (1 800 AT WAYNE)	
Invenco	877-515-0939	
Bennett	800-423-6638	

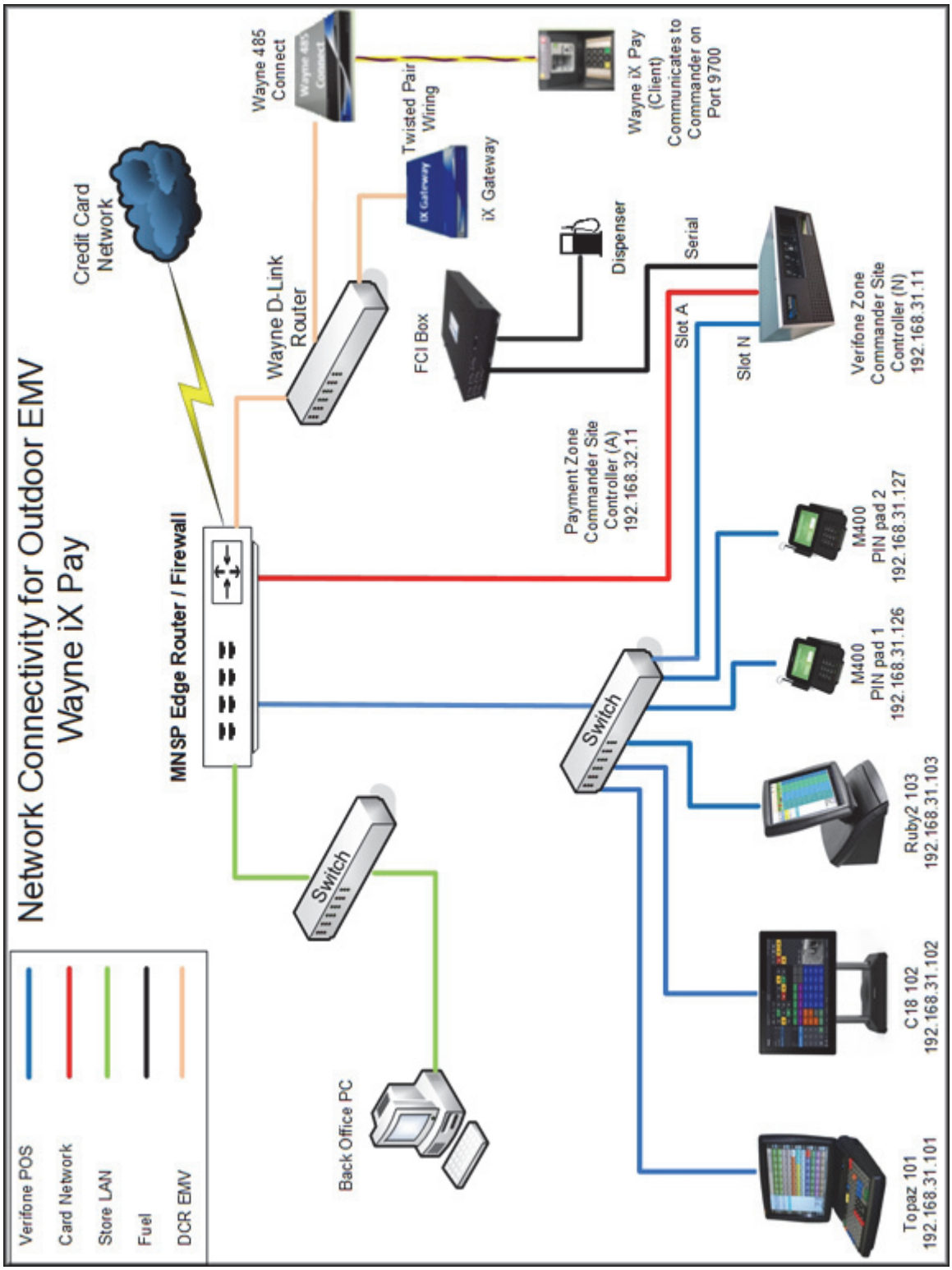
MNSP Network (AOR)	Phone number	Availability
Acumera	512-687-7401	24/7
AvaLAN	603-644-1461 Option 1	24/7
ControlScan	800-393-3246	24/7
Cybera	866-429-2372 Option 1	24/7
Hughes	866-350-8786	24/7
Mako Networks	844-807-0307 or 636-557-8888	24/7
Omega	610-639-7996 or 636-557-8888	24/7
SageNet	866-480-2263 or 918-505-2400	Monday - Friday 8:00am to 6:00pm CST
Transaction Network Services (TNS)	866-523-0661 or 800-240-4824, Option 5	24/7

C Diagrams

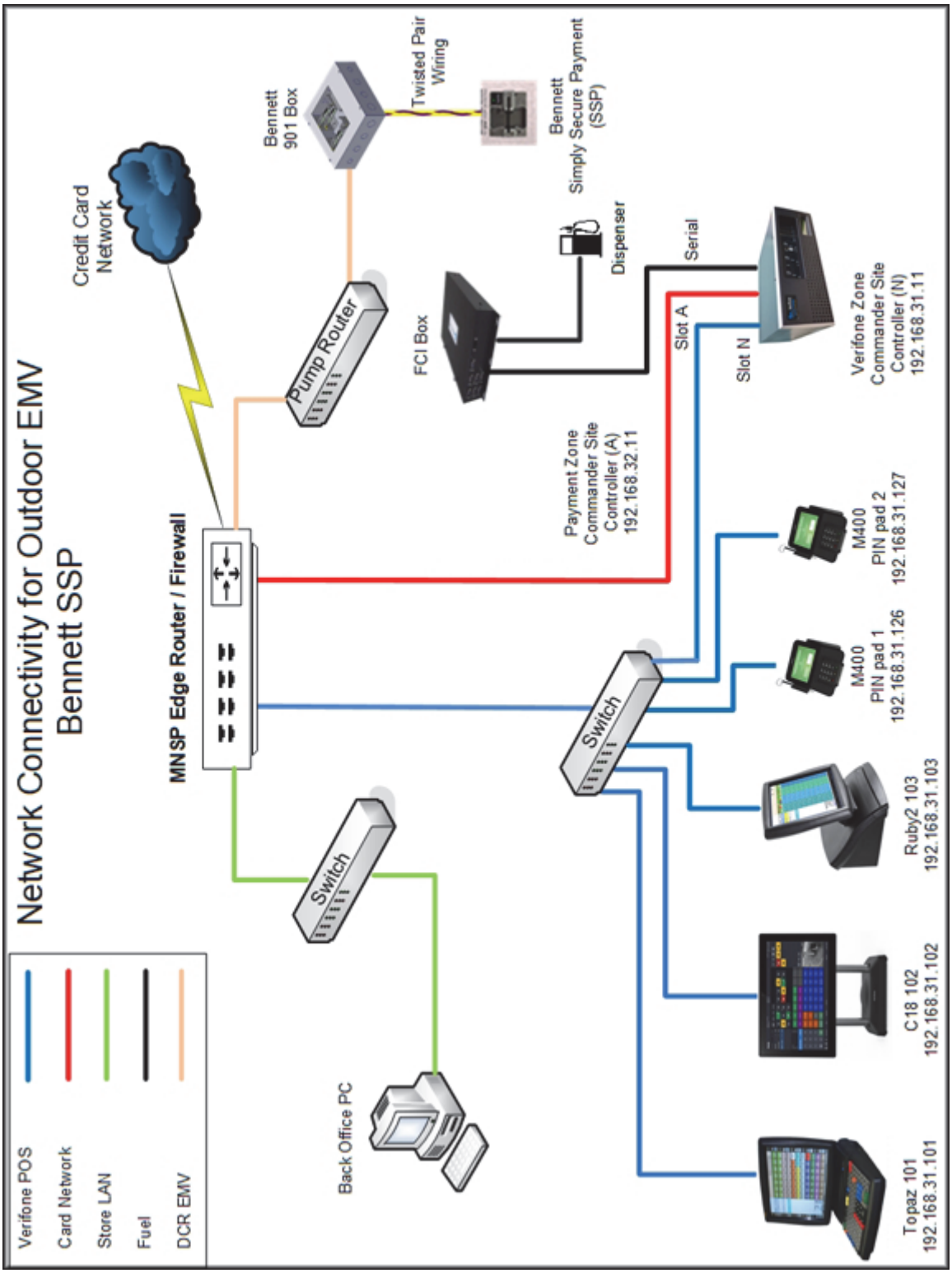
Gilbarco FlexPay with MNSP (AOR)



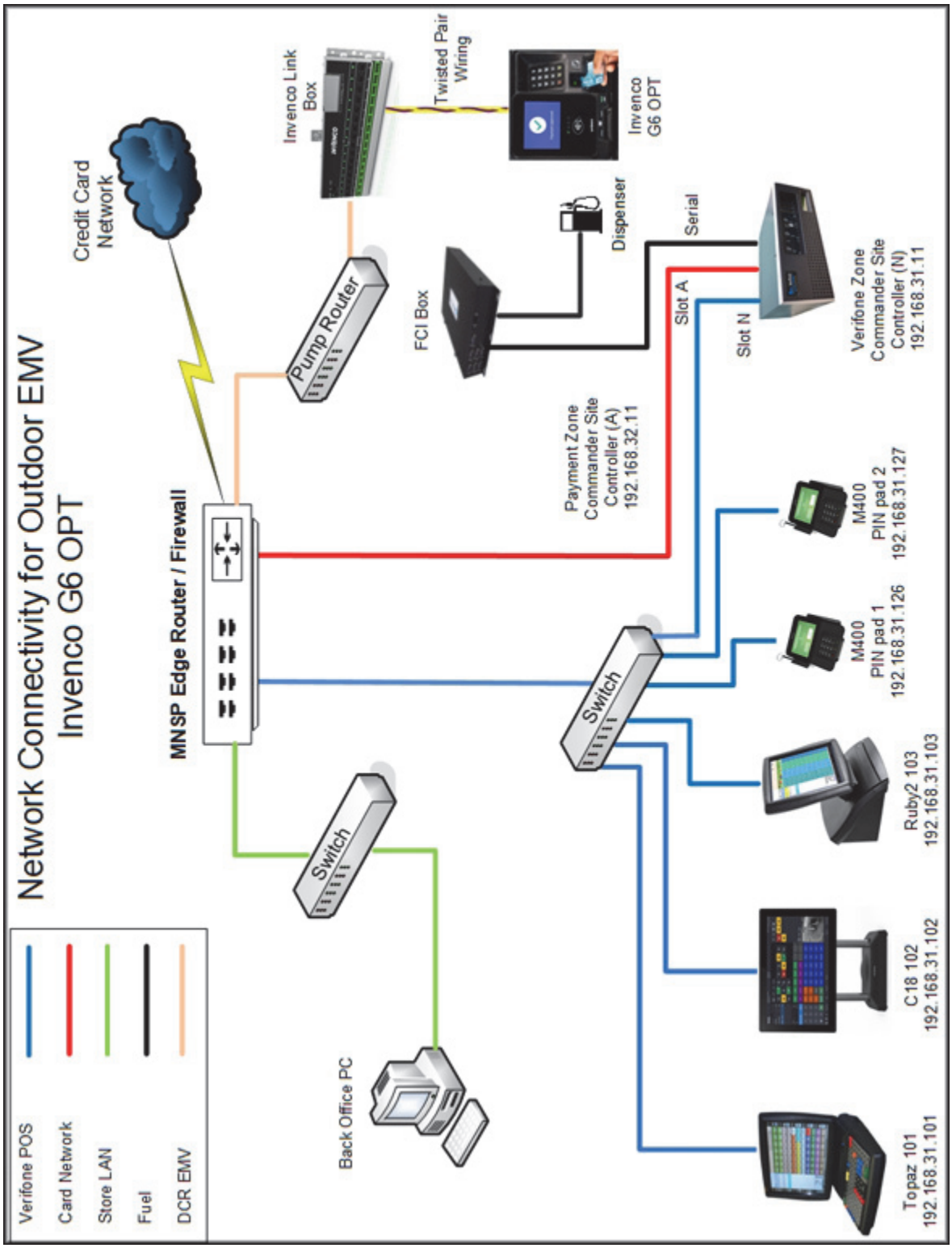
Wayne iX Pay with MNSP (AOR)



Bennett SSP with MNSP



Invenco G6 OPT with MNSP



D SHELL BRANDED SITES

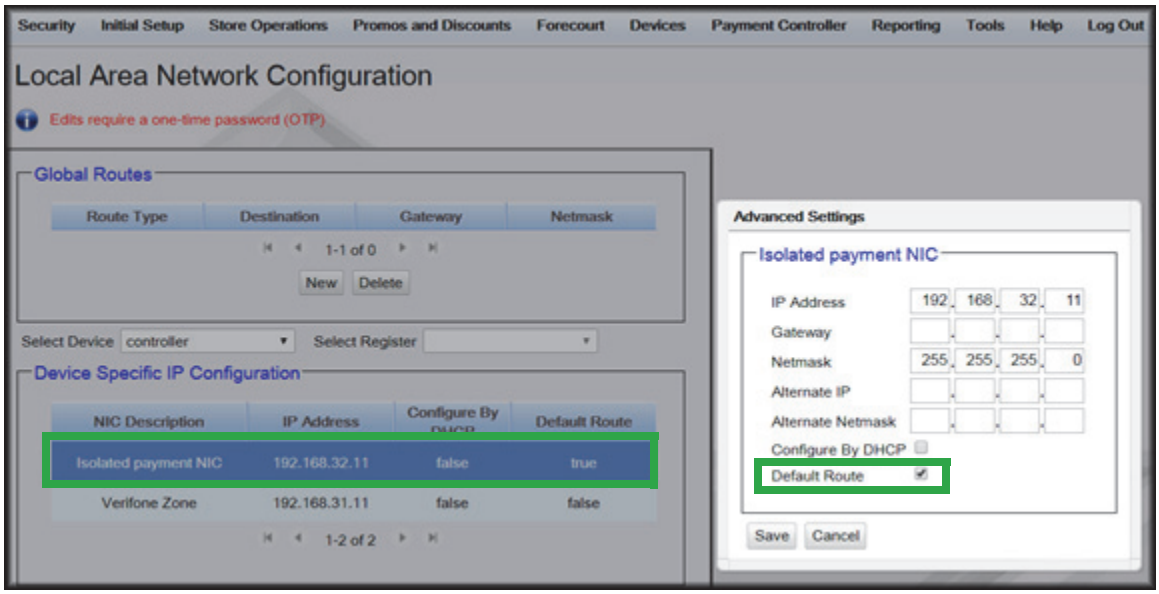
Gilbarco Local Area Network Configuration

The LAN needs to be configured for Gilbarco CRIND. In the Gilbarco configuration, the Commander is the CLIENT and the Gilbarco CRIND is the SERVER. The Outdoor EMV DCR IP traffic must be routed from Commander through the network IP of 192.168.31.31. Depending on which device specific IP configuration is selected for the site. Device Specific network routes might need to be added.

***For Shell branded sites with two routers MNSP**, see Shell Verifone Zone settings below. Follow the Isolated Payment NIC steps for Shell Single MNSP option.*

Isolated Payment NIC

1. In Configuration Client, navigate to Initial Setup > Local Area Network Configuration.
2. Select Isolated Payment NIC in Device Specific IP Configuration.
3. Verify if “Default Route” parameter is checked. If the parameter is checked then, continue to the next steps. If not checked, then skip to EPS Global Configuration Section.



Using the IP address entered in the EMV Parameter in DCR configuration, add a network destination route with the 4th octet (last) set to ZERO. i.e. 10.5.55.0. This should cover all the IP ranges from 10.5.55.1 through10.5.55.255.

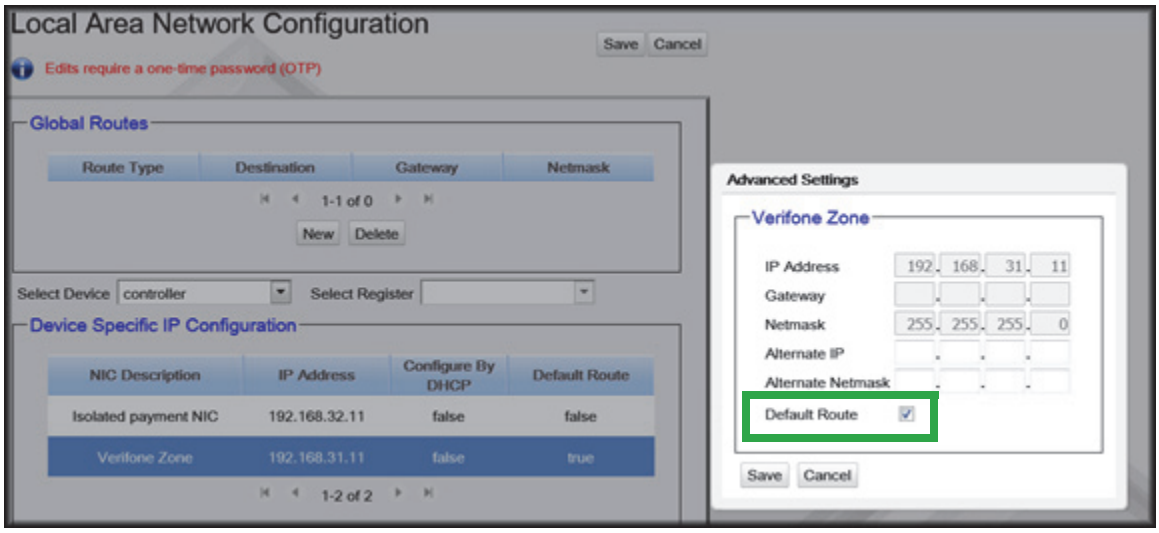
If Default Route is checked, then add New Route Config to the Device Specific Routes per site.

- **Route Type**: Network
- EMV Parameter IP Address (Forecourt > DCR > DCR Position Attributes) with the 4th octet set to 0.
- **Gateway**: 192.168.31.31
- **Netmask**: 255.255.255.0

4. Save the configuration changes and reboot the site controller.

Verifone Zone (Shell - Two router MNSP LAN Settings)

1. Verify if “Default Route” parameter is checked. If the parameter is checked then continue to next step.



Wayne Local Area Network Configuration

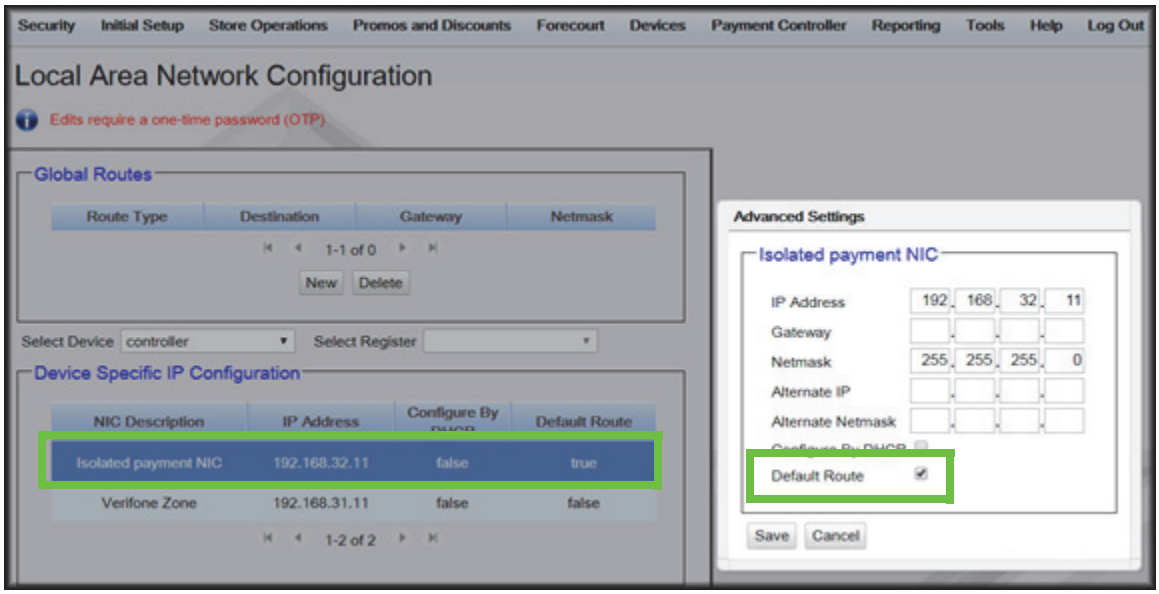
Verify Gateway IP addresses have been setup for EMV and the MNSP (Switch) Vendor has pushed the correct rules and polices.

The LAN is required to be configured for Wayne CAT. In the Wayne configuration, the Commander is the SERVER and the Wayne CAT is the CLIENT. The Outdoor EMV DCR IP traffic must be routed from the Commander through the Network IP Address 192.168.31.31. Depending on which Device Specific IP Configuration is selected for the site, Device Specific Network Routes may need to be added.

***For Shell branded sites with two routers MNSP**, see Shell Verifone Zone settings below. Follow the Isolated Payment NIC steps for the Shell Single MNSP option.*

Isolated Payment NIC

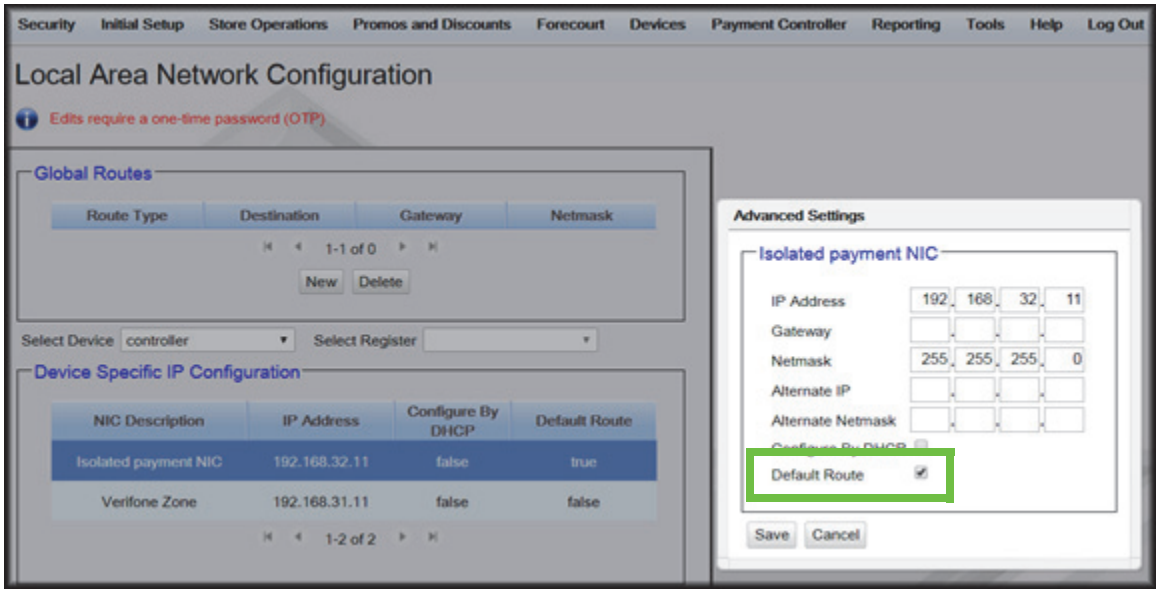
1. In Configuration Client, navigate to Initial Setup > Local Area Network Configuration.
2. Click on Isolated Payment NIC in the Device Specific IP Configuration.
3. Verify if the “Default Route” parameter is checked. If the parameter is checked, then continue with the next steps. If not checked, then skip to the EPS Global Configuration Section.



Using the Wayne DCR IP addresses, add a Network Destination Route with the 4th octet (last) set to ZERO. i.e. if the DCR IP addresses were 172.29.1.1. to 172.29.1.10, then the IP address used for this route would be 172.29.1.0.

4. If the Default Route is checked, then add New Route Config to the Device Specific Routes per site.
   a. **Route Type**: Network
   b. Enter in the IP address used for the DCRs with the last octet set to 0. See the note above for more details.
   c. **Gateway**: 192.168.31.31
   d. **Netmask**: 255.255.255.0

5. Click **Save** and then reboot the Commander.

Verifone Zone (Shell - Two router MNSP LAN Settings)

Verify if the “Default Route” parameter is checked. If the parameter is checked, then continue with the next section.