



GILBARCO
VEEDER-ROOT

MDE-5221J

October 2019

FlexPay™ IV CRIND® Start-up Manual



This page is intentionally left blank.



Table of Contents

SECTION 1 - INTRODUCTION **PAGES 1-2**

Purpose	1
Intended Users	1

SECTION 2 - IMPORTANT SAFETY INFORMATION **PAGES 3-4**

Important Safety Information	3
------------------------------------	---

SECTION 3 - FLEXPAYIV START-UP **PAGES 5-24**

Prerequisites	5
FlexPay IV Start-up	6
Configuring CRIND (Side A)	8
Secure Menu Configuration (CRIND Time, IP Addresses, and Activation)	11
Jumper Settings for DCM2.1/DCM2.2	14
Configuring CRIND IP Addresses for Units with SSoM	16
Configuring CRIND IP Addresses for Units without SSoM	18
Configuring CRIND (Side B)	20
Configuring Applause Media System	21
Completing Start-up	24

SECTION 4 - REFERENCE INFORMATION **PAGES 25-26**

Related Documents	25
Abbreviations and Acronyms	25

SECTION 5 - APPENDIX **PAGES 27-60**

System Screens	27
Service Menu Start-Up Screen	27
Maintenance Menu	30
System Menu	30
Retrieve System Information	31
Device Configuration	33
Application Configuration Screen	43
Software Update	47
Selfcheck Tool	48
Cloud	51
Secure Menu	51
Performing Maintenance Operations in Secure Menu	53

This page is intentionally left blank.

SECTION 1 - INTRODUCTION

Purpose

1

This manual provides start-up instructions for FlexPay™ IV CRIND®. The FlexPay IV CRIND provides an outdoor terminal platform that is EMV®-certified and Payment Card Industry PIN Entry Device (PCI-PED) certified.

For units with the Omnia board, use *MDE-5369 FlexPay IV (with Omnia) Programming and Service Manual* for start-up instructions. For SmartCRIND units, use *MDE-5366F SmartCRIND™ Installation and Startup Manual for SmartCRIND for FlexPay IV CRIND (M7)*.

Intended Users

This manual is intended for Gilbarco®-trained and certified Authorized Service Contractors (ASCs).

SECTION 1 - INTRODUCTION

1

This page is intentionally left blank.

SECTION 2 - IMPORTANT SAFETY INFORMATION

Important Safety Information

Notes: 1) *Save this Important Safety Information section in a readily accessible location.*

- 2) *Although DEF is non-flammable, Diesel is flammable. Therefore, for DEF cabinets that are attached to Diesel dispensers, follow all the notes in this section that pertain to flammable fuels.*

This section introduces the hazards and safety precautions associated with installing, inspecting, maintaining, or servicing this product. Before performing any task on this product, read this safety information and the applicable sections in this manual, where additional hazards and safety precautions for your task will be found. Fire, explosion, electrical shock, or pressure release could occur and cause death or serious injury, if these safe service procedures are not followed.



Preliminary Precautions

You are working in a potentially dangerous environment of flammable fuels, vapors, and high voltage or pressures. Only trained or authorized individuals knowledgeable in the related procedures should install, inspect, maintain, or service this equipment.

Emergency Total Electrical Shut-Off

The first and most important information you must know is how to stop all fuel flow to the pump/dispenser and island. Locate the switch or circuit breakers that shut off all power to all fueling equipment, dispensing devices, and Submerged Turbine Pumps (STPs).

⚠ WARNING

The EMERGENCY STOP, ALL STOP, and PUMP STOP buttons at the cashier's station WILL NOT shut off electrical power to the pump/dispenser. This means that even if you activate these stops, fuel may continue to flow uncontrolled.

You must use the TOTAL ELECTRICAL SHUT-OFF in the case of an emergency and not the console's ALL STOP and PUMP STOP or similar keys.

Total Electrical Shut-Off Before Access

Any procedure that requires access to electrical components or the electronics of the dispenser requires total electrical shut off of that unit. Understand the function and location of this switch or circuit breaker before inspecting, installing, maintaining, or servicing Gilbarco equipment.

Evacuating, Barricading, and Shutting Off

Any procedure that requires access to the pump/dispenser or STPs requires the following actions:



- An evacuation of all unauthorized persons and vehicles from the work area
- Use of safety tape, cones, or barricades at the affected unit(s)
- A total electrical shut-off of the affected unit(s)

Read the Manual

Read, understand, and follow this manual and any other labels or related materials supplied with this equipment. If you do not understand a procedure, call the Gilbarco Technical Assistance Center (TAC) at 1-800-743-7501. It is imperative to your safety and the safety of others to understand the procedures before beginning work.

Follow the Regulations

Applicable information is available in National Fire Protection Association (NFPA) 30A; *Code for Motor Fuel Dispensing Facilities and Repair Garages*, NFPA 70; *National Electrical Code (NEC)*, Occupational Safety and Health Administration (OSHA) regulations and federal, state, and local codes. All these regulations must be followed. Failure to install, inspect, maintain, or service this equipment in accordance with these codes, regulations, and standards may lead to legal citations with penalties or affect the safe use and operation of the equipment.

Replacement Parts

Use only genuine Gilbarco replacement parts and retrofit kits on your pump/dispenser. Using parts other than genuine Gilbarco replacement parts could create a safety hazard and violate local regulations.

Federal Communications Commission (FCC) Warning

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment.

Safety Symbols and Warning Words

This section provides important information about warning symbols and boxes.

Alert Symbol



This safety alert symbol is used in this manual and on warning labels to alert you to a precaution which must be followed to prevent potential personal safety hazards. Obey safety directives that follow this symbol to avoid possible injury or death.

Signal Words

These signal words used in this manual and on warning labels tell you the seriousness of particular safety hazards. The precautions below must be followed to prevent death, injury, or damage to the equipment:



DANGER: Alerts you to a hazard or unsafe practice which will result in death or serious injury.



WARNING: Alerts you to a hazard or unsafe practice that could result in death or serious injury.



CAUTION with Alert symbol: Designates a hazard or unsafe practice which may result in minor injury.

CAUTION without Alert symbol: Designates a hazard or unsafe practice which may result in property or equipment damage.

Working With Fuels and Electrical Energy

Prevent Explosions and Fires

Fuels and their vapors will explode or burn, if ignited. Spilled or leaking fuels cause vapors. Even filling customer tanks will cause potentially dangerous vapors in the vicinity of the dispenser or island. DEF is non-flammable. Therefore, explosion and fire safety warnings do not apply to DEF lines.

SECTION 2 - IMPORTANT SAFETY INFORMATION

No Open Fire



Open flames from matches, lighters, welding torches, or other sources can ignite fuels and their vapors.

No Sparks - No Smoking



Sparks from starting vehicles, starting, or using power tools, burning cigarettes, cigars, or pipes can also ignite fuels and their vapors. Static electricity, including an electrostatic charge on your body, can cause a spark sufficient to ignite fuel vapors. Every time you get out of a vehicle, touch the metal of your vehicle, to discharge any electrostatic charge before you approach the dispenser island.

Working Alone

It is highly recommended that someone who is capable of rendering first aid be present during servicing. Familiarize yourself with Cardiopulmonary Resuscitation (CPR) methods, if you work with or around high voltages. This information is available from the American Red Cross. Always advise the station personnel about where you will be working, and caution them not to activate power while you are working on the equipment. Use the OSHA Lockout/Tagout procedures. If you are not familiar with this requirement, refer to this information in the service manual and OSHA documentation.

Working With Electricity Safely

Ensure that you use safe and established practices in working with electrical devices. Poorly wired devices may cause a fire, explosion, or electrical shock. Ensure that grounding connections are properly made. Take care that sealing devices and compounds are in place. Ensure that you do not pinch wires when replacing covers. Follow OSHA Lockout/Tagout requirements. Station employees and service contractors need to understand and comply with this program completely to ensure safety while the equipment is down.

Hazardous Materials

Some materials present inside electronic enclosures may present a health hazard if not handled correctly. Ensure that you clean hands after handling equipment. Do not place any equipment in the mouth.

WARNING

The pump/dispenser contains a chemical known to the State of California to cause cancer.

WARNING

The pump/dispenser contains a chemical known to the State of California to cause birth defects or other reproductive harm.



Gilbarco Veeder-Root encourages the recycling of our products. Some products contain electronics, batteries, or other materials that may require special management practices depending on your location. Please refer to your local, state, or country regulations for these requirements.

In an Emergency

Inform Emergency Personnel

Compile the following information and inform emergency personnel:

- Location of accident (for example, address, front/back of building, and so on)
- Nature of accident (for example, possible heart attack, run over by car, burns, and so on)
- Age of victim (for example, baby, teenager, middle-age, elderly)
- Whether or not victim has received first aid (for example, stopped bleeding by pressure, and so on)
- Whether or not a victim has vomited (for example, if swallowed or inhaled something, and so on)

WARNING



Gasoline/DEF ingested may cause unconsciousness and burns to internal organs. Do not induce vomiting. Keep airway open. Oxygen may be needed at scene. Seek medical advice immediately.

WARNING

DEF generates ammonia gas at higher temperatures. When opening enclosed panels, allow the unit to air out to avoid breathing vapors. If respiratory difficulties develop, move victim away from source of exposure and into fresh air. If symptoms persist, seek medical attention.

WARNING



Gasoline inhaled may cause unconsciousness and burns to lips, mouth, and lungs. Keep airway open. Seek medical advice immediately.

WARNING



Gasoline/DEF spilled in eyes may cause burns to eye tissue. Irrigate eyes with water for approximately 15 minutes. Seek medical advice immediately.

WARNING



Gasoline/DEF spilled on skin may cause burns. Wash area thoroughly with clear water. Seek medical advice immediately.

WARNING

DEF is mildly corrosive. Avoid contact with eyes, skin, and clothing. Ensure that eyewash stations and safety showers are close to the work location. Seek medical advice/recommended treatment if DEF spills into eyes.

IMPORTANT: Oxygen may be needed at scene if gasoline has been ingested or inhaled. Seek medical advice immediately.

Lockout/Tagout

Lockout/Tagout covers servicing and maintenance of machines and equipment in which the unexpected energization or start-up of the machine(s) or equipment or release of stored energy could cause injury to employees or personnel.

Lockout/Tagout applies to all mechanical, hydraulic, chemical, or other energy, but does not cover electrical hazards.

Subpart S of 29 CFR Part 1910 - Electrical Hazards, 29 CFR Part 1910.333 contains specific Lockout/Tagout provision for electrical hazards.

SECTION 3 - FLEXPAY IV START-UP

Prerequisites

Before you proceed with the FlexPay IV startup:

- 1 Ensure that Windows® 7, Windows 8, or Windows 10 Operating Systems (OSs) are installed in the unit to run the FlexPay IV Maintenance Tool.
- 2 If using a Passport™ Point of Sale (POS), ensure that you have a minimum software version of V10 Service Pack P or later to support FlexPay IV CRIND.
- 3 Ensure that you establish the Internet Protocol (IP) scheme for the entire site before startup.
 - For information on CRIND IP scheme for units with Secure Systems on Module (SSoM), refer to [“CRIND IP Scheme for Units with SSoM”](#) on [page 16](#).
 - For information on CRIND IP scheme for units without SSoM, refer to [“CRIND IP Scheme for Units without SSoM”](#) on [page 18](#).
 - For information on units having Applause™ Media System, refer to [“Completing Start-up”](#) on [page 24](#).
- 4 Version 42.06.11 or later allows the use of the Gilbarco Diagnostic Card to enter CRIND programming (Maintenance Menu).

IMPORTANT INFORMATION



Applies to kits only: Both the Universal Payment Module (UPMs) by default have the same IP address. Unplug the UPM and the card reader Ethernet® connection on side B before power up to prevent an IP conflict. For factory-built units, the default IP addresses have already been set.

The CRIND IP scheme will match the default IP addresses for each dispenser on the forecourt.

SECTION 3 - FLEXPAY IV START-UP

FlexPay IV Start-up

3

IMPORTANT INFORMATION





During any power cycle, ensure that you leave the power off for at least five seconds before reapplying power. This gives all the devices time to fully shut down.

Note: For kits, ensure that the side B UX300 and UPM Ethernet cable is disconnected.

- 1 Isolate the two-wire connection from POS and any Ethernet/network connections.
- 2 When ready, turn on power to the dispenser.
- 3 Ensure that the printer paper is loaded into the CRIND Universal Serial Bus (USB) printer.
- 4 Once the Gilbarco Veeder-Root® white screen is displayed, press **1** to enter setup (displayed in left bottom portion of CRIND screen). After the blue System Online screen, when CRIND BIOS is running, swipe the Gilbarco Diagnostic Card to enter CRIND programming.

Note: Version 42.06.11 or later allows the use of the Gilbarco Diagnostic Card to enter CRIND programming (Maintenance Menu).

Figure 1: Software and Hardware Versions

<p>VGD= Vanguard platform Firmware version 003D = boot version/FPGA version 03101 = OS version 40005 = Pinpad version 1501E = Verifone FWR version 03GC001 = Resource Package version 32F4 = Single resources version APP = Vanguard platform applications version CLD002=Cloud version CRB001= Crindbios version DIA006 = Diagnostic package version DM001= Display Manager version EMV001 = EMV package version OPT005 = OPT package version UPM = Vanguard platform hw version</p>	 <p>GILBARCO VEEDER-ROOT</p> <p>VGD..003D..03101..40005..1501E..03GC001-32F4DEV APP..CLD002..DIA006..DM001..EMV001 APP..OPT005</p> <p>UPM.....</p> <p><--></p>	<p>VGD= Vanguard platform Firmware version 005D = boot version/FPGA version 03101 = OS version 50009 = Pinpad version 1501F = Verifone FWR version 03GU007 = Resource Package version 0 = 0 = D795 = Single resources version APP = Vanguard platform applications version CLD002=Cloud version CRB001= Crindbios version DIA006 = Diagnostic package version DM002= Display Manager version EMV001 = EMV package version OPT006 = OPT package version PEX001 = printer extender package version UPM = Vanguard platform hw version</p>	 <p>GILBARCO VEEDER-ROOT</p> <p>VGD..005D..03101..50009..1501F..03GU007..0..0-D795 APP..CLD002..CRB001..DIA006..DM002 APP..EMV001..OPT006..PEX001</p> <p>UPM..04..0E..1446..00000000GNJ00083</p> <p><1> enter setup</p>
<p>(i)</p> <p>Software Version 42.06.XX</p> <p><i>Note: This is an example only; software version numbers will vary.</i></p>		<p>(ii)</p> <p>Software Version 42.11.XX/52.10.06 or Higher (PCI 5)</p>	

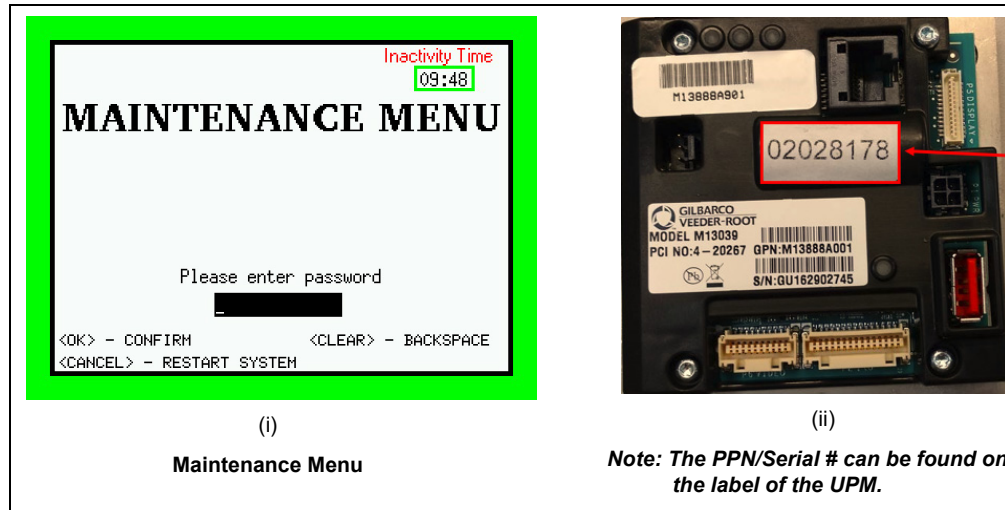
SECTION 3 - FLEXPAY IV START-UP

- 5 On the Maintenance Menu screen, the “**Please enter password**” message is displayed. Enter the last six digits of the Product Part Number (PPN), for example, 028178 (printed on the UPM label).

Notes: 1) The PPN is displayed for about 10 seconds during the boot up process.

2) Main menu timeout is 10 minutes of inactivity. (An unused menu number can be pressed on the keypad to reset the timer.)

Figure 2: Entering Password



Note: When starting up the system, there is a software version control in the UX300 card reader. If the software version is not up-to-date, it will be updated during the boot up process when the card reader IP address has been assigned (update can take up to 10 minutes). A yellow pop-up window will be displayed (see [Figure 3](#)).

Figure 3: Secure Device Update in Progress



SECTION 3 - FLEXPAY IV START-UP

Configuring CRIND (Side A)

Note: Side A is where the calibration switch is located.

3

IMPORTANT INFORMATION



(For kits only) - Ensure that the side B card reader and UPM Ethernet cable are disconnected before configuring the CRIND. Factory-built dispensers have a default IP set and do not require disconnecting the side B card reader and UPM cables.

Note: The following steps are in an order as applicable for Software Version 42.06.XX. Information about options for different versions of software is indicated in the following table:

Software Version	Refer to the following instructions
42.06.XX (PCI 4)	"Device Selection" on page 34.
42.11.XX (PCI 4)	"Device Selection" on page 34.
52.10.XX (PCI 5)	"Device Selection" on page 34.

To configure the CRIND, proceed as follows:

- 1 On the Device Selection screen, select <1> Contact Card Reader.
Note: When configuring devices or adding CRIND option kits (for example, adding contactless kits), run a test in a Selfcheck menu, make sure the device is turned ON in the POS, and verify any network configuration changes.
- 2 Press <2> UX300 Reboot. The options available are: scheduled/default. Scheduled means that the Daily Check (DC) is performed at the local time set in steps 3 and 4. Default means that the DC is performed by the unit 24 hours after the latest DC.
- 3 Press <3> UX300 Reboot Hour. The option available is: 00 to 23. This configuration option sets the hour in local time when the DC will be performed on the UX300.
Note: Option 24 is not available.
- 4 Press <4> UX300 Reboot Min. The options available are: 00 - 15 - 30 - 45. This configuration option sets the minutes of the hour in local time when the DC will be performed on the UX300.
- 5 Press <5> PRINTER PORT. The options available are: NONE/USB. This configuration option sets the printer configuration. If no printer is available, the configuration must be set to NONE.
- 6 Press <6> BARCODE. The options available are: NONE/GVR-SCANNER. This configuration option sets the 2D barcode scanner. The configuration must be set as GVR-SCANNER if a 2D scanner is present.
Note: M7 does not have a 1D scanner option.
- 7 Press <7> Bank Note Acceptor (BNA) DEVICE. The options available are: NONE/YES. This configuration option sets the BNA. The configuration must be set as YES if a JCM or SODECO MEI is present.
- 8 Press **OK** to move to the next page.

SECTION 3 - FLEXPAY IV START-UP

*Note: To return to the previous menu, press **Cancel**.*

- 9 Press <1> Transmitter/Receiver in Dispenser (TRIND®) READER. The options available are: NONE/YES. This configuration option is about the TRIND reader [specific for North America (NA) customization]. The configuration must be set as YES, if present.

*Note: To return to the previous menu, press **Cancel**.*

- 10 On the System Menu screen, select <3> APP CONFIG.

Note: For units in Canada with Software Version 42.06.14 or higher installed, the App Config menu is present but functions are not available.

- 11 On the App Config screen, select <1> CRINDBIOS.

- 12 Press <1> CRIND.

- 13 In the CRIND menu, set CRIND **MODE**, CRIND **ID** (any numeric value entry requires pressing OK/Enter to accept the value), and set E700 Compatibility to **ENABLE**, leaving BAUD RATE at 4800 and set Display Security check to **ENABLE**.

Note: If set to the incorrect BAUD RATE, POS communications will fail.

- 14 Follow instructions at the bottom of the screen, and then press **CANCEL** to exit.

- By default, Predictor is set to **ENABLE**. Change the setting to **DISABLE**.
- Leave personality screen set to default.

- 15 Select <3> DIAGNOSTICS.

- 16 In DIAGNOSTICS, leave LOG LEVEL to default setting "INFO".

- 17 Leave TWO-WIRE DEBUG to default setting "Disable".

- 18 Set PURGE to **ENABLE** (this purge will prepare for a clean POS download).

Note: Leave Factory Reset as disabled. If the screen displayed does not match the display size, then set Factory Reset as Enable; You can re-program the CRIND BIOS settings after next restart.

- 19 Press **CANCEL** one time to go back to the **CRIND BIOS** screen.

- 20 Select <4> **PUMP**, <1> **PUMP ID**. Entering the pump ID prevents the card reader security screen from being displayed during fueling.

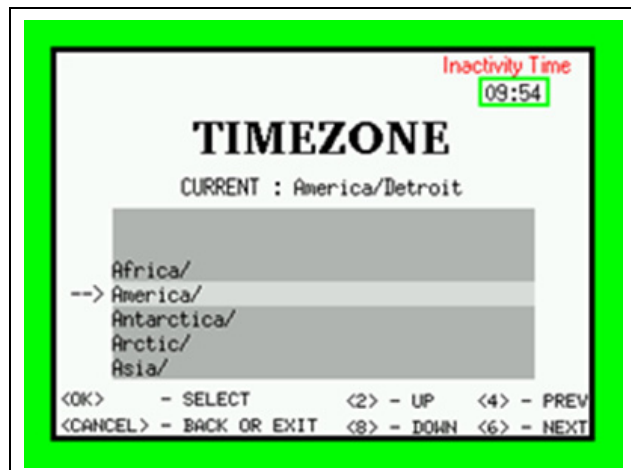
Note: The pump ID and CRIND ID do not always match.

SECTION 3 - FLEXPAY IV START-UP

If the Coordinated Universal Time (UTC) local Date and Time is set in the secure menu, then skip the next step and proceed to step 22. Timezone setting must be set to default Etc/UTC.

- 21 Set up the time zone using the keypad function; it is recommended to select the time zone value based on the installation location. If a time zone is not set, the default setting is UTC.

Figure 4: Timezone Menu



- 22 Press **CANCEL** several times until the unit goes through a complete warm-start.

Note: If no configuration changes stop at System Menu screen, then proceed with “Secure Menu Configuration (CRIND Time, IP Addresses, and Activation)” on page 11.

- 23 Press **1** on the white Gilbarco screen to enter setup again once the unit reboots. Proceed to “Secure Menu Configuration (CRIND Time, IP Addresses, and Activation)” on page 11.

SECTION 3 - FLEXPAY IV START-UP

Secure Menu Configuration (CRIND Time, IP Addresses, and Activation)

Notes: 1) Unit will be shipped from the factory with UPM and card reader deactivated. It is important to follow the procedure for best results.

2) Secure Menu timeout is 60 seconds in case of inactivity. Pressing a number that is not on the Secure Menu (for example 9) will reset the timer back to 60 seconds.

3) For information on IP scheme, refer to the following:

- “CRIND IP Scheme for Units with SSoM” on page 16 for units with SSoM
- “CRIND IP Scheme for Units without SSoM” on page 18 units without SSoM
- “Configuring Applause Media System” on page 21 for units with Applause Media System

To configure the Secure Menu, proceed as follows:

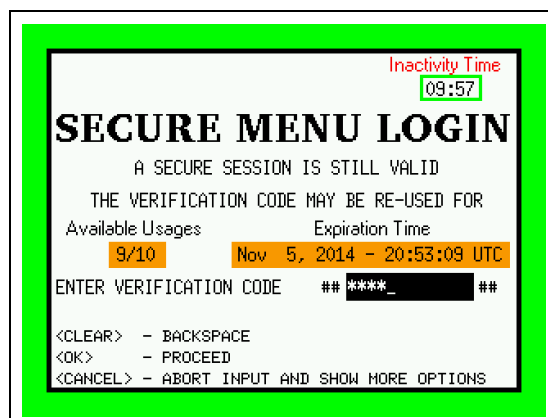
1 Press <1> to enter setup (if not in the System Menu); the System Menu is displayed.

2 From the System Menu, select <8> SECURE MENU.

Notes: 1) The screen border color is orange in secure screens.

2) From the Secure Menu, set the CRIND Time and Date, IP addresses, and System Activation.

Figure 5: Secure Menu Login



SECTION 3 - FLEXPAY IV START-UP

- 3 Call Gilbarco Support Center at 1-800-800-7498 (or use the Gilbarco Online Activation Tool) and obtain a verification code. Provide Gilbarco with a challenge number and the check digit after verifying that the check digit matches with the one on the screen. Provide the eight-digit PPN. Gilbarco will provide a verification code.

3

IMPORTANT INFORMATION

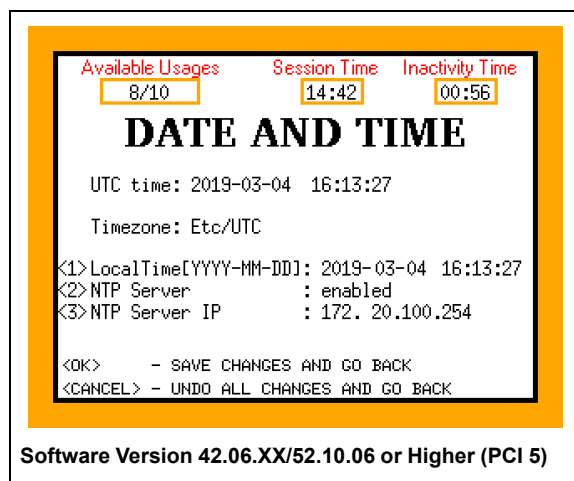
Write down the verification code number on the worksheet provided in the manual (refer to “[Completing Start-up](#)” on [page 24](#)). It can be reused before system activation (usable for 10 secure screen entries within a 12-hour period). Once the activation is complete, any entry into a secure screen will require a new verification code from Gilbarco.



Note: Place the worksheet in an accessible location for a future visit.

- 4 To set the time manually, press **1**. To set the time and date from the NTP Server (if instructed by the customer), select **enabled** and enter the IP address of the NTP server.

Figure 6: Date and Time Menu



*Note: Pressing **Enter** will tab to the next field.*

- 5 Press **OK** to save changes.
- 6 Select **<3>** to perform System Activation. Follow instructions on the CRIND screen to perform the activation. You will see three modules on the CRIND screen.

Note: To perform a system activation, the UPM and card reader should have a paired IP address. The card reader will have an IP + 1 of the UPM.

The following are typical results before activation (displayed on the screen):

- Display Module: Enabled
- UPM Security Module: Disabled
- Reader Security Module: Disabled

SECTION 3 - FLEXPAY IV START-UP

7 Select <1> UNIT ACTIVATION (in a few seconds, the unit displays the message, “All dismounting sensors enabled - unit activated”). The following are typical results after successful activation (displayed on the screen):

- Display Module: Enabled
- UPM Security Module: Enabled
- Reader Security Module: Enabled

After you have a successful activation, a new verification code is required from Gilbarco to enter the Secure Menu again.

In case the following error messages are displayed, refer to the action/explanation provided against them for troubleshooting.

Symptom	Action/Explanation
Reader Security Module shows “ERROR”	This does not necessarily mean the card reader is defective. It can take up to 2-3 minutes for the card reader and the UPM to sync after the card reader IP is set. The main thing to look for is the pop-up screen that says “All dismounting sensors enabled-unit activated”.
“Disabled” status is displayed on any of the three modules	Troubleshoot and restart the activation process. Look for dismount switch problem on the UPM or card reader, or look for a display cable problem if Display Module = disabled.
Error message is displayed in any one of the three modules	Refer to <i>MDE-5223 FlexPay IV CRIND Service/Troubleshooting Guide</i> .

8 Once the unit is successfully activated, proceed to configuring IP addresses for the peripherals of the unit:

- To configure IP addresses for units with SSoM, refer to [“Configuring CRIND IP Addresses for Units with SSoM”](#) on [page 16](#).
- To configure IP addresses for units without SSoM, refer to [“Configuring CRIND IP Addresses for Units without SSoM”](#) on [page 18](#).
- Refer to [“Configuring Applause Media System”](#) on [page 21](#) for units with Applause Media System.

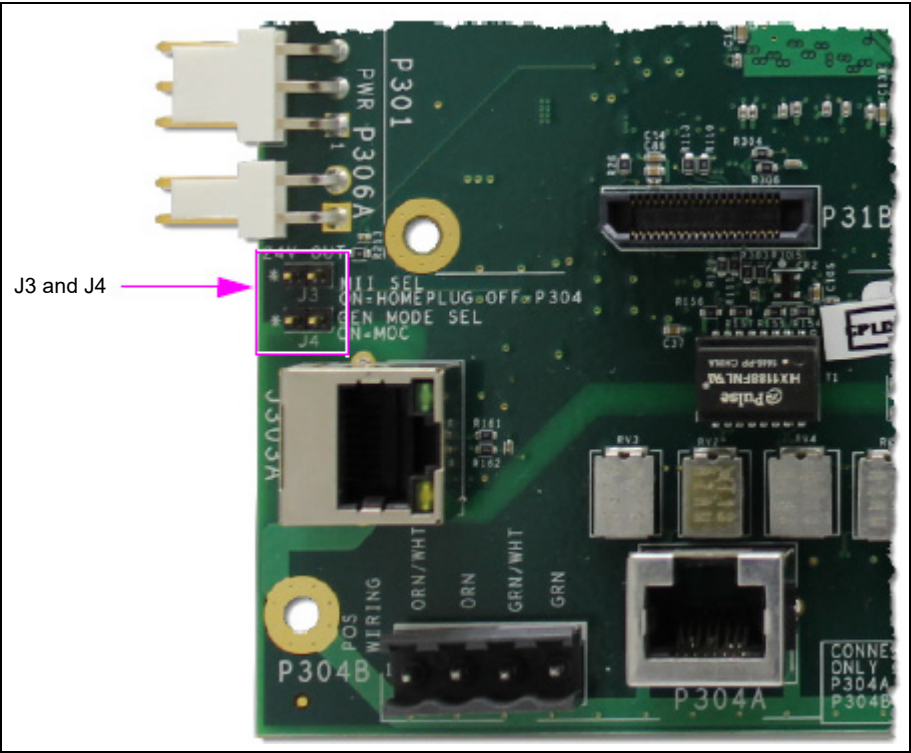
SECTION 3 - FLEXPAY IV START-UP

Jumper Settings for DCM2.1/DCM2.2

The following table describes jumper settings for Dispenser Communication Module (DCM)2.1/DCM2.2:

Jumper	ON	OFF	Function
J3	X		High-speed connection active. P304 A/B disabled.
		X	High-speed connection inactive. P304A and P304B connects to Category 5 (CAT5) running through the conduit for high speed connection (if used).
J4	X		Unit is connected to a Passport POS Major Oil Company (MOC)
		X	Unit is connected to a third party POS (Generic)
J5	X		VLAN is enabled (DCM2.2 only)
		X	VLAN is disabled (DCM2.2 only)
J6	B		Install the Jumper on the B position for the 45 mA Current loop (DCM2.2 only)

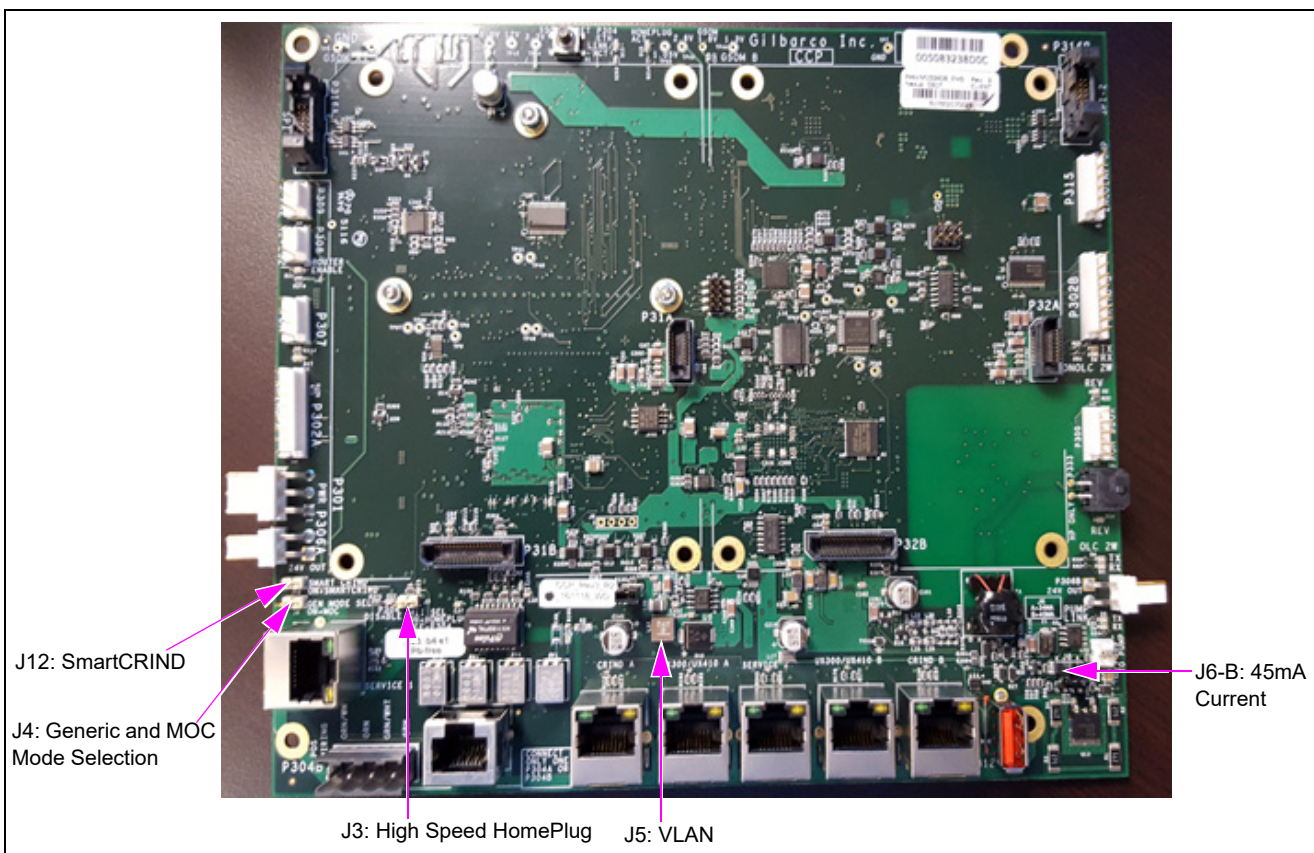
Figure 7: M15399A001 DCM2.1



SECTION 3 - FLEXPAY IV START-UP

Figure 8: M15737A001 DCM2.2 Assembly

3



SECTION 3 - FLEXPAY IV START-UP

Configuring CRIND IP Addresses for Units with SSoM

To configure CRIND IP addresses for units with SSoM, proceed as follows:

- 1 Press <2> to go to the **Network Menu**. Press <1> to set CRIND IP addresses according to the following IP scheme.

*Notes: 1) Pressing **Enter** moves the cursor to the next field.*

2) IP scheme may vary depending on the customer's IP scheme requirements.

3) The Gilbarco Systems on Module (GSoM) IP Addresses can only be configured from Side A (see [Figure 28](#) on [page 55](#)).

CRIND IP Scheme for Units with SSoM

Internal IP Scheme for Units with SSoM

The following "Internal" CRIND IP scheme must be set for units equipped with DCM2.1 or later.

Unit	IP Address
UPM Side A	172.16.100.1
CR Side A	172.16.100.2
UPM Side B	172.16.100.3
CR Side B	172.16.100.4
GSoM Side A	172.16.100.5
GSoM Side B	172.16.100.6
Applause Site Server IP	10.5.55.66

Notes: 1) These IP Addresses are subject to change based on the direction of the site's IT personnel.

2) The SSoMs communicate to the backroom hardware via two external IPs (one IP per side).

These IPs will match the backroom network IP scheme, i.e. 10.5.55.XX. The SSoMs IP addresses will be configured from the SSoM application. For more details, see MDE-5314 Remote Management Installation, Start-up and Service Manual.

Internal IP Scheme FlexPay II/FlexPay IV			
Fueling Position	Side	CRIND IP Address	Default Gateway
1/2	A	172.16.100.1	172.16.100.254
	B	172.16.100.3	172.16.100.254
3/4	A	172.16.100.1	172.16.100.254
	B	172.16.100.3	172.16.100.254
5/6	A	172.16.100.1	172.16.100.254
	B	172.16.100.3	172.16.100.254
7/8	A	172.16.100.1	172.16.100.254
	B	172.16.100.3	172.16.100.254
9/10	A	172.16.100.1	172.16.100.254
	B	172.16.100.3	172.16.100.254
11/12	A	172.16.100.1	172.16.100.254
	B	172.16.100.3	172.16.100.254
	Etc.	Etc.	Etc.

Note: The table shows IP addresses that are used for FlexPay II and FlexPay IV.

SECTION 3 - FLEXPAY IV START-UP

External IP Scheme FlexPay II/FlexPay IV					
Fueling Position	Side	SSoM External IP Address	Backroom Router IP Address	Subnet Mask	Primary DNS
1/2	A	10.5.55.71	10.5.55.1	255.255.255.0	10.5.55.1
	B	10.5.55.72	10.5.55.1	255.255.255.0	10.5.55.1
3/4	A	10.5.55.73	10.5.55.1	255.255.255.0	10.5.55.1
	B	10.5.55.74	10.5.55.1	255.255.255.0	10.5.55.1
5/6	A	10.5.55.75	10.5.55.1	255.255.255.0	10.5.55.1
	B	10.5.55.76	10.5.55.1	255.255.255.0	10.5.55.1
7/8	A	10.5.55.77	10.5.55.1	255.255.255.0	10.5.55.1
	B	10.5.55.78	10.5.55.1	255.255.255.0	10.5.55.1
9/10	A	10.5.55.79	10.5.55.1	255.255.255.0	10.5.55.1
	B	10.5.55.80	10.5.55.1	255.255.255.0	10.5.55.1
11/12	A	10.5.55.81	10.5.55.1	255.255.255.0	10.5.55.1
	B	10.5.55.82	10.5.55.1	255.255.255.0	10.5.55.1
.	Etc.	Etc.	Etc.	Etc.	Etc.

Notes: 1) Primary Domain Name Server (DNS) value is provided by the customer or is considered to be 10.5.55.1 (if the site uses Gilbarco-provided RV042 Router).

2) The table shows addresses that are subject to change with the site networking scheme. Values provided in the table are EXAMPLE ONLY. For example, if the site backroom Router is 10.5.48.1, the SSoM External IP addresses will have to be 10.5.48.71, etc. The primary DNS will likely be 10.5.48.1, etc.

2 Set Subnet mask to **255.255.255.0**.

3 If an SSoM is present, the UPMs access the site through the SSoM gateway. Set the UPM default gateway to **172.16.100.254**.

4 Set Dynamic Host Configuration Protocol (DHCP) client to **DISABLE** (default).

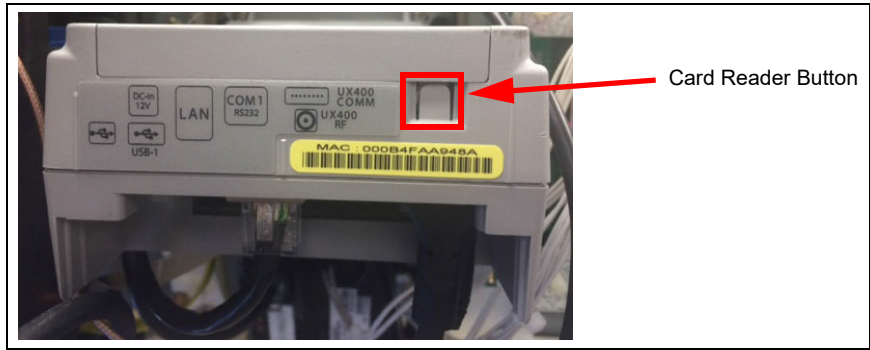
5 Press **OK/Enter** to set the IPs; when prompted, press the button on the card reader one time (1-2 seconds) and follow the CRIND screen instructions.

Notes: 1) Do not hold the card reader button too long. Pressing the button for five seconds or longer sends the card reader into a service mode where a warm-start is required to return the card reader to its normal state. After you release the button, the green and yellow Light Emitting Diode (LED)s at the front of the card reader toggle.

2) During the IP assignment procedure, the side A CRIND will try to configure the GSoM as well. If it is not connected or configured properly, the CRIND reports an error.

SECTION 3 - FLEXPAY IV START-UP

Figure 9: Card Reader Button



- 3
- 6 Remove power to the unit, and then plug in the UPM and the card reader Ethernet connection on side B. Perform steps 1 on page 8 through 19 on page 9 before configuring side B.
- Notes: 1) (Kit only) Side B gets an IP address UPM 1 + 2 (for example, if side A is set to 172.16.100.1, side B should be set to 172.16.100.3).
- 2) After following steps 1 on page 11 through step 5 on page 12, the card reader will automatically take on the IP address of the UPM +1 on all fueling positions.

Configuring CRIND IP Addresses for Units without SSoM

To configure CRIND IP addresses for units without SSoM, proceed as follows:

- 1 Press <2> to go to the **Network Menu**. Press 1 to set CRIND IP addresses according to the IP scheme planned in step 3 in “Prerequisites” on page 5.
- Notes: 1) Pressing **Enter** moves the cursor to the next field.
- 2) IP scheme may vary depending on the customer’s IP scheme requirements.
- 3) The GSoM IP Addresses can only be configured from Side A (see Figure 28 on page 55).

CRIND IP Scheme for Units without SSoM

The CRIND IP scheme assignment for the dispensers that do not have an SSoM (DCM2.0 or earlier) is as follows:

Dispenser 1	
Unit	IP Address
UPM Side A	10.5.55.71
CR Side A	10.5.55.72
UPM Side B	10.5.55.73
CR Side B	10.5.55.74
GSoM Side A	10.5.55.75
GSoM Side B	10.5.55.76
Applause Site Server IP	10.5.55.66

SECTION 3 - FLEXPAY IV START-UP

3

Dispenser 2	
Unit	IP Address
UPM Side A	10.5.55.81
CR Side A	10.5.55.82
UPM Side B	10.5.55.83
CR Side B	10.5.55.84
GSoM Side A	10.5.55.85
GSoM Side B	10.5.55.86
Applause Site Server IP	10.5.55.66

Dispenser 3	
Unit	IP Address
UPM Side A	10.5.55.91
CR Side A	10.5.55.92
UPM Side B	10.5.55.93
CR Side B	10.5.55.94
GSoM Side A	10.5.55.95
GSoM Side B	10.5.55.96
Applause Site Server IP	10.5.55.66

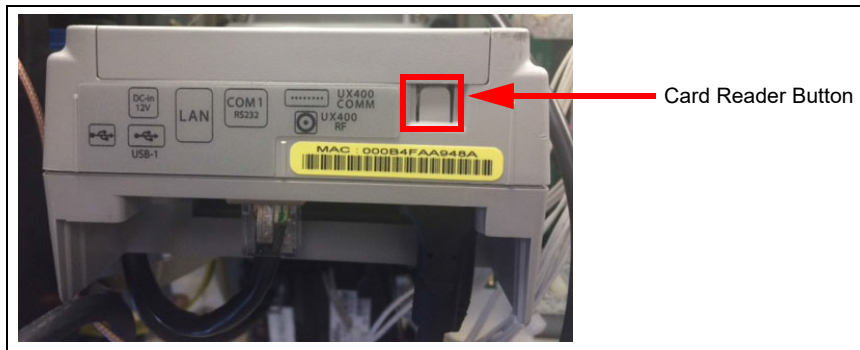
- 2 Set Subnet mask to **255.255.255.0**.
- 3 Set Default gateway for the site (for example) to **10.5.55.1**.
- 4 Set DHCP client to **DISABLE** (default).
- 5 Press **OK/Enter** to set the IPs; when prompted, press the button on the card reader one time (1-2 seconds) and follow the CRIND screen instructions.

Notes: 1) Do not hold the card reader button too long. Pressing the button for five seconds or longer sends the card reader into a service mode where a warm-start is required to return the card reader to its normal state. After you release the button, the green and yellow LEDs at the front of the card reader toggle.

2) During the IP assignment procedure, the side A CRIND will try to configure the GSoM as well. If it is not connected or configured properly, the CRIND reports an error.

SECTION 3 - FLEXPAY IV START-UP

Figure 10: Card Reader Button



- 6 Remove power to the unit, and then plug in the UPM and the card reader Ethernet connection on side B. Perform steps 1 on [page 8](#) through 19 on [page 9](#) before configuring side B.

Notes: 1) (Kit only) Side B gets an IP address UPM 1 + 2 (for example, if side A is set to 10.5.55.71, side B should be set to 10.5.55.73).

2) After following steps 1 on [page 11](#) through step 5 on [page 12](#), the card reader will automatically take on the IP address of the UPM +1 on all fueling positions.

Configuring CRIND (Side B)

To configure the CRIND for side B, go to “[Configuring CRIND \(Side A\)](#)” on [page 8](#) and repeat the steps for side B.

SECTION 3 - FLEXPAY IV START-UP

Configuring Applause Media System

To configure at startup, proceed to step 1. Alternately, you can access the Auxiliary Feature Processor (AFP) Diagnostics Login Screen by pressing the SW Recovery button located at the front of the GSoM (see Figure 11).

Figure 11: SW Recovery Button on GSoM



The current default IP addresses of Applause Media System Server and the Back Room Communication Module (BRCM) are as follows:

Unit	IP Address
Applause Media System Server	10.5.48.66
BRCM	10.5.48.135

After the dispenser IP addresses are configured to reflect the 10.5.55.XXX IP the Applause Media System and BRCM IP addresses should be set as follows:

Unit	IP Address
Applause Media System Server	10.5.55.66
BRCM	10.5.55.135

Note: For more information, refer to MDE-4699 Applause Media System Installation, Service, and Parts Manual, MDE-4917 FlexPay Connect Distribution Box Installation Manual, MDE-5314 Insite360™ Encore® Remote Management Installation, Start-up, and Service Manual, and MDE-5265 BRCM2 Installation and Upgrade Instructions.

SECTION 3 - FLEXPAY IV START-UP

To configure Applause Media System for FlexPay IV, proceed as follows:



IMPORTANT INFORMATION

Before configuring the Applause Media System, ensure that the Applause Site Server is running the latest released software version.

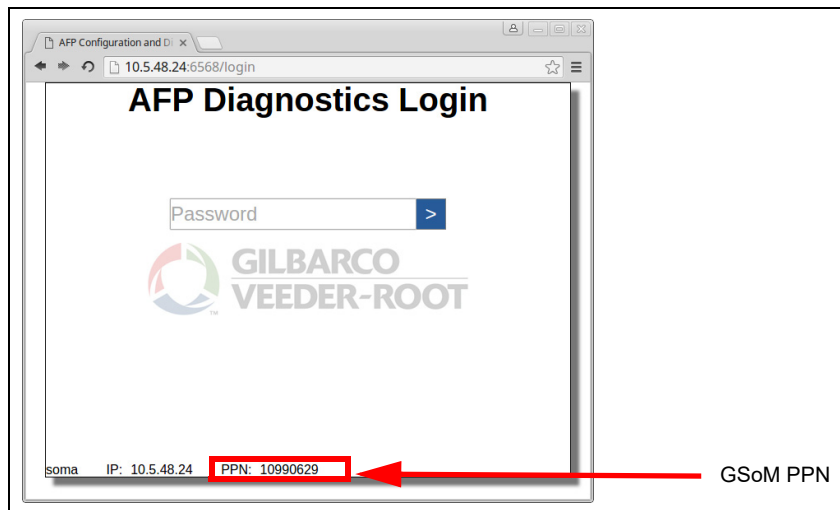
- 1 Connect your laptop to the AFP/DCM2 using an Ethernet cable.
- 2 Using Google®, Chrome™, or Mozilla Firefox® web browser, go to <http://<GSoM IP address>:6568>.
For example, <http://10.5.55.75:6568>.

- 3 Log in to the Diagnostics Server using the password.

Notes: 1) The password is the last six digits of the GSoM PPN displayed on the login screen.

2) If a laptop is not available, you can open the Diagnostics Menu on the unit (assuming the UPM is functional) by pressing the recovery button (the top button) on the GSoM and holding it for at least 3-5 seconds. The GSoM Diagnostics Menu is displayed on the CRIND display. Use the soft keys to navigate as the UPM keypad is unavailable to diagnostics for security reasons.

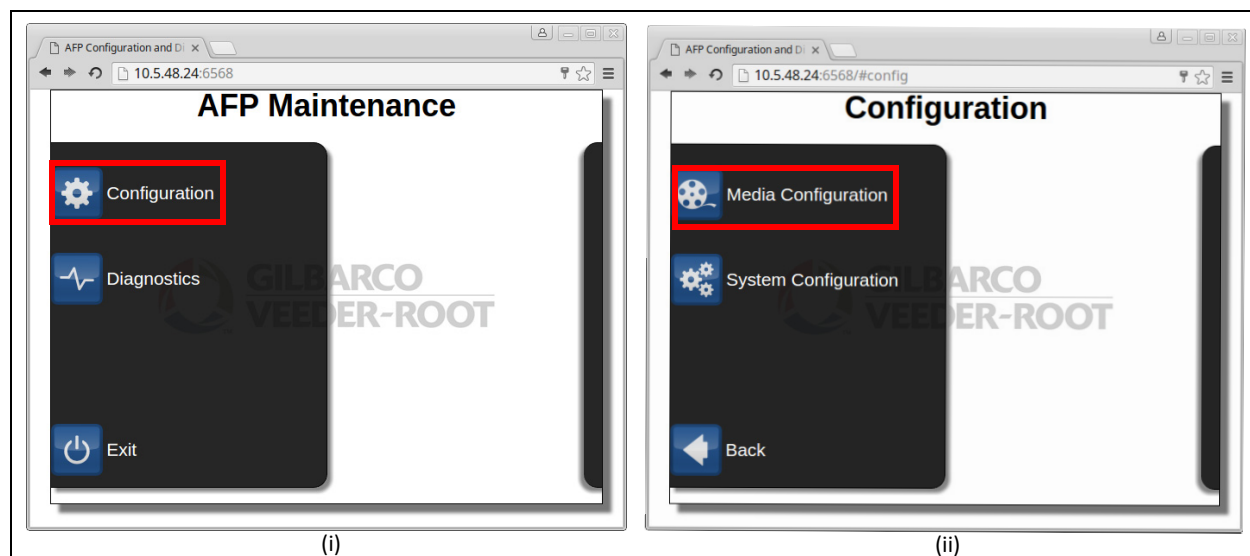
Figure 12: AFP/DCM2 Diagnostics Login Screen



SECTION 3 - FLEXPAY IV START-UP

4 In the Diagnostics mode, navigate to **Configuration > Media Configuration**.

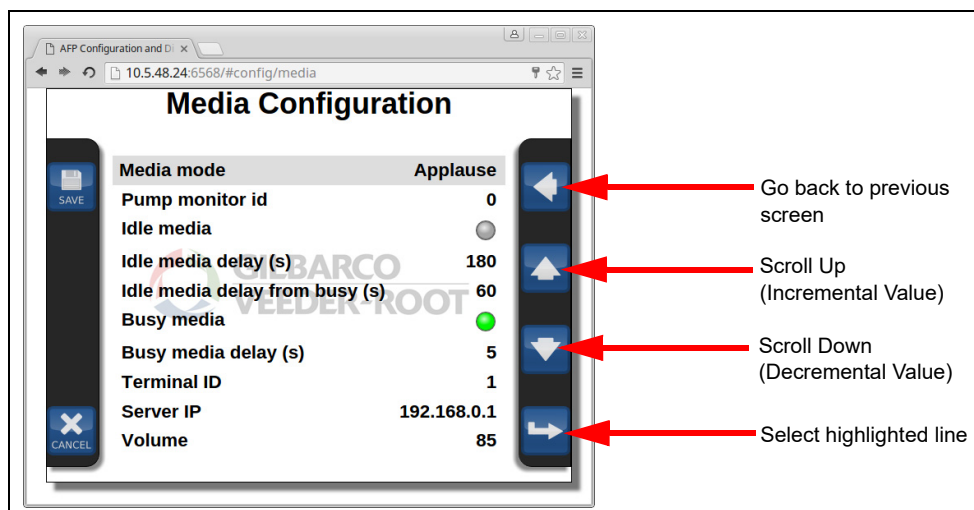
Figure 13: Navigating to Media Configuration Screen



5 Set the Media mode to **Applause**.

Note: This is where you configure the system for Applause.

Figure 14: AFP/DCM2 Diagnostics Login Screen



6 Set **Pump monitor id**. Set this number to match the actual pump ID programmed in the unit programming. (If connected to Passport POS system all IDs will be 7 and 11).

7 Turn on or turn off **Idle media**. Select to turn on (green ball) if you want media to run when the unit is in an idle condition. If you do not want media to run when the unit is idle, leave the ball gray.

Note: If idle is turned on (green), media ads can start showing during a POS application download.

Gilbarco recommends disconnecting the Applause Media System Server or waiting to turn on idle media until the units are fully up and running with the POS.

SECTION 3 - FLEXPAY IV START-UP

3

- 8 Set **Idle media delay (s)**. Set the time that you want the unit to wait before starting the media after a power-on or warmstart (or a start-up).
- 9 Set **Idle media delay from busy (s)**. Set the time that you want the unit to wait after the handle has been dropped before starting to show media ads.
- 10 Turn on or off **Busy media**. Select to turn on (green ball) if you want media to play while customers are fueling. If you do not want media to play while customers are fueling, leave the ball gray.
- 11 Set **Busy media delay (s)**. Set the time that you want the unit to wait before starting the media once fueling has started.
- 12 Set **Terminal ID**. Set this number to match the actual forecourt fueling position number.
- 13 Set **Server IP**. Program the IP address of the Applause Site Server located inside the building, for example, 10.5.55.66.
- 14 Set **Volume**. Set the volume for the Applause ads that are shown on the CRIND display.
- 15 Select **Save**.

Completing Start-up

To complete start-up, proceed as follows:

- 1 Reconnect the CRIND two-wire cable and any Ethernet/network connections, and initiate a POS download.
Note: If idle is turned on (green), media ads can start showing during a POS application download. Gilbarco recommends disconnecting the Applause Media System Server or waiting to turn on idle media until the units are fully up and running with the POS.
- 2 Ensure that all the CRIND options are functional using the Selfcheck Tool.
- 3 Verify communication with the POS. For more information, refer to list of reference documents for the FlexPay IV Kit Installation Instructions in the [“Related Documents”](#) section on [page 25](#).
- 4 Verify if the paper is installed properly in the printer by observing transaction printout or CRIND printer test. For more information, refer to [“Selfcheck Tool”](#) on [page 48](#).
- 5 Run a debit/credit transaction and verify operation of any peripherals. For more information, refer to [“Selfcheck Tool”](#) on [page 48](#).

Ensure that the unit is fully operational and all options are functional.

SECTION 4 - REFERENCE INFORMATION

Related Documents

Document No.	Title
MDE-4699	Applause Media System Installation, Service, and Parts Manual
MDE-4917	FlexPay Connect Distribution Box Installation Manual
MDE-5220	FlexPay IV CRIND Retrofit Kit Installation Instructions for Encore S E-CIM™
MDE-5222	FlexPay IV CRIND Retrofit Kit Installation Instructions for Encore 300/500
MDE-5223	FlexPay IV CRIND Service/Troubleshooting Guide
MDE-5224	FlexPay IV CRIND Retrofit Kit Installation Instructions for The Advantage® Series
MDE-5226	FlexPay IV CRIND Retrofit Kit Installation Instructions for Encore 500 S
MDE-5227	M7 Maintenance Tool User Guide
MDE-5265	BRCM2 Installation and Upgrade Instructions
MDE-5314	Insite360 Encore Remote Management Installation, Start-up and Service Manual
PT-1936	Encore Series Pumps and Dispensers Illustrated Parts Manual
PT-1937	Encore 300, Encore 500/500 S, Encore 550, Encore 700 S, Eclipse® Recommended Spare Parts Manual

4

Abbreviations and Acronyms

Term	Description
ADA	Americans with Disabilities Act
AFP	Auxiliary Feature Processor
ASC	Authorized Service Contractor
BIOS	Basic Input/Output System
BNA	Bank Note Acceptor
BRCM	Back Room Communication Module
CAT5	Category 5
CRIND	Card Reader in Dispenser
DC	Daily Check
DCM	Dispenser Communication Module
DEF	Diesel Exhaust Fluid
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
E-CIM	Enhanced Customer Interface Module
EMV	Europay®, MasterCard®, and Visa®
GSoM	Gilbarco Systems on Module
IP	Internet Protocol
LED	Light Emitting Diode
MOC	Major Oil Company
NA	North America
NEC	National Electrical Code
NFPA	National Fire Protection Association
OS	Operating System
OSHA	Occupational Safety and Health Administration

SECTION 4 - REFERENCE INFORMATION

4

Term	Description
PCB	Printed Circuit Board
PCI	Payment Card Industry
PCI-PED	Payment Card Industry PIN Entry Device
PIP	Peripheral Interface PCB
PPN	Product Part Number
POS	Point of Sale
SSoM	Secure Systems on Module
TAC	Technical Assistance Center
TLS	Transport Layer Security
TRIND	Transmitter/Receiver in Dispenser
UPM	Universal Payment Module
USB	Universal Serial Bus
UTC	Coordinated Universal Time

SECTION 5 - APPENDIX

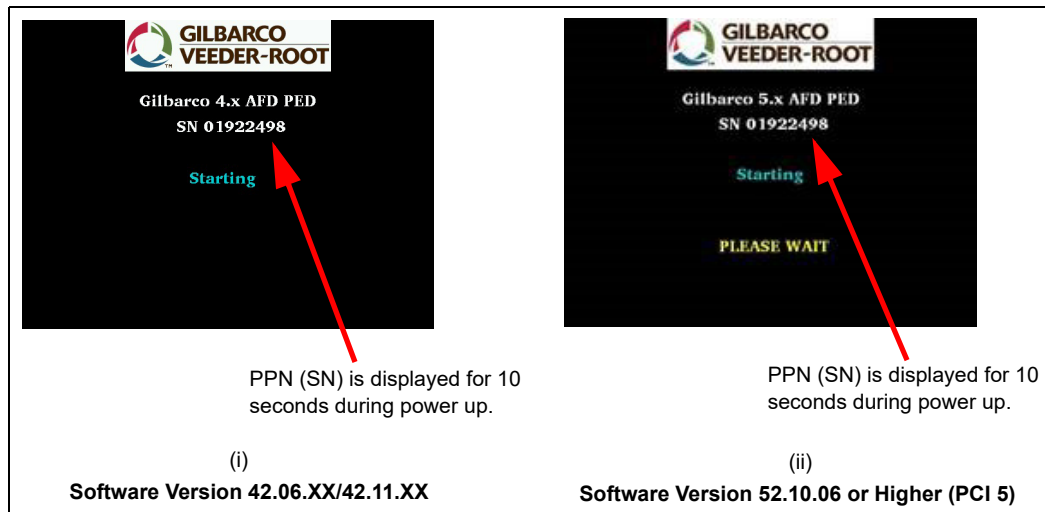
System Screens

This section describes the various FlexPay IV CRIND system screens.

Service Menu Start-Up Screen

At start-up, the display shows the Device Serial Number. The last six digits of this number comprise the password for the in Service Menu.

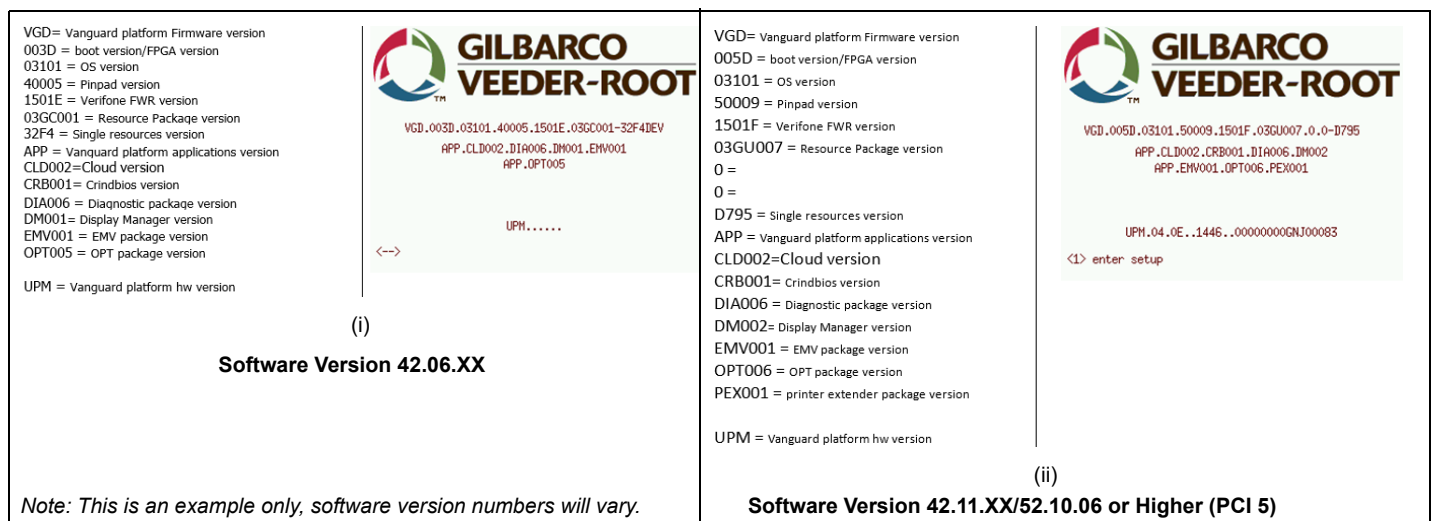
Figure 1: Service Menu - Start-up



After the boot procedure, a white screen with the Gilbarco logo, the software version, and hardware version is displayed.

Note: Figure 2 is an example only. The screen might be different depending on your software version.

Figure 2: Software and Hardware Versions



On the bottom left corner of the screen, “<1> enter setup” is displayed.

SECTION 5 - APPENDIX

Press **1** and enter the last six digits of the PPN to enter the Service Menu. If **1** is not pressed, the CRIND display will show one of the following screens:

System Offline

The blue screen indicates that the system is running and it has been activated; the system is waiting for a master device connection.

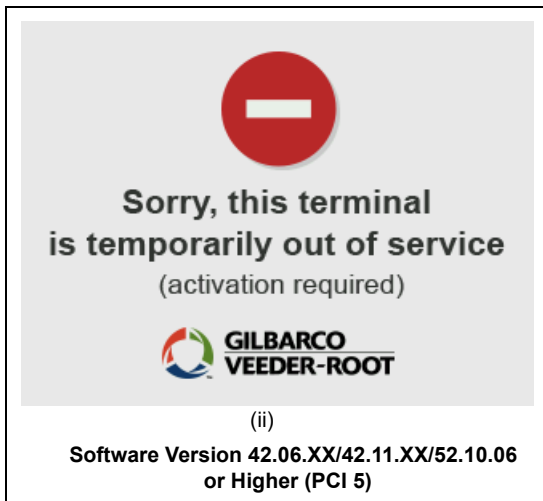
Figure 3: Blue Screen - System Offline (Without CRIND BIOS)



Out of Service

The out of service screen indicates that the system is running but has not yet been activated using the activation procedure.

Figure 4: Out of Service Screen



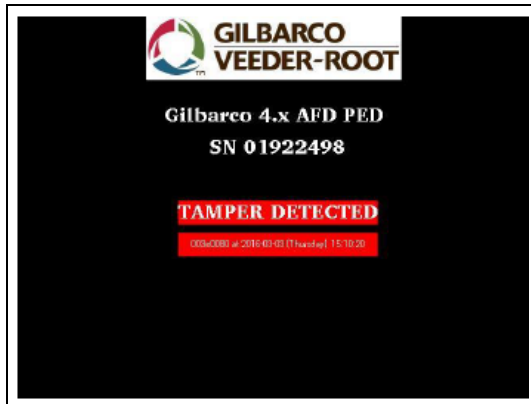
Note: The Out of Service screen indicates that the unit needs to be activated. Power cycle the unit to get out of the screen.

SECTION 5 - APPENDIX

Tamper Detected

This screen is displayed only at start-up. The Tamper Detected state prevents the unit from proceeding through the start-up process. The unit in this case has an alarm(s) running in the module and a steady RED LED on the UPM cover.

Figure 5: Tamper Detected Screen



5

Software Update

Figure 6 shows the Software Update Screen.

Figure 6: Software Update Screen

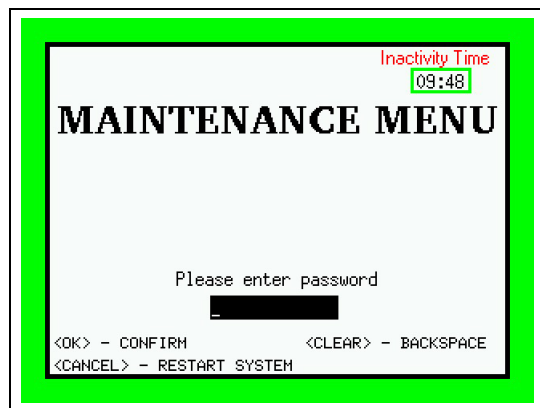


SECTION 5 - APPENDIX

Maintenance Menu

You need the password to enter the Service Menu; that is the last six digits of PPN. Enter the password and press **OK** to confirm.

Figure 7: Maintenance Menu

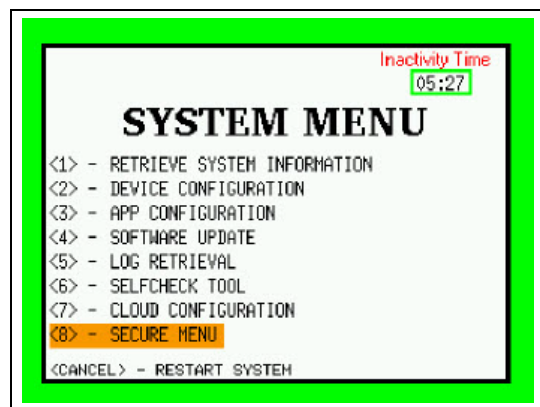


5

System Menu

The System Menu contains eight options as shown in [Figure 8](#).

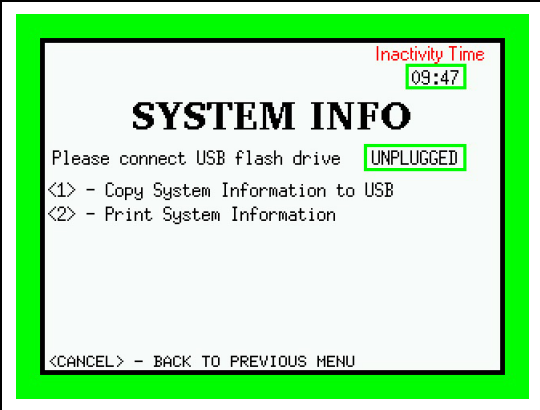
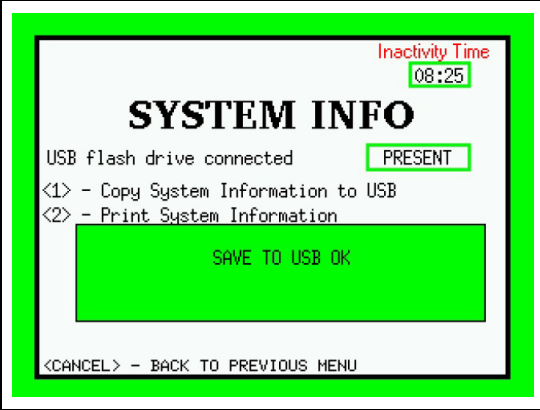
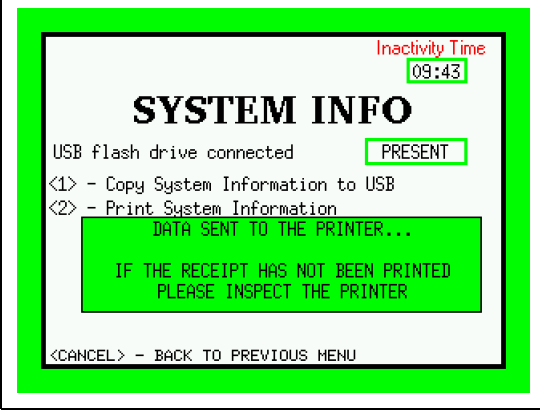
Figure 8: System Menu



SECTION 5 - APPENDIX

Retrieve System Information

System Info has the following options:

Description	Screen
<p>In this menu, it is possible to retrieve all system information.</p> <p>The following are the two different ways to retrieve system info:</p> <ul style="list-style-type: none">• Saving the information on to a USB memory stick.• Using a printer device.	
<p><1> Copy System Information to USB.</p> <p>Connect a USB stick to external board Peripheral Interface PCB (PIP) 3. The system detects the USB stick and reports PRESENT in status area.</p> <p>When the USB is detected, press <1> to store the system information to the plugged in USB stick.</p>	
<p><2> Print System Information to send the system information to the printer.</p> <p><i>Note: The system at this point does not know the state of the printer; check the connection and paper status manually to ensure the printer is ready and able to print correctly.</i></p>	

SECTION 5 - APPENDIX

Figure 9 shows an example of system information that can be downloaded or printed.

Figure 9: System Information

<p>- GILBARCO VEEDER ROOT -</p> <p>-----</p> <p>Date 2017-November-09 UTC Time 18:25:10</p> <p> ---- TIMEZONE ---- </p> <p>America/Detroit</p> <p>Date 2017-November-09 Time 13:25:10</p> <p> ---- SYSTEM INFORMATION ---- </p> <p>UPM serial number = 01982492</p> <p>keypadType = Numeric_Rev#0</p> <p>CR serial number = 986071491</p> <p>CR model = Verifone UX300</p> <p>Contactless serial number =</p> <p>Contactless model = Verifone UX400</p> <p>Touchscreen serial number =</p> <p>Touchscreen model =</p> <p>Display Resolution = 320x240 pixels - Color</p> <p>Depth = 16 bits</p> <p>Aggregated info</p> <p>PCI FWR Version:</p> <p>VGD.005D.03101.50009.1501F.03GU007.0.0-D795</p> <p>PCI APP Version:</p> <p>APP.CLD002.CRB001.DIA006.DM002</p> <p>APP.EMV001.OPT006.PEX001</p> <p>PCI ISDK Version:</p> <p>HWR Version:</p> <p>UPM.04.0E..1446..00000000GNJ00083</p> <p>Network Configuration</p> <p>Side=B</p> <p>BCIP="disabled"</p> <p>IP="172.20.100.3"</p> <p>MSK="255.255.255.0"</p> <p>GW="172.20.100.254"</p> <p>DHCP="disabled"</p> <p>Not secure device Configuration</p> <p>printerPort="USB"</p> <p>communicationModule="OMNIA"</p> <p>barcode="GVR_SCANNER"</p> <p>enabledBNA="NO"</p> <p>enabledTrind="NO"</p> <p>Secure device Configuration</p> <p>cardReader="VFI_MANUAL"</p> <p>UntrustedClientMode="enabled"</p> <p>readerWarning="enabled"</p> <p>contactLessWarning="disabled"</p> <p>dailyCheckFixedHourNewVers="scheduled"</p> <p>rebootHour="03"</p> <p>rebootMinutes="00"</p> <p>contactLessModule="VFI"</p> <p> ---- SYSTEM VERSION ---- </p> <p>Firmware and Application info</p> <p>BOOT = 01.04p9995</p> <p>OS = 06.01p10195</p> <p>CLOUD = 01.02p10194</p> <p>CRINDBIOS = 01.05p1176</p> <p>DIAGNOSTIC = 01.07p10197</p> <p>DISPLAYMANAGER = 02.00p10194</p> <p>EMV = 03.09.0p1</p>	<p>OPT = 01.07p10194</p> <p>PRINTEREXTENDER = 01.00p9995</p> <p>RESOURCES = 07.01.pa000</p> <p>VFI = 03.04p10194</p> <p>Card Reader FWR info</p> <p>Version = 6541 -30470400</p> <p>Contactless FWR info</p> <p>Version =</p> <p>Build Number info</p> <p>[BOOT] 52.10.06</p> <p>[OS] 52.10.06</p> <p>[CLOUD] 52.10.06</p> <p>[CRINDBIOS] 40.2.44</p> <p>[DIAGNOSTIC] 52.10.06</p> <p>[DISPLAYMANAGER] 52.10.06</p> <p>[EMV] 52.10.06</p> <p>[OPT] 52.10.06</p> <p>[PRINTEREXTENDER] 52.10.06</p> <p>[RESOURCES]</p> <p>[VFI] 52.10.06</p> <p> ---- SYSTEM HEALTH REPORT - --- </p> <p>- UNIT IS ACTIVATED</p> <p>- TLS certificate status: OK</p> <p>#### UPM ####</p> <p>Communication OK? = YES</p> <p>Dismount OK? = YES</p> <p>Other error = NO</p> <p>#### CARD READER ####</p> <p>Communication OK? = YES</p> <p>Dismount OK? = YES</p> <p>Other error = NO</p> <p>#### CONTACTLESS MODULE ####</p> <p>Communication OK? = YES</p> <p>Dismount OK? = YES</p> <p>Other error = NO</p> <p>#### TOUCHSCREEN ####</p> <p>Touchscreen connected = NO</p> <p>#### DISPLAY ####</p> <p>Dismount OK? = YES</p> <p> ---- KEY NAME ---- </p> <p>TLS_VGD_RCSH</p> <p>TLS_3PA</p> <p>EPHEMERALKEY#09</p> <p>EPHEMERALKEY#01</p> <p>emv4-t3</p> <p> ---- HIERARCHIES ---- </p> <p>3PA_ID</p> <p>RCSH_CA</p> <p>RCSH_ID</p> <p> ---- MAC-MODE ---- </p> <p>Resource: NOT STORED</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

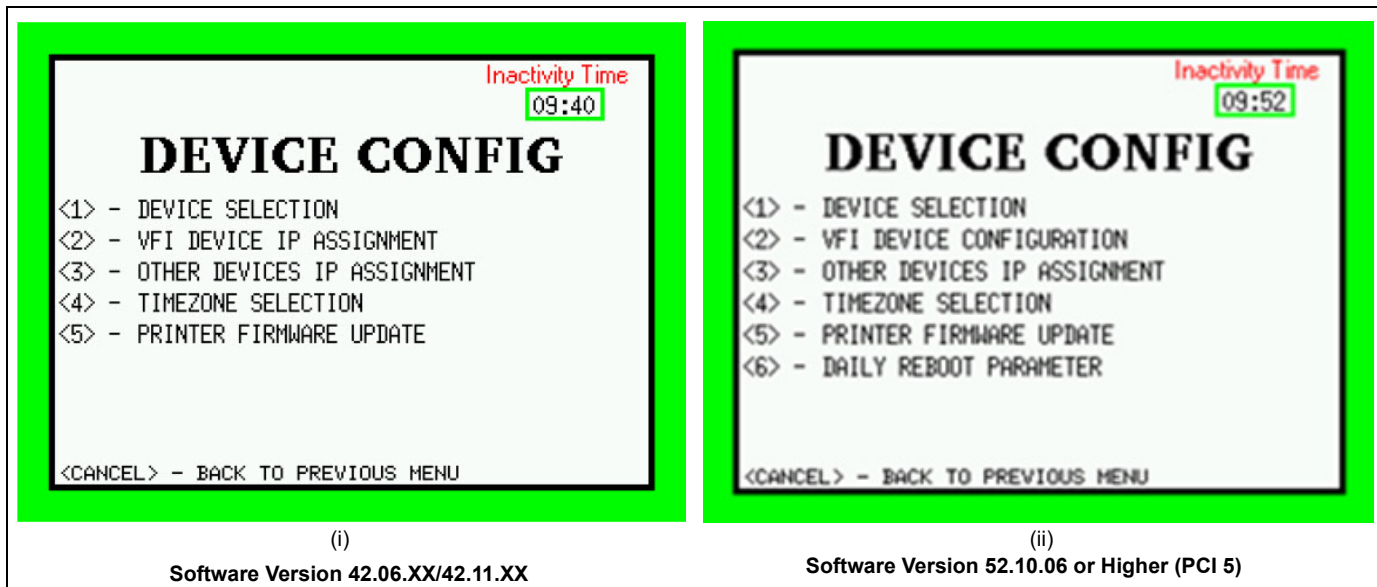
SECTION 5 - APPENDIX

Device Configuration

External devices can be connected to the FlexPay IV system from the Device Configuration menu.

After the first start-up, verify that the devices are configured correctly. When a new device is configured, a reboot is required.

Figure 10: Device Configuration Screen



5

IP Scheme

In a unit (side A and B), the IP configuration scheme is defined as follows:

Component	IP Address
UPM A	A.B.C.D
UX-300 A	A.B.C.(D+1)
UPM B	A.B.C.(D+2)
UX-300 B	A.B.C.(D+3)
GSoM A	A.B.C.(D+4)
GSoM B	A.B.C.(D+5)
(Future)	A.B.C.(D+6)
(Future)	A.B.C.(D+7)
(Future)	A.B.C.(D+8)
(Future)	A.B.C.(D+9)

As described in “Card Reader IP Assignment” on page 37 and “Other Device IP Assignment” on page 39, the assignment of IP address to the card reader and GSoM are provided by a wizard procedure. The ASC has to set UPM IP address, subnet mask, and default gateway.

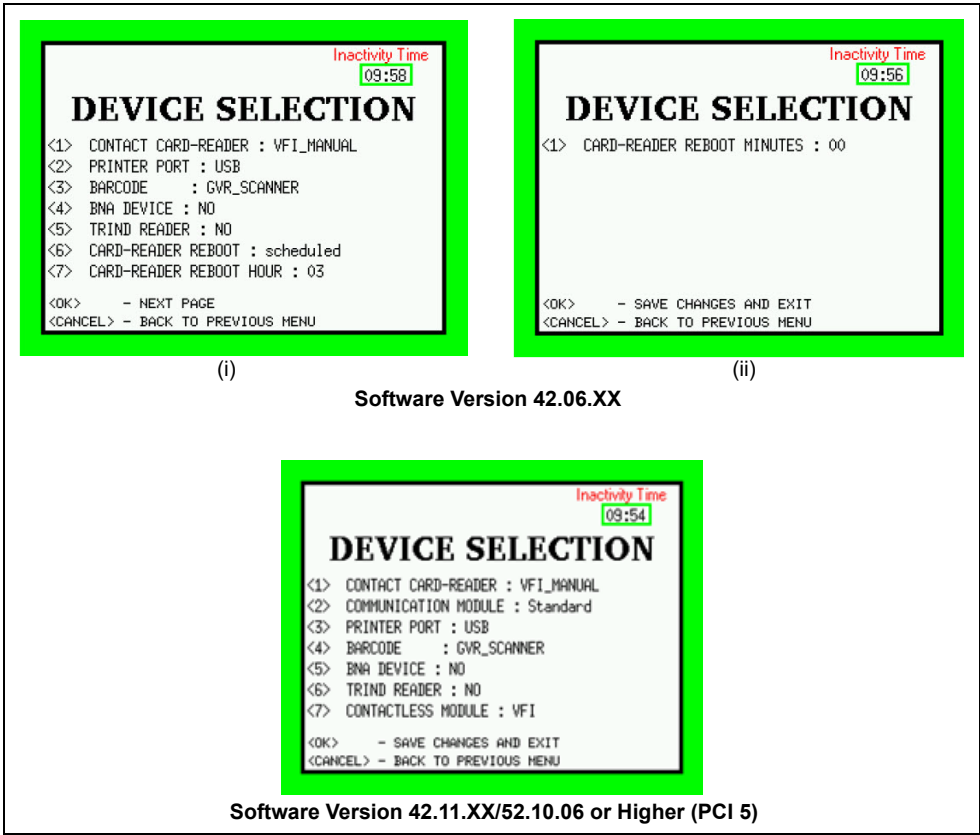
SECTION 5 - APPENDIX

Device Selection

The following are all the possible options available from the Device Selection menu:

Note: Your FlexPay IV CRIND version may show fewer options depending on the country/customer customization.

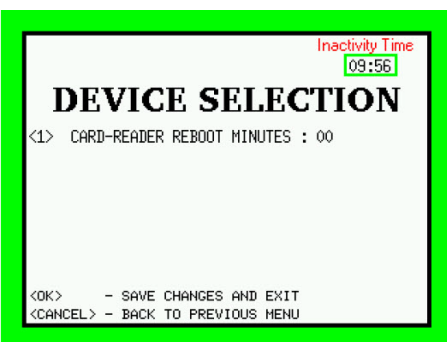
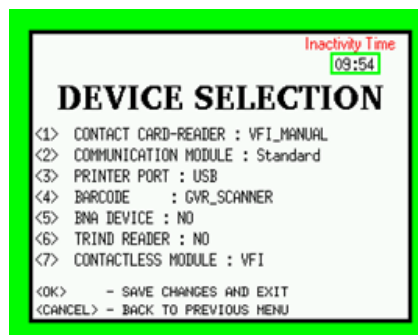
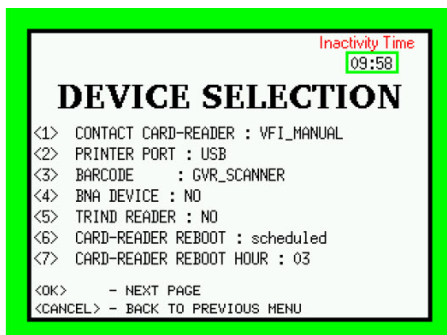
Figure 11: Device Selection Screen(s)



SECTION 5 - APPENDIX

Software Version 42.06.XX

Software Version 42.11.XX/52.10.06 or Higher (PCI 5)



5

<1> CONTACT CARD-READER:

Options available are:

NONE/LEGACY_MOTORIZED/VFI_MANUAL (Version 42.06.11 or higher)

This configuration option is about the card reader configuration. If no card reader type has been selected during the initialization, you will have a red notification "CARD READER ERROR/NOT READY/ POWER OFF".

Note: The None option works if the reader warning has been disabled.

<1> CONTACT CARD-READER:

(Options are the same as those for Software Version 42.06.XX.)

N/A

<2> COMMUNICATION MODULE

Options available are: Standard

This configuration option identifies the connection module used by the dispenser: use Standard for CCP/AFP.

<2> PRINTER PORT

Options available are: NONE/USB

This configuration option is about the printer configuration. The configuration must be set as USB if a Custom or Hengstler® printer is present.

<3>PRINTER PORT

(Options are the same as those for Software Version 42.06.XX.)

<3> BARCODE

Options available are: NONE/GVR-SCANNER

This configuration option is about the barcode scanner. The configuration must be set as GVR-SCANNER if a 1D or 2D scanner is present.

<4>BARCODE

(Options are the same as those for Software Version 42.06.XX.)

<4> BNA DEVICE

Options available are: NONE/YES

This configuration option is about the banknote acceptor. The configuration must be set as YES if a JCM or SODECO MEI is present.

<5> BNA DEVICE

(Options are the same as those for Software Version 42.06.XX.)

SECTION 5 - APPENDIX

Software Version 42.06.XX

<5> TRIND READER

Options available are: NONE/YES

This configuration option is about the TRIND reader (Specific for NA customization). The configuration must be set to YES if present.

N/A

Software Version 42.11.XX/52.10.06 or Higher (PCI 5)

<6> TRIND READER

(Options are the same as those for Software Version 42.06.XX.)

<7>CONTACTLESS MODULE

Options available are: NONE/VFI

This configuration option is about the contactless device; VFI parameters specify that a UX400 is connected to the device.

<6> CARD-READER REBOOT

Options available are: scheduled/default

Scheduled: DC is performed at the local time set in steps 3 and 4.
Default: DC is performed automatically by the unit after 24 hours from the latest DC.

N/A

<7> CARD-READER REBOOT HOUR

Options available are: 00 to 24

This configuration option sets the local time (hour) at which the DC will be performed on the card reader.

N/A

<8> CARD-READER REBOOT MINUTES

Options available are: 00 - 15 - 30 - 45

This configuration option sets the local time (minutes of the previous hour) at which the Dc will be performed on the card reader.

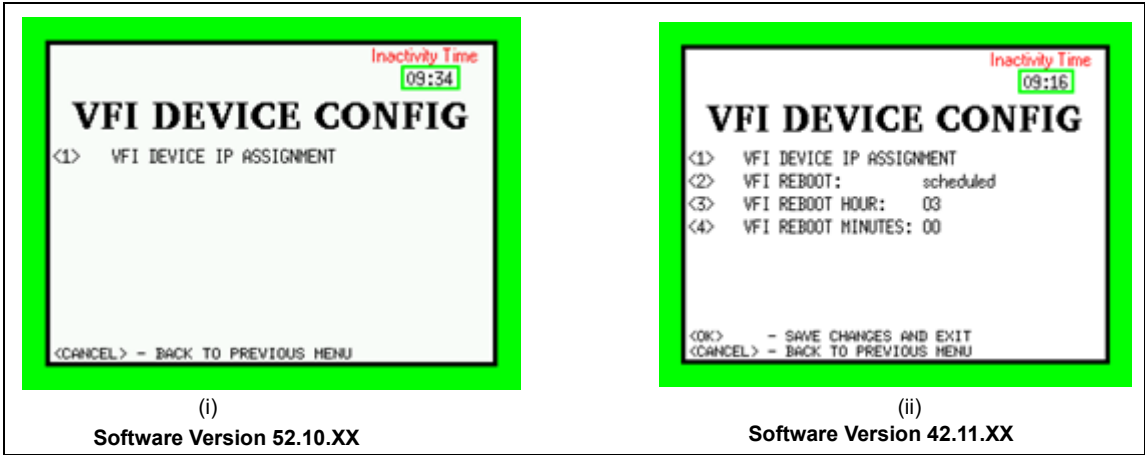
N/A

SECTION 5 - APPENDIX

Card Reader IP Assignment

From the VFI Device Config menu, you can set up the VFI device IP address; this functionality can be used in case of new installation or a reader replacement.

Figure 12: Device Configuration Screen



5

Description	Screen
Press the VFI device back button for one second.	



The reader LEDs start to blink and the display shows the message "Reader message received. Please Wait".

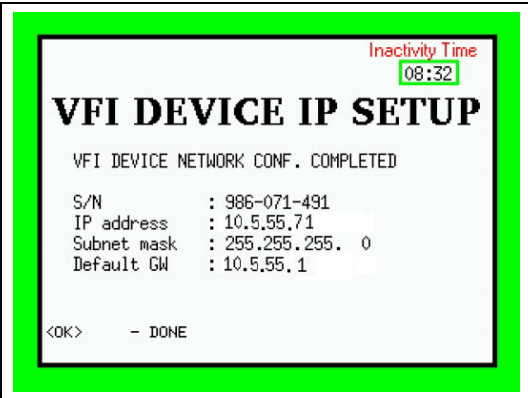


SECTION 5 - APPENDIX

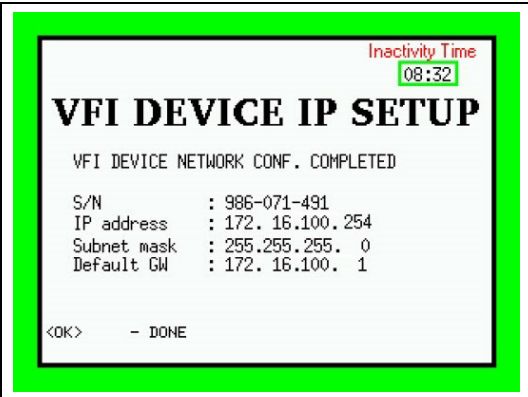
Description	Screen
-------------	--------

At the end of the procedure, the display shows the new configured VFI device IP address (+1 of UPM).

For DCM2.0 or Earlier (without SSoM)



For DCM2.1 or Later (with SSoM)




SECTION 5 - APPENDIX

Other Device IP Assignment

From the Other Dev Setup menu, set up GSoM A/B IP address; this functionality can be used for new installation or device replacement.

The other device IP setup can just be run on side A units.

Description	Screen
The unit checks for other devices. The display shows the "Other Dev Discovery. Please Wait." message.	

The GSoM information is displayed.

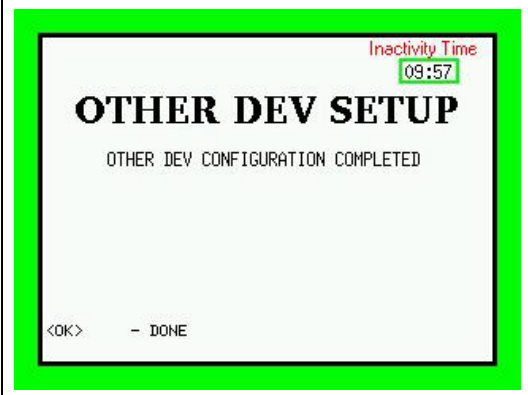
For DCM2.0 or Earlier (without SSoM)



For DCM2.1 (with SSoM)



SECTION 5 - APPENDIX

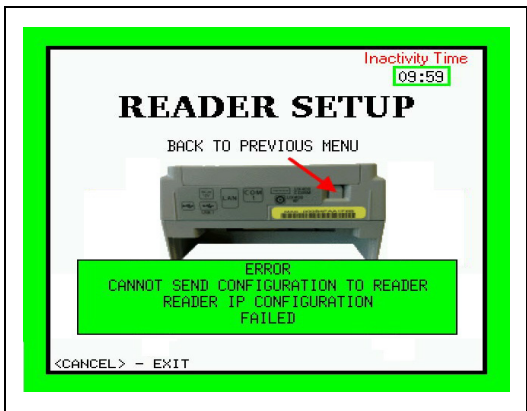
Description	Screen
Selecting <OK> starts the IP assignment and a confirmation screen is displayed. <i>Note: The IP assigned is not shown on this screen.</i>	

5

Error Message

In case of an IP conflict or communication trouble with the devices, a pop-up message is displayed to inform that a problem occurred.

Figure 13: Reader Setup Screen - Error Message

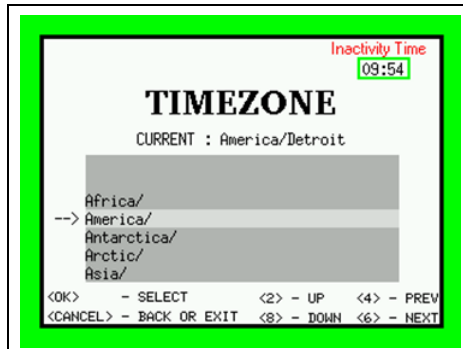


SECTION 5 - APPENDIX

Timezone Selection

From the Timezone Selection menu, it is possible to set up the time zone by using the keypad function button. It is recommended to select the proper time zone value based on the installation location. If a time zone is not set, the default setting is UTC.

Figure 14: Timezone Menu



Printer Firmware Update

From the printer Firmware Update menu, it is possible to update Hengstler C-56 printer firmware using a USB stick.

The firmware must be stored inside the USB stick in a specific folder structure:

X:\gvr\DualAuthentication\printer With: "*. C56BIN" extension.

This is a critical operation and the firmware must be approved and provided by Gilbarco.

Figure 15: Printer Firmware Update



SECTION 5 - APPENDIX

Daily Reboot

From the Daily Reboot menu, you can set up the time for the daily restart of the system.

Figure 16: Software Versions 42.11.XX and 52.10.XX



Option	Description
REBOOT MODE	Options available are: scheduled/default. Scheduled means that the restart is performed at the local time set in point 3 and 4. Default means that the restart is performed automatically by the unit after 24 hours from the latest restart.
REBOOT HOUR	Options available are: 00 to 24. This configuration option sets the local time hour at which the DC will be performed.
REBOOT MINUTES	Options available are: 00 - 15 - 30 - 45. This configuration option set the local time minutes of the previous hour at which the daily reboot will be performed.

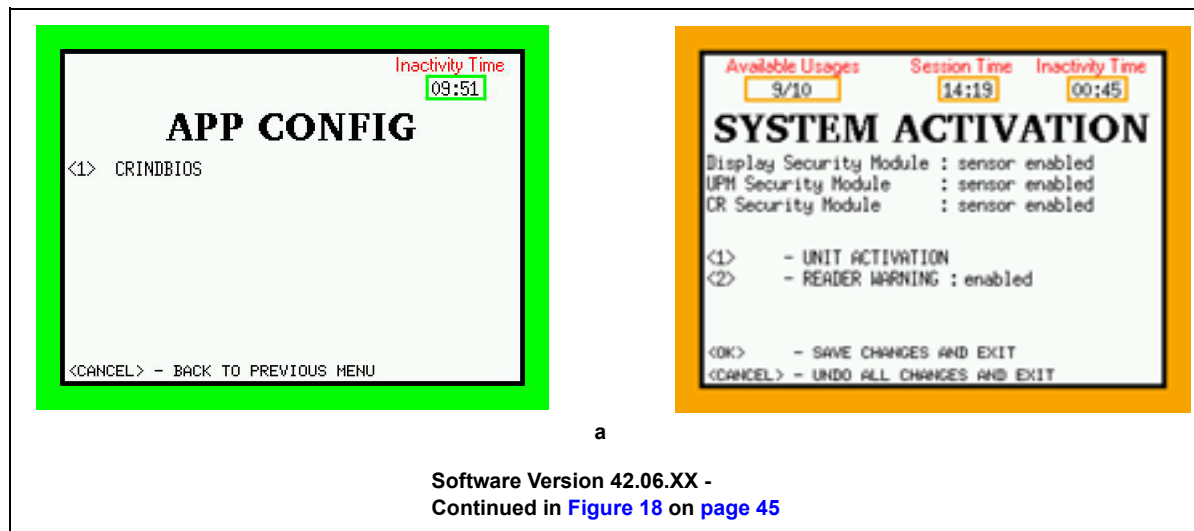
SECTION 5 - APPENDIX

Application Configuration Screen

In the Application Configuration menu, you can perform internal specific application configuration.

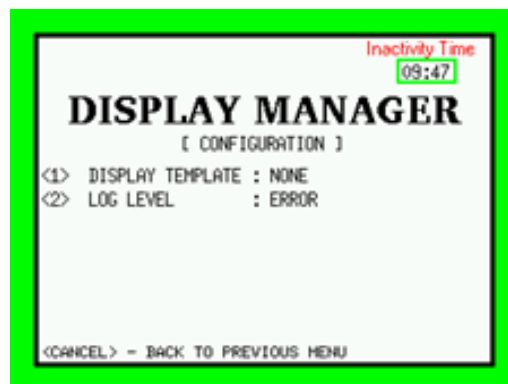
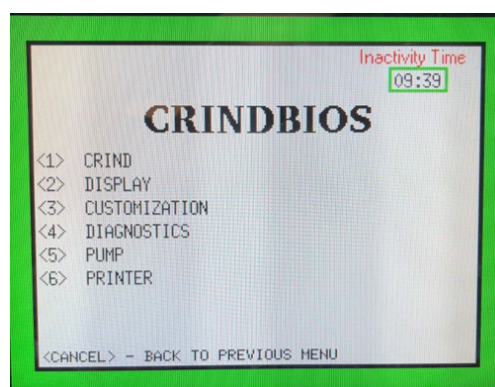
Note: For units in Canada with Software Version 42.06.14 or higher installed, the App Config menu is present but functions are not available.

Figure 17: FlexPay IV CRIND Customization Screens



Note: If the menu is empty, then no additional configuration is required.

SECTION 5 - APPENDIX



b

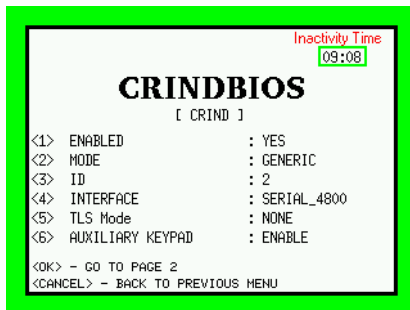
Software Version 42.11.XX/52.10.06
or Higher (PCI 5) - Continued in
[Figure 19 on page 46](#)

- <1> DISPLAY TEMPLATE: NONE/
POS_ON_LEFT/ POS_CENTERED/
POS_ON_RIGHT/
- <2> LOG LEVEL: ERROR/WARNING/INFO/
DEBUG

SECTION 5 - APPENDIX

Figure 18: CRIND BIOS Screens (Software Version 42.06.XX)

5



CRIND Menu (42.06.XX)

CRIND Menu (42.06.XX)

<1> ENABLED: YES/NO

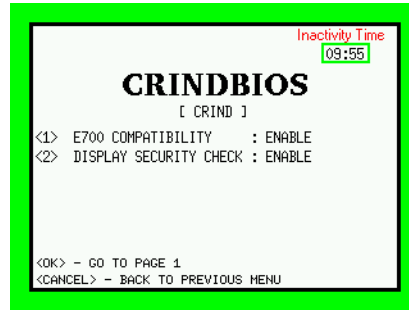
<2> MODE: GENERIC/MOC/MOC_KIOSK

<3> ID: 1-99

<4> INTERFACE:
a) SERIAL_4800
b) SERIAL_9600
c) SERIAL_19200
d) IP

<5> TLS Mode: YES/NONE

<6> AUXILIARY KEYPAD: ENABLE/DISABLE

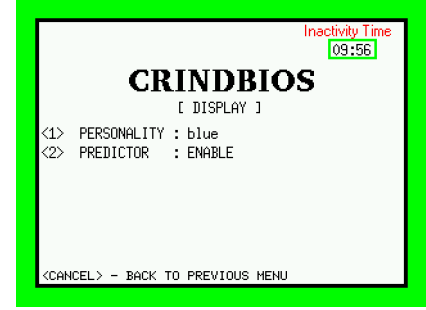


CRIND Menu Page - 2 (42.06.XX)

CRIND Menu - Page 2 (42.06.XX)

<1> E700 COMPATIBILITY: ENABLE/DISABLE

<2> DISPLAY SECURITY CHECK: ENABLE/DISABLE

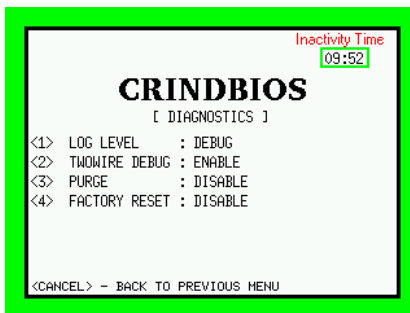


CRIND Display Menu (42.06.XX)

CRIND Display Menu (42.06.XX)

<1> PERSONALITY: blue

<2> PREDICTOR: ENABLE/DISABLE



CRIND Diagnostics Menu (42.06.XX)

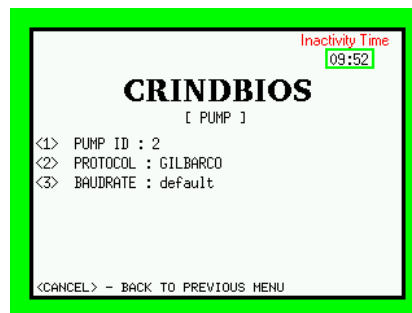
CRIND Diagnostic Menu (42.06.XX)

<1> LOG LEVEL: ERROR/WARNING/INFO/DEBUG

<2> TWOWIRE DEBUG: DISABLE/ENABLE

<3> PURGE: DISABLE/ENABLE

<4> FACTORY RESET: DISABLE/ENABLE



Pump Menu (42.06.XX)

Pump Menu (42.06.XX)

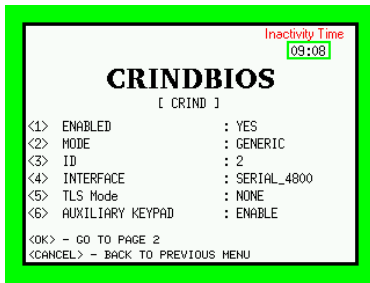
<1> PUMP ID: 1-16

<2> PROTOCOL: GILBARCO/ WAYNE

<3> BAUDRATE: default/1200/2400/4800/9600/19200/
38400/57600/115200

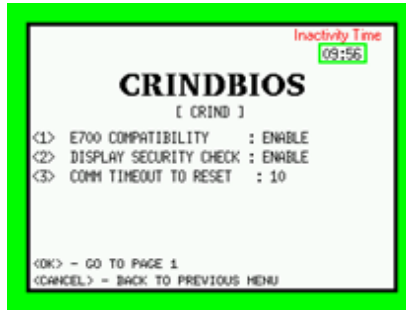
SECTION 5 - APPENDIX

Figure 19: CRIND BIOS Screens for Software Version 42.11.XX/52.10.06 or Higher (PCI 5)



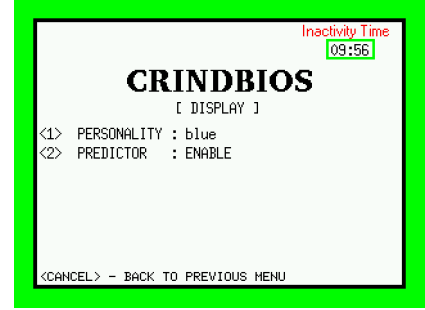
CRIND Menu Software Version 52.10.06 or Higher (PCI 5)

- <1> ENABLED: YES/NO
- <2> MODE: GENERIC/MOC/MOC_KIOSK
- <3> ID: 1-99
- <4> INTERFACE:
 - a) SERIAL_4800
 - b) SERIAL_9600
 - c) SERIAL_19200
 - d) IP
- <5> TLS Mode: YES/NONE
- <6> AUXILIARY KEYPAD: ENABLE/DISABLE



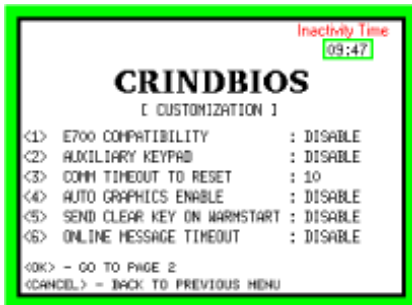
CRIND Menu Page - 2 Software Version 52.10.06 or Higher (PCI 5)

- <1> E700 COMPATIBILITY: ENABLE/DISABLE
- <2> DISPLAY SECURITY CHECK: ENABLE/DISABLE



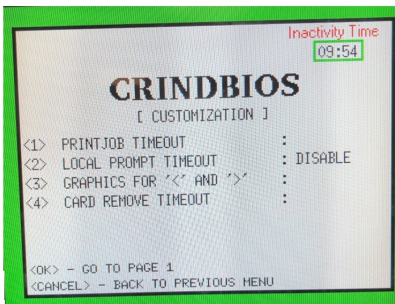
CRIND Display Menu Software Version 52.10.06 or Higher (PCI 5)

- <1> PERSONALITY: blue
- <2> PREDICTOR: ENABLE/DISABLE



CRINDBIOS Customization Menu Page 1
Software Version 42.11.XX or Higher

- <1> E700 COMPATIBILITY: ENABLE/DISABLE
- <2> AUXILIARY KEYPAD: ENABLE/DISABLE
- <3> COMM TIMEOUT TO RESET
- <4> AUTO GRAPHICS ENABLE
- <5> SEND CLEAR KEY ON WARMSTART
- <6> ONLINE MESSAGE TIMEOUT :
ENABLE/ DISABLE

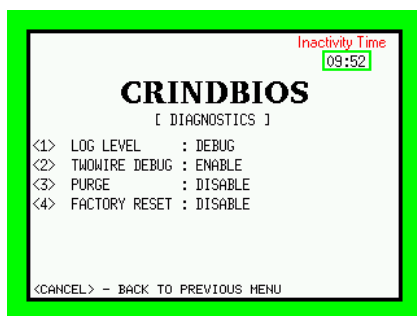


CRINDBIOS Customization Menu Page 2
Software Version 42.11.XX or Higher

- <1> PRINTJOB TIMEOUT
- <2> LOCAL PROMPT TIMEOUT:
ENABLE/DISABLE
- <3> GRAPHICS FOR '<' AND '>'
- <4> CARD REMOVE TIMEOUT : 10

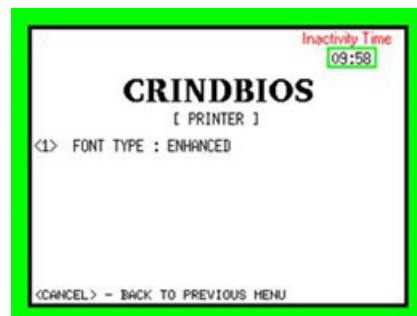
Note : The default time before an error message is displayed to alert the customer to remove the card from the card reader is 10 seconds.

SECTION 5 - APPENDIX



**CRIND Diagnostics Menu Software Version
42.11.XX/52.10.06 or Higher (PCI 5)**

<1> LOG LEVEL: ERROR/WARNING/INFO/
DEBUG
<2> TWOWIRE DEBUG: DISABLE/ENABLE
<3> PURGE: DISABLE/ENABLE
<4> FACTORY RESET: DISABLE/ENABLE



**Pump Menu Software Version
42.11.XX/52.10.XX or Higher (PCI 5)**

<1> FONT TYPE: ENHANCED/NORMAL

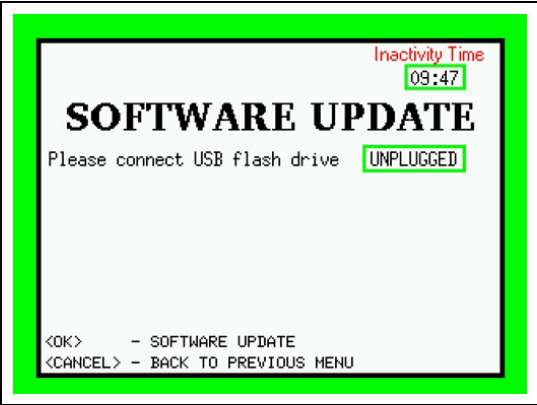
**Pump Menu Software Version
42.11.XX/52.10.06 or Higher (PCI 5)**

<1> PUMP ID: 1-16
<2> PROTOCOL: GILBARCO/ WAYNE
<3> BAUDRATE: default/1200/2400/4800/9600/19200
/38400/57600/115200

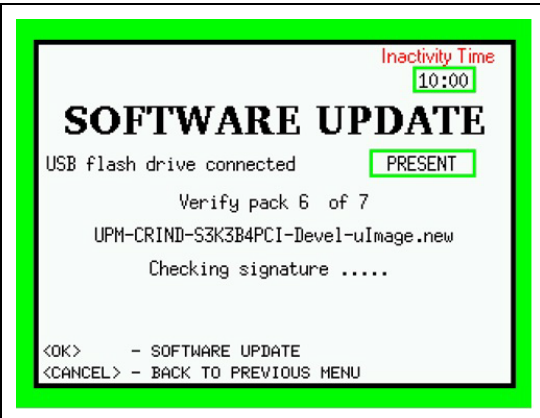
SECTION 5 - APPENDIX

Software Update

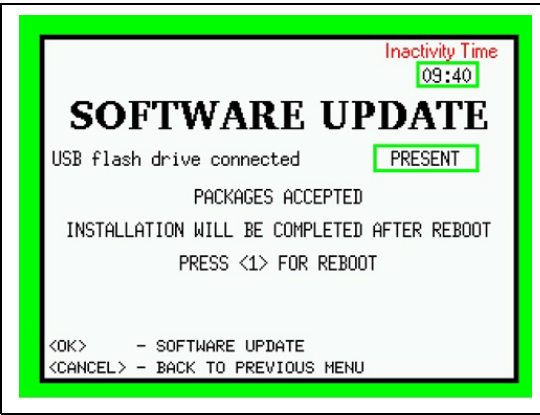
The following table describes software update features:

Description	Screen
<p>In the Software Update menu, you can update the current M7 software version using a USB stick.</p> <p>The status strings displayed are "Please connect USB flash drive" when the USB is unplugged and "USB flash drive connected" when it is plugged in.</p> <p>A box indicates the status "UNPLUGGED" or "PRESENT". The system goes back to the previous menu when the USB unplug event is triggered.</p> <p><i>Note: The USB stick with the correct software version update must be prepared with M7 maintenance tool.</i></p>	 <p>The screenshot shows a green-bordered screen titled "SOFTWARE UPDATE". At the top right, "Inactivity Time" is displayed as "09:47". The main text says "Please connect USB flash drive" followed by a green box containing the word "UNPLUGGED". At the bottom, there are two options: "<OK> - SOFTWARE UPDATE" and "<CANCEL> - BACK TO PREVIOUS MENU".</p>

All the packages of the software to be used for the update must be stored inside the USB stick in a specific folder structure: X:\gvr\software\ with *.new extensions.



After the USB has been plugged in, press **OK** to start the software update. When the software download is completed, press **1** to reboot the unit and flash the software.



SECTION 5 - APPENDIX

USB stick folders:

The root folder is “gvr”. Folders listed below are within the “gvr” folder.

- **Software folder:** in this folder the software has to be updated (both applications and firmware).
 - The binary files have to be “.new” extension.
- **standard_log folder:** where standard log is saved/retrieved.
 - PPN sub folders
- **secure_log folder:** where PCI secure log is saved/retrieved.
 - PPN sub folders
- **systemInfo folder:** where system information is saved/retrieved.
 - PPN sub folders

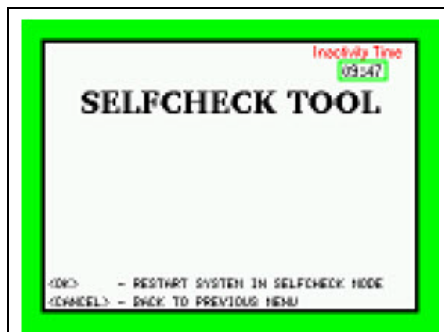
Selfcheck Tool

In the Selfcheck Tool menu, you can start the M7 Diagnostic application to verify:

- Keypad
- Display
- Card Reader
- Softkeys
- Printer
- TRIND
- Switch Video
- Americans with Disabilities Act (ADA) Keypad
- Contactless Card Reader
- Banknote Acceptor
- Barcode Scanner
- Card Data Encryption (PCI 5.X)

Press **OK** and after few seconds the unit restarts in the diagnostic mode.

Figure 20: Selfcheck Tool



SECTION 5 - APPENDIX

Figure 21: Diagnostic Mode - 42.06.XX

<div> <div>Auto Exit 179 secs</div> <div>CONFIGURATION IN PROGRESS</div> <div>Please wait ...</div> <div>SPOTCheck V04.00.06 rev.1082</div> </div>														
<div> <div>Auto Exit 160 secs</div> <div>Main Menu</div> <div> <div>DEVICE STATUS</div> <table border="1"> <tr> <td>CardR:</td> <td>[OK]</td> <td>ClassOR:</td> <td>[OK]</td> </tr> <tr> <td>Printer:</td> <td>[OK]</td> <td>TRIND:</td> <td>[NC]</td> </tr> <tr> <td>Barcode S:</td> <td>[ERR]</td> <td>BNA:</td> <td>[NC]</td> </tr> </table> </div> <div> <div>Exit</div> <div>SPOTCheck V04.00.06 rev.1082</div> <div>Refresh</div> </div> </div>	CardR:	[OK]	ClassOR:	[OK]	Printer:	[OK]	TRIND:	[NC]	Barcode S:	[ERR]	BNA:	[NC]	<div> <div>Auto Exit 177 secs</div> <div>Test Menu 1</div> <div> <div>TRIND</div> <div>Card Readers</div> <div>Barcode Scanner</div> <div>Previous Menu</div> </div> <div> <div>Printer</div> <div>Keyboards</div> <div>Display</div> <div>Next Page</div> </div> <div> <div>SPOTCheck V04.00.05 rev.1078</div> </div> </div>	<div> <div>Auto Exit 173 secs</div> <div>Test menu 2</div> <div> <div>Feature Connector</div> <div>Bank Note Acceptor</div> <div>Secure Audio</div> <div>Previous Page</div> </div> <div> <div>SPOTCheck V04.00.05 rev.1078</div> </div> </div>
CardR:	[OK]	ClassOR:	[OK]											
Printer:	[OK]	TRIND:	[NC]											
Barcode S:	[ERR]	BNA:	[NC]											
<div> <div>Auto Exit 179 secs</div> <div>Card Reader menu</div> <div> <div>Card Reader Diagnostics</div> <div>Type: Manual</div> <div>Model: Verifone LP300</div> <div>S/N: 86037446</div> <div>Firmware Ver: 53332 -00190400</div> <div>Show test Statistics</div> <div>Insert SPOTCheck Diagnostic Test Card</div> <div>Previous Menu</div> </div> <div> <div>SPOTCheck V04.00.05 rev.1078</div> </div> </div>	<div> <div>Auto Exit 179 secs</div> <div>CTLS Reader Menu</div> <div> <div>Contactless Reader Diagnostics</div> <div>S/N: 86037446</div> <div>Model: UA400</div> <div>Show test Statistics</div> <div>Present SPOTCheck contactless diagnostic test card in front of reader.</div> <div>Previous Menu</div> </div> <div> <div>SPOTCheck V04.00.05 rev.1078</div> </div> </div>	<div> <div>Auto Exit 177 secs</div> <div>Keyboards Menu</div> <div> <div>Keyboard test selector</div> <div>Main Keypad</div> <div>Soft Keys</div> <div>ADA Keypad</div> <div>Previous Menu</div> </div> <div> <div>SPOTCheck V04.00.00 rev.909</div> </div> </div>												
<div> <div>Auto Exit 176 secs</div> <div>TRIND Menu</div> <div> <div>TRIND Diagnostics</div> <div>Show test Statistics</div> <div>Present test Tag in front of the TRIND</div> <div>Previous Menu</div> </div> <div> <div>SPOTCheck V04.00.00 rev.909</div> </div> </div>	<div> <div>Auto Exit 150 secs</div> <div>Barcode menu</div> <div> <div>Barcode Scanner Diagnostics</div> <div>S/N:</div> <div>Model: Ust2DImager</div> <div>Present barcode in front of scanner.</div> <div>0000</div> <div>Previous Menu</div> </div> <div> <div>SPOTCheck V04.00.05 rev.1078</div> </div> </div>	<div> <div>Auto Exit 156 secs</div> <div>BNA Menu</div> <div> <div>Bank Note Acceptor Diagnostics</div> <div>Bank Note Acceptor F/W:</div> <div>SODECO—58-06</div> <div>BNA Test Statistics</div> <div>Begin Test</div> <div>Previous Menu</div> </div> <div> <div>SPOTCheck V04.00.05 rev.1078</div> </div> </div>												
<div> <div>Auto Exit 176 secs</div> <div>Display menu</div> <div> <div>DISPLAY Diagnostics</div> <div>Type: A4</div> <div>Model: LCD module</div> <div>Resolution: 640pxX480pxX16 bit color.</div> <div>Press Begin Test to start the test.</div> <div>Summary at any time will bypass tests.</div> <div>Previous Menu</div> </div> <div> <div>SPOTCheck V04.00.00 rev.909</div> <div>Summary</div> </div> </div>	<div> <div>Auto Exit 176 secs</div> <div>Feature connector menu</div> <div> <div>Feature Connector</div> <div>Previous Page</div> </div> <div> <div>SPOTCheck V04.00.00 rev.909</div> </div> </div>	<div> <div>Auto Exit 176 secs</div> <div>Secure Audio Menu</div> <div> <div>Secure Audio Diagnostics</div> <div>Begin Test</div> <div>Press Begin Test to start the test.</div> <div>Summary at any time will bypass tests.</div> <div>Previous Menu</div> </div> <div> <div>SPOTCheck V04.00.00 rev.909</div> <div>Summary</div> </div> </div>												
<div> <div>Auto Exit 158 secs</div> <div>Print Menu</div> <div> <div>Printer test and report printouts</div> <div>Sys. Health Report</div> <div>Device Type: Thermal Printer</div> <div>Device Model: C56</div> <div>Test Report</div> <div>Previous Menu</div> </div> <div> <div>SPOTCheck V04.00.08 rev.1132</div> </div> </div>														

SECTION 5 - APPENDIX

Figure 22: Diagnostic Mode - Software Version 42.11.XX/52.10.XX (PCI 5)

<div>Auto Exit 178 secs</div> <div>CONFIGURATION IN PROGRESS</div> <div>Please wait ...</div> <div>SPOTCheck V04.00.06 rev. 1082</div>	<div>Auto Exit 104 secs</div> <div>INITIALIZATION PHASE</div> <div>Please wait ...</div> <div>SPOTCheck V04.00.12 rev. 1262</div>	<div>Auto Exit 160 secs</div> <div>Main Menu</div> <div>DEVICE STATUS</div> <table><tr><td>CardR:</td><td>[OK]</td><td>Class-CR:</td><td>[OK]</td></tr><tr><td>Printer:</td><td>[OK]</td><td>TRIND:</td><td>[N/C]</td></tr><tr><td>Barcode S:</td><td>[ERR]</td><td>BNA:</td><td>[N/C]</td></tr></table> <div>SPOTCheck V04.00.06 rev. 1082</div> <div>Exit</div> <div>Refresh</div>	CardR:	[OK]	Class-CR:	[OK]	Printer:	[OK]	TRIND:	[N/C]	Barcode S:	[ERR]	BNA:	[N/C]
CardR:	[OK]	Class-CR:	[OK]											
Printer:	[OK]	TRIND:	[N/C]											
Barcode S:	[ERR]	BNA:	[N/C]											
<div>Test Menu 1</div> <div>Auto Exit 177 secs</div> <div>TRIND</div> <div>Printer</div> <div>Card Readers</div> <div>Keyboards</div> <div>Barcode Scanner</div> <div>Display</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.05 rev. 1078</div> <div>Next Page</div>	<div>Test Menu 2</div> <div>Auto Exit 167 secs</div> <div>Feature Connector</div> <div>Card Data Encryption</div> <div>Bank Note Acceptor</div> <div>Secure Audio</div> <div>Previous Page</div> <div>SPOTCheck V04.00.12 rev. 1262</div>	<div>TRIND Menu</div> <div>Auto Exit 176 secs</div> <div>TRIND Diagnostics</div> <div>Test LED</div> <div>Show test Statistics</div> <div>Present test Tag in front of the TRIND</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.00 rev. 309</div>												
<div>Card Reader</div> <div>Card Reader Selector</div> <div>Auto Exit 177 secs</div> <div>Contact CardReader</div> <div>Contactless CardReader</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.12 rev. 1262</div>	<div>Contact Reader menu</div> <div>Card Reader Diagnostics</div> <div>Type: Manual</div> <div>Model: Vasilone U-3000</div> <div>S/N: 86007446</div> <div>Firmware Ver: 53332 30190900</div> <div>Show test Statistics</div> <div>Insert SPOTCheck Diagnostic Test Card.</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.05 rev. 1078</div>	<div>CTLS Reader Menu</div> <div>Contactless Reader Diagnostics</div> <div>S/N: 86007446</div> <div>Model: U4400</div> <div>Show test Statistics</div> <div>Present SPOTCheck contactless diagnostic test card in front of reader.</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.05 rev. 1078</div>												
<div>Barcode menu</div> <div>Barcode Scanner Diagnostics</div> <div>S/N:</div> <div>Model: Ust2DImager</div> <div>Present barcode in front of scanner.</div> <div>0000</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.05 rev. 1078</div>	<div>Printer menu</div> <div>Printer test and report printouts</div> <div>Device Type: Thermal Printer</div> <div>Device Model: C56</div> <div>Sys. Health Report</div> <div>Test Report</div> <div>Extend Rec Test</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.12 rev. 1262</div>	<div>Extended receipt menu</div> <div>Auto Exit 156 secs</div> <div>ADA Extend Receipt Diagnostics</div> <div>ADA Extend Receipt: Supported</div> <div>Press Begin Test to start the test.</div> <div>Show Test Statistics</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.12 rev. 1262</div>												
<div>Keyboards Menu</div> <div>Keyboard test selector.</div> <div>Auto Exit 177 secs</div> <div>Main Keypad</div> <div>Soft Keys</div> <div>ADA Keypad</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.00 rev. 309</div>	<div>Main Keypad Menu</div> <div>Keypad Diagnostics</div> <div>Hardware ID: 0000</div> <div>Type: Numeric</div> <div>S/N: 0002061101582962</div> <div>Begin Test</div> <div>Show Statistics</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.12 rev. 1262</div>	<div>Softkeys Menu</div> <div>Auto Exit 176 secs</div> <div>Begin Test</div> <div>Show Statistics</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.12 rev. 1262</div>												
<div>ADA Menu</div> <div>Auto Exit 173 secs</div> <div>Begin Test</div> <div>Show Statistics</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.12 rev. 1262</div>	<div>Display menu</div> <div>DISPLAY Diagnostics</div> <div>Type: A4</div> <div>Model: LCD module</div> <div>Resolution: 640pxX480pxX16 bit color.</div> <div>Press Begin Test to start the test.</div> <div>Summary at any time will bypass tests.</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.00 rev. 309</div> <div>Summary</div>	<div>Feature connector menu</div> <div>Auto Exit 178 secs</div> <div>Feature Connector</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.00 rev. 309</div>												
<div>Banknote acceptor menu</div> <div>Bank Note Acceptor Diagnostics</div> <div>Auto Exit 155 secs</div> <div>Bank Note Acceptor F/W: SODECO—5806</div> <div>BNA Test Statistics</div> <div>Begin Test</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.05 rev. 1078</div>	<div>Secure Audio Menu</div> <div>Secure Audio Diagnostics</div> <div>Auto Exit 176 secs</div> <div>Begin Test</div> <div>Press Begin Test to start the test.</div> <div>Summary at any time will bypass tests.</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.00 rev. 309</div> <div>Summary</div>	<div>Card Data Encryption</div> <div>Card Data Encryption</div> <div>Auto Exit 167 secs</div> <div>Vaultfield Plugin</div> <div>Previous Menu</div> <div>SPOTCheck V04.00.12 rev. 1262</div>												

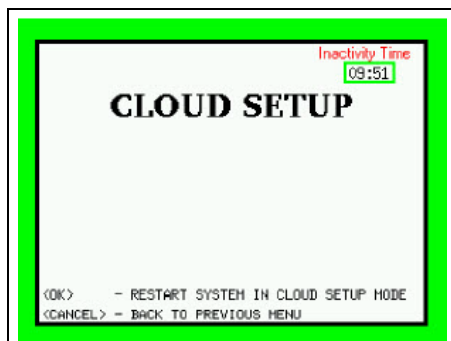
For more information, refer to *MDE-5223 FlexPay IV CRIND Service/Troubleshooting Guide* and *MDE-5227 M7 Maintenance Tool User Guide*.

SECTION 5 - APPENDIX

Cloud

In the Cloud menu, open Cloud application to configure all the parameters to initialize the Cloud remote application.

Figure 23: Cloud Setup



5

Secure Menu

To access the Secure Menu, proceed as follows:

- 1 Contact the Gilbarco Support Center at 1-800-800-7498 for a secure verification code.
Note: The code provided can be reused 10 times in 12 hours and is valid until the system activation is performed.

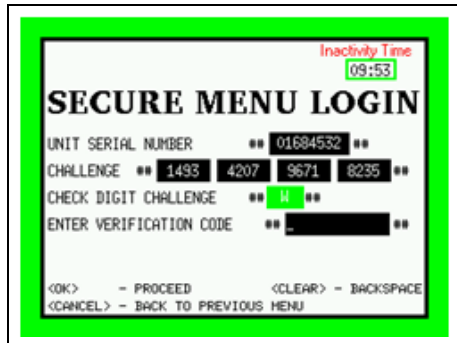
The Challenge Menu is shown when there is no secure session ongoing.

- 2 Provide the UNIT SERIAL NUMBER and the Challenge code to the Gilbarco Support Center when you call for a verification code.
Notes: 1) The Check digit is useful to verify if the Challenge code is properly understood by the Gilbarco Support Center.
2) The Challenge code will be available for 10 minutes, after which it is mandatory to generate a new one.

If you return to the system menu after 10 minutes of inactivity and press Secure Menu again, a new Challenge code is generated.

SECTION 5 - APPENDIX

Figure 24: Secure Menu Login



Accessing Secure Menu During Ongoing Session

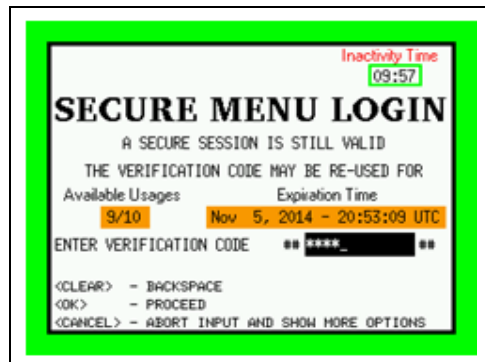
To access the Secure Menu during an ongoing session, proceed as follows:

- 1 Enter the right verification code retrieved in the previous maintenance session to access the Secure Menu.

The current available usages and the Secure session expiration time are shown (see [Figure 25](#)).

This menu is also shown when the user tries to enter the Secure Menu after timing out from inactivity.

Figure 25: Secure Session - Expiration Timeout



- 2 Press **Cancel** and select **<1>** to start a new maintenance session.

Notes: 1) The token session is invalidated and a new Challenge code is generated and displayed.

- 2) *The unit restarts after three consecutive unsuccessful attempts of entering verification code.*

SECTION 5 - APPENDIX

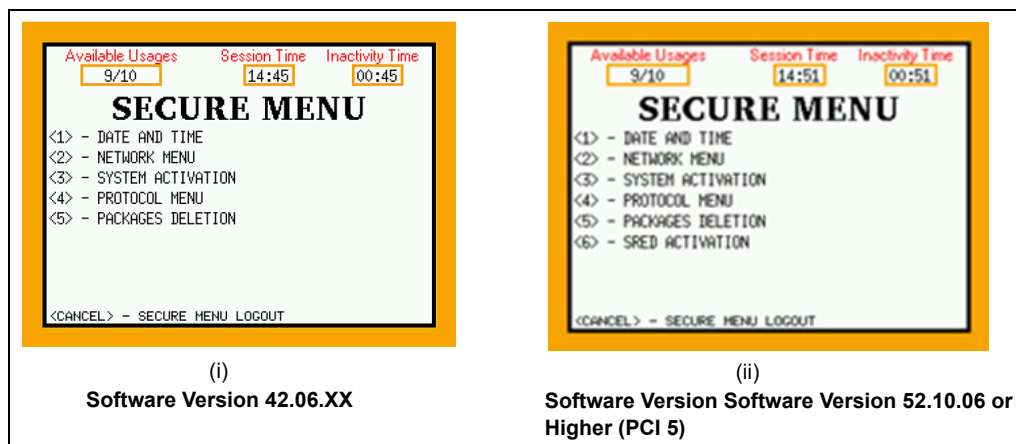
Performing Maintenance Operations in Secure Menu

The following maintenance operations can be performed in the Secure Menu:

- Set Date and Time
- Set Network
- Activate the Unit
- Enable/disable mutual authentication connection
- Delete Packages
- Enable SRED mode (PCI 5 only)

Note: The menu lists sensitive operations.

Figure 26: Secure Menu - Maintenance Operations



Unlike the case in Non-Secure (green) Menu, the Secure Menu has two different time-out options:

- **Session Time-out (15 minutes):** A secure session cannot be longer than 15 minutes. If the time-out expires, the system is directed back to the Authentication menu.
- **Inactivity Time-out (1 minute):** Press a key to keep the session alive, otherwise the session expires and the system is directed back to the Authentication menu.

SECTION 5 - APPENDIX

Date and Time Menu

In the Date and Time menu, the user can configure and properly set the date and time of the unit.

Notes: 1) Aligned date and time is important for log analysis and troubleshooting.

2) Ensure that the time zone is set in the green menu.

Figure 27: Date and Time Menu Screen

Available Usages Session Time Inactivity Time

9/10 14:12 00:41

DATE AND TIME

UTC time: 2016-09-20 16:41:16

Timezone: America/Chicago

<1>LocalTime[YYYY-MM-DD]: 2016-09-20 11:41:16

<OK> - SAVE CHANGES AND GO BACK

<CANCEL> - UNDO ALL CHANGES AND GO BACK

Software Version 42.06.XX/42.11.XX/52.10.06
or Higher (PCI 5)

SECTION 5 - APPENDIX

Network Menu

In the Network Menu, you can configure and set the system network configuration. If the VFI device is connected and the FlexPay IV CRIND is a Side A, the reader and external GSoM IP configuration can be performed following the wizard procedure:

- 1 Set UPM <1> IP address, <2> Subnet mask, and <3> Default gateway.
- 2 Press **OK** to proceed or <5> for Auto Configuration.

In sequence, the procedure will set the card reader and other devices (GSoM) IP address for both sides.

Figure 28: Configuring System Network



Notes: 1) The IP value must be chosen after analyzing the complete configuration (GSoM, card reader, SmartCRIND, etc.). If an IP address > 240 is chosen, a warning is displayed on the UPM menu.

- 2) The GSoM IP address set is not confirmed in the above screen. To check it, refer to ["Other Device IP Assignment"](#) on [page 39](#).

SECTION 5 - APPENDIX

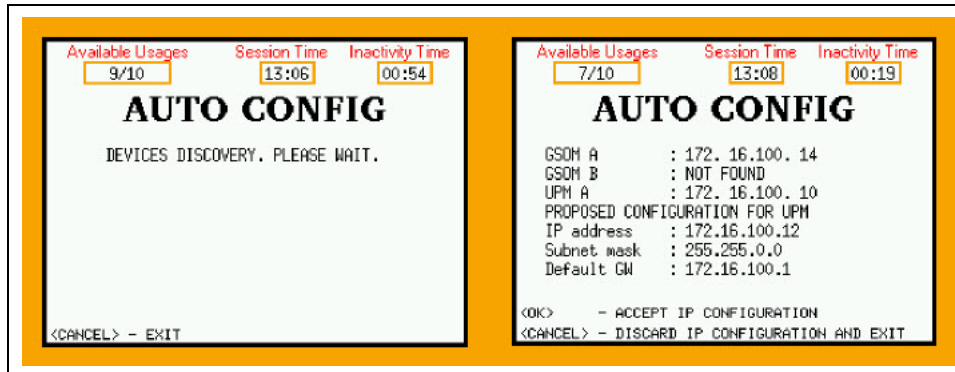
Autoconfiguration <5>

Auto Configuration proposes a network configuration for a UPM based on the IP addresses of the devices already present into a dispenser. This procedure is useful when a user wants to replace a UPM in a dispenser and doesn't know the previous IP address, or during Side B configuration.

A new screen with a suggested configuration is shown:

If the user presses <OK>, the Network Menu screen is displayed again with the updated IP address, subnet mask, and default gateway and the procedure to set the configuration can begin.

Figure 29: Auto Config Screen



Error Case

In case of connection problems with devices or IP collision, the procedure could fail. Specific error messages are provided to inform about the problem.

To resolve the IP conflict, proceed as follows:

- 1 Set UPM IP address to a known value that is not used (i.e., x.x.x.100).
- 2 Press **OK**.
- 3 Press **Cancel** when the system prompts to press VFI device config button.
- 4 Press **Cancel** twice to restart the unit.
- 5 Select the network config menu.
- 6 Set the required UPM IP address.
- 7 Set the subnet mask.
- 8 Press **OK** to confirm (see sequence above).
- 9 Restart the unit.

SECTION 5 - APPENDIX

System Activation Menu

In the System Activation menu, you can activate all the dismounting sensors of the system.

Activation is required in the following cases:

- Display cable is disconnected from UPM.
- UPM removal sensor is disengaged.
- Card reader removal sensor is disengaged.

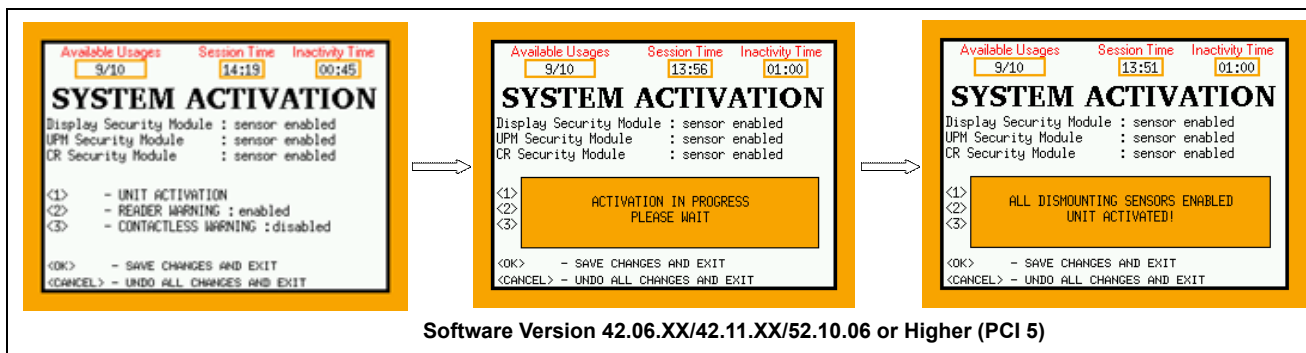
The System Activation menu displays the current activation status of the unit.

Note: The unit is not operative when any or all of the three dismounting sensors are not activated.

To activate the unit, press <1> when all the sensors are engaged.

Note: Successful activation procedure invalidates the verification code. The code provided can be reused 10 times in 12 hours and is valid until any part of the system is activated.

Figure 30: System Activation - Enabling Dismounting Sensors



Every time a module is activated, the external switches or the dismounting sensors have to be engaged.

IMPORTANT INFORMATION



Ensure that the units in use (typically development use) are not left loose (not mounted on any chassis in a way that sensors are kept closed). The activation process might be prevented if the sensors are left open.

SECTION 5 - APPENDIX

To activate a master device means to activate the dismounting sensor/external switch monitoring the part and to let the software start waiting for a master device (POS) connection.

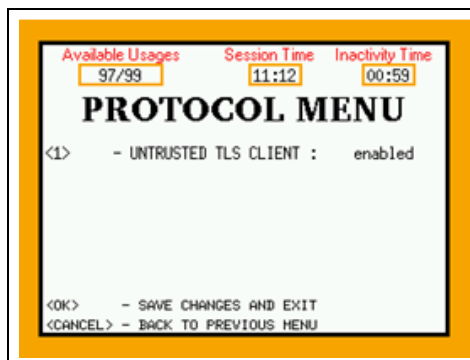
Note: After restarting the system following the activation, a screen with a blue background is displayed, indicating the SYSTEM OFFLINE status, until the connection to a master device is established.

Protocol Menu

In the Protocol Menu, the user can enable or disable mutual authentication on the unit.

Note: Set UNTRUSTED Transport Layer Security (TLS) CLIENT to enabled. If disabled, POS is forced to have valid TLS certificates stored.

Figure 31: Protocol Menu Screen

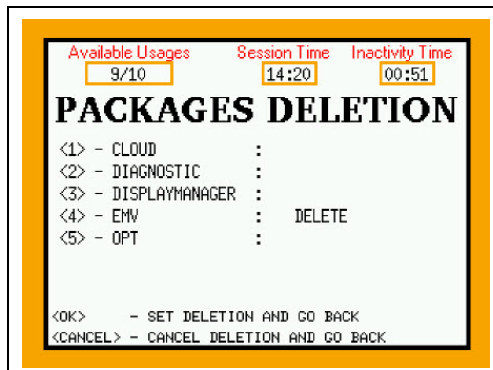


5

Package Deletion

In the Package Deletion menu, you can delete application packages in case of unrecoverable error or a wrong spot software update.

Figure 32: Packages Deletion Screen



Select the package to remove pressing the relative keypad button and press **OK**. At the first reboot, the spot removes the requested package.

SECTION 5 - APPENDIX

SRED Activation

In the SRED Activation menu, you can permanently activate SRED functionality on the system.

Figure 33: SRED Activation



5

Note: This operation is one-way only; once enabled, SRED cannot be disabled.

After the SRED is activated, the system reports the message “SRED Enabled” on the Splash screen.

Figure 34: SRED Enabled



SECTION 5 - APPENDIX

5

This page is intentionally left blank.

The Advantage® Series, CRIND®, Eclipse®, Encore®, Gilbarco®, and TRIND® are registered trademarks of Gilbarco Inc. Applause™ Media System, E-CIM™, FlexPay™, Insite360™, Passport™, and SmartCRIND™ are trademarks of Gilbarco Inc. Chrome™ is a trademark of Google Inc. EMV® is a registered trademark of EMVCo LLC. Ethernet® is a registered trademark of Xerox Corporation. Europay® and MasterCard® are registered trademarks of MasterCard International Inc. Firefox® is a registered trademark of Mozilla Corporation. Google® is a registered trademark of Google Inc. Hengstler® is a registered trademark of Danaher Corporation. Windows® is registered trademarks of Microsoft Corporation. NEC® and NFPA 70® are registered trademarks of the National Fire Protection Association. Veeder-Root® is a registered trademark of Veeder-Root Company. Visa® is a registered trademark of Visa Inc.



© 2019 Gilbarco Inc.
7300 West Friendly Avenue · Post Office Box 22087
Greensboro, North Carolina 27420
Phone (336) 547-5000 · <http://www.gilbarco.com> · Printed in the U.S.A.
MDE-5221J FlexPay™ IV CRIND® Start-up Manual · October 2019