

FlexPay™ IV (with Omnia) Programming and Service Manual Insite360™ Forecourt with Applause® Media System

Computer Programs and Documentation

All Gilbarco Inc. and/or Veeder-Root Company computer programs (including software on diskettes and within memory chips) and documentation are copyrighted by, and shall remain the property of, Gilbarco Inc. and/or Veeder-Root Company. Such computer programs and documents may also contain trade secret information. The duplication, disclosure, modification, or unauthorized use of computer programs or documentation is strictly prohibited, unless otherwise licensed by Gilbarco Inc. and/or Veeder-Root Company.

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.

Supplier's Declaration of Conformity

47 CFR § 2.1077 Compliance Information

Unique Identifier: OMNIA M16183

Responsible Party – U.S. Contact Information

Gilbarco Veeder-Root
7300 West Friendly Avenue
Greensboro, North Carolina, USA
27410-6200
1-336-547-5000

FCC Compliance Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interferences that may cause undesired operation.

Approval

Gilbarco is an ISO 9001:2008 registered company.

Underwriters Laboratories (UL):

UL File#	Products listed with UL
MH1941	All Gilbarco pumps and dispensers that bear the UL listing mark.
MH8467	Transac System 1000 and PAM 1000
E105106	Dell DHM Minitower
E165027	G-SITE and Passport Systems

California Air Resources Board (CARB):

Executive Order #	Product
G-70-52-AM	Balance Vapor Recovery
G-70-150-AE	VaporVac

National Conference of Weights and Measures (NCWM) - Certificate of Conformance (CoC):

Gilbarco pumps and dispensers are evaluated by NCWM under the National Type Evaluation Program (NTEP). NCWM has issued the following CoC:

CoC#	Product	Model #	CoC#	Product	Model #
02-019	Encore	Nxx	02-036	Legacy	Jxxx
02-020	Eclipse	Exx	02-037	G-SITE Printer (Epson)	PA0307
02-025	Meter - C Series	PA024NC10		G-SITE Distribution Box	PA0306
	Meter - C Series	PA024TC10		G-SITE Keyboard	PA0304
02-029	CRIND	—		G-SITE Mini Tower	PA0301
02-030	TS-1000 Console	—		G-SITE Monitor	PA0303
	TS-1000 Controller	PA0241		G-SITE Printer (Citizen)	PA0308
	Distribution Box	PA0242	02-038	C+ Meter	T19976
	Meter - EC Series	PA024EC10	02-039	Passport	PA0324
	VaporVac Kits	CV	02-040	Ecometer	T20453
			05-001	Titan	KXXY Series

Trademarks

Non-registered trademarks

CIM™	G-CAT™	Making Things Better™	Super-Hi™
C-PAM™	Gilbert™	MPD™	Surge Management System™
Dimension™	G-SITE® Link™	Optimum Series™	Tank Monitor™
Ecometer™	G-SITE® Lite™	PAM 1000™	TCR™
ECR™	G-SITE™	PAM 5000™	Titan™
EMC™	Highline™	PAM™	The Advantage™ Series
Eclipse™	Horizon™	SMART CRIND™	Ultra-Hi™
e-CRIND™	InfoScreen™	SMART Meter™	ValueLine™
FlexPay™	MultiLine™	SmartPad™	

Registered trademarks

Applause® Media System
CRIND®
Encore®
Gilbarco®
Legacy®
Passport®
Performer®
Transac®
TRIND®
VaporVac®

Service mark

GOLD SM

Additional U.S. and foreign trademarks pending.

All product names, logos, and brands are the property of their respective owners and are for identification purposes only.

Use of these names, logos, and brands does not imply endorsement.

Table of Contents

1 – Introduction	1-1
Purpose	1-1
Overview	1-1
Insite360 Forecourt Escalation for Technicians	1-2
Forecourt Networking Scheme	1-2
Physical Connectivity	1-4
Using FlexPay Connect v2	1-4
Using Direct Ethernet (CAT5/CAT6 or Equivalent) Connections	1-5
Using Pre-existing FlexPay Connect v1	1-6
Common Types of Site Networking Schemes	1-7
Required Tools, Equipment, Parts, and Software	1-7
Recommended High-Level Installation Process Scenarios	1-8
New FlexPay IV CRIND High-Level Installation	1-8
Retrofit Installation Process from FlexPay II	1-8
Retrofit Installation Process from FlexPay IV	1-9
Related Documents	1-10
Abbreviations and Acronyms	1-11
2 – Important Safety Information	2-1
3 – Installation Checklists	3-1
4 – Configuring FlexPay IV	4-1
Pre-requisites for Installing Omnia in FlexPay IV	4-1
Configuring UPM Settings	4-2
Configuring CRINDBIOS	4-6
5 – Configuring Omnia PCB	5-1
Verifying the UPM and Software Versions	5-1
Logging In to Omnia	5-1
Omnia Configurator - Creating a New Configuration	5-8
Omnia Configurator - General Settings	5-8
Omnia Configurator - Applause	5-12
Omnia Configurator - Insite 360	5-14
Omnia Configurator - Open Apps Configuration	5-17
Omnia Configurator - RTP Proxy Configuration (Optional)	5-18
Omnia Configurator - Tools	5-19
Omnia Configurator - Diagnostic	5-33
Viewing and Testing Sniffer, Certificates, and Serial Connection	5-40
Registering Omnia to Insite 360 Forecourt	5-43
Insite360 Auto-Registration	5-50
Omnia Home Page	5-52
Status Icons and Virtual LEDs	5-57

6 – Omnia Maintenance Through USB	6-1
Introduction	6-1
Requirements	6-1
USB Drive Preparation	6-1
LEDs Glowing Sequence	6-2
OmniaOp.JSON File Syntax	6-3
Installing Packages	6-4
Checking Package Installation Report on the USB Drive	6-5
Retrieving Logs	6-5
Log Retrieval Report and Checking Files on the USB Drive	6-6
Retrieving Omnia Configuration (NO Network Reset)	6-7
Retrieving the Omnia Configuration (YES Network Reset)	6-8
Retrieving the Omnia Configuration and Checking Files on the USB Report	6-9
7 – Troubleshooting	7-1
Enabling and Disabling the Beeper Alarm from the Web UI	7-2
Enabling and Disabling the Beeper Alarm from Insite360	7-3
Connection Board Light Emitting Diodes (LEDs)	7-6
Pump Serial Cable Disconnect Alarm	7-8
PIP3 Connections	7-9
Insite360 Forecourt Dispenser Troubleshooting	7-10
Omnia Encore Dispenser Troubleshooting	7-15
AWS IoT Registration and Migration Troubleshooting	7-20
De-Registration from AWS IoT Gateway	7-23
Retrieving the Omnia Network Configuration	7-26
Resetting the Network Configuration to Factory Values	7-27
Appendix A: Site Network Survey	A-1
Appendix B: FlexPay IV Applause® TV on Invenco Cloud Services (ICS) Migration	B-1
Software Requirements	B-1
Site Survey, Dispenser, and POS Requirements	B-1
Insite360 Forecourt Whitelisting/End Point Requirements for AWS-IoT and Invenco/ICS	B-2
Migration Instructions	B-3
Troubleshooting	B-4
Message “Warning! Update in progress! Verifying package signature”	B-4
“Errors during software updating - Errors installing OpenApp packages”	B-5
Verify Omnia is Ready to Connect to ICS and Installation is Successful	B-6
Appendix C: Legacy Gateway	C-1
Registering Omnia to Insite360 Forecourt	C-1
Completing the Programming	C-3
De-registering Omnia from Insite360 Forecourt	C-4
GVR Cloud Registration Error Cases	C-5
Index	Index-1

1 – Introduction

Purpose

This manual provides instructions for the following:

- Set or modify the IP configuration for FlexPay™ IV CRIND®
- Configure the Omnia board
- Set up the Applause® Media System connectivity
- Register with Insite360™ Forecourt for remote management

This manual also includes common troubleshooting and verification steps to ensure network connectivity of dispensers.

Overview

The Omnia Printed Circuit Board (PCB) inside the dispenser serves the following purposes:

- Creating a Local Area Network (LAN) within the dispenser, so that the Internet Protocol (IP) addresses of the Ethernet® connected devices inside the dispenser are no longer exposed on the site Wide Area Network (WAN).
- Functioning as a router and firewall, only exposing the A and B side CRIND devices to the forecourt.
- The configuration of the forecourt IP address, media, and Insite360 is performed on a single web page.
- Running two-wire proxy applications that allow connection from the Point of Sale (POS) to the CRIND and the pump.
- Allows the pump and CRIND serial interfaces to run through the Omnia board instead of the UPM. The UPM and Omnia manage the pump and CRIND through TCP.
- FlexPay IV GSoMs are removed and the media client runs on the Omnia.
- SSoM is removed and the Omnia manages the remote connection to the Insite360 server.

This manual provides service information and guidance on the following:

- Networking configuration of FlexPay IV CRIND terminals equipped with Omnia
- Software configuration of Omnia (network settings/Cloud/media)
- Registration of the dispensers to the Insite360 Forecourt

Note: Site network rules MUST be updated to allow access to AWS IoT servers (Customer IT personnel or supporting ASC technician for site) prior to any Omnia software upgrades and AWS IoT registration attempt. This may have to be done way in advance as Network approval can take time. Contact the customer IT department to ensure that this has been completed.

Insite360 Forecourt Escalation for Technicians

For issues that occur while installing and starting up Insite360 Forecourt, you can escalate as follows:

Issues	Contact Information
All third-party devices	Consult the third-party device support or Site IT Specialist.
For network-related query regarding any existing backroom configurations and/or the site-specific network IP scheme (such as Default Gateway/DNS IPs, Internet Service Provider (ISP) router location and rules/firewall setup, etc.)	Consult the Site IT Specialist or Site Management to fill out the Network Survey Form in "Appendix A: Site Network Survey" on page A-1 .
For Insite360 Forecourt registration issues	Contact the Insite360 Forecourt Help Desk at 877-503-4971.
For any Gilbarco® Insite360 Forecourt hardware in the dispenser or backroom issues	Call Service Station Equipment (SSE) Technical Assistance Center (TAC) at 1-800-743-7501.
For any Insite360 Forecourt site configuration issues during start-up (beyond Registration and Feature Testing)	Call Service Station Equipment (SSE) TAC at 1-800-743-7501.

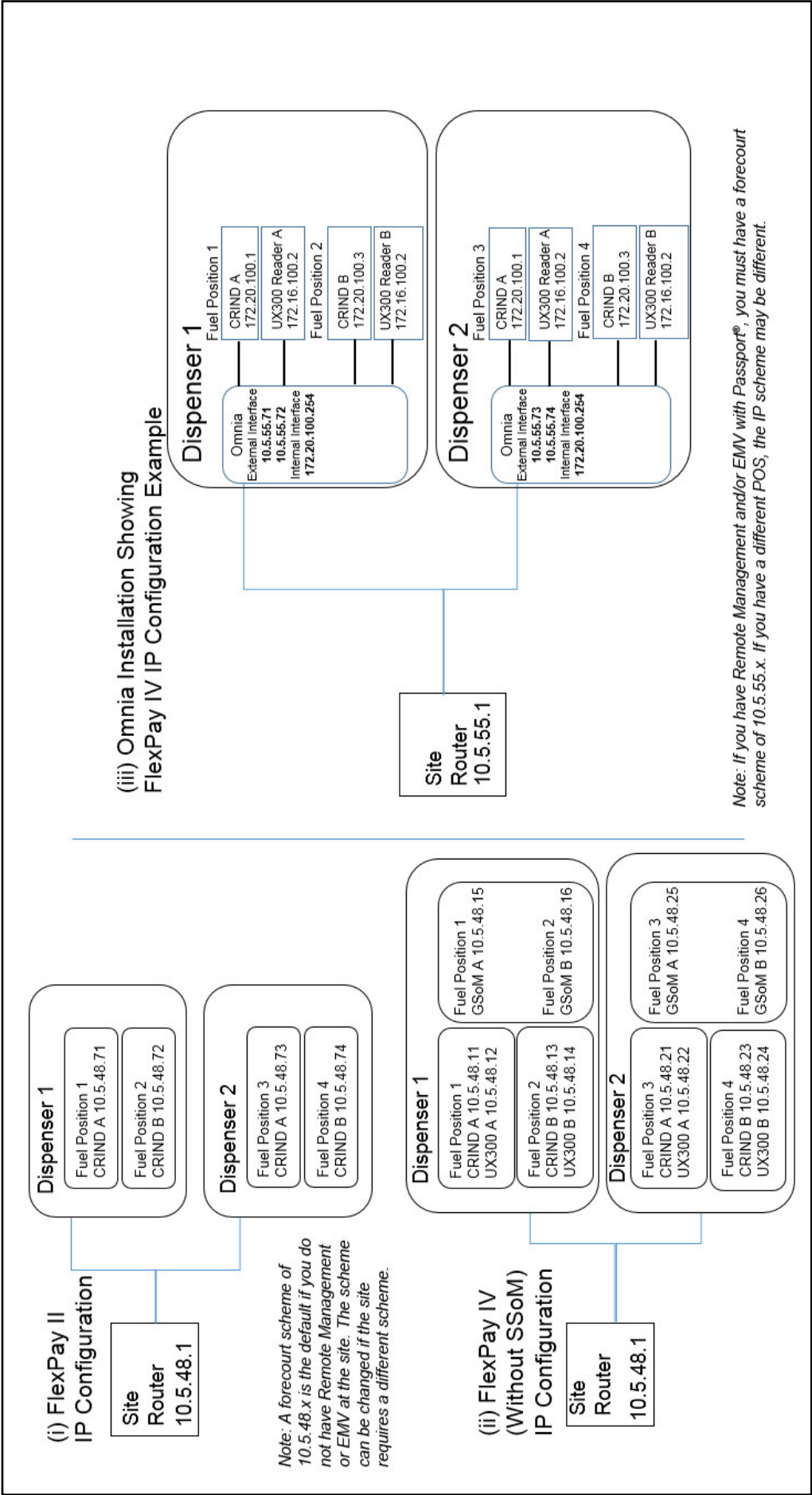
Forecourt Networking Scheme

The main difference introduced by the Omnia in the site networking scheme is that the payment terminal (FlexPay IV) IP addresses are no longer directly exposed on the site WAN.

Only the Omnia external IP addresses are visible within the site WAN. [Figure 1-1](#) on [page 1-3](#) shows how the networking scheme is modified due to installation of Omnia.

Note: The Omnia internal CRIND IPs required for the Dispenser Connection Module (DCM) 2.x CRINDs have changed from 172.16.100.1/3 to 172.20.100.1/3. This IP is set automatically on the Universal Payment Modules (UPMs) when Omnia is selected in the CRIND configuration.

Figure 1-1: IP Configuration Comparison based on Applause, Remote Management, EMV®, and POS



The network configuration after Omnia installation, as shown in the example in [Figure 1-1](#) on [page 1-3](#), has the following characteristics:

- The Omnia performs the function of a router inside the dispenser.
- The Omnia provides two external IP addresses to the site router in the back room. These are the external addresses of side A and side B of the CRIND.
- The new CRIND internal IP addresses configured in each dispenser are the same scheme (172.20.100.1 for side A and 172.20.100.3 for side B) in all dispensers for the site as the dispenser networks are isolated from each other by the Omnia.
- Once the Omnia parameter is selected in CRIND programming, the CRIND IP will automatically be set (hardcoded) in the UPMs, and the UX300 Card Readers will always use the default 172.16.100.2.

The Omnia has a VLAN and dedicated device ports, which allow this new simplified IP configuration.

Physical Connectivity

The high-speed Ethernet connectivity between the forecourt and the backroom can be set up in the following three ways:

- FlexPay Connect v2 [Backroom Communication Module (BRCM2) or BRCM2.1 and DCM2.x, DCM3]
- Direct Ethernet [Category 5 (CAT5) or CAT6 or equivalent]
- FlexPay Connect v1 [BRCM and DCM, Global Long-Range Ethernet (GLRE)]

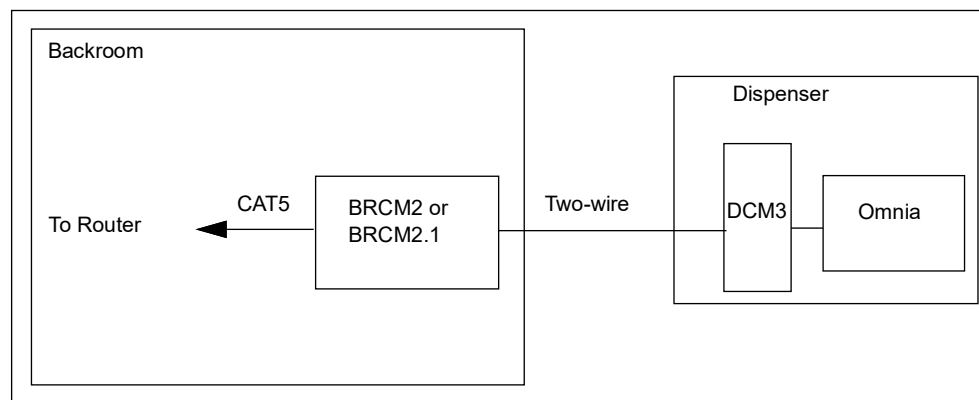
Using FlexPay Connect v2

FlexPay Connect v2 is used on sites that had no previous Ethernet connectivity to the dispensers.

FlexPay Connect v2 is usually installed by upgrading the existing Distribution Box (D-Box) in the backroom and installing an Omnia Assembly in every dispenser.

There is a 16-dispenser limit on FlexPay Connect v2. If the site has more than 16 dispensers, FlexPay Connect or direct Ethernet must be used.

Figure 1-2: Using FlexPay Connect v2 - Backroom Hardware



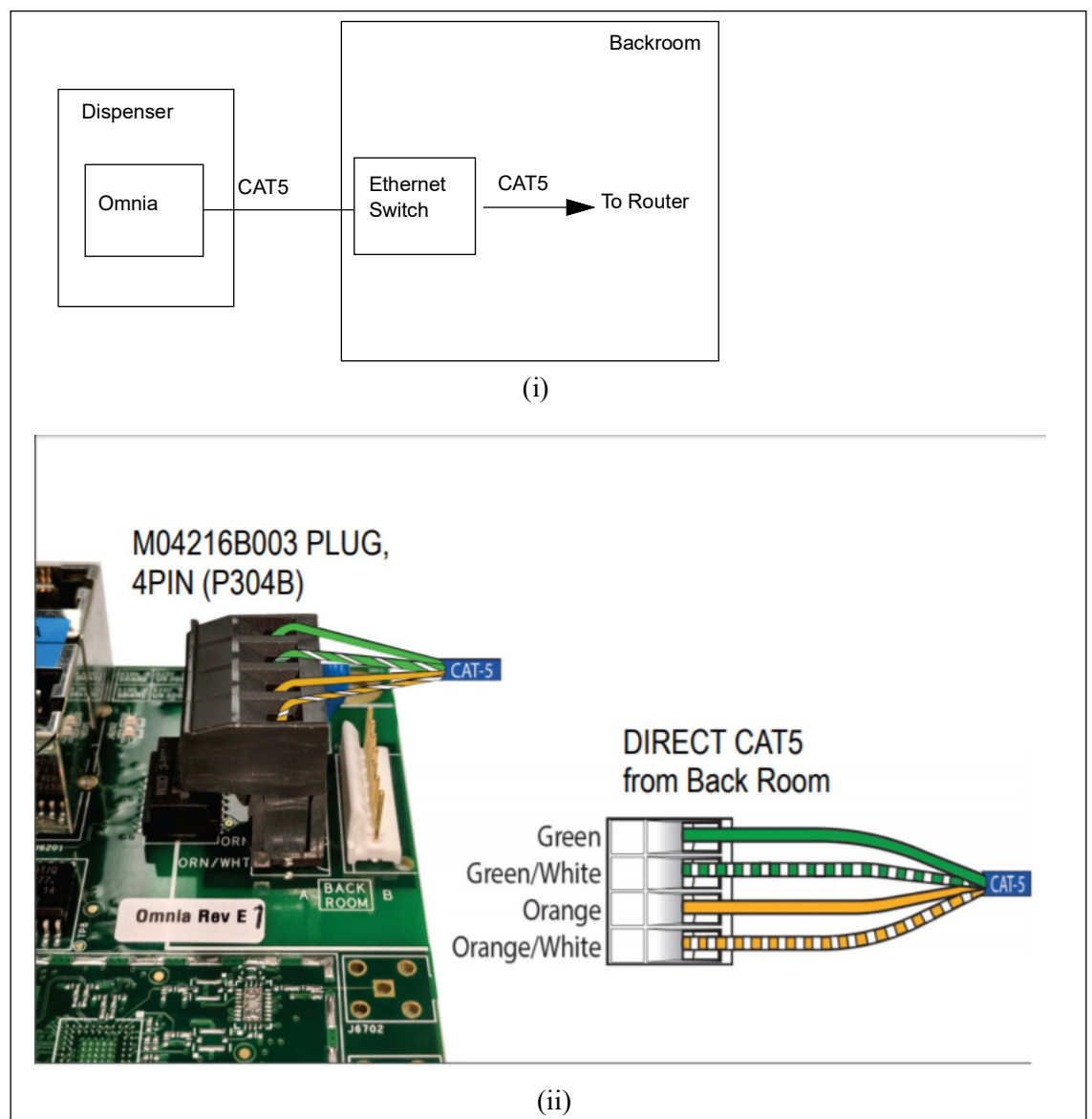
Using Direct Ethernet (CAT5/CAT6 or Equivalent) Connections

Sites where dispensers are connected directly to the backroom by Ethernet cables will require a switch to connect cables from all the dispensers.

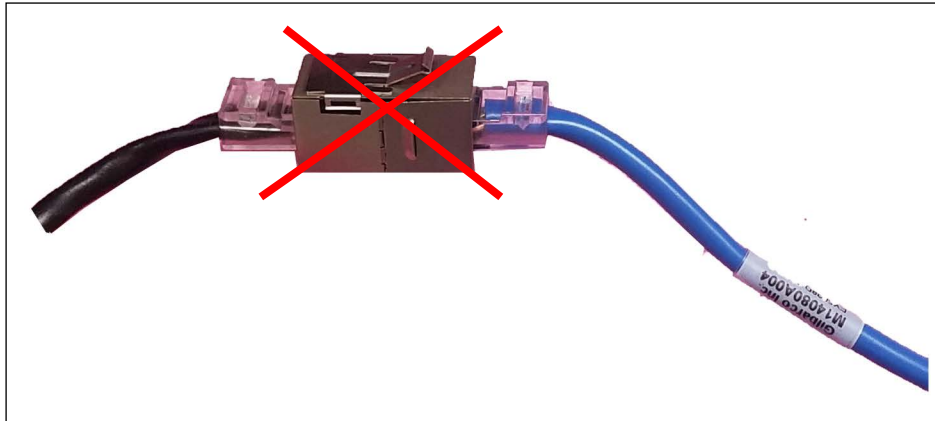
Note: Follow specific requirements when running direct CAT5 cable (for example, maximum run of 280 feet). For more information on requirements for CAT5 runs, refer to MDE-4246 Dispenser Network Connectivity Kit for Monochrome Encore 500, Encore S and Eclipse® Installation Instructions.

When using a direct CAT5 connection from the backroom for high speed, ensure that the high speed connection is disconnected from the DCM3. Do not connect P304 to the DCM3.

Figure 1-3: Using Direct Ethernet Connections - Backroom Hardware



Note: Do not use CAT5 couplers in this connection; their use can result in loss of the high speed connection.

Figure 1-4: Do Not Use Couplers

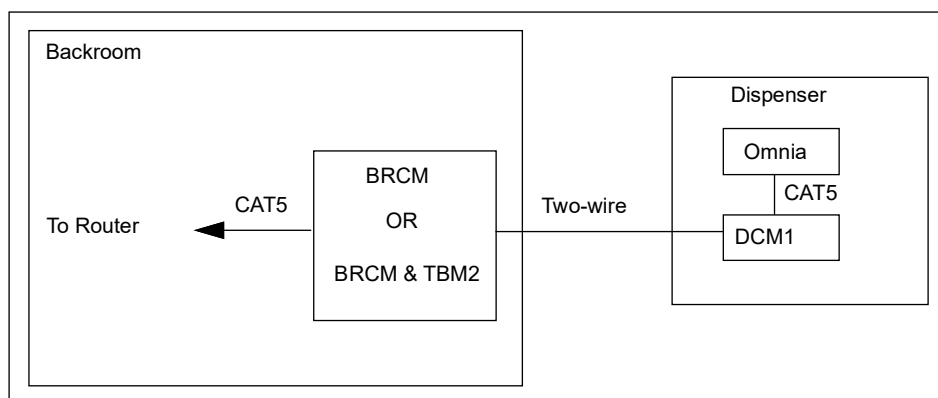
Notes: 1) The couplers can be used for lab use. Do not use the couplers in a field installation.
 2) Use the kit M18405K001 if a RJ-45 forecourt connection is desired. The RJ-45 adapter can be mounted directly on the Omnia and does not degrade the Ethernet signal like the commercial adapters.

Using Pre-existing FlexPay Connect v1

Sites equipped with FlexPay Connect v1 do not require any hardware upgrade in the backroom. These sites can continue to use the existing BRCM.

Replace the Ethernet cable with the M14080A004 Cable provided in the kit to connect to the pre-existing DCM.

Note: DCM3 is not compatible with a BRCM (GLRE).

Figure 1-5: Using Pre-existing FlexPay Connect v1 - Backroom Hardware

Common Types of Site Networking Schemes

Several details of the networking configuration (namely **External Interface IPs, Default Gateway IP, etc.**) depend on the site type and its networking scheme. For this reason, identifying the characteristics of the network at every site is a requirement for a correct installation and configuration of the devices.

Sites Using Customer-defined Networking Schemes

In some sites, the customer dictates the IP addresses to be used for the devices on the forecourt (Omnia) and in the backroom (BRCM2 or BRCM2.1, Applause Media System Site Server, and so on). This is typically the case of customers who run a sophisticated network. In these cases, it is required to comply with the customer's networking schemes.

When the networking scheme is predefined by the customer, the customer site IT department should do the following:

- Complete the Configuration Worksheet in [“Appendix A: Site Network Survey”](#) on [page A-1](#).
- Provide sufficient number of IP addresses to cover all the fueling positions, the BRCM2 or BRCM2.1, and the Applause Media System Site Server (if present).
Note: The recommended CRIND External IP addresses is 10.5.55.XX, which is as per the default IP scheme.
- Locate the router to be used to connect the BRCM2 or BRCM2.1.
- Grant access to the Internet and Domain Name System (DNS) servers.

Sites Using Default Networking Scheme

These sites use a pre-determined IP range (10.5.55.XX) to connect the dispensers. They can be further divided into two categories:

- **Applause Media System is not installed at the site**
This will require additional backroom hardware, including BRCM2 or BRCM2.1, router, CAT5 cables, etc.
- **Applause Media System is installed at the site**
These sites may be configured for dual Network Interface Card (NIC) on the Applause Site Server. This will require the use of an additional router to reconfigure the Applause Site Server to a single NIC setup.

Required Tools, Equipment, Parts, and Software

The following tools and equipment are necessary to accomplish all steps of the software configuration (Omnia, CRIND, and pump):

- Laptop computer running Windows 7, Windows 8, or Windows 10 operating systems and Chrome™ web browser
- CAT5 or CAT6 cable to connect the laptop to the Omnia Board
- RS-232 Serial cable to upgrade the pump software
- Pre-installation checklist (refer to [“Installation Checklists”](#) on [page 3-1](#))

Recommended High-Level Installation Process Scenarios

The following sections outline high-level processes for different installation scenarios.

New FlexPay IV CRIND High-Level Installation

The following installation steps are in the recommended order and are applicable for a new FlexPay IV CRIND installation with Omnia:

- 1 Utilize pre-installation, installation, and post-installation checklists in [“Installation Checklists”](#) on [page 3-1](#).
- 2 Install the Applause Media Server, if required. Refer to *MDE-4699 Applause Media System Installation, Service, and Parts Manual*.
- 3 Install the dispenser hardware in one dispenser. For more information on the Retrofit Kit or Upgrade Kit Installation Instructions, see [“Related Documents”](#) on [page 1-10](#).
- 4 Configure Omnia through Omnia Configurator Web User Interface [(UI) including Insite360 registration]. For more information, see [“Verifying the UPM and Software Versions”](#) on [page 5-1](#).
- 5 Test and verify operation of one dispenser including Applause Media System, before configuring additional dispensers.
Note: Do not proceed with the entire forecourt installation if a problem is detected with the first dispenser.
- 6 Repeat steps 3 and 4 to proceed with the next dispenser until the site is completed.
Note: You may add additional dispensers based on the number of dispensers the customer will allow to be down at a time.

Retrofit Installation Process from FlexPay II

The following installation steps are in the recommended order and are applicable for a retrofit FlexPay IV CRIND with Omnia installation in an environment where FlexPay II was installed:

- 1 Pre-installation checklist. For more information, see [“Installation Checklists”](#) on [page 3-1](#).
- 2 Install FlexPay IV door; install Omnia in one dispenser. For more information on the Retrofit Kit or Upgrade Kit Installation Instructions, see [“Related Documents”](#) on [page 1-10](#).
- 3 Install Applause Media Server, if required. Refer to, *MDE-4699 Applause Media System Installation, Service, and Parts Manual*.
- 4 Update UPM software to the latest version approved by the customer.

- 5 Configure Omnia from the Omnia Web page (includes Insite360 registration). For more information, see [“Verifying the UPM and Software Versions”](#) on [page 5-1](#).
- 6 Test and verify operation of one dispenser including Applause Media System, before configuring additional dispensers.
Note: Do not proceed with the entire forecourt installation if a problem is detected with the first dispenser.
- 7 Repeat for each dispenser until the site is completed.

Retrofit Installation Process from FlexPay IV

The following installation steps are in the recommended order and are applicable for an installation of Omnia in an environment in which FlexPay IV is already installed.

- 1 Pre-installation checklist.
- 2 Install Omnia in one dispenser. For more information, refer to [“Related Documents”](#) on [page 1-10](#).
- 3 Install Applause Media Server, if required.
- 4 Update UPM software to the latest version approved by the customer.
- 5 Configure Omnia from the Omnia Web UI (includes Insite360 registration).
- 6 Test and verify operation of one dispenser including Applause Media System, before configuring additional dispensers.
Note: Do not proceed with the entire forecourt installation if a problem is detected with the first dispenser.
- 7 Repeat for each dispenser until the site is completed.

Related Documents

Document Number	Title	GOLD SM Library
MDE-3860	Programming Quick Reference Guide	• Encore and Eclipse • Encore and Eclipse Installers
MDE-4246	Dispenser Network Connectivity Kit for Monochrome Encore 500, Encore S and Eclipse Installation Instructions	• Applause Media System • Encore and Eclipse • SMARTConnect™
MDE-4699	Applause Media System Installation, Service, and Parts Manual	• Applause Media System • Encore and Eclipse • SMARTConnect
MDE-4771	Encore S Enhanced FlexPay EMV CRIND Start-up/Service Manual	• Encore and Eclipse • FlexPay Connect
MDE-4917	FlexPay Connect D-Box Installation Manual	FlexPay Connect
MDE-5221	FlexPay IV CRIND Start-up Manual	FlexPay IV
MDE-5265	BRCM2.x Installation and Upgrade Instructions	• The Advantage® Series and Legacy • Encore and Eclipse • FlexPay Connect
MDE-5314	Insite360 Encore Remote Management Installation, Start-up and Service Manual	• FlexPay EPP and SCR • FlexPay IV
MDE-5359	FlexPay IV CRIND (with Omnia) Retrofit Kit Installation Instructions for Encore 500 S	FlexPay IV, Omnia
MDE-5360	FlexPay IV CRIND (with Omnia) Retrofit Kit Installation Instructions for Encore S E-CIM	FlexPay IV, Omnia
MDE-5362	FlexPay IV CRIND (with Omnia) Retrofit Kit Installation Instructions for Encore 300/500	FlexPay IV, Omnia
MDE-5382	Secure Zone Router (Acumera) Installation Instructions	Passport®
MDE-5402	FlexPay IV Applause Media Kit (M16183K001) Installation Instructions	FlexPay IV, Omnia
MDE-5686	Configuring Invenco Outdoor Payment Terminals for Gilbarco Dispensers	Invenco
MDE-5690	FlexPay 6 (Invenco OPT) Start-Up and Service Manual	FlexPay 6, Invenco

Abbreviations and Acronyms

Term	Description
ASC	Authorized Service Contractor
BOM	Bill of Material
BRCM	Backroom Communication Module
CAT5/CAT6	Category 5/Category 6
CPR	Cardiopulmonary Resuscitation
CRIND	Card Reader in Dispenser
D-Box	Distribution Box
DCM	Dispenser Connection Module
DEF	Diesel Exhaust Fluid (automotive)
DNS	Domain Name System
EMV	Europay®, MasterCard®, and Visa®
FAT	File Allocation Table
FCC	Federal Communications Commission
FP	Fueling Position
GOLD	Gilbarco Online Documentation
GLRE	Global Long-Range Ethernet
ICS	Invenco Cloud Services
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Multiple Access Control
MOC	Major Oil Company
NEC	National Electrical Code
NFPA	National Fire Protection Association
NIC	Network Interface Card
NTP	Network Time Protocol
OSHA	Occupational Safety and Health Administration
PCB	Printed Circuit Board
PCN	Pump Control Node
PIP	Peripheral Interface PCB
POS	Point of Sale
PPN	Product Part Number
SSE	Service Station Equipment
STP	Submerged Turbine Pumps
TAC	Technical Assistance Center
UDP	User Datagram Protocol
UI	User Interface
UPM	Universal Payment Module
USB	Universal Serial Bus
VLAN	Virtual LAN
WAN	Wide Area Network

This page is intentionally left blank.

2 – 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 fluid lines.

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

In the event of inclement weather, including snow, ice, or flooding that makes driving conditions dangerous, please avoid servicing units. Always use available door stops to secure upper doors against unwanted/unexpected movement, especially during high winds. If necessary, reschedule service to avoid damage to the equipment. Weather may change unexpectedly; be aware of local weather conditions. During service, if conditions develop making service unsafe, close the unit(s) and proceed to a safe location.

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.

Hazards and Actions

 WARNING	
	Spilled fuels, accidents involving pumps/dispensers, or uncontrolled fuel flow create a serious hazard.
	Fire or explosion may result, causing serious injury or death.
	Follow established emergency procedures.
	DEF is non-flammable. However it can create a slip hazard. Clean up spills promptly.

The following actions are recommended regarding these hazards:



Collision of a Vehicle with Unit

Fire at Island

Fuel Spill

- Do not go near a fuel spill or allow anyone else in the area.
- Use station EMERGENCY CUTOFF immediately. Turn off all system circuit breakers to the island(s).
- Do not use console E-STOP, ALL STOP, and PUMP STOP to shut off power. These keys do not remove AC power and do not always stop product flow.
- Take precautions to avoid igniting fuel. Do not allow starting of vehicles in the area. Do not allow open flames, smoking or power tools in the area.
- Do not expose yourself to hazardous conditions such as fire, spilled fuel or exposed wiring.
- Call emergency numbers.

This page is intentionally left blank.

3 – Installation Checklists

Contact Information

Insite360 Help Desk	1-800-997-7725
Gilbarco Technical Assistance Center	1-800-743-7501



The Pre-Installation checklist must be completed before installation begins.

Pre-Installation Checklist

☐ Contact site IT department and submit the form to get networking data.	The form is located in "Appendix A: Site Network Survey" on page A-1 .
☐ Check software versions of Omnia, CRIND, and pump software and determine if updates are necessary.	Note: Always use the latest software version approved by the customer. Minimum Required Versions: • Gilbarco Legacy Gateway (Omnia V04.04) • AWS Gateway (Omnia V05.06) • FlexPay IV CRIND latest version approved by the customer. • Pump 4.1.22 or later • Insite360 Auto-Registration (Omnia V05.08)
☐ Verify that the site survey is accurate and dispensers meet minimum requirements (software version for POS, Applause Media System, dispensers, etc.)	Verify that site survey action items have been completed.
☐ Verify parts in kit against the Bill Of Material (BOM).	Confirm that all parts are included in the kit.
☐ Determine the current POS to forecourt communication hardware configuration. <i>Note: This will help determine if any additional hardware is required to support remote management, such as Ethernet switches or BRCM2.</i>	• Standard Gilbarco two-wire protocol (D-Box) • FlexPay Connect v1/v2 [BRCM/DCM/Two-wire Board Module 2 (TBM2)]
☐ If the site has Applause Media System, determine how it will communicate to the forecourt. This will determine the Insite360 Cloud configuration. <i>Note: This will help determine if any additional hardware is required to support remote management.</i>	Three options: • FlexPay Connect v1 • FlexPay Connect v2 (BRCM2) • Direct Ethernet (CAT5)
☐ If the site has GSTV/ICS Media, then ensure that the MNISP whitelists the following URLs:	• https://icsapiprod.applause.gilbarco.com (Port 443) or • *applause.gilbarco.com
☐ Ensure that you have a static strap available.	

Pre-Installation Checklist

☐ Ensure that you have identified all relevant network parameters.	Backroom Router IP address (Default Gateway) _____ Primary DNS IP address _____ External IP addresses for the dispensers: _____ Subnet mask _____
☐ Ensure that all requirements are in place for Insite360 auto-registration (beginning with Omnia V05.08).	If the site has an Insite360 contract, program the Omnia and register the site manually. If the site does not have a contract with Insite360, program the Omnia as you would normally, and then do the following: • Set Side A Fueling Position and Side B Fueling Position correctly in General Configuration Settings. <i>Note: If these values are incorrect or a duplicate of another dispenser at the site, the unit will fail to automatically register or could show incorrectly on the Insite360 dashboard.</i> • In Insite 360 Configuration > Settings, program the GVR ID. • Program the DNS IP properly so that when the customer wants to connect to Insite360 in future, the device will auto register without a tech visit. • Ensure that all AWS-IoT URLs are whitelisted.
☐ The AWS IoT URLs must be set up prior to software upgrades and any attempt to register with Insite360 through AWS. Ensure that network rules are done by the customer IT department or MNSP provider. Registration will fail if the network rules are not set up.	The following URLs are used for Insite360 Forecourt through AWS IoT Gateway: • aatnf1k6u65sn-ats.iot.us-east-1.amazonaws.com • cfvuav3n0omj9.credentials.iot.us-east-1.amazonaws.com • device-download-prod.s3.amazonaws.com • s3.amazonaws.com/prod.i360.device.fileupload/* • omnia-checkin.prod.insite360.gilbarco.com (Port 443 only) <i>Notes:</i> 1 All these endpoints need access to three TCP ports: 443, 8443, 8883. 2 Access to UDP is not necessary. 3 Omnia must be connected to NTP Servers to sync time. 4 Some customer networks do not allow wildcards (*) in the URL white-listing. You can also identify the URL host name without the wildcard path. Consult the network IT team. 5 The URL omnia-checkin.prod.insite360.com, port 443, is used for the auto-registration feature.
☐ If a custom NTP server is not used, access must be allowed to the following NTP Servers for AWS IoT to enable devices (Omnia, SSoM) to synchronize clock timing.	NTP Servers destinations: 0.debian.pool.ntp.org 1.debian.pool.ntp.org 2.debian.pool.ntp.org 3.debian.pool.ntp.org Destination Port = 123 Protocol = UDP
☐ If TLS Pump Proxy is used, ensure that Port 5789 is open for Omnia Pump Proxy.	<i>Note: Contact the MNSP at least 24 hours before start-up to enable Port 5789.</i>

Day of Installation Checklist

- ☐ Follow standard safety procedures during installation activities.
- ☐ Lockout/tagout dispenser before beginning the installation.
- ☐ Review installation process using the block diagram.
- ☐ Before working on the dispenser, ensure that media is running on all fueling positions.
- ☐ Ensure that all dispensers are functioning properly before beginning the installation.

Post-installation Checklist

- | | | |
|--------------------------|--|---|
| ☐ | Verify that the date and time of dispenser and CRIND are accurate. | |
| ☐ | If the registration process fails, call the Remote Management Help Desk at 1-800-997-7725. | Refer to "Related Documents" on page 1-10 .
For more information, refer to "Troubleshooting" on page 7-1 . |
| ☐ | For all dispensers, complete the Insite360 Cloud feature test, if present. | Call the Remote Management Help Desk to perform feature testing. |
| ☐ | Verify the dispenser operation including media, if present. | Run a transaction and confirm that media is being displayed on the CRIND. |

This page is intentionally left blank.

4 – Configuring FlexPay IV

Note: The following instructions are applicable only while performing a FlexPay IV upgrade.

Pre-requisites for Installing Omnia in FlexPay IV

Before starting up and configuring Omnia, ensure that the following pre-requisites are met:

- UPM software version is the latest version approved by the customer.
- PCN software version is 4.1.22 or later for PCN3 and PCN4, or version 6.0.52 for PCN5.
- Omnia parameter is set in the Device Configuration menu.

Note: Always update devices to latest customer approved software.

If the UPM has not been updated or configured, proceed as follows:

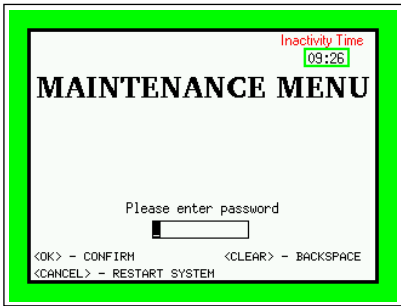
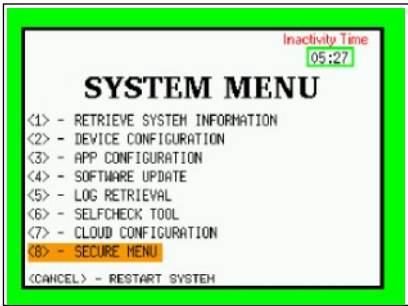
- 1** Upgrade the UPM to the required software version using the FlexPay IV CRIND (M7) Maintenance tool.
- 2** After the SECURE DEVICE UPDATE is complete and the UPM reboots, press **1** to enter the Setup Menu.
- 3** Change the connection module of FlexPay IV CRIND (M7) dispenser to Omnia and reboot the dispenser.
- 4** After the Omnia parameter is configured, there will be a Card Reader error on the display. The error resolves itself after the Omnia hardware is installed and the CRIND Card Reader (UX300) IP is set back to the default setting.
- 5** When the Omnia parameter is set in the UPM, the internal UPM IP address is set automatically: Side A 172.20.100.1, Side B 172.20.100.3.

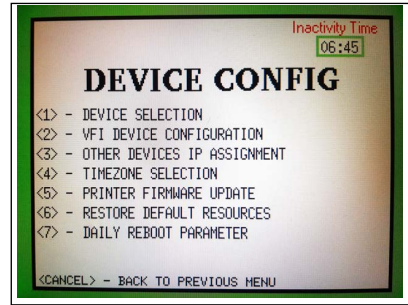
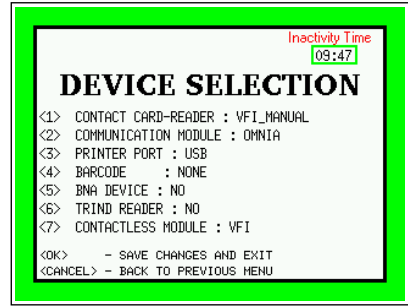
Notes: 1) When running Omnia with a Commander POS, the CRIND Baud Rate must be set to 9600 Baud in the CRIND settings in the UPM, and at the Commander POS.

2) All other POS types can remain default 4800 Baud.

Configuring UPM Settings

If FlexPay IV was already installed, configure the Omnia settings in the CRIND UPMs. For a newly installed FlexPay IV CRIND with Omnia, the device configuration is already set. To configure Omnia settings in the CRIND UPMs, proceed as follows:

Description	Screen
1 Note the serial numbers that are displayed on the black screen immediately after powering ON the dispenser. The Serial Number can also be obtained by looking at the printed label on the UPM.	
2 When the white screen opens, wait for "<1> enter setup" to appear and then press <1> on the PIN Pad.	
3 In the Maintenance Menu, enter the password. This is the last six digits of the serial number that you recorded in step 1.	
4 In the System Menu, press <2> for Device Configuration.	

Description	Screen
5 In the Device Config menu, press <1> for Device Selection.	
6 In the Device Selection, press <2> to set the Communication Module to be OMNIA and press the following: • Press OK to Save Changes and Exit. • Press CANCEL. • Press CANCEL to restart the system.	

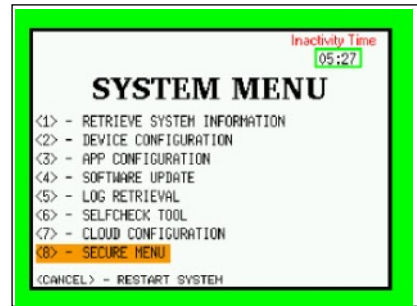
The internal scheme becomes 172.20.100.1/3 (A/B). The jumper on the Peripheral Interface PCB (PIP) board determines A or B side.

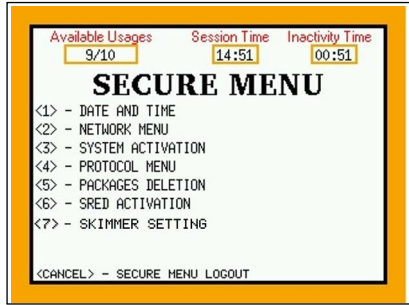
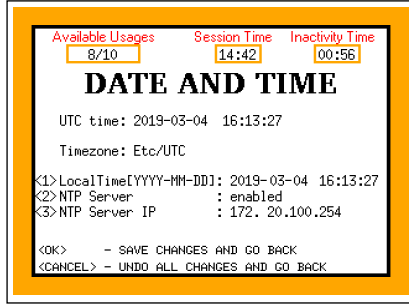
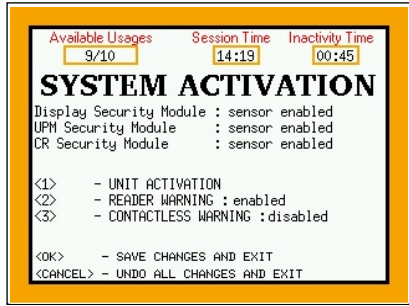
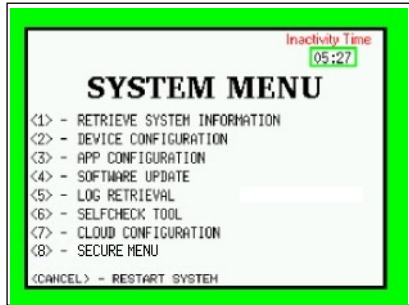
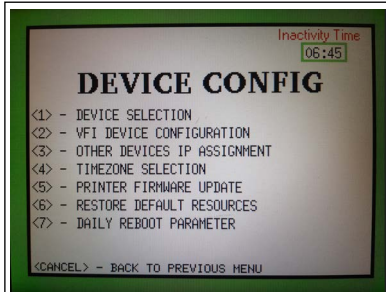
*Notes: 1) When running Omnia with a Commander POS, the CRIND Baud Rate must be set to 9600 Baud in the CRIND settings in the UPM, and at the Commander POS.
2) All other POS types can remain default 4800 Baud.*

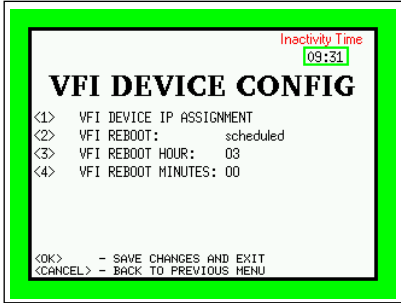
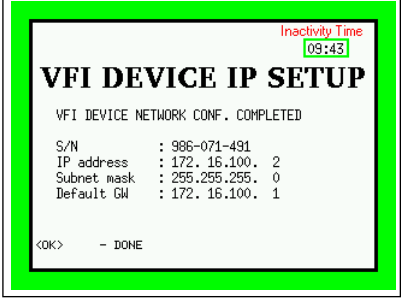
Install hardware. For more information, refer to *MDE-5402 FlexPay IV Applause Media Kit with Omnia (M16183K001) Installation Instructions*.

Note: If a FlexPay IV CRIND is already installed in the dispenser, restore the default IP address of the card reader after Omnia is installed.

To configure final UPM settings in the Maintenance Menu, proceed as follows:

Description	Screen
1 Press <8> to open the Secure Menu.	

Description	Screen
2 Press <1> to open the Date and Time.	
3 Set date and time and press <OK> to return to the Secure Menu.	
4 If PIP3 was replaced, an activation is required. Press <3> System Activation from the Secure Menu.	
5 In the System Menu, press <2> for Device Configuration.	
6 In the Device Config, press <2> for VFI Device Configuration.	

Description	Screen
7 In the VFI Device Config, press <1> for VFI device IP assignment.	
8 Follow the wizard procedure and push the Device Back button.	
9 The message "Device message received. Please wait..." is displayed on the screen.	
After the procedure is complete, the system will report the new IP address of the VFI device (default value from factory is 172.16.100.2); then, proceed with the following: 10 Press OK. 11 Reboot the system.	

Note: *The card reader will return to the default address. Both Side A and Side B card readers will have the same IP address of 172.16.100.2; therefore, any replacement of a card reader during a future service will come out of the box set properly (no need to set IP). Omnia VLAN combined with the location of CAT5 cables on Omnia associates the card reader to the UPM for each side (card reader A with UPM A; card reader B with UPM B).*

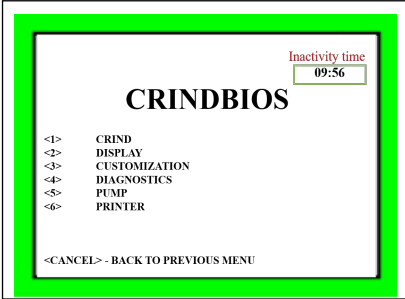
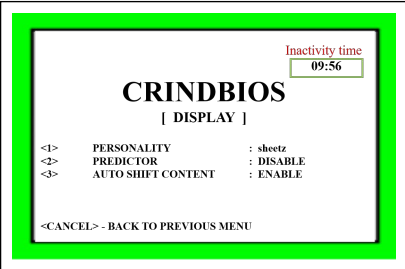
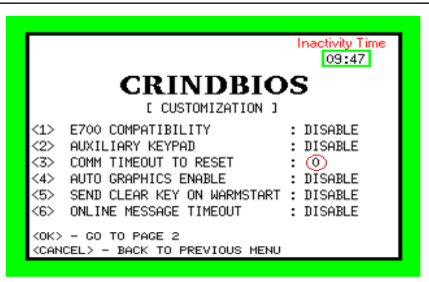
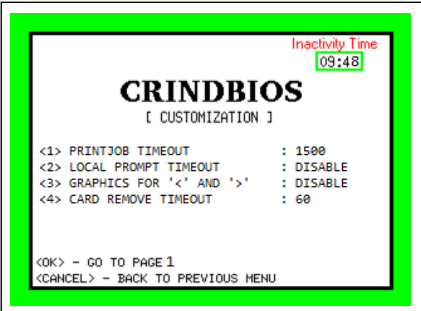
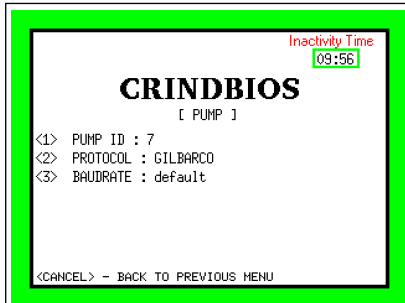
Configuring CRINDBIOS

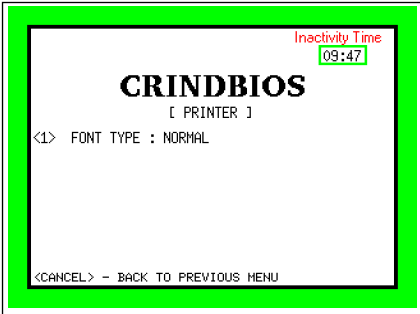
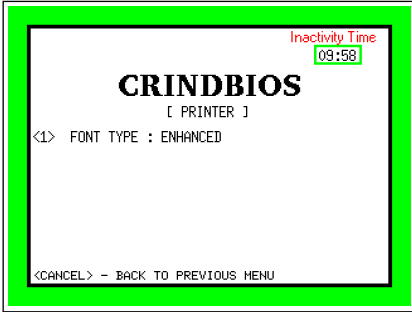
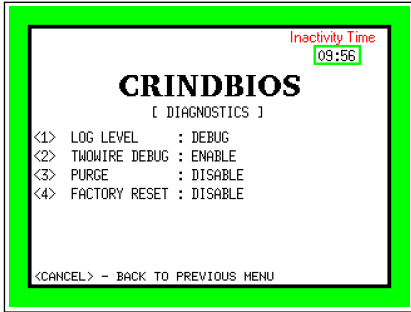
IMPORTANT INFORMATION

The menus and options on the screens might differ slightly depending on the version of software.

To configure CRINDBIOS settings, proceed as follows:

Description	Screen
1 In the System Menu, press <3> App Configuration. 2 For units with the 15.6-inch display option, optimize settings for the large display. a In the App Config menu, press <2> Display Manager, and change the Display Template setting to None. b Press Cancel to go back to the App Config menu. 3 In the App Config menu, press <1> CRINDBIOS.	
4 In the CRINDBIOS menu, press <1> CRIND and check or set each of the following settings: • CRIND • DISPLAY • CUSTOMIZATION • DIAGNOSTICS • PUMP • PRINTER	
5 Press <1> and set to Yes. 6 Press <2> and set Generic or MOC based on the POS type. 7 Press <3> and set the CRIND ID. 8 Press <4> and set Interface type: Serial_4800/9600/19200 or IP (for EMV) or COIP. <i>Note: Must be set to 9600 Baud for Commander POS, if the serial interface is used.</i> 9 Press <5> and set TLS mode if the IP interface mode type depends on the POS configuration. 10 Press <6> and set Display Security Check to Enable. 11 Press Cancel to save and go back to the previous menu.	

Description	Screen
12 From the CRINDBIOS menu, press <2> DISPLAY. 13 From the DISPLAY menu, check and adjust the following settings: - Verify the Personality and Predictor settings. - For Encore 900 or 15.6-inch display, press <3> AUTO SHIFT CONTENT: ENABLE. - Press <CANCEL> to return to the previous menu. 14 From the CRINDBIOS menu, press <3> Customization and check or set the parameters. 15 Press <3> Comm Timeout to Reset and set the timeout to 0 minutes. This setting is mandatory with an Omnia PCB. This setting will disable the auto reset on communication timeout events. Disabling this feature is very important for sites with Omnia, where the POS is turned off overnight. 16 Set all other parameters based on the POS type: AUTO GRAPHICS ENABLE: When enabled, the CRIND will enable the GRAPHICS two-wire command by default. SEND CLEAR KEY ON WARMSTART: When enabled, the CRIND will automatically send a CLEAR key press on warm start or poll resume (for Radiant site). ONLINE MESSAGE TIMEOUT (minutes): If disabled, the CRIND only sends a startup message to the POS after the CRIND is powered up. When Enabled, the POS stops polling (or goes offline with TCP), the CRIND will send a startup message after the communication resumes. THIS IS CRUCIAL TO ENABLE AND REDUCE THE SERVICE CALLS. PRINTJOB TIMEOUT: This is the timeout associated with a printjob. Not all POSs send a cut/end of receipt message. This is the time (in seconds) that the CRIND waits before printing the receipt. LOCAL PROMPT TIMEOUT: When enabled, the CRIND will start a timer when an automatic local prompt 'One Moment Please' is displayed while waiting for the POS to respond. GRAPHICS FOR '<' and '>': When enabled, the CRIND will also include the characters '<' and '>' for softkey arrow (touchpoints on the LTD) substitution like the '[' and ']' characters. CARD REMOVE TIMEOUT: The time (in seconds) that the CRIND waits after a card is inserted before indicating that the card was not read. Recommended setting for this parameter is 60 seconds. To disable this option, set the parameter to 0. 17 Press Cancel to save and return to the previous menu.	   
18 From the CRINDBIOS menu, press <5> PUMP and check or set the following: - Set Pump ID. - Set Protocol. - Set BAUDRATE.	

Description	Screen
19 Press Cancel to save and return to the previous menu. 20 From the CRINDBIOS menu, press <6> Printer . 21 From the PRINTER menu, press <1> to toggle between Normal and Enhanced font type.	 The screen displays the CRINDBIOS menu with the PRINTER option selected. It shows the font type set to NORMAL. The inactivity time is 09:47. Navigation options include <1> to toggle font type and <CANCEL> to return to the previous menu.
	 The screen displays the CRINDBIOS menu with the PRINTER option selected. It shows the font type set to ENHANCED. The inactivity time is 09:58. Navigation options include <1> to toggle font type and <CANCEL> to return to the previous menu.
22 Press Cancel to save and return to the previous menu. 23 From the CRINDBIOS menu, press <4> Diagnostics . • Set Purge to Enable and press Cancel to restart.	 The screen displays the CRINDBIOS menu with the DIAGNOSTICS option selected. It shows settings for LOG LEVEL (DEBUG), TWOWIRE DEBUG (ENABLE), PURGE (DISABLE), and FACTORY RESET (DISABLE). The inactivity time is 09:56. Navigation options include <1> to LOG LEVEL, <2> to TWOWIRE DEBUG, <3> to PURGE, <4> to FACTORY RESET, and <CANCEL> to return to the previous menu.

5 – Configuring Omnia PCB

Verifying the UPM and Software Versions

Note: For the Omnia hardware and configuration to work properly, the UPM software must be at the minimum required version, and the OMNIA parameter set in the UPM. Verify all software versions in the UPM and pump. Minimum requirements are listed in this manual. For more information on hardware installation, refer to MDE-5360 FlexPay IV and Omnia Kit Installation Instructions.

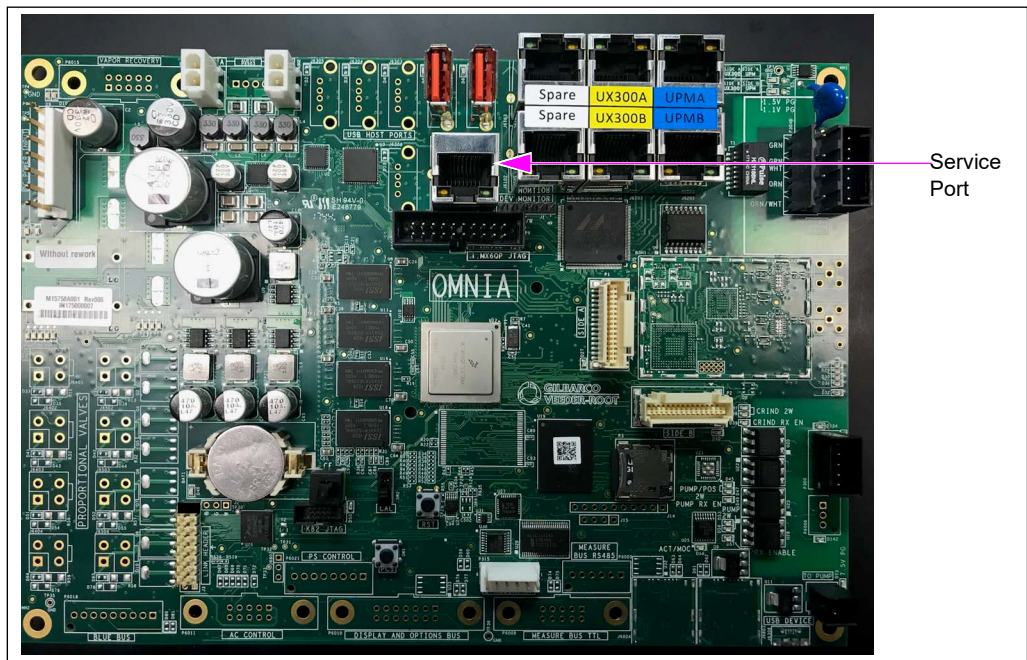
Before configuring the Omnia PCB, verify the software version and upgrade to the latest approved version on the extranet. If this is the first time that an Omnia has been installed in this dispenser, you must use the Service Port to access the Omnia Web page. After the Omnia is configured, the Omnia Web page can be accessed from the back room via the external IP address (for example, 10.5.55.71:3000).

Logging In to Omnia

To configure the Omnia PCB, proceed as follows:

- 1 Using a laptop, set laptop static IP address to 172.20.100.15 and the subnet mask to 255.255.255.0.

Figure 5-1: Service Port Location



- 2 Connect the laptop to the Service Port on the Omnia PCB using a standard CAT5 cable.

- 3 Open the Chrome web browser and type <http://172.20.100.254:3000> in the address field.

Note: This is the default IP address. If a different IP address was assigned, take note of the address and type it here to access the correct location.

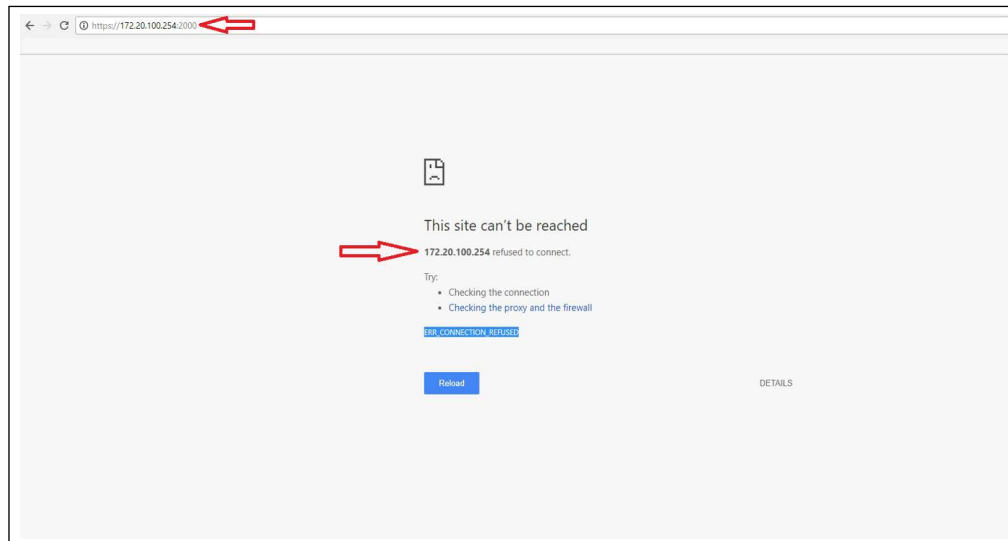
Figure 5-2: Entering IP Address



IMPORTANT INFORMATION

Beginning with version 03.02, http connections are redirected to https. With earlier versions of the Omnia software, when connecting to an Omnia PCB with a previous version of the Omnia software, the browser may redirect to https on port 2000. The address in the browser shows <https://172.0.100.254:2000> and displays the message "172.20.100.254 refused to connect." This is because Chrome browser pulls files from the cache memory.

Figure 5-3: Re-directing to https with Omnia Versions Lower Than 03.02



In such cases, enter <http://172.20.100.254:3000?> (question mark "?" appended) in the address bar of Chrome browser to bypass the redirection (See [Figure 5-4](#)).

Figure 5-4: Entering IP Address to Bypass Browser Wrong Re-direction

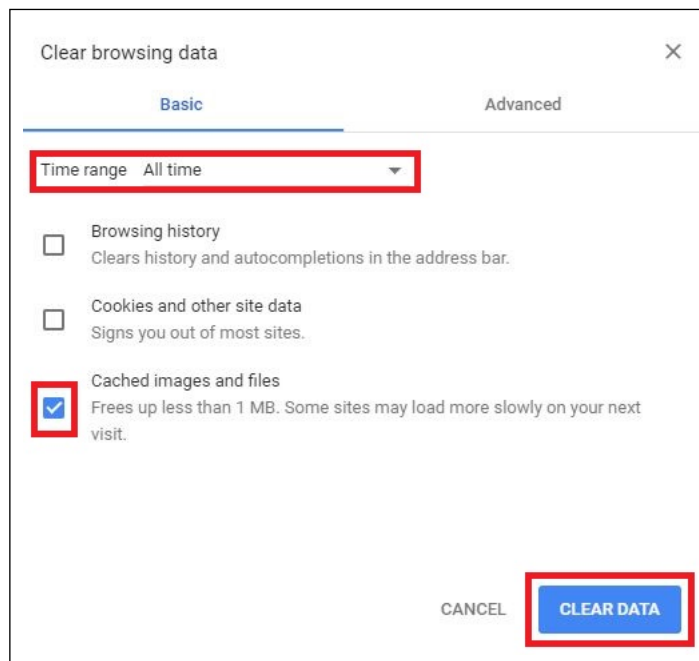


Clear the browser cache to avoid wrong re-direction.

To clear the browser cache, proceed as follows:

- a** Press **Ctrl + Shift + Delete** on the keyboard. The Clear browsing data window opens.
 - b** Select **All time** from the Time range drop-down field and then select **Cached images and files**.
- 4** Click **CLEAR DATA**. Clearing the browser cache is an alternative to appending the question mark as described above.

Figure 5-5: Clearing Browsing Data



- 5 Enter <http://172.20.100.254:3000> in the address bar. To accept the https certificate, click **ADVANCED**.

Figure 5-6: Extending ADVANCED Security Settings of the Browser

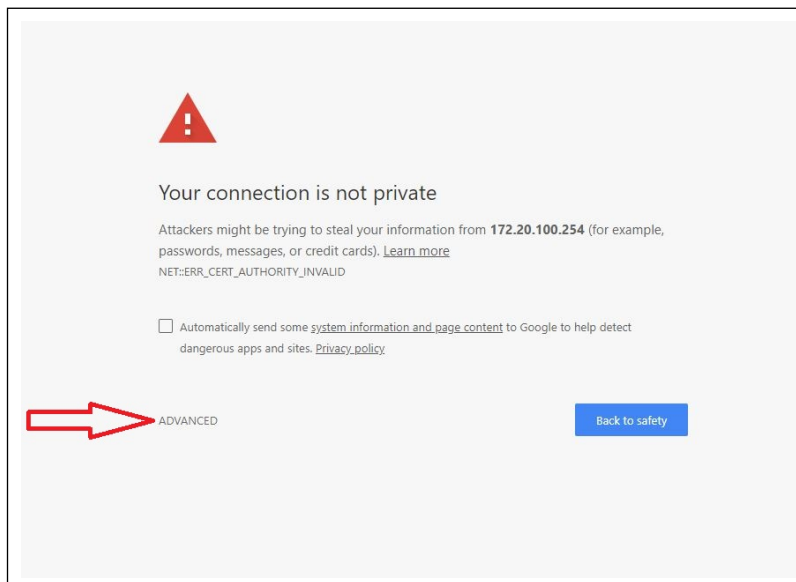
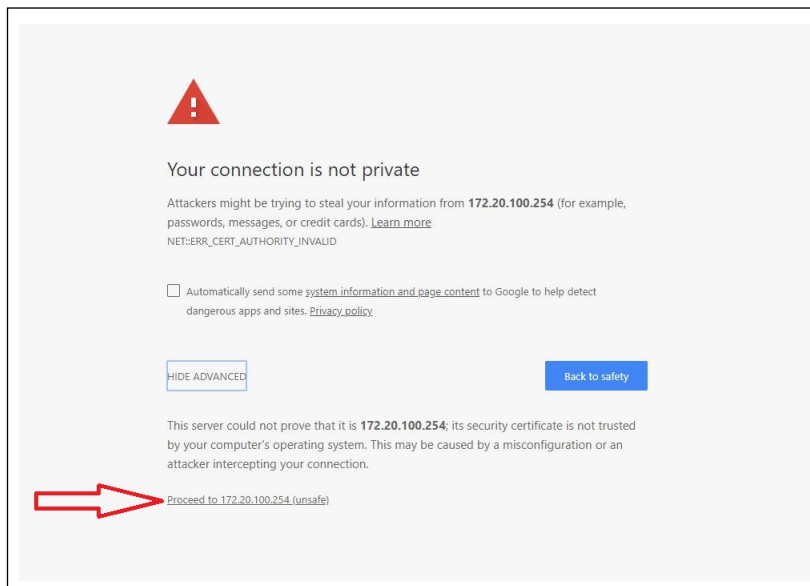


Figure 5-7: Accepting https Certificate



- 6 Click **Proceed to 172.20.100.254 (unsafe)**.

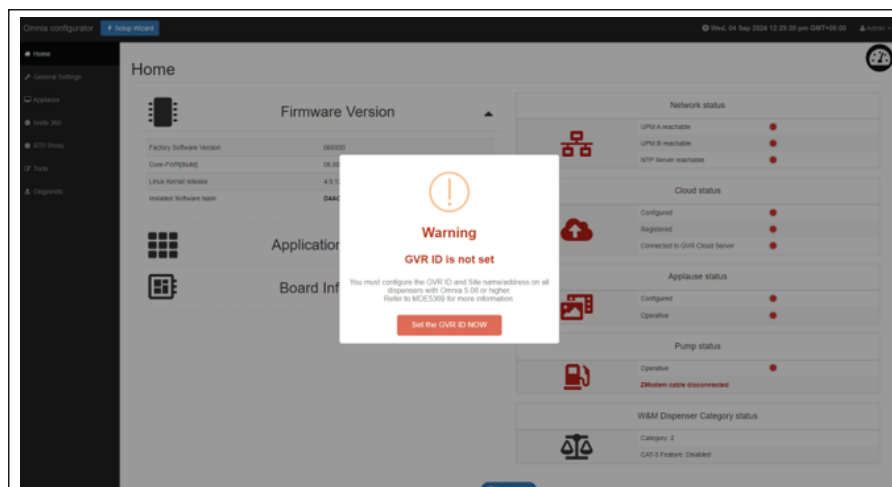
- 7 Depending on the configured login mode, the Omnia login page opens (See [Figure 5-8](#)).

Figure 5-8: Default Login Page

Note: Password is the last 6 digits of the Product Part Number (PPN) displayed at the bottom right. PPN is a GVR identifier unique to each Omnia boards derived from Ethernet MAC-address. The time shown is the board time and not the system time.

If logging in the first time for a new installation, and GVR ID is not set, the following message prompts you to set a GVR ID.

Figure 5-9: GVR ID Not Set Warning Message



- a** Click **Set the GVR ID NOW** takes you to the Insite 360 Configuration page, where you can set the GVR ID.

b Complete the Insite 360 Configuration page and click **Save**.

*Note: Without saving, the **Warning: GVR ID is not set** message is displayed again.*

Figure 5-10: Setting the GVR ID

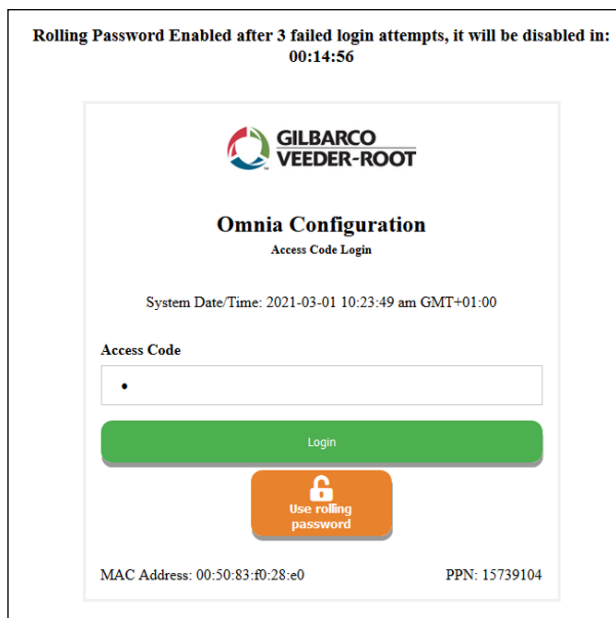
- 8** All Omnia IP addresses can be changed by accessing the proper sub-menu/page and by resetting the default mechanism provided to prevent the forgotten IP-changes. A push-button is available on the Omnia board to reset the IP address. Default IP address: **172.20.100.254**.

Figure 5-11: Login Page for Access Code Mode

Note: Every failed login attempt is warned by an error popup displaying the relative error message.

Figure 5-12: Rolling Password Fallback

Rolling Password Enabled after 3 failed login attempts, it will be disabled in:
00:14:56



**GILBARCO
VEEDER-ROOT**

Omnia Configuration
Access Code Login

System Date/Time: 2021-03-01 10:23:49 am GMT+01:00

Access Code

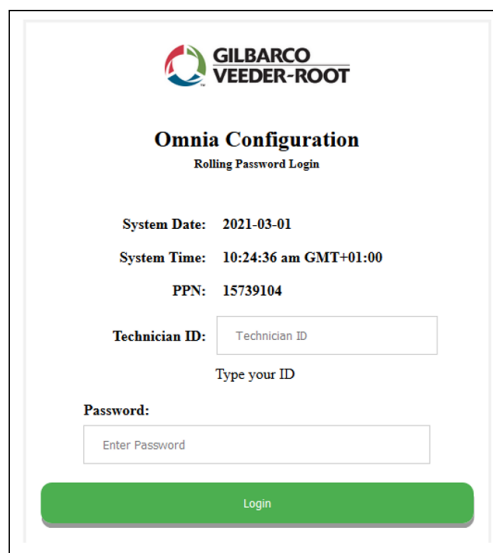
•

Login

Use rolling password

MAC Address: 00:50:83:f0:28:e0 PPN: 15739104

- Notes: 1) Access code is provided by the customer. The access code must meet the following requirements: Between 6 and 40 characters that can include lowercase and uppercase letters, numbers, and special characters, and excluding spaces.
- 2) If the relative option is enabled (in wizard or advanced settings) the user can switch to Rolling Password authentication for 15 minutes after three failed login attempts. The countdown at the top of the page shows the remaining time.

Figure 5-13: Login Page for Rolling Password Mode


**GILBARCO
VEEDER-ROOT**

Omnia Configuration
Rolling Password Login

System Date: 2021-03-01

System Time: 10:24:36 am GMT+01:00

PPN: 15739104

Technician ID:

Type your ID

Password:

Login

Note: Type your Technician ID. Password is provided by the ASC Online Activation Tool (recommended) or the Gilbarco Help Desk.

9 Enter the requested credentials and click **Login**.

Omnia Configurator - Creating a New Configuration

You can create or modify a new Omnia configuration by going through each page of the Omnia Configurator Web UI.

Omnia Configurator - General Settings

- 1 Click **General Settings** to open the configuration page as shown in [Figure 5-14](#).

Note: For Door Sensor dispenser only: In the case of an update from 03.xx to 04.xx release, it is necessary to re-configure Dispenser Model and Pump connection to Encore and RTP_serial settings.

Figure 5-14: General Settings

Omnia configurator [Setup Wizard](#)

- Home
- General Settings**
- Insta 300
- RTP Proxy
- Tools
- Diagnostics

General Settings

General configuration

Select Dispenser Model	Encore
Select Payment Type	MT
Select Dispenser Type	Dual side
Select TwoWire Connection Type	MOC
Select Pump Baud Rate	DEFAULT (57600)
Fill in Dispenser Serial Number	EN123456
Side A Fueling Position	1
Side B Fueling Position	2
Select Pump Connection Type	RTP-serial

Network Settings [Advanced settings](#)

Side A External IP Address	10.5.55.71
Side B External IP Address	10.5.55.72
Side A-B External Netmask	255.255.255.0
Backroom Router IP Address (Gateway)	10.5.55.1
Primary DNS	8.8.8.8 This field can be empty if Cloud app is disabled
Secondary DNS	8.8.4.4 This field can be empty if Cloud app is disabled

Login Mode Settings

Current Login Mode	Basic Authentication
--------------------	----------------------

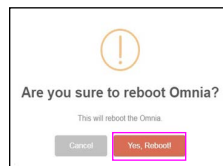
[Cancel](#) [Save](#)

2 Use the following table for Omnia configuration settings:

Field	Configuration Settings
Dispenser Model	Encore, Latitude, or AtlasX
Payment Type	M7 or Invenco (Select M7 for FlexPay IV)
Site dispenser type	Dual-sided or Single-sided Unit
Select Two-wire Connection Type	MOC, Generic, or TLS IP. Ensure that the UPM and Omnia are set to the same connection type. <i>Note: TLS IP is supported only when dispenser type is Encore.</i>

Dispenser Type	Payment Type	Two-Wire Connection Type	POS Connection	POS
Encore	M7 (FlexPay IV)	Generic	Direct Pump Loop (4-wire)	Third-Party POS
Encore	M7 (FlexPay IV)	MOC	CRIND BIOS	Passport
Encore	M7 (FlexPay IV)	TLS IP	TLS Pump Proxy	Passport (Future)
Encore	Invenco (FlexPay 6)	Generic	Direct Pump Loop (4-wire)	Third-Party POS
Encore	Invenco (FlexPay 6)	TLS IP	TLS Pump Proxy	Passport
Latitude	M7 (FlexPay IV)	Generic	Direct Pump Loop (4-wire)	Third-Party POS

When the two-wire connection type (MOC, Generic, or TLS IP) is changed, a reboot is required. Reboot the Omnia board from the Tools tab or warmstart the dispenser. Wait for 10 seconds before reapplying power.



Select Pump Baud Rate	No change. Setting should remain at Default (5787).
Dispenser Serial Number	Enter the serial number given on the dispenser side label.
SIDE A fueling position	Fueling position number of Side A. Side A is the side where the Calibration Switch is located. Possible values are 1 - 989. Ensure that you set the proper fueling position with no duplicates across the forecourt.
SIDE B fueling position	Fueling position number of Side B. Possible values are 1 - 989. Ensure that you set the proper fueling position with no duplicates across the forecourt.
Pump Connection Type	Select from the following options: • RTP-Ethernet - Latitude units. • ZModem - For Encore or AtlasX units without door sensors. This is the default value. • RTP-Serial - For Encore or AtlasX units with door sensors (PCN version 04.xx or later). To manage door sensors remotely through the Cloud, program the pump to use Real time Protocol (RTP-Serial). For more information, refer to <i>MDE-3860 Programming Quick Reference Guide</i>.
Invenco Side A External IP Address	For Invenco Side A External IP address configuration, refer to <i>MDE-5686 Configuring Invenco Outdoor Payment Terminals for Gilbarco Dispensers</i> manual.
Invenco Side B External IP Address (not used for single-side configuration)	For Invenco Side B External IP address configuration, refer to <i>MDE-5686 Configuring Invenco Outdoor Payment Terminals for Gilbarco Dispensers</i> manual.
Omnia External IP Address	For Omnia External IP address configuration, refer to <i>MDE-5686 Configuring Invenco Outdoor Payment Terminals for Gilbarco Dispensers</i> manual.

Field	Configuration Settings
Side A External IP Address	For Side A External IP address configuration, refer to "IP Scheme FlexPay IV" on page 5-11 for Gilbarco default settings. This field is auto-populated with 10.5.55.XX (XX depends on Side A fueling position entered, 70 + ID). Will need to be changed if site using custom External IP Addresses. <i>Note: These IP addresses may be different based on the site's IP scheme.</i>
Side B External IP Address	For Side B External IP address configuration, refer to "IP Scheme FlexPay IV" on page 5-11 for Gilbarco default settings. This field is auto-populated with 10.5.55.XX (XX depends on Side A fueling position entered, 70 + ID). Will need to be changed if site using custom External IP Addresses. <i>Note: These IP addresses may be different based on the site's IP scheme.</i>
Side A-B External Netmask	External subnet mask (default 255.255.255.0)
Backroom Router IP Address (Gateway)	Backroom Router IP address.
(Generic CRIND) Pump 2-Wire ID Side A (1-16)	<i>Note: For MOC, the pump ID for side A will be hard-coded 7.</i>
(Generic CRIND) Pump 2-Wire ID Side B (1-16)	<i>Note: For MOC, the pump ID for side B will be hard-coded 11.</i>
Primary DNS	Enter the customer-provided DNS IP address or enter 10.5.55.1 as default. Note that this field may also use non-default values. Consult the site's IT Department for IP Settings in the back room. The GVR ID and Primary DNS must be input by the technician for auto-registration to work properly. <i>Note: These IP addresses may be different based on the site's IP scheme.</i>
Secondary DNS	Google Public IP 8.8.8.8. Be aware that this field may also use non-default values. Consult the site's IT Department for IP Settings in the back room. <i>Note: These IP addresses may be different based on the site's IP scheme.</i>
Advanced Settings	Omnia Internal Subnet Mask: 255.255.255.0 Omnia Internal IP Address: 172.20.100.254
Current Login Mode	Indicates if No Authentication, Access Code (set by customer), or Rolling Password (ASC Tool).

Note: Ensure that the UPM and Omnia are set to the same connection type. When this parameter is changed (from MOC to Generic or Generic to MOC), a reboot is required.

The following table provides details to select an appropriate Internal CRIND IP address for the associated fueling position:

Internal IP Scheme FlexPay IV			
Fueling Position	Side	CRIND IP Address	Default Gateway
1/2	A	172.20.100.1	172.20.100.254
	B	172.20.100.3	172.20.100.254
3/4	A	172.20.100.1	172.20.100.254
	B	172.20.100.3	172.20.100.254
Card Reader	N/A	172.16.100.2	172.16.100.1
Etc.	Etc	Etc.	Etc.

Note: The table shows IP addresses that FlexPay IV automatically assigns as internal IP address based on the detected Side (A/B).

Note: After changing general settings while Idle loop is playing, an Omnia reboot is needed to restore Applause Multimedia System functionalities. For more information, refer to "Reboot" section on [page 5-31](#).

The following table provides details to select appropriate external CRIND IP address for the associated fueling position:

External IP Scheme FlexPay IV					
Fueling Position	Side	Omnia External IP Address	IP Address	Backroom Router 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 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 for EXAMPLE ONLY.

- 3 When the configuration is complete, click **Save** and go back to the Home page.

Omnia Configurator - Applause

- 1 If applicable, click **Applause** in the left navigation menu to open the Applause Configuration page as shown in [Figure 5-15](#).

Figure 5-15: Applause Configuration Settings

The screenshot shows the 'Applause Configuration' page in the Omnia Configurator. The left sidebar has a 'Setup Wizard' button and a navigation menu with 'Home', 'General Settings', 'Applause', 'Insta 360', 'RTP Proxy', 'Tools', and 'Diagnostic'. The main area is titled 'Applause Configuration' and contains the following fields:

- Mode: Applause (dropdown)
- Side A:
 - Terminal ID: 13 (input field with checkmark)
 - Pump ID: 13 (input field with checkmark)
- Side B:
 - Terminal ID: 14 (input field with checkmark)
 - Pump ID: 14 (input field with checkmark)
 - Idle Loop Enabled: ☒ (checkbox)
 - Idle Loop Delay: 180 (input field with checkmark)
 - Idle Loop Delay From Busy: 60 (input field with checkmark)
 - Busy Loop Enabled: ☒ (checkbox)
 - Busy Loop Delay: 5 (input field with checkmark)
 - Source: Server (dropdown)
 - Server: 10.5.48.66 (input field with checkmark)
 - Volume: 85 (input field with checkmark)

At the bottom of the form are 'Cancel' and 'Save' buttons. On the right side of the page, there is a 'Media Utility' section with a 'Check Pump Monitor' button.

Notes: 1) Scroll down to see all programming fields on the configuration pages.
2) Ensure to check the Idle Loop Enabled and Busy Loop Enabled boxes for sites applicable.

Field	Configuration Settings
Mode	Set the Media mode to Applause Media System.
Side A - Terminal ID	Set the Terminal ID to match the actual CRIND ID programmed in the unit programming or fueling position.
Side A - Pump ID	Set the Pump Monitor ID to match the actual pump ID programmed in the unit programming. (If connected to Passport POS system, all IDs will be 7 for side A and 11 for side B).
Side B - Terminal ID	Set the Terminal ID to match the actual CRIND ID programmed in the unit programming or fueling position.
Side B - Pump ID	Set the Pump Monitor ID to match the actual pump ID programmed in the unit programming. (If connected to Passport POS system, all IDs will be 7 for side A and 11 for side B).
Idle Loop Enabled	Enable or disable the Idle Media. Select to turn ON if you want the media to run when the unit is in idle condition. If you do not want media to run when the unit is idle, set as disable.
Idle Loop Delay(s)	Number of seconds of delay before starting idle media loop.
Idle Loop Delay From Busy	Number of seconds of delay before starting idle media loop after busy loop.
Busy Loop Enabled	Turn the Busy Media ON or OFF. Select to turn ON if you want the media to run when the unit is in busy condition. If you do not want the media to run when the unit is busy, set as Delay.
Busy Loop Delay(s)	Number of seconds to delay before starting the busy media loop.

Field	Configuration Settings
Source	Server
Server IP	Applause server IP address should be changed (recommended 10.5.55.66).
Volume	Video volume 1-100

Notes: 1) If Idle Media is enabled, media advertisements can run during a POS application download. Gilbarco recommends disconnecting the Applause Media System Site Server or waiting to turn ON the Idle Media until the units are fully up and running with the POS.

2) Side A/B A/V, Idle and Busy tests were removed and replaced with “Diagnostic A/V tests” in version 03.02 and higher. For more information, refer to “[Omnia Configurator - Diagnostic](#)” on [page 5-33](#).

Figure 5-16: Applause Configuration Settings - 2

Idle Loop Delay From Busy: 60 ✓

Busy Loop Enabled: ☒ ✓

Busy Loop Delay: 5 ✓

Source: Server ✓

Server IP: 10.5.55.66 ✓

Volume: 85 ✓

Back Next

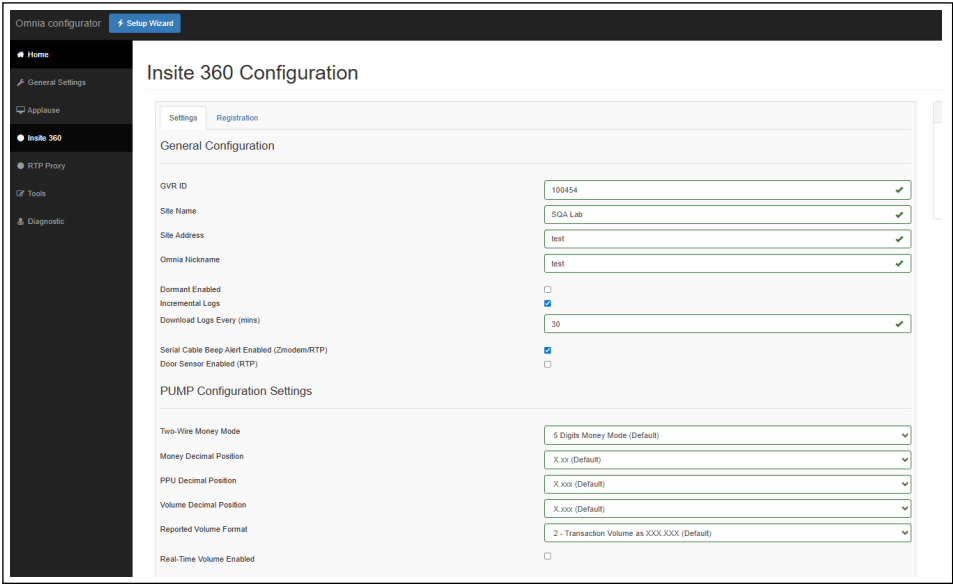
Note: Ensure that you select the Idle Loop Enabled and Busy Loop Enabled boxes for sites applicable.

2 Click Next.

Omnia Configurator - Insite 360

- 1
- Click **Insite 360** in the left navigation to open the Insite360 Configuration page as shown in [Figure 5-17](#).

Figure 5-17: Insite 360 Configuration Settings



Field	Configuration Settings
GVR ID	GVR ID. This must be set correctly for auto-registration to Insite360.
Site Name	Input the store's name. Confirm with the customer for proper format.
Site Address	Physical location listed in Insite360.
Omnia Nickname	Site name. <i>Note: Use the same name for all units.</i>
Dormant Enabled	The dispenser is connected to Insite360 but no messages are exchanged between the dispenser and Insite360. The status in the Insite360 portal for the dispenser is the last one sent before getting into "Dormant Mode". Gilbarco can still "wake up" the units remotely to perform updates and log collection when needed. Default settings when upgrading to Omnia V04.07 or higher or SSoM V3.3.3 or higher: • If the device is not registered to Insite360, the system will default Dormant mode to Enabled (check box is selected). • If the device is registered to Insite360, the system will default the setting to Not Enabled (check box is cleared).
Incremental logs	Ensure that the check box is selected (Download Enabled).
Download Logs Every (mins)	Leave at 30 minutes unless directed to change by Gilbarco.
Serial Cable Beep Alert Enabled	Enable/Disable the serial cable beep alert.

Field	Configuration Settings
Door Sensor Enabled (RTP)	Select to enable the Door Sensor option. The following are the default settings when upgrading to V05.09 or higher: - If the Omnia Pump Protocol was set to RTP before the software upgrade, the door sensor option will be automatically selected (enabled). - If the Omnia Pump Protocol was not set to RTP, the door sensor option will not be enabled and the check box will be clear. <i>Note: Omnia and PCN must both have RTP selected for the door sensor feature to work.</i>

- Set the PUMP configuration to match the PCN settings. The steps vary depending on whether Two-Wire Connection Type is Generic or MOC.

Figure 5-18: Pump Configuration Settings

The screenshot displays the 'Insite 360 Configuration' window. On the left is a dark sidebar with navigation options: Home, General Settings, Applications, Insite 360 (selected), RTP Proxy, Tools, and Diagnostics. The main area is titled 'Insite 360 Configuration' and contains several sections:

- General Configuration:** Includes fields for OVR ID (155454), Site Name (SQA Lab), Site Address (test), and Omnia Nickname (test). It also has checkboxes for 'Domant Enabled' and 'Download Logs Every (mins)' (set to 30).
- PUMP Configuration Settings:** Includes dropdown menus for 'Two-Wire Money Mode' (5 Digit Money Mode (Default)), 'Money Decimal Position' (5 Digit Money Mode (Default)), 'PPU Decimal Position' (X.xxx (Default)), 'Volume Decimal Position' (X.xxx (Default)), and 'Reported Volume Format' (2 - Transaction Volume as XXX.XXX (Default)). There is also a checkbox for 'Real-Time Volume Enabled'.
- CRIND Configuration Settings:** Includes checkboxes for 'Barcode Scanner Side A present', 'Printer Side A present', 'Barcode Scanner Side B present', and 'Printer Side B present'.

At the bottom right of the configuration area are 'Cancel' and 'Save' buttons.

In most cases, the default values are fine. However, if a 6-digit money volume is selected (for example, aircraft or marina location), the PCN values need to be configured. The Pump Configuration Settings are configurable and must match the PCN. For more information on the relevant command codes, refer to *MDE-3860 Programming Quick Reference Guide*.

In Generic mode, all five fields within Pump Configuration Settings are configurable and must match the PCN.

- Omnia “Two-Wire Money mode”: PCN CC 47->FC 1
- “Money Decimal Position”: PCN CC 42 ->FC 1
- “PPU Decimal Position”: PCN CC ->FC 4
- “Volume Decimal Position”: PCN CC 42 ->FC 2
- “Reported Volume Format”: PCN CC 47->FC 2

In MOC mode, the configuration of the PCN will be detected automatically by Omnia, and the first four parameters within Pump Configuration Settings are grayed out (see [Figure 5-19](#) on [page 5-16](#)). Reported Volume Format must be configured to match the setting in the PCN (CC 47 -> FC 2).

Field	Pump Configuration Settings
Two-Wire Money Mode	5-digit Money Mode or 6-digit Money Mode are available. The default is 5-digit Money Mode.
Money Decimal Position	X.xx is the default value.
PPU Decimal Position	X.xxx is the default value.
Volume Decimal Position	X.xxx is the default value.
Reported Volume Format	2 - Transaction Volume as XXX.XXX is the default value.
Real-Time Volume Enabled	The default value is not selected.

- 3 Select the CRIND Configuration Settings according to the hardware present on the dispenser:
- Barcode Scanner Side A Present
 - Printer Side A Present
 - Barcode Scanner Side B Present
 - Printer Side B Present

Figure 5-19: Pump Configuration Settings Grayed Out

The screenshot displays the 'Insite 360 Configuration' window. On the left is a dark sidebar with navigation links: Home, General Settings, Applications, Insite 360, RTP Proxy, Tools, and Diagnostic. The main area is titled 'Insite 360 Configuration' and contains two tabs: 'Settings' (active) and 'Registration'. Under the 'Settings' tab, there are three sections: 'General Configuration', 'PUMP Configuration Settings', and 'CRIND Configuration Settings'. The 'PUMP Configuration Settings' section contains several fields: 'Two-Wire Money Mode' (set to '5 Digit Money Mode (Default)'), 'Money Decimal Position' (set to 'X.xx (Default)'), 'PPU Decimal Position' (set to 'X.xxx (Default)'), 'Volume Decimal Position' (set to 'X.xxx (Default)'), 'Reported Volume Format' (set to '2 - Transaction Volume as XXX.XXX (Default)'), and 'Real-Time Volume Enabled' (unchecked). These fields are all grayed out. The 'CRIND Configuration Settings' section contains four checkboxes: 'Barcode Scanner Side A present' (unchecked), 'Printer Side A present' (checked), 'Barcode Scanner Side B present' (unchecked), and 'Printer Side B present' (checked). At the bottom right of the configuration area are 'Cancel' and 'Save' buttons. A small graphic of a dispenser is visible on the right side of the window.

- 4 Click **Save**.

Omnia Configurator - Open Apps Configuration

- 1 Click **Open Apps** in the left navigation to open the Open Apps Configuration page.

Figure 5-20: Open Apps Configuration

The screenshot shows the 'Open Apps Configuration' page in the Omnia Configurator. The left sidebar contains navigation links: Home, General Settings, Insula 363, Open Apps (selected), RTP Proxy, Xsper Tool v2.1.3, Tools, and Diagnostics. The main content area has the title 'Open Apps Configuration'. Below the title, there are several configuration fields with dropdown menus and checkboxes, each with a green checkmark indicating it is set correctly. The fields are: Media State Enabled (set to Enabled), Idle Loop Delay (set to 10), Idle Loop Delay From Busy (set to 10), Busy Loop Delay (set to 5), Volume (set to 50), Server (set to 10.5.55.66), JavaScript Console (set to Disabled), Side A Pump ID (set to 7), and Side B Pump ID (set to 11). At the bottom of the form are 'Cancel' and 'Save' buttons. The browser address bar at the bottom shows the URL: https://10.80.32.50:4011/index#dynamicConfiguration.

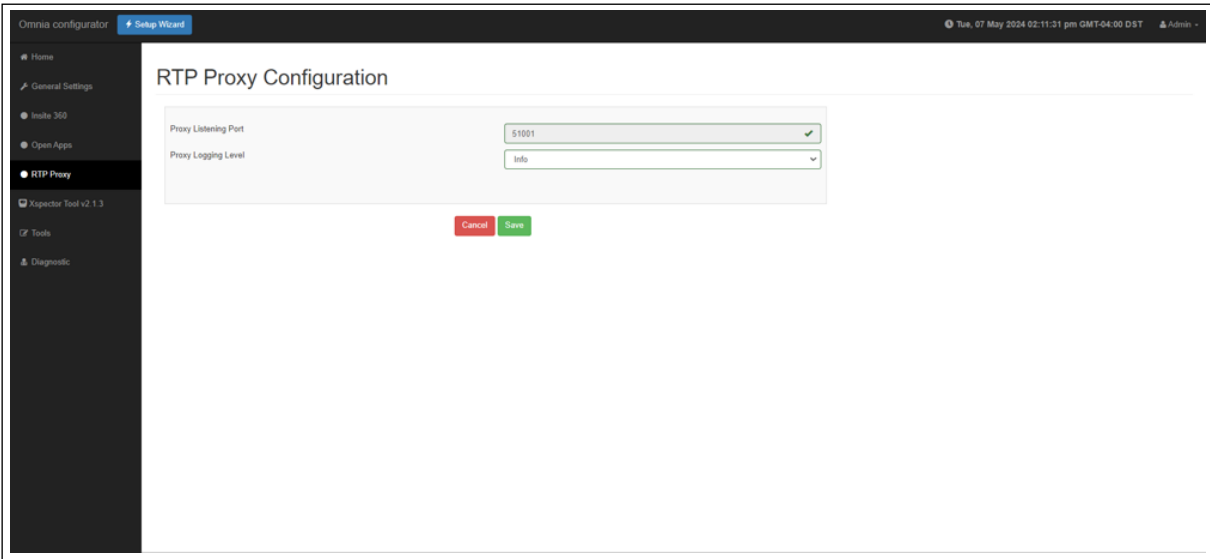
Field	Configuration Settings
Media State Enabled	When enabled, media states are emulated by the dispenser. When disabled, media states must be pushed from the POS.
Idle Loop Delay	Number of seconds of delay before starting idle media loop.
Idle Loop Delay From Busy	Number of seconds of delay before starting idle media loop after busy loop.
Busy Loop Delay	Number of seconds to delay before starting the busy media loop.
Volume	Video volume 1-100
Server	Applause server IP address should be changed (recommended 10.5.55.66).
JavaScript Console	Enables the JavaScript Console for additional debugging of Open Apps.
Side A - Pump ID	Set the Pump Monitor ID to match the actual pump ID programmed in the unit programming. (If connected to Passport POS system, all IDs will be 7 for side A and 11 for side B).
Side B - Pump ID	Set the Pump Monitor ID to match the actual pump ID programmed in the unit programming. (If connected to Passport POS system, all IDs will be 7 for side A and 11 for side B).

- 2 Click **Save**.

Omnia Configurator - RTP Proxy Configuration (Optional)

If Insite360 monitoring of door sensors is installed in the Omnia system, complete the configuration for RTP Proxy.

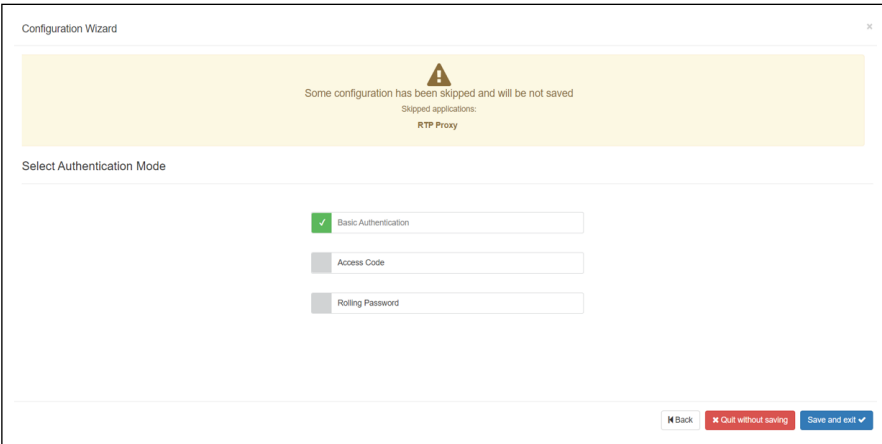
Figure 5-21: RTP Proxy Configuration



Field	Configuration Settings
Proxy Listening Port	TCP port for internal use. It is an informative field and cannot be changed.
Proxy Logging Level	Log verbosity level. Change only if more log data is required for troubleshooting.

The Dynamic configuration app pages displays a skip button. Clicking this will not save changes to relative app configuration on wizard closure. If there is a skipped configuration, the error shown in [Figure 5-22](#) is displayed.

Figure 5-22: Skipped Configuration Error



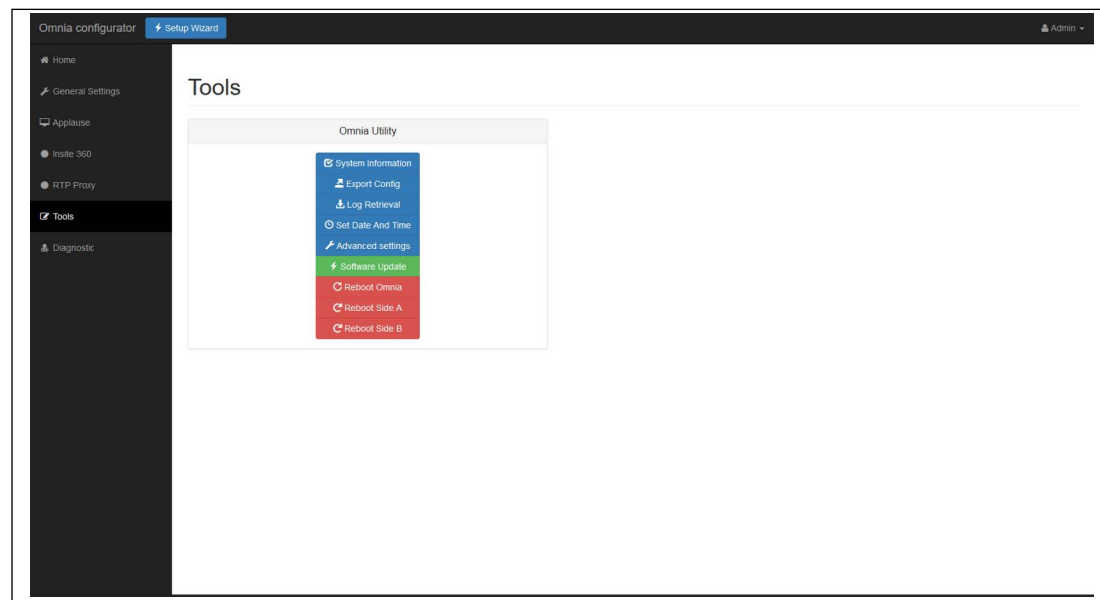
Omnia Configurator - Tools

Omnia device provides a set of utility functions to perform the following:

- Retrieve System Information
- Export Config
- Log Retrieval
- Set Date and Time
- Advanced settings
- Software Update
- Reboot Omnia
- Reboot Side A (Reboots UPM)
- Reboot Side B (Reboots UPM)

To access to the utility functions, click **Tools** on the left sidebar of the Omnia web page.

Figure 5-23: Omnia Tools Settings



Retrieve System information

Click **System Information** to the retrieve current hardware and software status of the device.

Figure 5-24: System Information

System Information

Hardware info

Board Version	OMNIA-D-DEVEL
Board Part Number	M15758A001
Board Model Name	OMNIA
Board Manufacturing Date	2018-03-13
Board Manufacturer	VeriFone
Board Serial Number	RV181000004
PPN	15739385
MAC	00:50:83:10:29:f9

Pump info

CRC	E89C
DSS	AE28E3 94FF27 A1B5FE E850C3 C519FF BB9B0B 5126
Date	1 17 2020
Version	05-003

Software Versions

Factory Software Version	040401a
Core-FWR[Build]	04.08.00-e-PROD.6869.1608296849
Linux Kernel release	4.9.123-svn1925-PROD
ipump	05.18.000
gvrsfdt	3.3.0r3504
omnia-gui	1.0.3.1977
mph	2.2.1
omnia-webui	04.08.00-e-6869.6869
dcc	3.0.3
rtpproxy	1.3.2.1953
openappsbase	3.0.5
App_gradeapp	1.2.1
App_media-app	01.00.04.14
gradeapp-content	1.0.0
orion-layout-5	1.0.0
orion-layout-1-media-app	1.0.0
orion-layout-6	1.0.0
OpenApp license:	enabled
OpenApp keys:	OANT-public

installed software hash: 41451677

Diagnostic

Date and time	Wed, 24 Feb 2021 16:03:51 +0100
Time zone	CET +0100
Up Time	up 10 hours, 54 minutes
Temperature sensors	62.4 °C / 33.000 °C / 34.500 °C
Memory usage	2.014G / 984M / 498M / 48%
Storage Main (/)	2.3G / 1.6G / 609M / 72%
Storage Data (/mnt/DATA)	11G / 1.4G / 8.8G / 14%
Load average(CPU %)	2.95(73%) / 2.64(66%) / 2.46(61%)

Refresh Info
Export

Close

Export system information during troubleshooting; the file contains all system versions and diagnostic information. To export system information, click **Export**. A text file is saved on the computer.

Log Retrieval

Log Retrieval page allows to retrieve logs of OmniaOS/CloudApp/MediaApp. The log will be uploaded to the web page as a zip file with file name extension: ppn_dateandtime.zip.

From Log Retrieval, you can select the range of dates and the required log level.

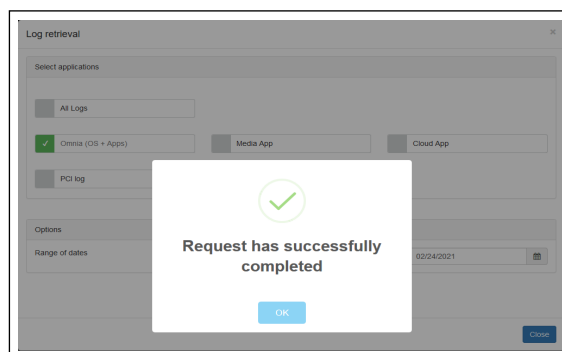
Note: Beginning with version 03.02, it is possible to retrieve all time and PCI-DSS relevant logs. "Log level required" option was removed (see [Figure 5-25](#)).

Figure 5-25: Log Retrieval

To retrieve logs, proceed as follows:

- 1 Select applications for which you want to retrieve logs.
- 2 Select the range of dates.
- 3 Select the required log level: Error - Warning - Info - Debug (only for Omnia running versions lower than 03.02).
- 4 Press **Download** for selected logs.

Figure 5-26: Log Retrieval Successful Message



Advanced Settings

The Advanced Setting page includes the following options:

Figure 5-27: Advanced Settings

Advanced settings

Platform Log level

debug

Log suppression

Enabled

Log Suppression will turn on after

24 hours

Force Display Size Algorithm (LAB usage Only)

Default

Set Authentication Login Mode

Basic Authentication

Cancel

Save

Close

Figure 5-28: Log Suppression Disabled

Advanced settings

Platform Log level

debug

Log suppression

Disabled

Automatically enabled in

2:59:50

Force Display Size Algorithm (LAB usage Only)

Default

Set Authentication Login Mode

Basic Authentication

Cancel

Save

Close

Field	Description
Logging level	There are two modes: standard and debug. - Standard is the default logging level during Omnia installation and initial startup, or during an Omnia software upgrade. - The Debug setting can be requested by Engineering or Service. It can be used for field trial monitoring or troubleshooting. The log level can be set remotely using Insite360.
Log suppression	Can be set to Enabled or Disabled using the toggle button. If disabled, a countdown until timeout will be shown.
Force Display Size Algorithm	Includes the following three options: Default, ForceA, and ForceB.
Set Authentication Login Mode	Includes the following three options: - No Authentication - This is the default option. - Access Code - Access code is provided by the customer. The access code must meet the following requirements: Between 6 and 40 characters that can include lowercase and uppercase letters, numbers, and special characters, and excluding spaces. - Rolling Password is generated from "System date", "PPN" and "Technician ID", and provided by Gilbarco Help Desk through the ASC Online Activation Tool. Select "Allow Rolling password as a secondary access method" if the customer wants to fall back to Rolling password rolling mode in case Access code is lost (see Figure 5-29 on page 5-23).

Note: If "Access code" login mode is chosen, an access code is requested and should be entered by the customer (see "Omnia Configurator - Diagnostic" on [page 5-33](#)).

In Set Authentication Login Mode, if the **Access Code** login mode is selected it will display the rolling password fallback option screen.

Figure 5-29: Login Mode with Access Code

The screenshot shows the 'Advanced settings' window. The 'Set Authentication Login Mode' dropdown is set to 'Access Code'. Below this, there are three input fields: 'Current Code', 'New Code', and 'Confirm New Code'. The 'Confirm New Code' field has a placeholder text 'Type the new code again'. At the bottom of the settings section, there is a toggle for 'Allow Rolling Password as Secondary Access Method' which is currently set to 'Yes'. At the very bottom of the window are 'Cancel', 'Save', and 'Close' buttons.

Figure 5-30: Login Mode with Rolling Password Selected

Advanced settings

Platform Log level: debug

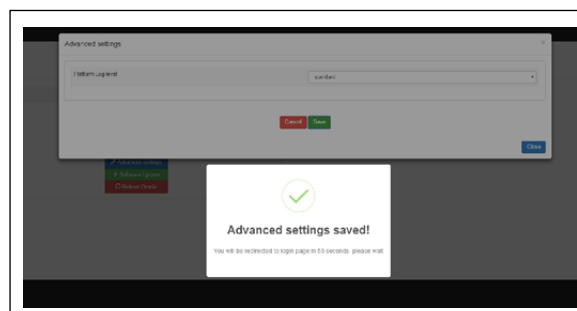
Log suppression: Enabled. Log Suppression will turn on after 24 hours.

Force Display Size Algorithm (LAB usage Only): Default

Set Authentication Login Mode: Rolling Password

Buttons: Cancel, Save, Close

After setting the desired values, click **Save**. Advanced settings will be saved.

Figure 5-31: Saving Advanced Settings

Set Date and Time

The Set Date and Time page allows to set the date, time and time zone of the Omnia system. From the Set Date and Time page, you can configure the NTP server settings and disable, if not required.

Note: If the device is connected to Internet and the public NTP URLs are reachable, then the date and time are automatically synchronized.

Figure 5-32: Setting Date And Time

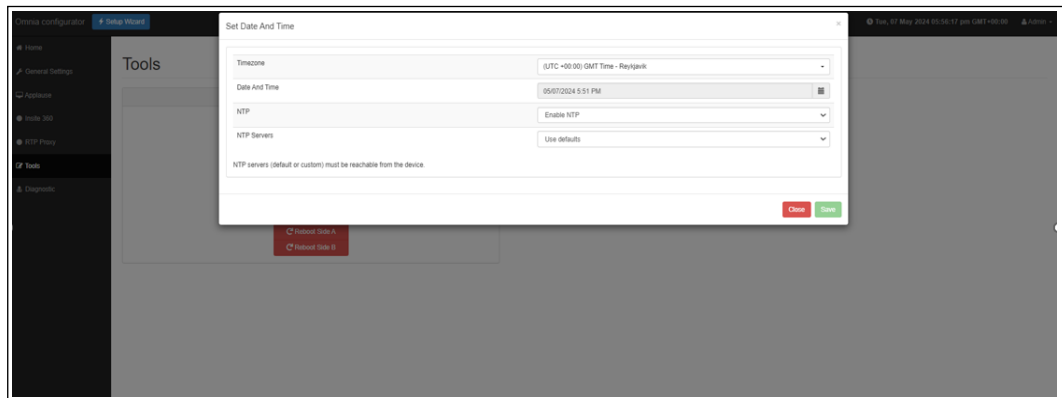
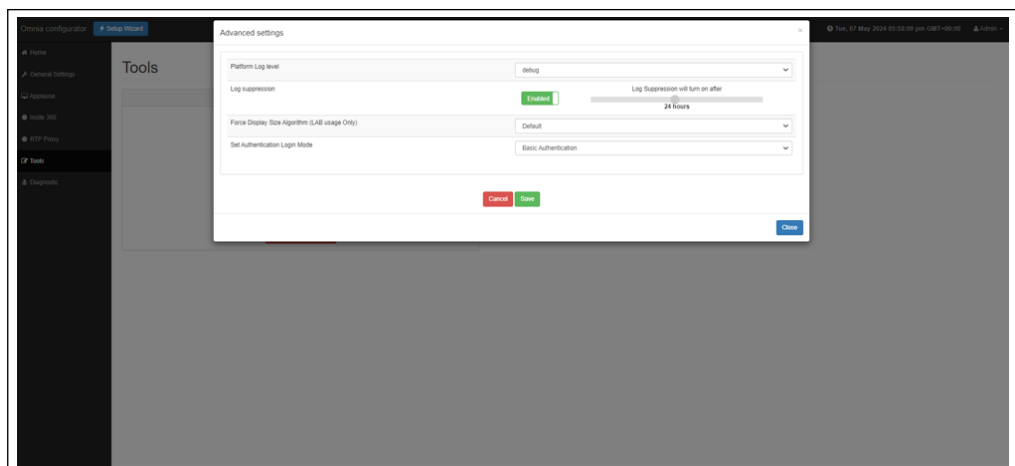


Figure 5-33: Tools > Advanced Settings



Field	Configuration Settings
Timezone	Region of the globe that observes a uniform standard time.
Date And Time	Current time (not available if NTP is enabled because the time is synced with NTP Server).
NTP	• ENABLE NTP (Omnia automatically syncs date and time with configured NTP server/s). • DISABLE NTP (Omnia uses system clock configured).
NTP Servers	Configure this parameter following customer IT requirement: use default server list or configure customer specific NTP servers IP address.

Notes: 1) If NTP servers are not available at the time of registration, manually set the date and time, and then re-enable NTP for future sync.

2) Verify that the LED on the homepage is green after setting the date and time.

WARNING

If LED is not lit green, the I360 functionality will be impacted..

Software Update

From the Software Update page, you can update the Omnia software: Core-Firmware, TW Proxy, CloudApp, MultimediaApp, RTP Proxy, OpenApp Framework, and OpenApps.

Requirements for Software Update

The software update page allows you to upload a zip file (zipped) that contains multiple debian signed packages. The software must be uploaded in a zipped format. Only use the zip file provided by Gilbarco to update the software (extranet). The zip file must not be extracted and should be uploaded as it is.

Expectations for the Software Update Process

- 1 The software upgrade process takes approximately 20-25 minutes.
- 2 After 12 minutes has passed, the dispenser goes offline from the forecourt. The pump flashes an error code 50. After 8-10 more minutes, the dispenser comes back online.

- 3 [Figure 5-36](#) on [page 5-29](#) shows the message that indicates when the software update is completed. Reboot to continue.

⚠ WARNING

1. Do not drag and drop entire folders.
2. Do not drag and drop files from archive explorer applications, which can cause installation failures.

To update the software, proceed as follows:

- 1 Select zip file.

Figure 5-34: Software Update - Upload Queue

Software update

1. Select files

Drop files here

Choose files

2. Upload queue

Name	Size	Progress	Status	Action
omnia-gui_1.0.3.1977_armhf.deb	3.30 MB	100 %	Done	Remove

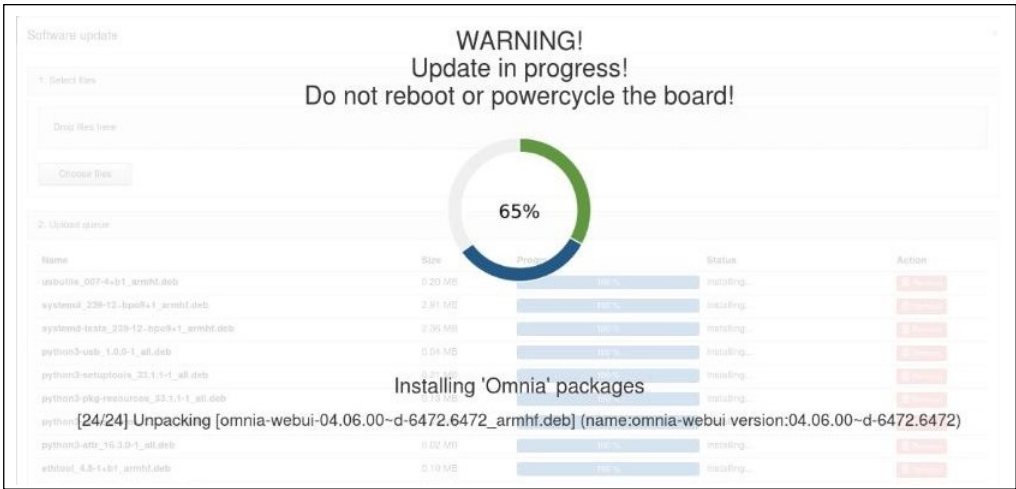
Overall uploading progress: 100 %

Upload all Remove all

Close

- 2 Wait until the Omnia packages are installed.

Figure 5-35: Software Update – Waiting Screen



IMPORTANT INFORMATION



Rebooting or power cycling the Omnia while a software update is in progress could potentially make the Omnia inoperative, and a PCB replacement might be required.

Note: From this point, the upgrade process takes approximately 20-22 minutes.

- 3 After 12 minutes has passed, the dispenser goes offline from the forecourt.
- 4 If an Error Code 50 is displayed, wait. It should clear when communication is re-established with the POS.

- 5 After 8-10 more minutes, the dispenser comes back online. [Figure 5-36](#) shows the message that indicates when the software update is completed. Reboot to continue.

Figure 5-36: Software Update Successful Completion Message

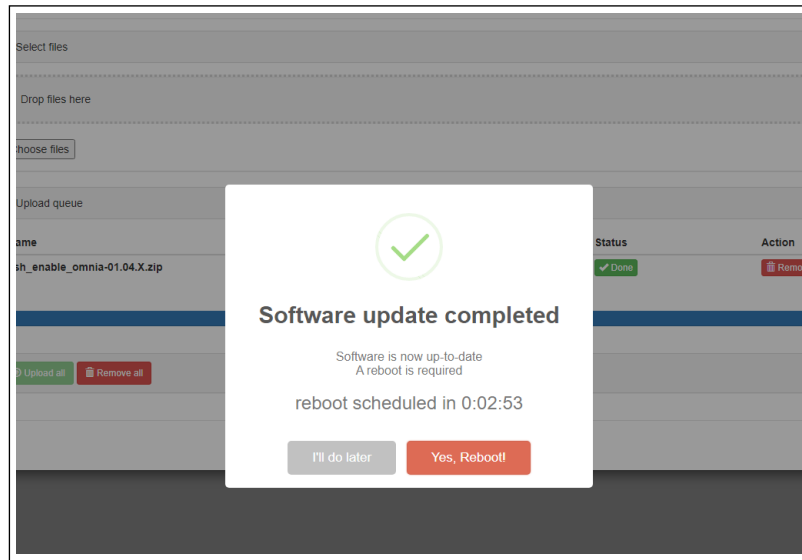
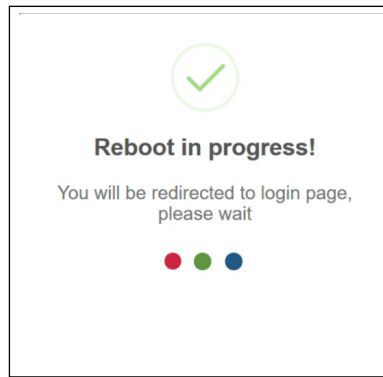
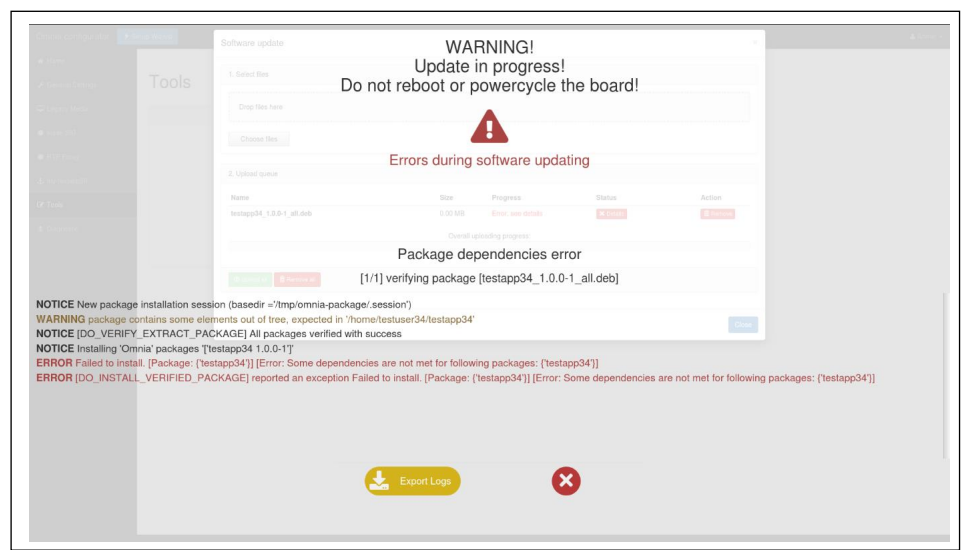


Figure 5-37: Initiating Reboot Message



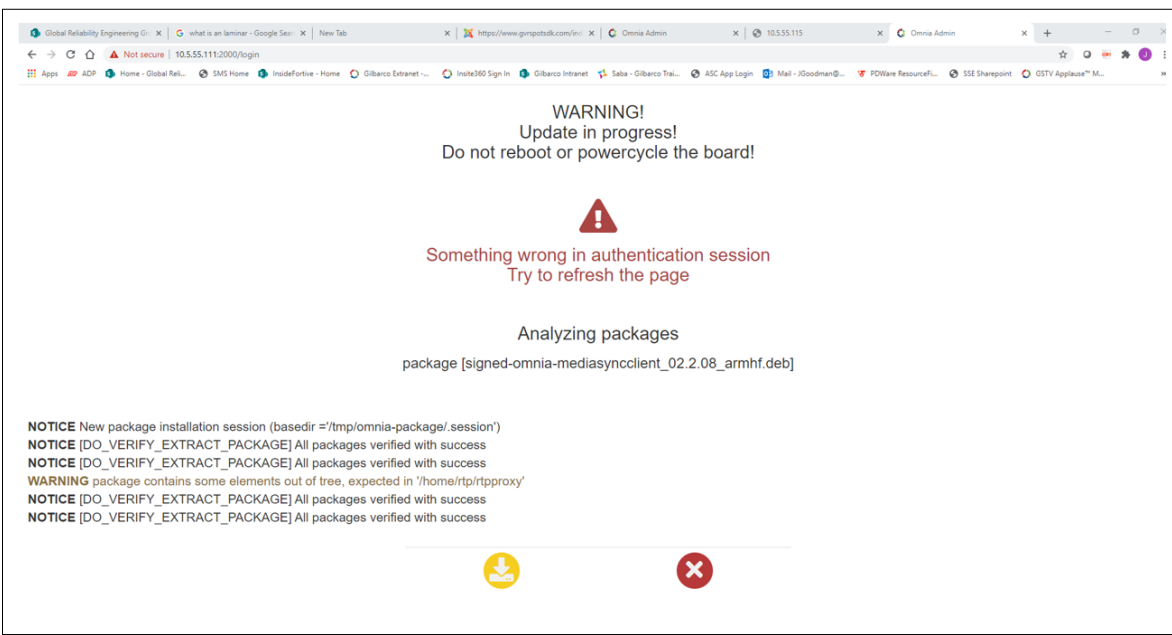
- 6 In case of errors in the software update, the progress indicator stops and an error message is displayed. Export the installation logs using the Export Logs button and close the page.

Figure 5-38: Software Update Error



Note: A warning could be issued sometimes due to loss of synchronization between WebUI and installing process (see Figure 5-39). Updates in background continue even if the error is present. Refresh the page to restore the installation information.

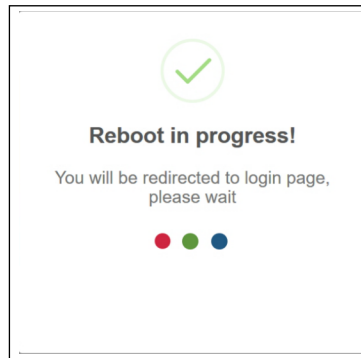
Figure 5-39: Warning Authentication Session



Reboot

Reboot the dispenser a second time.

Figure 5-40: Reboot Status

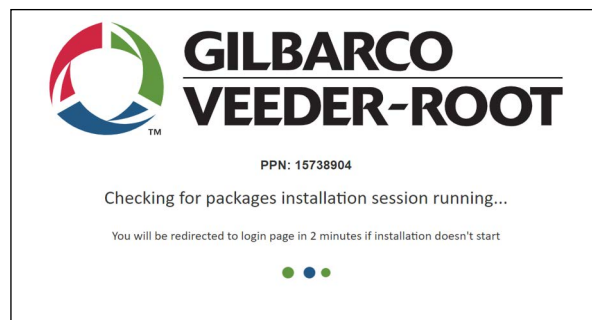


Software Update (From Version 04.07 or later)

The Software Update is a two-step process:

- 1 The first step checks for packages with system updates required by new versions of apps.

Figure 5-41: Software Update Packages



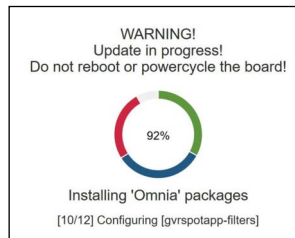
- 2 There is a prompt to reboot.

Figure 5-42: Software Update Reboot



- 3 All other apps are installed. The progress page is displayed.

Figure 5-43: Software Update Progress



- 4 After the Omnia reboots, you are prompted to log in.
- 5 On the Insite360 Configuration page, verify the status of the **Dormant Enabled** check box. If the customer has a contract for Insite360, the check box is not enabled. If the customer does not have a contract for Insite360, register the unit and enable the **Dormant Enabled** check box.

Figure 5-44: Insite 360 Configuration

Insite 360 Configuration

Settings Registration

General Configuration

GVR ID: 100454 ✓

Site Name: SQA Lab ✓

Site Address: test ✓

Omnia Nickname: test ✓

Dormant Enabled: ☐ (highlighted with a pink box)

Incremental Logs: ☒ ✓

Download Logs Every (mins): 30 ✓

Serial Cable Beep Alert Enabled (Zmodem/RTP): ☒ ✓

Door Sensor Enabled (RTP): ☐

PUMP Configuration Settings

Two-Wire Money Mode: 5 Digits Money Mode (Default) ✓

Money Decimal Position: X.xxx (Default) ✓

PPU Decimal Position: X.xxx (Default) ✓

Volume Decimal Position: X.xxx (Default) ✓

Reported Volume Format: 2 - Transaction Volume as XXX.XXX (Default) ✓

Real-Time Volume Enabled: ☐

CRIND Configuration Settings

Barcode Scanner Side A present: ☐

Printer Side A present: ☒ ✓

Barcode Scanner Side B present: ☐

Printer Side B present: ☒ ✓

Cancel Save

Accessing Omnia from the Backroom

After the Omnia is configured and if it is on a site LAN, it can be accessed from the backroom. To access the Omnia, use the external IP of A or B side UPM, followed by “:3000”. For example, 10.5.55.71:3000. From there, you can perform Omnia maintenance functions that do not require opening the dispenser, such as software upgrades, Applause testing, and log retrieval. Ensure that you cone off the dispenser that is impacted.

Omnia Configurator - Diagnostic

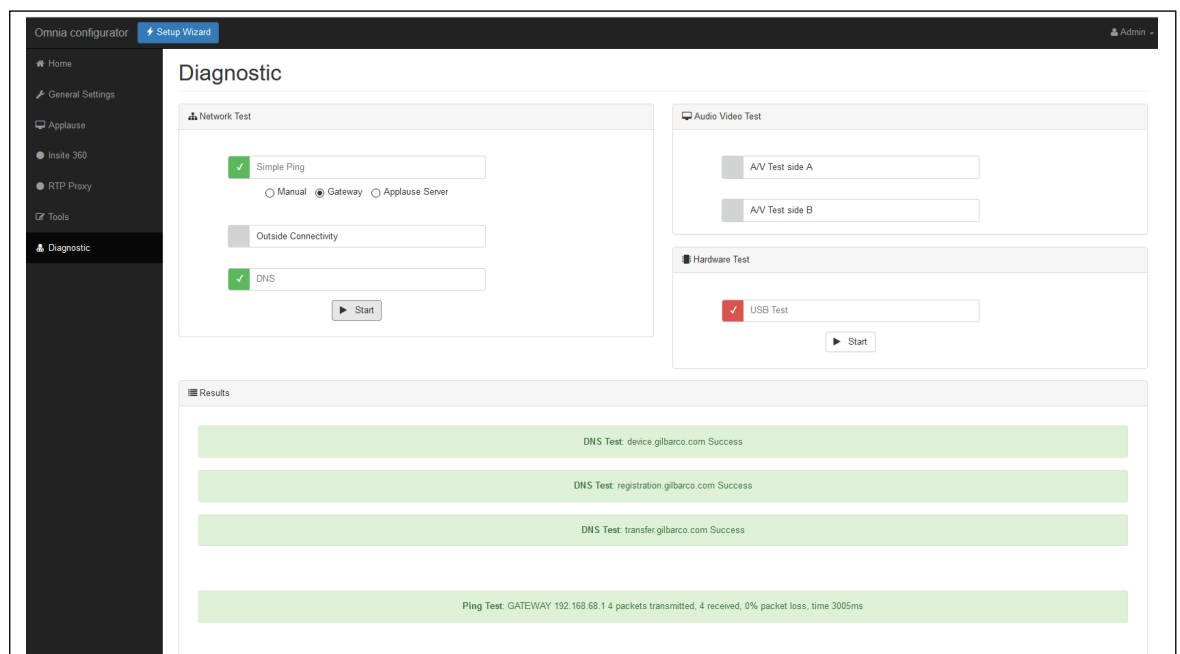
Omnia provides a set of utility functions to perform the following diagnostic tests:

- Networking diagnostics
- Audio video
- Hardware

Note: Diagnostic testing is not available when the Payment Type is Invenco.

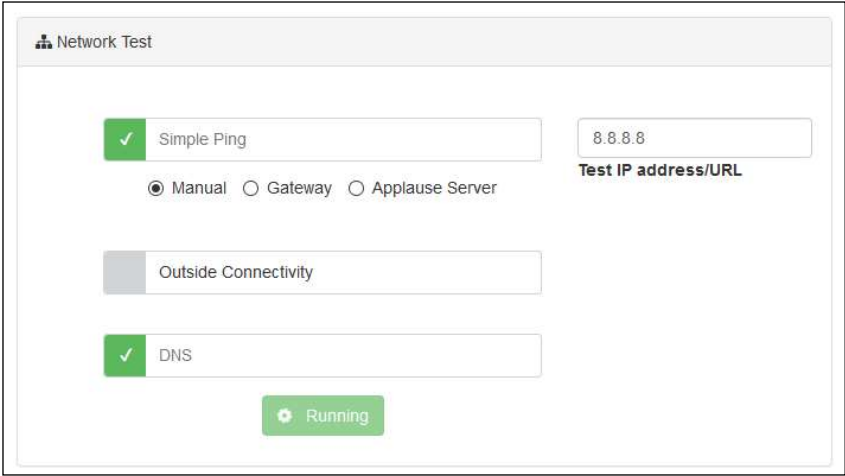
To access the Diagnostic page, click **Diagnostic** on the left pane of the Web interface.

Figure 5-45: Omnia Diagnostic Page



Every test group can be executed simultaneously by selecting the check box and clicking the corresponding **Start** button. While a test group (network or audio/video) is running, the corresponding Start button indicates the state with the label “Running” and a spinning cog.

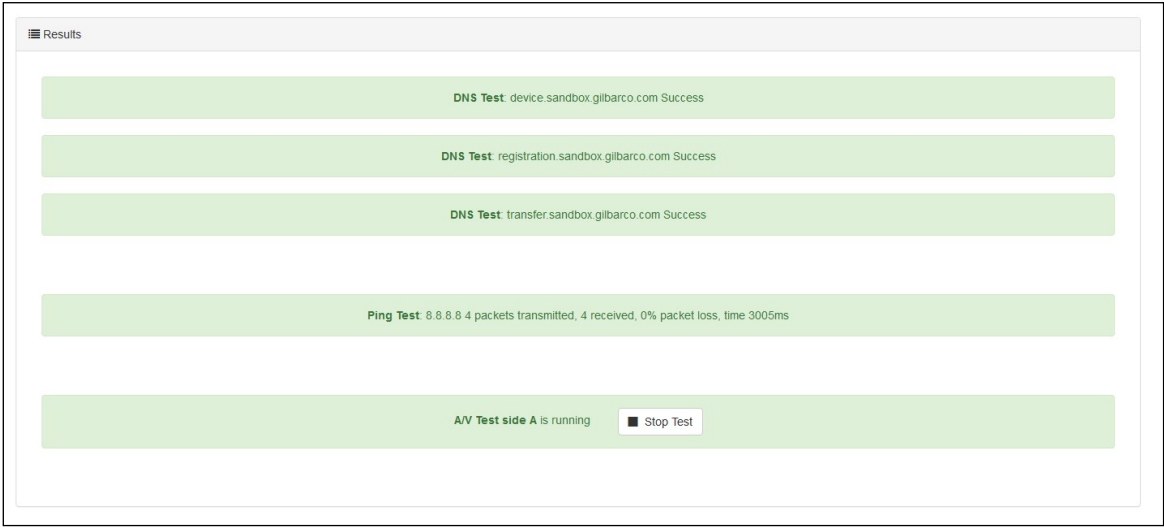
Figure 5-46: Network Test



The user cannot cancel or clear the selected tests while the corresponding test group is running.

All test results are reported on lower panel in the page.

Figure 5-47: Results Screen



Network Tests

These tests check network base functionalities.

Ping Test

This will perform a simple ping test to one of these hosts:

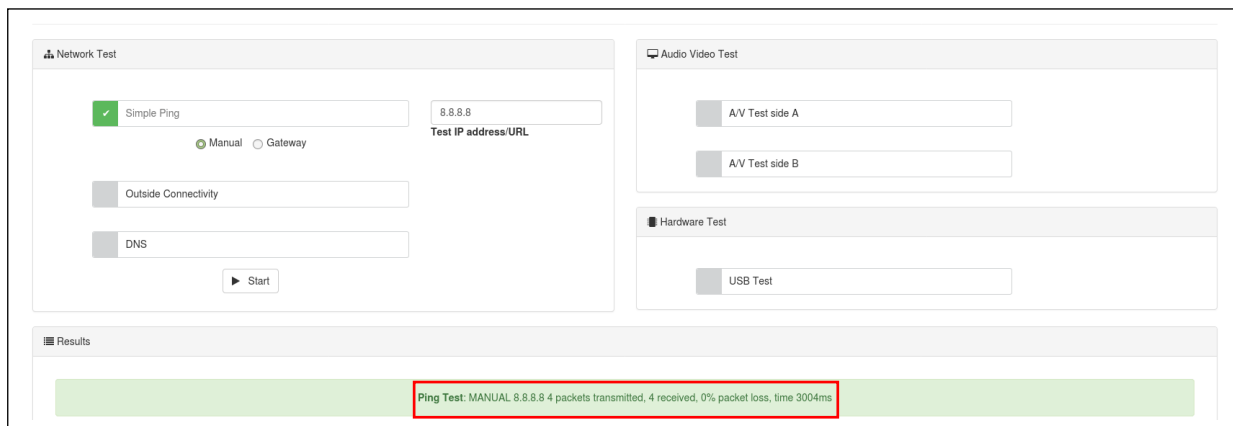
- 1 Default Ethernet gateway (defined in the network configuration section of General Settings page).
- 2 Applause Server (only if media or open apps are installed).
- 3 Manually chosen host (it can be an IP address or a URL).

Host can be an IP or a URL: in the case of a URL, a successful result means that DNS is functional.

To perform a ping test, proceed as follows:

- 1 Check **Simple Ping**.
- 2 Enter the IP address or URL to be pinged.
- 3 Click **Start**.
- 4 Select the test result in the “**Results**” section.

Figure 5-48: Ping Test



GVR Cloud Connectivity Test

If required, cloud connectivity can be tested as follows:

- 1 Select **Outside Connectivity**.
- 2 Click **Start**.
- 3 Select the test result in “Results” section.

Figure 5-49: GVR Cloud Connectivity Test

The screenshot displays the 'Diagnostic' interface with three main sections: Network Test, Audio Video Test, and Hardware Test. The Network Test section is active, showing 'Simple Ping', 'Outside Connectivity' (selected with a green checkmark), and 'DNS'. The 'Outside Connectivity' section has radio buttons for 'Legacy', 'AWS IOT' (selected), and 'Manual'. A 'Start' button is at the bottom. The Audio Video Test section has 'A/V Test side A' and 'A/V Test side B'. The Hardware Test section has 'USB Test'. The Results section at the bottom shows a table of test results, with a red box highlighting the 'Outside Connectivity Test' results.

Test Name	Result
Outside Connectivity Test: aatnf1k6u65sn-ats.iot.us-east-1.amazonaws.com:8883	Success
Outside Connectivity Test: cfvuav3n0omj9.credentials.iot.us-east-1.amazonaws.com:443	Success
Outside Connectivity Test: device-download-prod.s3.amazonaws.com:443	Success
Outside Connectivity Test: prod.i360.device.fileupload.s3.amazonaws.com:443	Success

DNS Test

If required, DNS configuration can be tested as follows:

- 1 Select **DNS**.
- 2 Click **Start**.
- 3 Select the test result in the Results section.

Figure 5-50: DNS Test

The screenshot displays the 'Diagnostic' interface with three main sections: 'Network Test', 'Audio Video Test', and 'Hardware Test'. In the 'Network Test' section, 'Simple Ping' and 'Outside Connectivity' are unselected, while 'DNS' is selected with a green checkmark. A 'Start' button is located below the 'DNS' selection. The 'Audio Video Test' section contains 'A/V Test side A' and 'A/V Test side B', both unselected. The 'Hardware Test' section contains 'USB Test', which is unselected. Below these sections is the 'Results' section, which contains three green bars representing test results. A red rectangle highlights the middle bar, which contains the text 'DNS Test: registration.sandbox.gilbarco.com Success'. The other two bars also show successful results for 'DNS Test' with different domain names.

Test Category	Test Name	Result
Network Test	Simple Ping	Unselected
	Outside Connectivity	Unselected
	DNS	Selected (Green Checkmark)
Audio Video Test	A/V Test side A	Unselected
	A/V Test side B	Unselected
Hardware Test	USB Test	Unselected
Results	DNS Test: device.sandbox.gilbarco.com	Success
	DNS Test: registration.sandbox.gilbarco.com	Success
	DNS Test: transfer.sandbox.gilbarco.com	Success

*Note: Networking tests can be performed simultaneously by selecting all of them and then clicking **Start**.*

Audio Video Test

If required, Omnia audio/video can be tested as follows:

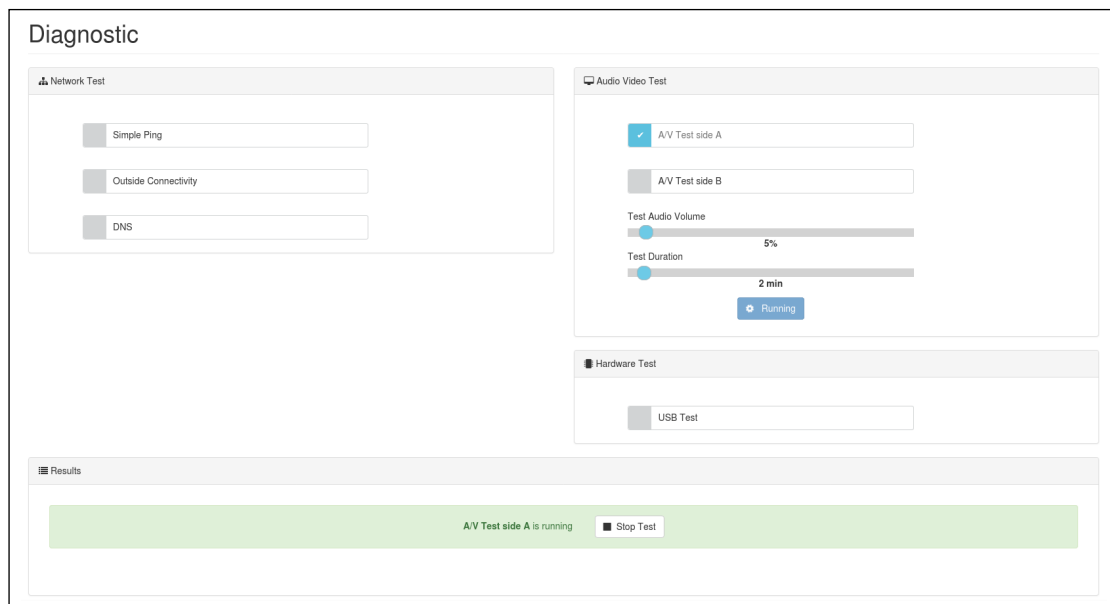
- 1 Select **A/V Test side A/B**.
- 2 Set the Test Audio Volume.
- 3 Set the Test Duration.
- 4 Click **Start**.

Notes: 1) If Idle/Busy loops videos are playing during the A/V test, the test may not complete properly. Disable the Applause Media System before starting the A/V test, and re-enable it again after the test is complete.

2) After the A/V test, with the Applause Media System disabled, the unit displays the CRINDBIOS Idle screen.

3) When running the A/V test on one side of the dispenser (side A/side B), the display on the other side shows either a black blank screen or POS screen.
- 5 Check if the test is running in the Results sections and the sample audio/video is playing.
- 6 The test can eventually be stopped by clicking **Stop** in Results section.

Figure 5-51: Audio Video Test



Note: A/V test controls both sides and stops all video playing even if test is performed on a side only.

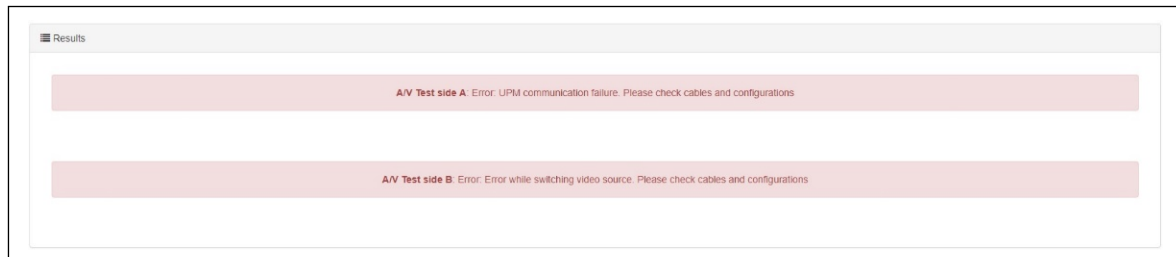
IMPORTANT INFORMATION



Do not forget to re-enable the Applause Media System if you disabled it intentionally before running the audio/video test.

- 7 If the sample audio/video is not playing, check errors in the Results section.

Figure 5-52: Audio Video Test in Error



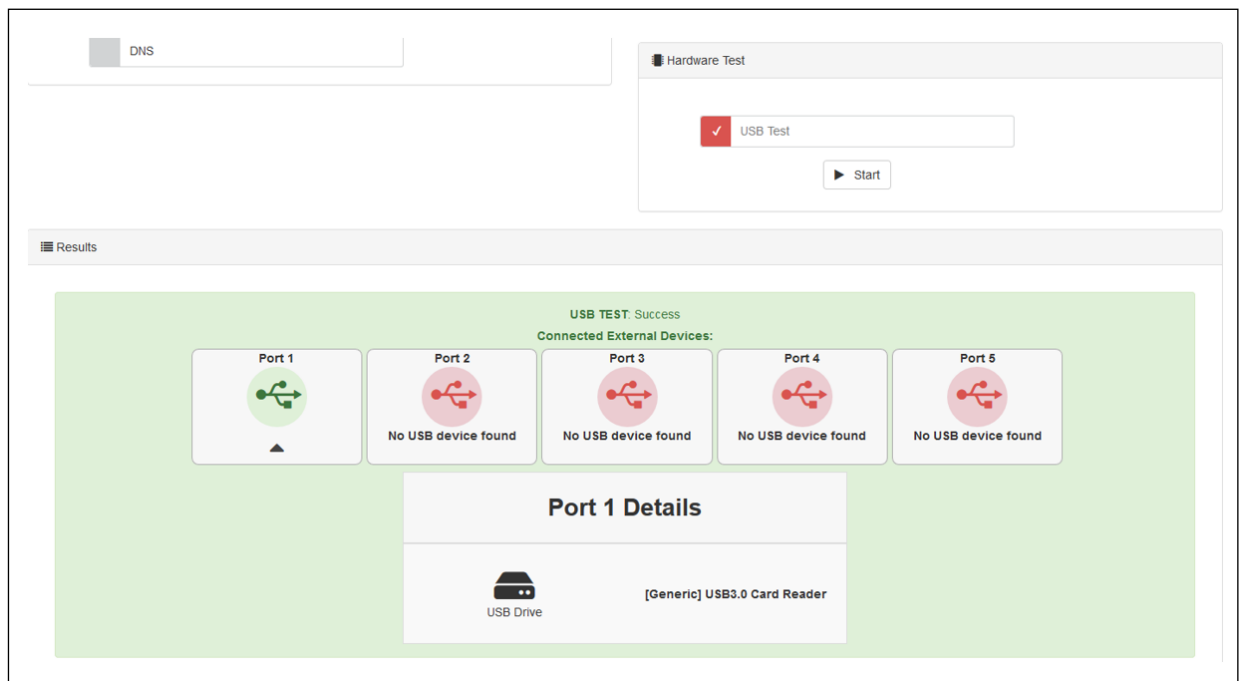
Hardware Test

This test group is dedicated to check hardware status on Omnia board.

USB Test

This test will check status of USB HUBs trying to detect devices connected to USB ports. It will try to detect device type for each port.

Figure 5-53: USB Test



Viewing and Testing Sniffer, Certificates, and Serial Connection

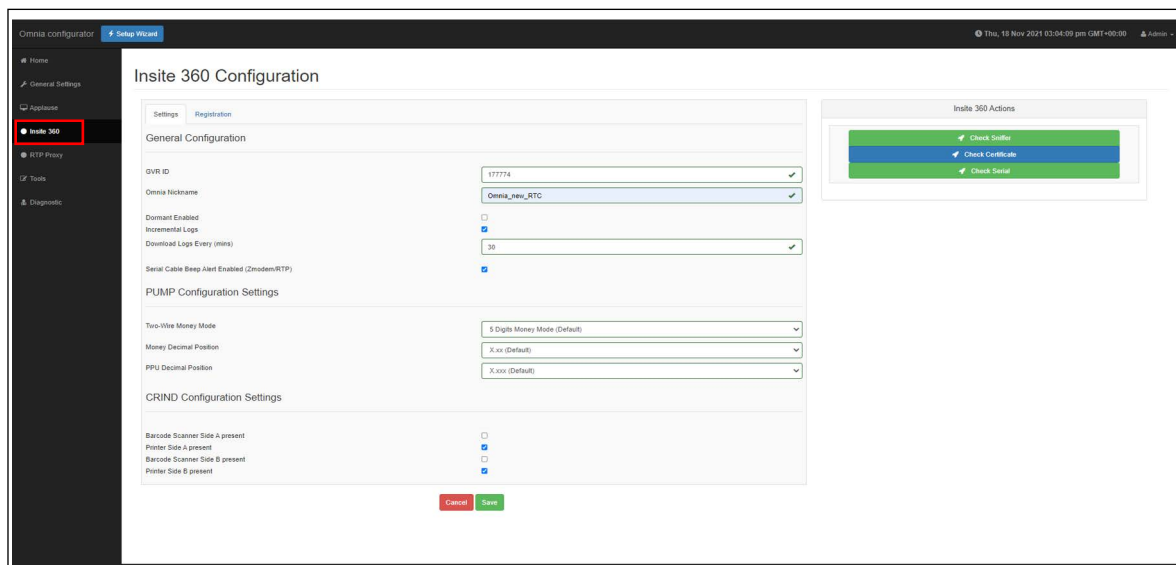
Before completing registration, The AWS IoT URLs must be set up prior to software upgrades and any attempt to register with Insite360 through AWS. Ensure that network rules are done by the customer IT department or MNSP provider. Registration will fail if the network rules are not set up. Refer to the [Pre-Installation Checklist](#) on [page 3-2](#) for a complete list of network rules.

Note: Omnia must be connected to NTP Servers to sync time.

To view, modify, and test current Insite360 Settings, proceed as follows:

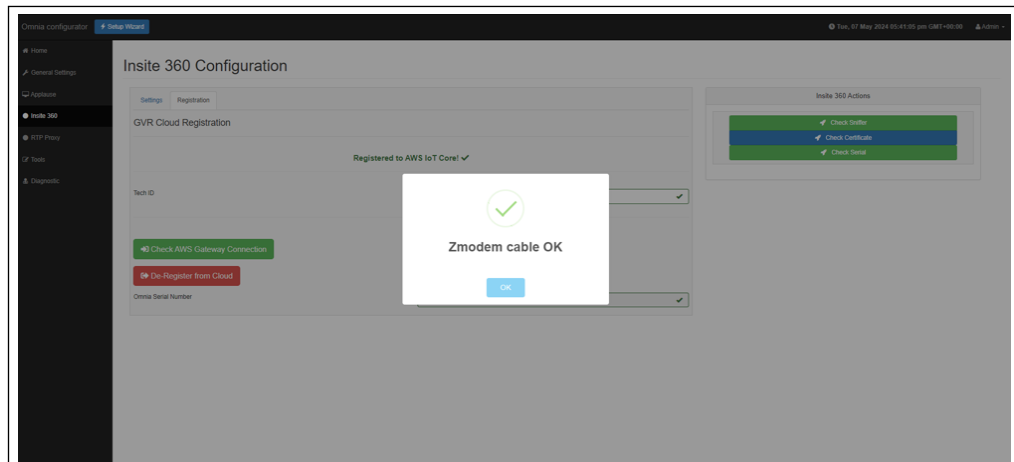
- 1 Select the **Insite 360** tab on the left sidebar.

Figure 5-54: Selecting the Insite 360 Configuration



2 Check the **ZModem** connection.

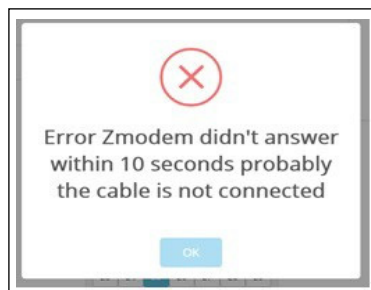
Figure 5-55: Checking Serial Interface Connection



In case of failure, an error message is displayed.

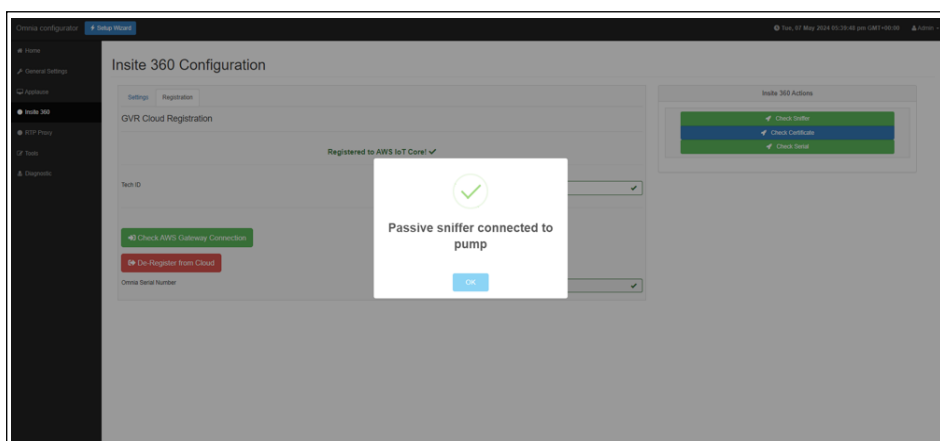
Note: For troubleshooting information, refer to “[Troubleshooting](#)” on [page 7-1](#).

Figure 5-56: ZModem Failure Message



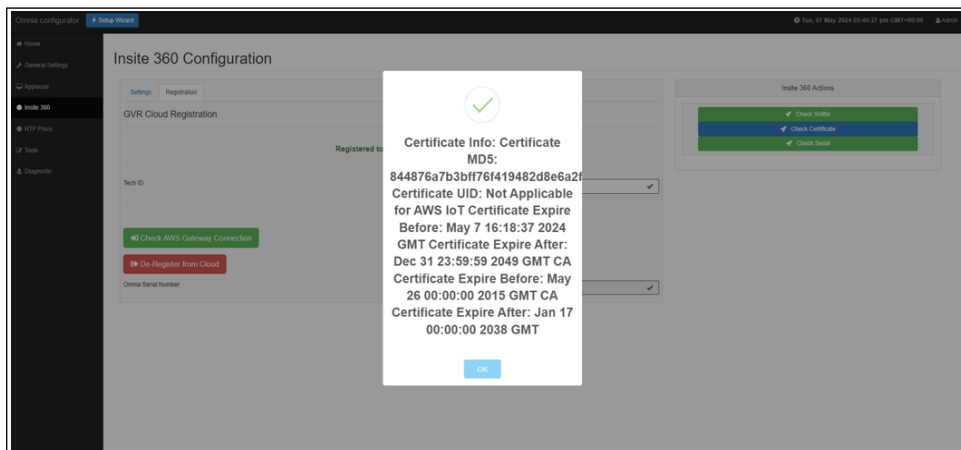
3 Check **Sniffer** connection using CLOUD Utility.

Figure 5-57: Checking Sniffer



In case the cloud connector cannot connect to Insite360, check the expiration date of the certificate.

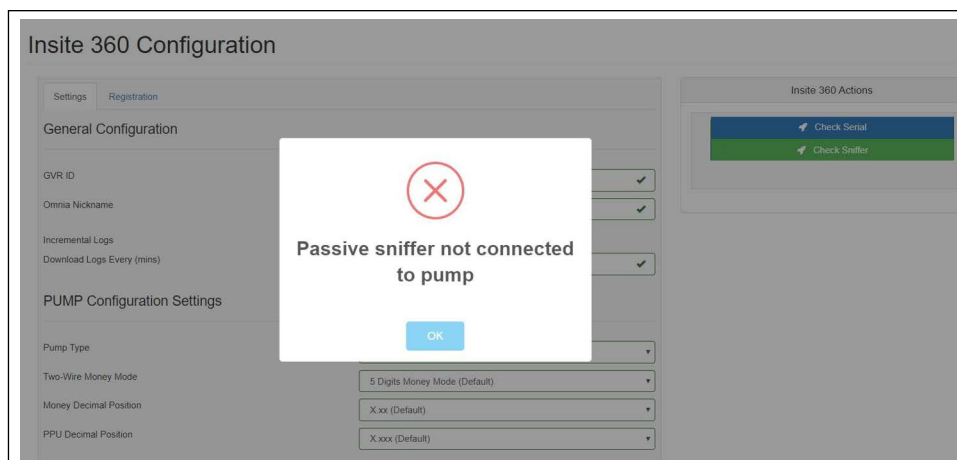
Figure 5-58: Check Certificate Message



In case of failure, an error message is displayed.

Note: For troubleshooting information, refer to “[Troubleshooting](#)” on [page 7-1](#).

Figure 5-59: Passive Sniffer Failure Message



Registering Omnia to Insite 360 Forecourt

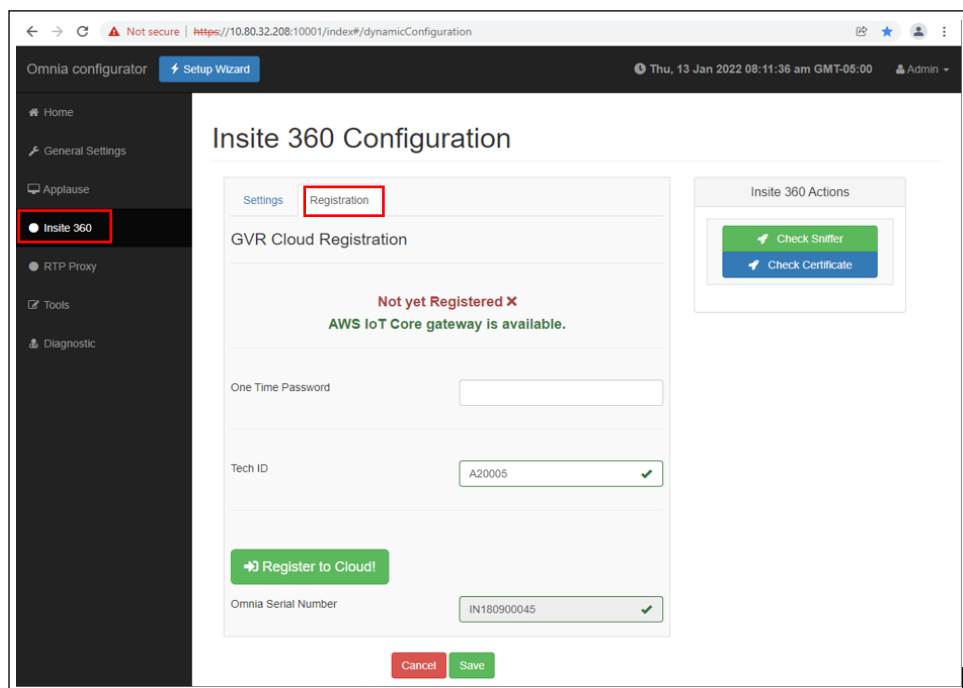
If AWS IoT Core is available (network rules in place locally), the message “AWS IoT gateway is available” is displayed in the UI.

- Notes:*
- 1) The AWS IoT URLs must be set up prior to software upgrades and any attempt to register through AWS. Ensure that network rules are done by customer IT department or MNSP provider. Registration will fail if not set up. The minimum software version of V05.06 or later must be loaded prior to AWS registration.
 - 2) Omnia must be connected to NTP Servers to sync time.
 - 3) Refer to the [Pre-Installation Checklist](#) on [page 3-2](#) for a complete list of network rules.

To register Omnia to Insite360 Forecourt, proceed as follows:

- 1 From the Insite 360 Configuration page, click the **Registration** Tab.

Figure 5-60: Insite 360 Configuration - Registration (AWS IoT Gateway)

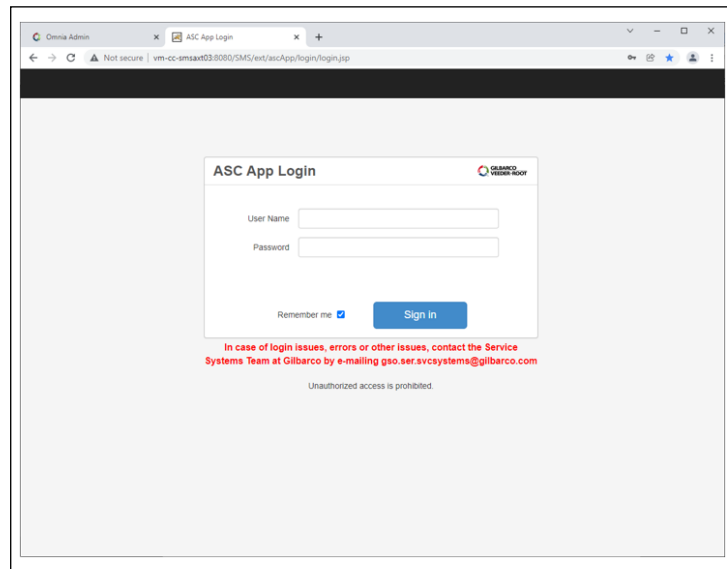


Note: To gain access to the one time password tool “I360 Device Pre-Registration” complete the mandatory tech training on “AWS OTP Registration module” in SABA.

- 2 Sign in to the ASC App at: <https://mymessage.gilbarco.com/SMS/ext/ascApp/login/login.jsp>.

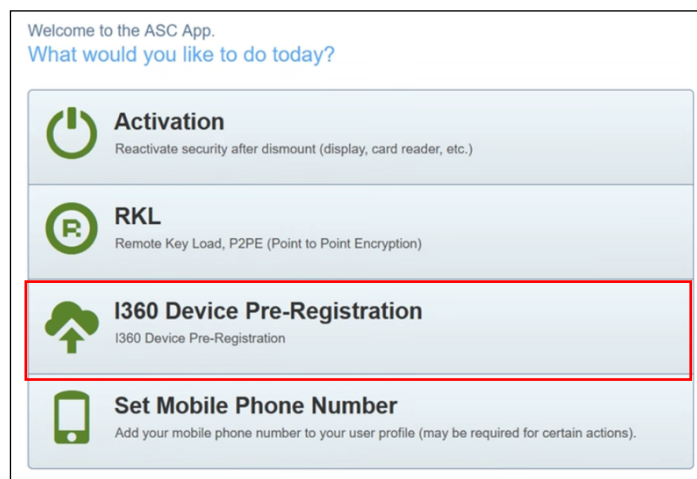
Registration to the AWS IoT Gateway requires a generated One-time Password (OTP) to be obtained from the Authorized Service Contractor ASC App.

Figure 5-61: ASC App Login



- 3 Select **I360 Device Pre-Registration** from the ASC App home page.

Figure 5-62: I360 Device Pre-Registration



*Note: The device serial number required for the ASC App is listed on the Insite 360 Registration page for the dispenser. **It is NOT the Device PPN used to log in to the UI.***

Figure 5-63: Omnia Registration Serial Number

- 4 At the ASC App, fill in the serial number for the device or devices that you want to register. Click **Add Next** for additional devices.

Note: You can add up to 20 devices per OTP.

Figure 5-64: Adding Additional Devices

In case of login issues, errors or other issues, contact the Service Systems Team at Gilbarco by e-mailing gso.ser.svcsystems@gilbarco.com

Step 1: Enter Serial Number

Serial Number *

serial1

serial2

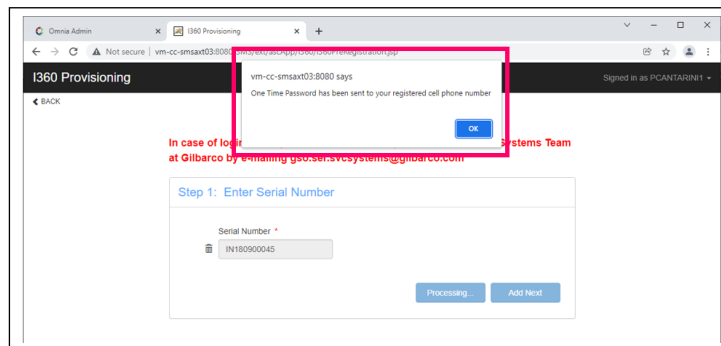
Done Add Next

IMPORTANT INFORMATION

The Omnia serial includes prefix letters; you **MUST** capitalize these letters when entering them into the serial number field and ensure that there are no spaces before and after the serial number or the OTP process will fail.

- 5 Ensure that you enter the correct serial number.
- 6 Click **Done** when all the serial numbers are entered.
- 7 An SMS message with the OTP is sent to the technician's registered phone number. One OTP can be used to register up to 20 devices, and the OTP is valid for 30 minutes.

Figure 5-65: SMS Message for OTP



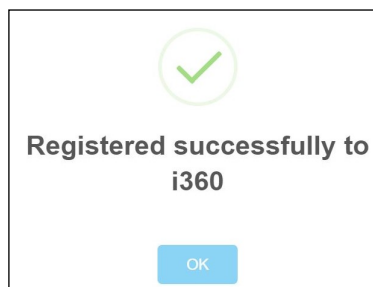
- 8 In the Insite 360 Configuration - Registration Tab, enter the OTP into the **One Time Password** field.

9 Enter **Tech ID** and click **Register to Cloud!**.

Figure 5-66: GVR Cloud Registration - AWS IoT Gateway Available

The screenshot shows the 'Insite 360 Configuration' page in a web browser. The browser address bar shows 'https://10.80.32.208:10001/index#/dynamicConfiguration'. The page has a dark sidebar on the left with the 'Insite 360' menu item selected. The main content area is titled 'Insite 360 Configuration' and has two tabs: 'Settings' and 'Registration'. The 'Registration' tab is active, showing 'GVR Cloud Registration'. A message at the top of the registration section says 'Not yet Registered X AWS IoT Core gateway is available.' Below this, there are four input fields, each with a green checkmark icon to its right: 'One Time Password' with value 'RplW-1Ep', 'Tech ID' with value 'A20005', 'Omnia Serial Number' with value 'IN180900045', and a 'Register to Cloud!' button which is highlighted with a red box. At the bottom of the registration section are 'Cancel' and 'Save' buttons. On the right side of the page, there is a box titled 'Insite 360 Actions' containing two buttons: 'Check Sniffer' and 'Check Certificate'.

Figure 5-67: Registration Successful Message



- 10 Upon successful registration, refresh the page to update the screen. The Insite 360 Configuration page displays a green message “Registered to AWS IoT Core” and the addition of a “De-Register from Cloud” button.

Figure 5-68: GVR Cloud Registration - Registered to AWS IoT

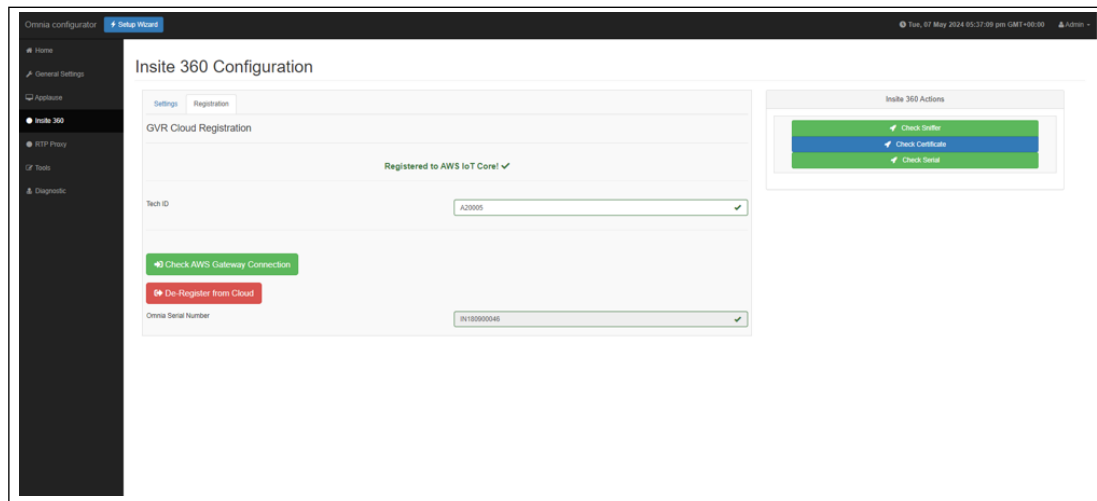
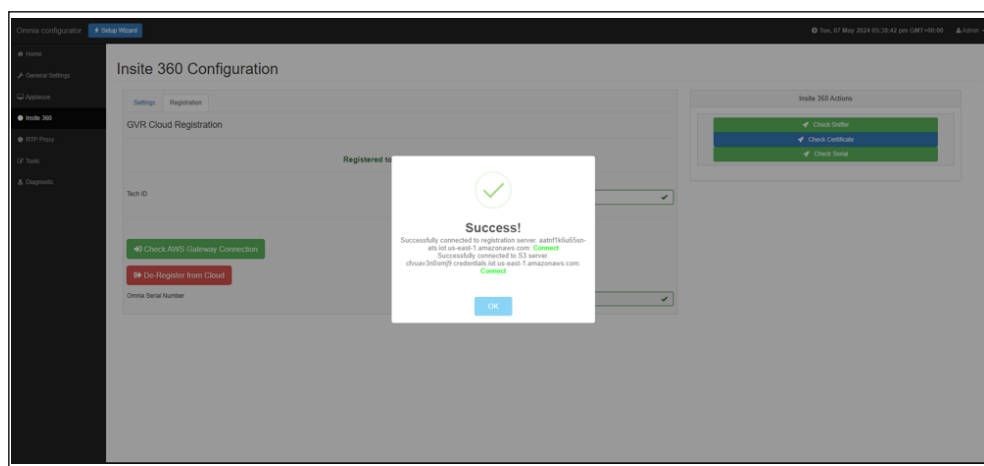


Figure 5-69: Connection Successful to AWS Message

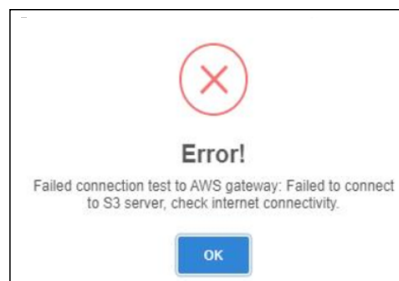


- 11 Refresh the page to update the screen.

The following are the top reasons for AWS Registration failure:

- 1 URL rules not set up properly at the site's network.
- 2 Serial numbers were entered into the ASC app incorrectly.
- 3 Date and Time on Omnia or SSoM is incorrect or not in sync.
Note: Omnia must be connected to NTP Servers to sync time.
- 4 Network Connectivity (physical, and network configuration).
- 5 If Insite360 site is not provisioned properly, registration will fail.

Figure 5-70: AWS Failed Connection Error Message



Insite360 Auto-Registration

IMPORTANT INFORMATION

If the customer already has an Insite360 contract, you **MUST** manually register the device. **DO NOT** leave the site without manually registering. The Omnia V05.08 software introduces the AWS-IoT feature allowing Omnia to make attempts to automatically register against AWS IoT if there is no contract. If the ICS registration fails, contact the site MNSP for setup, verification, and troubleshooting.

The GVR ID and Primary DNS must be entered by the technician for auto-registration to work properly.

- 1 If the Fueling Position field is updated remotely, a message “This field was automatically updated via cloud” is displayed (see [Figure 5-71](#)).

Figure 5-71: Fueling Position Updated By Insite360 Message

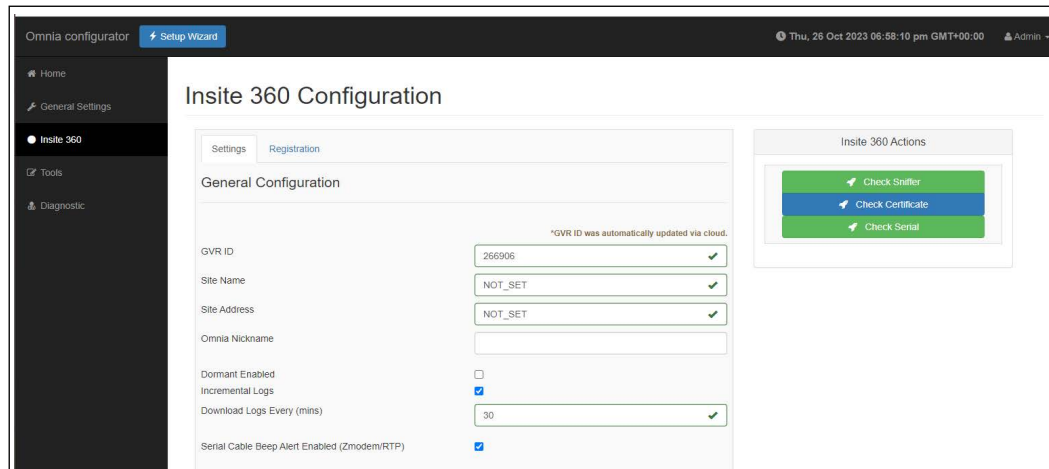
The screenshot shows the 'Omnia configurator' interface with the 'Setup Wizard' tab selected. The left sidebar contains navigation options: Home, General Settings (selected), Insite 360, Tools, and Diagnostic. The main area is titled 'General configuration' and contains several settings:

- Select Dispenser Model: Encore
- Select Payment Type: M7
- Select Dispenser Type: Dual side
- Select TwoWire Connection Type: GENERIC CRIND
- Select Pump Baud Rate: DEFAULT (5787)
- Fill in Dispenser Serial Number: (field with message box)
- Side A Fueling Position: 1
- Side B Fueling Position: 2
- Select Pump Connection Type: Zmodem
- Pump 2-Wire ID Side A (1-16): 1
- Pump 2-Wire ID Side B (1-16): 2

A black message box with white text is overlaid on the 'Fill in Dispenser Serial Number' field, stating: "This field was automatically updated via cloud".

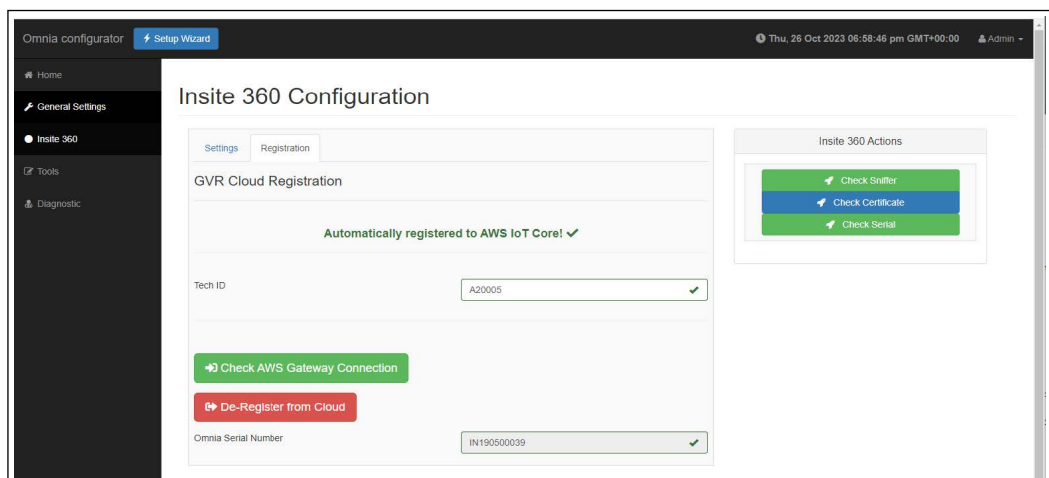
- 2 If GVR ID is updated remotely from Insite360, the message “GVR ID was automatically updated via cloud” is displayed.

Figure 5-72: GVR ID Updated Message



- 3 When the Omnia device is auto-registered, the message “Automatically registered to AWS IoT Core!” is displayed.

Figure 5-73: AWS IoT Core Message

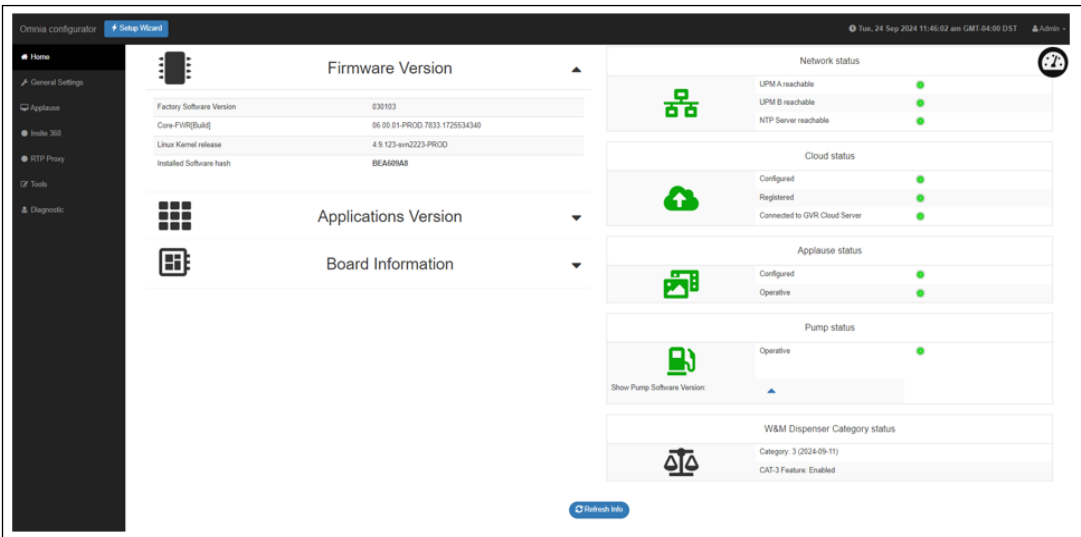


Omnia Home Page

Omnia home page provides a quick overview of the software installed, hardware version revision, date and time, Up time, Multiple Access Control (MAC) address, and PPN.

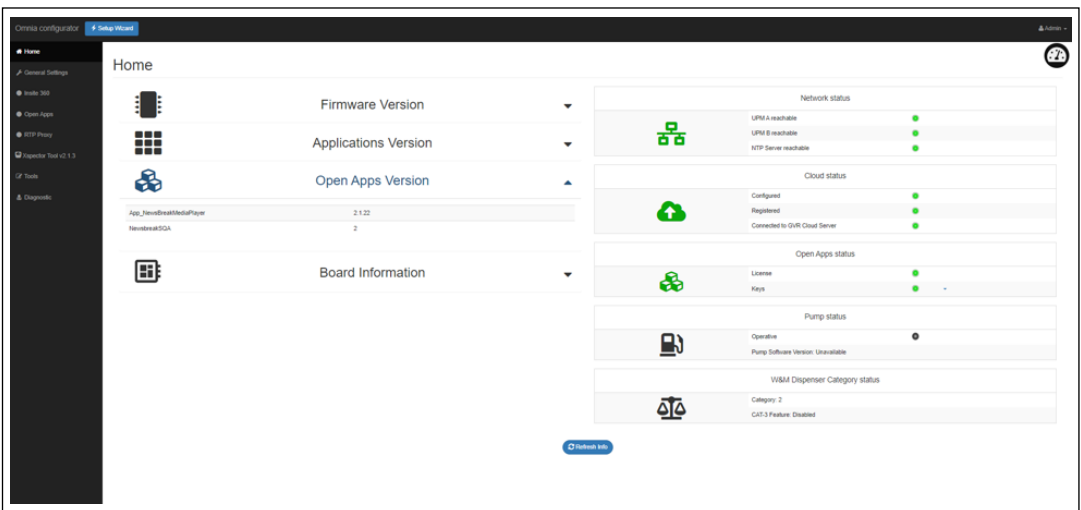
After successful login, the Omnia home page opens (see [Figure 5-74](#)).

Figure 5-74: Home Page - Showing Applause Media and Pump Status



Note: The Pump Status Panel is not displayed, if the “Pump Connection Type” is set to “None” in the General Settings Page.

Figure 5-75: Home Page - Encore Experience Installed



The Omnia home page includes the following:

Section	Tabs / Button
Setup Wizard button	Used for adding new configuration or importing existing configuration.
Firmware Version	Includes the following options: • Factory Software Version • Core-FWR[Build] • Linux Kernel release • Installed software hash
Applications Version	Includes the following options: • CloudApp version • ActivityMonitor version • Pumpproxy version • Crindproxy • Mediasyncclient • Mediamanager
Applause	Includes the following options: • Configured • Operative - Connected to the Media content server. <i>Note: This field is visible only when Applause multimedia system is enabled.</i>
Open Apps Version	Includes the following options: • List of installed Apps • List of OpenApps contents • List of OpenApps layout
Board Information	Includes the following options: • Board Version • Board Part Number • MAC Address • PPN • Up Time

A status images group with Networks status, CloudApp status, MultimediaApp, and Pump Status is displayed.

Notes: 1) OpenApps status data is shown only if related applications are configured/activated.

2) Pump status is shown only for Door Sensor, where the pump is connected via RTP protocol.

The page also includes a Meters button to display self-updating meters with CPU Average Load, CPU Temperature, and Memory Load.

Figure 5-76: Meters Button

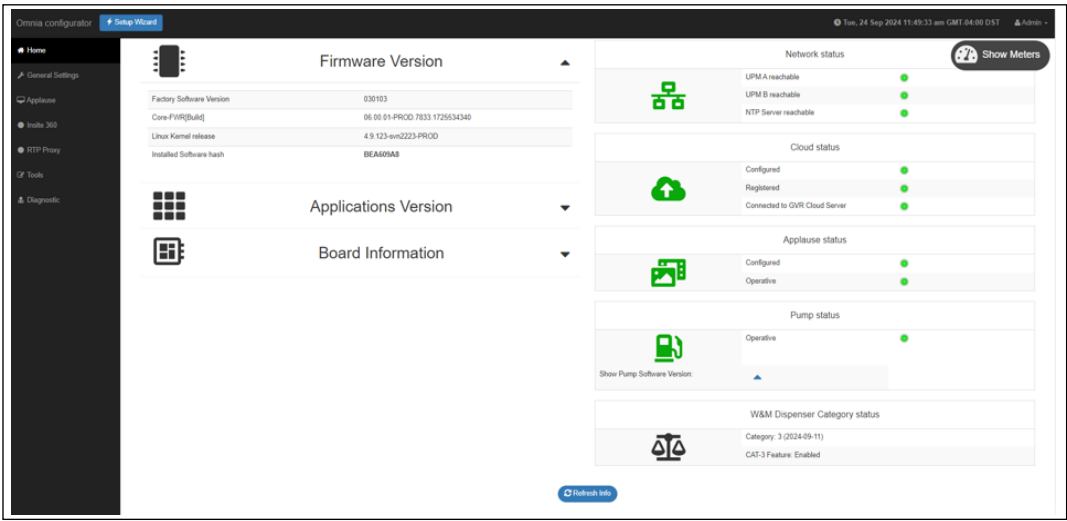
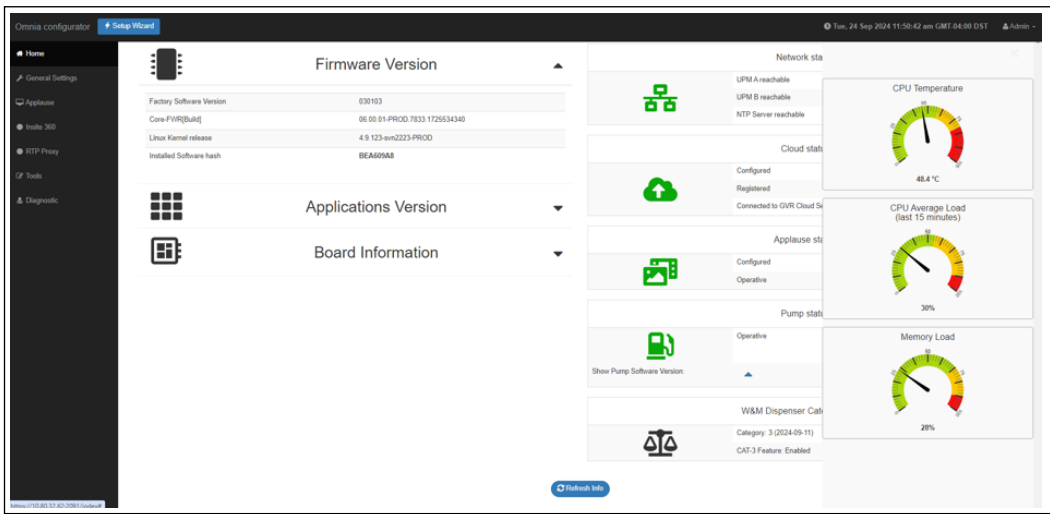
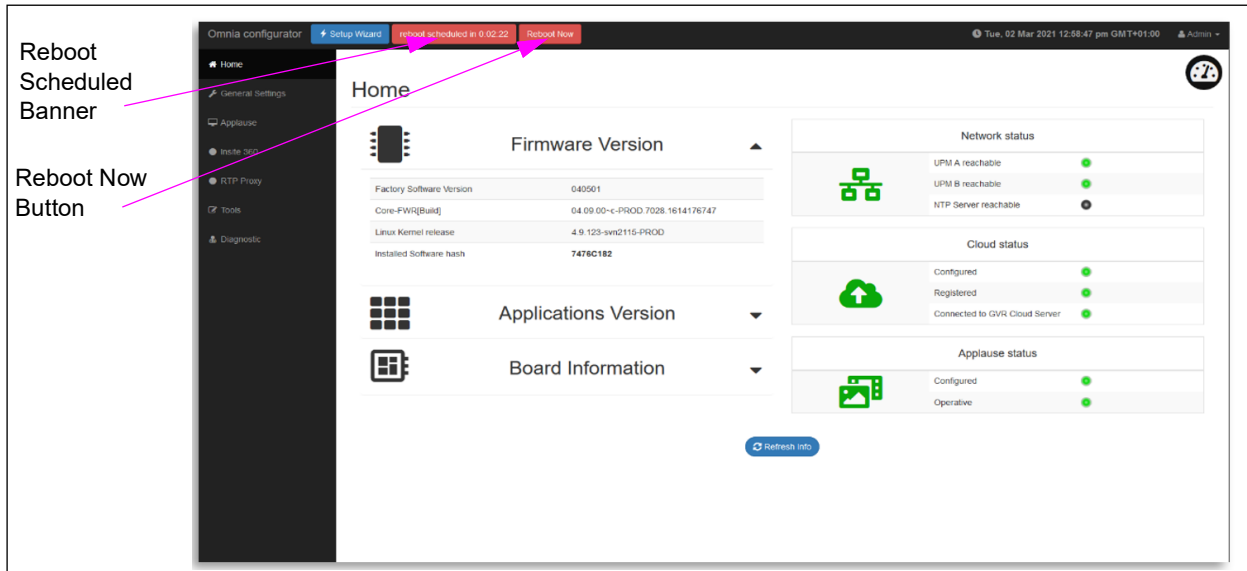


Figure 5-77: CPU Average Load, CPU Temperature, and Memory Load



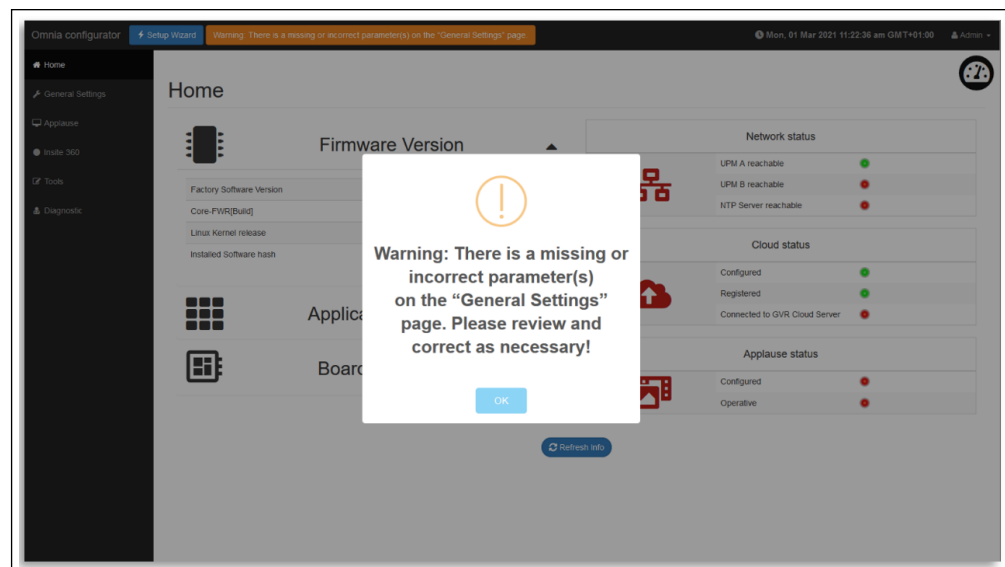
- 1 If a reboot is scheduled, a button shows the remaining time to reboot and enables the user to reboot the board immediately. The label refreshing time is 1 min.

Figure 5-78: Status with Reboot Banner



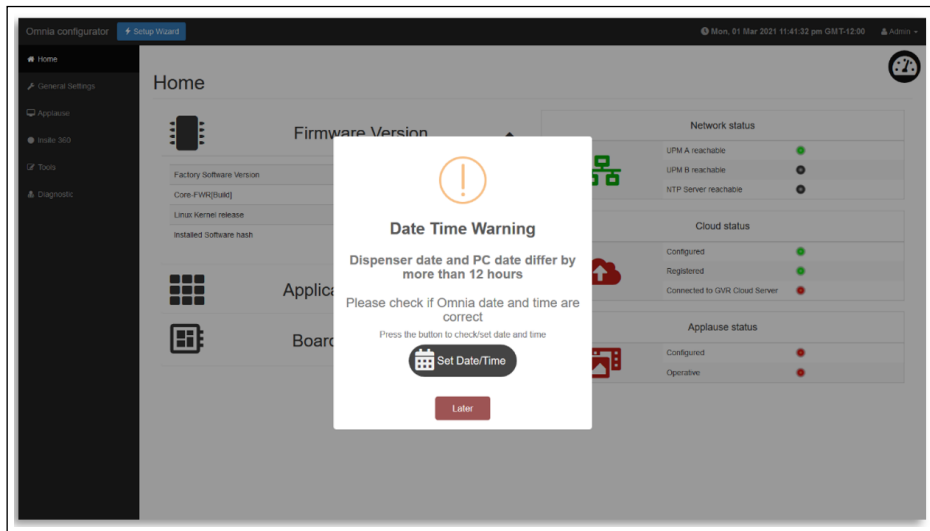
- 2 If there is something wrong in the configuration file (due to a corruption or an incorrectly configured parameter) a popup will be displayed advising the user about the problem; a related banner is displayed on top of all pages until the problem is solved.

Figure 5-79: General Settings: Warning



- At every login, the system compares the date/time on Omnia board with the local (user logged in computer) time. If the date/time information differs by more than 12 hours, a popup is displayed and a button on the popup redirects the user to the date/time configuration form. User can skip the date/time check and configure these controls later from the Tools page or by clicking the time banner on the top right of all pages.

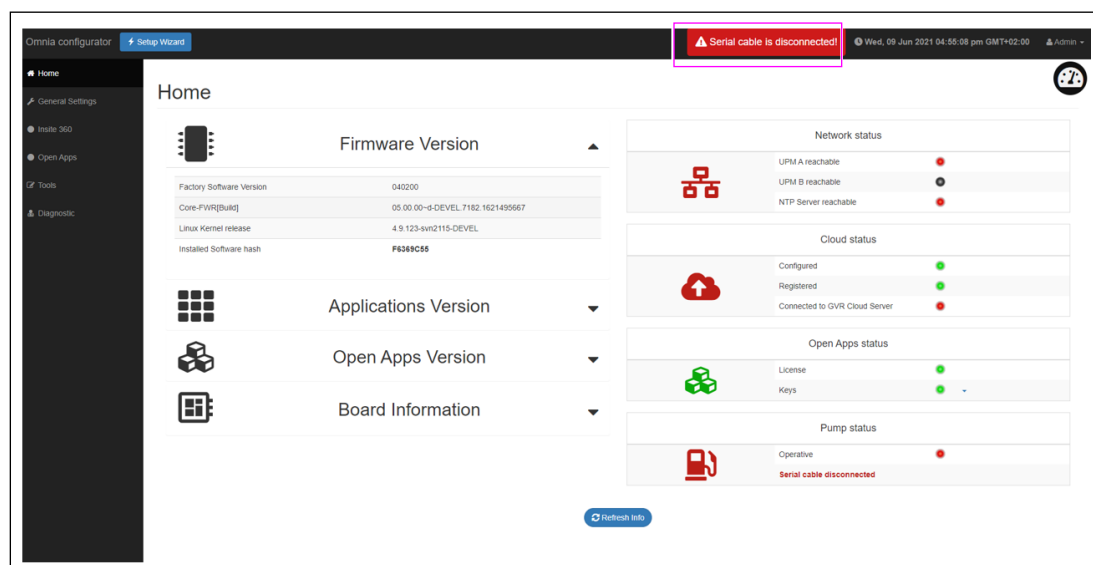
Figure 5-80: Date Time Warning



Note: The warning is displayed in case of a mismatch between local date/time and Omnia date/time. If this banner appears, check the date and time on the PC that is connected.

- If the cable to the pump is disconnected, a banner is displayed on the top of all pages.

Figure 5-81: Serial Cable Disconnected Banner

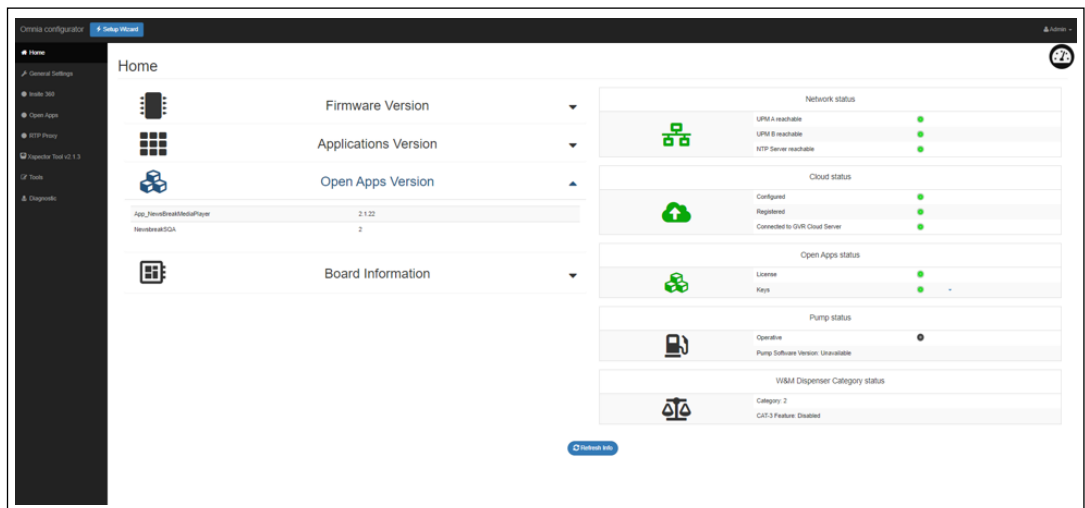


Status Icons and Virtual LEDs

The icons and virtual LEDs indicate Network, Cloud, Open Apps, and Pump Status. The meaning of the icons and definitions for status colors are described in the table “[Network – Cloud – Media – Open Apps - Pump Status](#)” on [page 5-58](#). In the case of [Figure 5-82](#) “Open Apps Status LEDs” shows a status of all Green LEDs.

Notes: 1) Open Apps Status is displayed only in the Encore Experience configuration.
2) Pump status is not displayed when the “**Select Pump connection type**” is set to “None” in the General Settings page (see [Figure 5-14](#) on [page 5-8](#)).

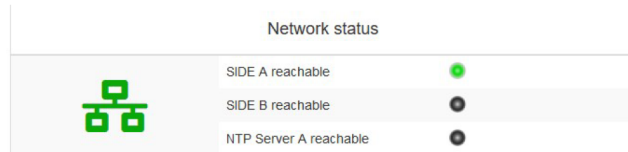
Figure 5-82: Open Apps Status LEDs



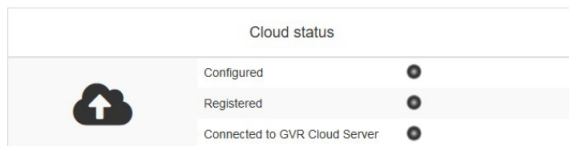
Network – Cloud – Media – Open Apps - Pump Status

Status Screen

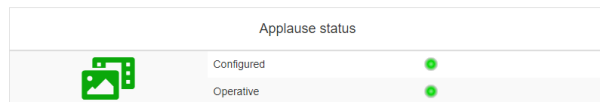
Description



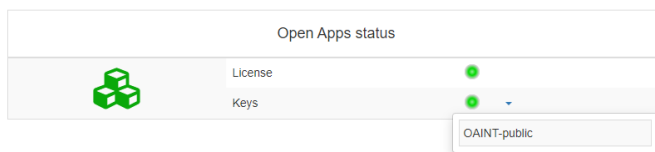
Green Network Icon = Connectivity OK.
Red Network Icon = Connectivity problems.
Black Network Icon = Programmed as a single-sided dispenser, showing only Side A status.
Green LED = Omnia can connect to SPOT/NTP Server.
Red LED = Omnia cannot connect to SPOT/NTP Server.
Black LED = (Not enabled) Configured to Disable NTP, in which Set Date and Time Manually.
 NTP (National Time Protocol) Server A reachable.
Note: Omnia must be connected to NTP Servers to sync time.



Green Cloud Icon = Cloud OK.
Red Cloud Icon = Cloud problems.
Black Cloud Icon = Cloud package not installed.
Configured: **Green LED** = Cloud application is configured.
Red LED: Cloud app not configured.
Black LED = Cloud package not installed.
Registered: **Green LED** = Omnia registered to Insite360.
Red LED: Omnia NOT registered to Insite360.
Black LED = Cloud package not installed.
Connected: **Green LED** = Omnia is able to reach Insite360 server.
Red LED: Omnia is not able to reach Insite360 server.
Black LED = Cloud package not installed.



Green Applause Icon = Media application OK.
Red Applause Icon = Media application problems.
Black Applause Icon = Media application package not installed.
Configured:
Green LED = Media application is configured (applause).
Red LED = Media application is not configured.
Black LED = Media package not installed.
Applause server reachable:
Green LED = Media application is configured (applause).
Red LED = Media application is not able to reach Applause server.
Black LED = Media package not installed.



Green Open Apps Icon = Open Apps OK.
Red Open Apps Icon = Open Apps problems.

License:
Green LED = License is active.
Red LED = License is not active.

Keys:
Green LED = At least one key is installed.
Red LED = No keys are installed.

The list of installed keys can be shown by clicking on the down-arrow right to the Keys Light.

Status Screen

Description



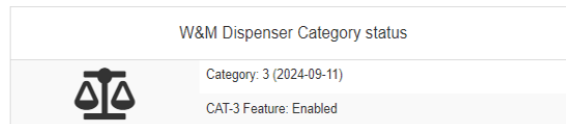
Green Pump Icon = Pump communication OK.
Yellow Pump Icon = Communication problems that can be recovered without intervention.
Red Pump Icon = Pump communication Down.



Operative:
Green LED = Pump connection OK.
Yellow LED = Connection problems that can be recovered without intervention.
Red LED = Pump communication Down.



If pump connection works, select the blue arrow to view the software version.
 In case of problems, an error message is displayed.



Weights&Measures Dispenser Category Status - Indicates the date when the dispenser was changed to Category 3.

CAT-3 Feature: Enabled - Indicates that the Category 3 feature is enabled from Insite360.



CAT-3 Feature: Disabled - Indicates that the Category 3 feature was disabled from Insite360. In this case, the dispenser is currently Category 2.

This page is intentionally left blank.

6 – Omnia Maintenance Through USB

This section guides the service technician through this feature, from the USB flash drive setup to the LED glowing sequence and its significance.

Introduction

Omnia USB Maintenance is a functionality that allows the ASC to perform the following operations using a well-formatted USB flash drive:

- Software Update/Media Content Upload
- Log Retrieval
- Configuration retrieval
- Network Restore

Requirements

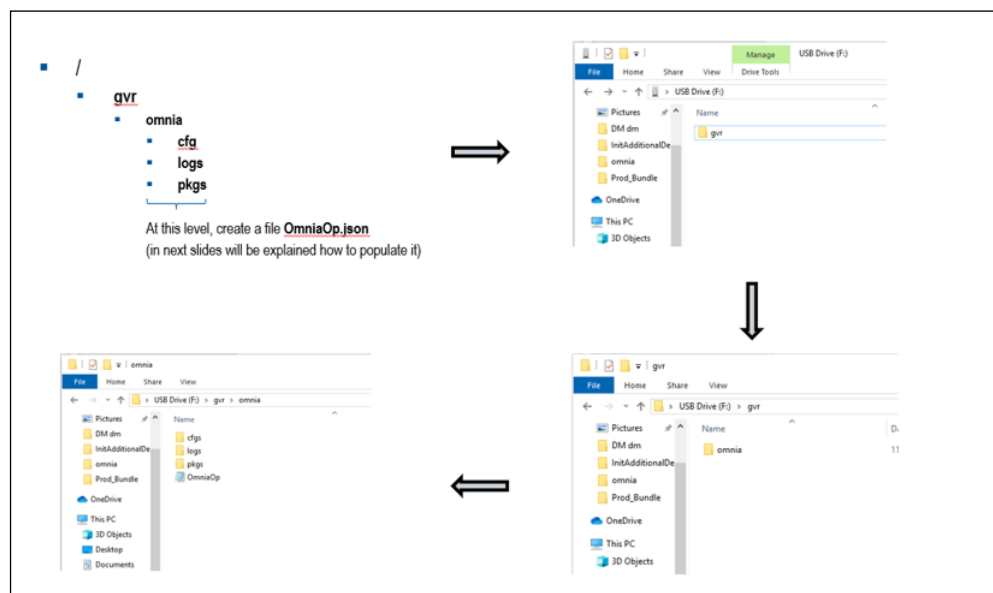
The following items are required for Setup Via USB Flash Drive:

- USB Flash Drive (hereafter referred to as “USB drive”) with at least 2GB free
- PC/Laptop
- Text Editor tool (e.g. Notepad++)

USB Drive Preparation

Plug USB drive into your PC/Laptop and create a folder tree as shown in the following figure:

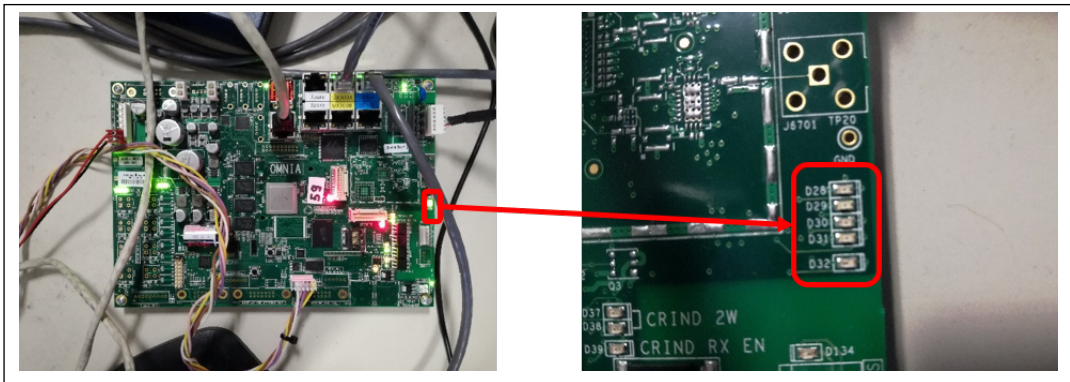
Figure 6-1: Folder Structure



LEDs Glowing Sequence

This section provides information about sequence in which the LEDs on Omnia board glow and its significance. The sequence in which LEDs glow signify different USB Maintenance operations.

Figure 6-2: LEDs (from D28 to D32)



The following are the LEDs involved:

D32 (Red)

- **Solid Red:** Indicates that maintenance operation in progress.
- **Blinking:** Indicates that Error on USB/JSON format or Error on operation.
- **Off:** Indicates that maintenance completed with No Errors.

*Note: **DO NOT REMOVE USB drive** when the status is ‘Solid Red’.*

D31 to D28 (Green)

- **Slow Blinking:** Indicates that related operation in Progress.
- **Fast Blinking:** Indicates that related operation completed with Error.
- **Solid Green:** Indicates that related operation completed with Success.

LED	Operation
D28	Reboot
D29	Retrieve Configuration/Reset Network
D30	Log Retrieval
D31	Packages Installation
D32	Maintenance In Progress/Formal Checks/Final Result

OmniaOp.JSON File Syntax

The OmniaOp.json script is a JSON syntax file that defines a sequence of maintenance operations. If the JSON syntax is not correct, the execution is not started (comments not included). The file must be populated with at least one of the operations as shown in the following figure:

Figure 6-3: Maintenance Operations

PACKAGE INSTALLATION	"Action": "InstallPackages"	Mandatory
LOG COLLECTION	"Action": "RetrieveLogs"	Mandatory
	"Logs": [<list>]	Optional List of log types to be retrieved. Values can be: 'system', 'pci', 'cloud', 'media'. If not present all types are collected.
RETRIEVE CONFIGURATION	"Action": "RetrieveConfig"	Mandatory
	"NetworkReset": True	Optional Reset of Omnia network configuration
REBOOT	"Action": "Reboot"	Mandatory
	"Time": MINUTES	Reboot time in minutes (>= 3)
NOP	"Action": "Sleep"	Mandatory
	"Time": SECONDS	Delay time in seconds

Note: The actions or parameters that are not supported are ignored.

The following figure shows the OmniaOp.json file content to perform all the operations:

Figure 6-4: OmniaOp.json File Content

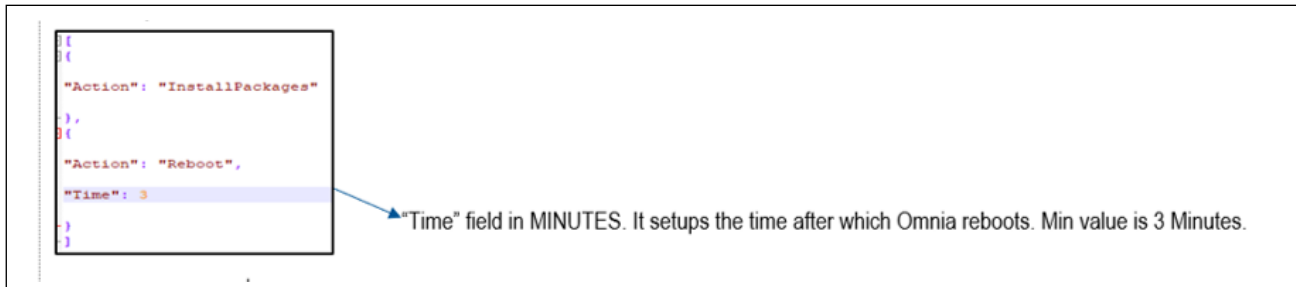
```
[
  {
    "Action": "InstallPackages"
  },
  {
    "Action": "RetrieveLogs",
    "Logs": ["system", "pci", "cloud", "media"]
  },
  {
    "Action": "RetrieveConfig",
    "NetworkReset": True
  },
  {
    "Action": "Reboot",
    "Time": MINUTES
  },
  {
    "Action": "Sleep",
    "Time": SECONDS
  }
]
```

Installing Packages

To install packages, proceed as follows:

- 1 Open **OmniaOp.json** file with a text editor (e.g. Notepad++).
- 2 Enter the time after which Omnia must reboot as shown in the following figure:

Figure 6-5: Entering Time After which Omnia Reboots



Note: The minimum value to be entered is 3 minutes.

- 3 Save the file.
- 4 Go to **gvr\omnia\pkgs** and load the packages to be uploaded (debians, archives).
- 5 Plug USB drive into Omnia board. Depending on the success or failure of the operations, LEDs start glowing as follows:
 - LED D32 goes Solid RED and LED D31 starts blinking slow.
 - LED D31 goes Solid GREEN, indicating that the operation is successfully completed.
 - LED D31 will start blinking fast, indicating that the operation failed.
 - LED D28 starts blinking slow and becomes Solid GREEN when the command is sent successfully (almost immediately).
 - LED D28 will start blinking fast, indicating that the operation failed.

If both operations are successful, LED D32 goes OFF. If one or more of the operations fails, LED D32 will start blinking together with the LED related to the failed operation.

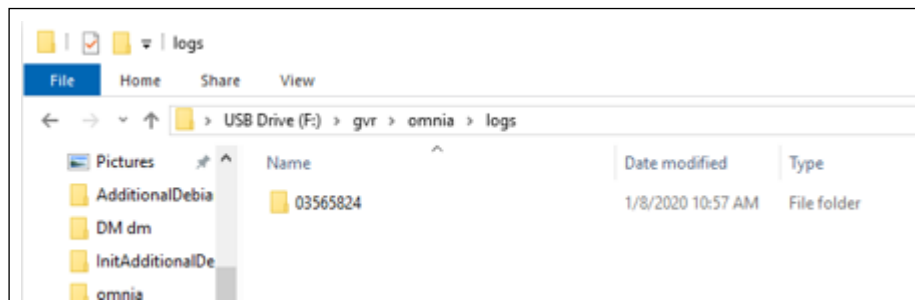
- 6 Remove the USB drive.
- 7 Omnia will reboot in the time specified in step 2.

Checking Package Installation Report on the USB Drive

To view the package installation report, proceed as follows:

- 1 Insert the USB drive used to install packages on Omnia in your PC/Laptop.
- 2 Go to **gvr\omnia\logs**. Open the folder with the name of the Omnia PPN, as shown in the following figure:

Figure 6-6: Folder Named with Omnia PPN



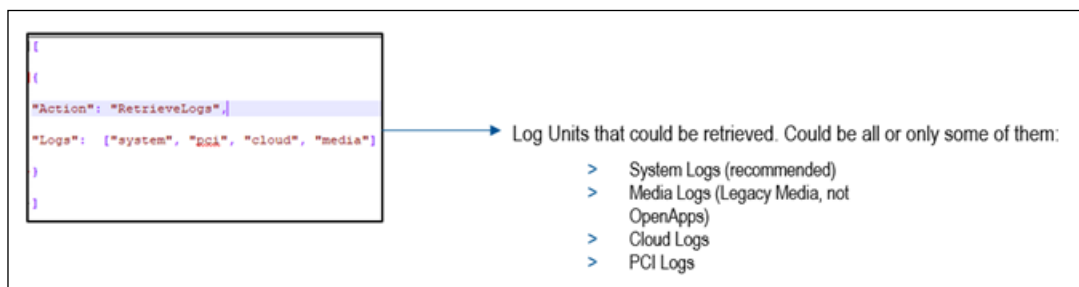
- 3 Open the file named “OmniaSession-YYYYMMDDhhmmss.txt”. The file includes information about all of the operations performed during Maintenance session (until the USB drive was attached to the Omnia board). Check that file to validate the maintenance operations performed.

Retrieving Logs

To retrieve logs, proceed as follows:

- 1 Open **OmniaOp.json** file with a Text Editor (for example, Notepad++).
- 2 Specify the log units that you want to view, as shown in the following figure:

Figure 6-7: Log Retrieval



- 3 Save the file.

- 4 Plug the USB drive into the Omnia board. Depending on the success or failure of the operation, LEDs start glowing as follows:
 - LED D32 goes Solid RED and LED D30 starts blinking slowly.
 - LED D30 goes Solid GREEN, indicating that operation is completed successfully.
 - LED D30 will start blinking fast, indicating that the operation failed.

If the operation is successful, LED D32 goes **OFF**. If the operation fails, LED D32 will start blinking together with LED D30.

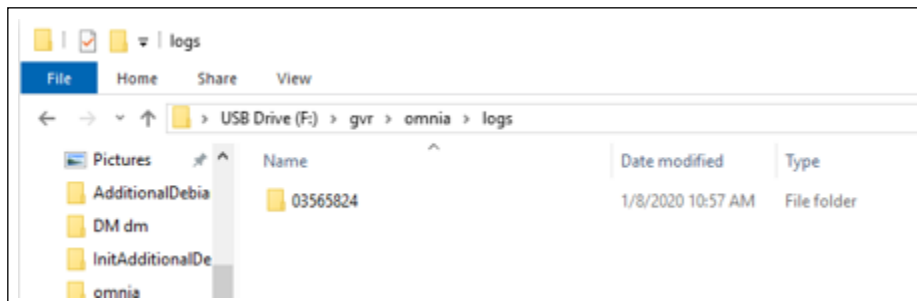
- 5 Remove the USB drive.

Log Retrieval Report and Checking Files on the USB Drive

To perform this operation, proceed as follows:

- 1 Insert the USB drive used to install packages on Omnia into your PC/Laptop.
- 2 Go to **gvr\omnia\logs**. Open the folder with the name of the Omnia PPN, as shown in the following figure:

Figure 6-8: Omnia PPN Log Folder



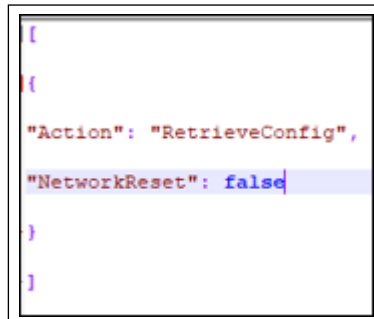
- 3 Open the file named “OmniaSession-YYYYMMDDhhmmss.txt” and all the log files retrieved in the operation zipped by Unit and Date, for example, “SYSTEM_YYYYMMDD000000_YYYYMMDD235959.zip”. The text file includes information about all the operations performed during maintenance session (until the USB is attached to Omnia).
- 4 Check the file to validate the maintenance operations performed.

Retrieving Omnia Configuration (NO Network Reset)

To retrieve Omnia configuration (NO Network Reset), proceed as follows:

- 1 Open **OmniaOp.json** file with a Text Editor (e.g. Notepad++).
- 2 Enter the information as shown in the following figure:

Figure 6-9: Omnia Configuration Retrieval - NO Network



```
{
{
  "Action": "RetrieveConfig",
  "NetworkReset": false
}
}
```

- 3 Save the file.
- 4 Plug the USB drive into the Omnia board. Depending on the success or failure of the operation, LEDs start glowing as follows:
 - LED D32 goes Solid RED, LED D29 starts blinking slowly.
 - LED D29 goes Solid GREEN, indicating that the operation is completed successfully.
 - LED D29 will start blinking fast, indicating that the operation failed.

If operation is successful, LED D32 goes OFF. If the operation fails, LED D32 will start blinking together with LED D29.

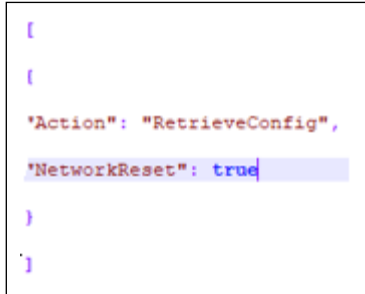
- 5 Remove the USB drive.

Retrieving the Omnia Configuration (YES Network Reset)

To retrieve the Omnia Configuration (YES Network Reset), proceed as follows:

- 1 Open the **OmniaOp.json** file with a Text Editor (e.g. Notepad++).
- 2 Enter the information as shown in the following figure.

Figure 6-10: Omnia Configuration Retrieval - YES Network



```
[
{
  'Action': "RetrieveConfig",
  'NetworkReset': true
}
```

- 3 Save the file.
- 4 Plug the USB drive into Omnia board. Depending on the success or failure of the operation, LEDs start glowing as follows:
 - LED D32 goes Solid RED, LED D29 starts blinking slowly.
 - LED D29 goes Solid GREEN, indicating that the operation is successfully completed.
 - LED D29 will start blinking fast, indicating that the operation failed.

If the operation is successful, LED D32 goes OFF. If the operation fails, the LED D32 will start blinking together with LED D29.

- 5 Remove the USB drive.

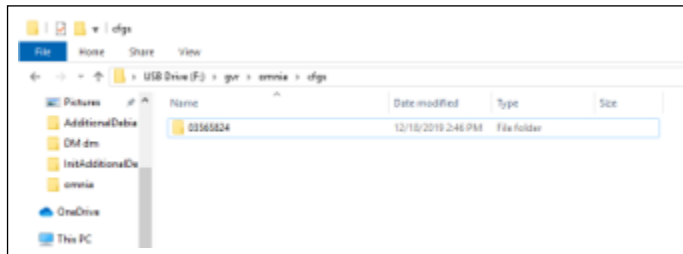
Note: After this operation, Omnia external IP address will be no longer available. Omnia WebUI will be reachable only at the Internal IP Address 172.20.100.254 by connecting an Ethernet cable from your PC/Laptop to Service Port.

Retrieving the Omnia Configuration and Checking Files on the USB Report

To perform the operation, proceed as follows:

- 1 Insert the USB drive used to install packages on Omnia in your PC/Laptop.
- 2 Go to **gvr\omnia\cfgs**. Open the folder with the name of the Omnia PPN, as shown in the following figure:

Figure 6-11: Omnia PPN Folder Structure



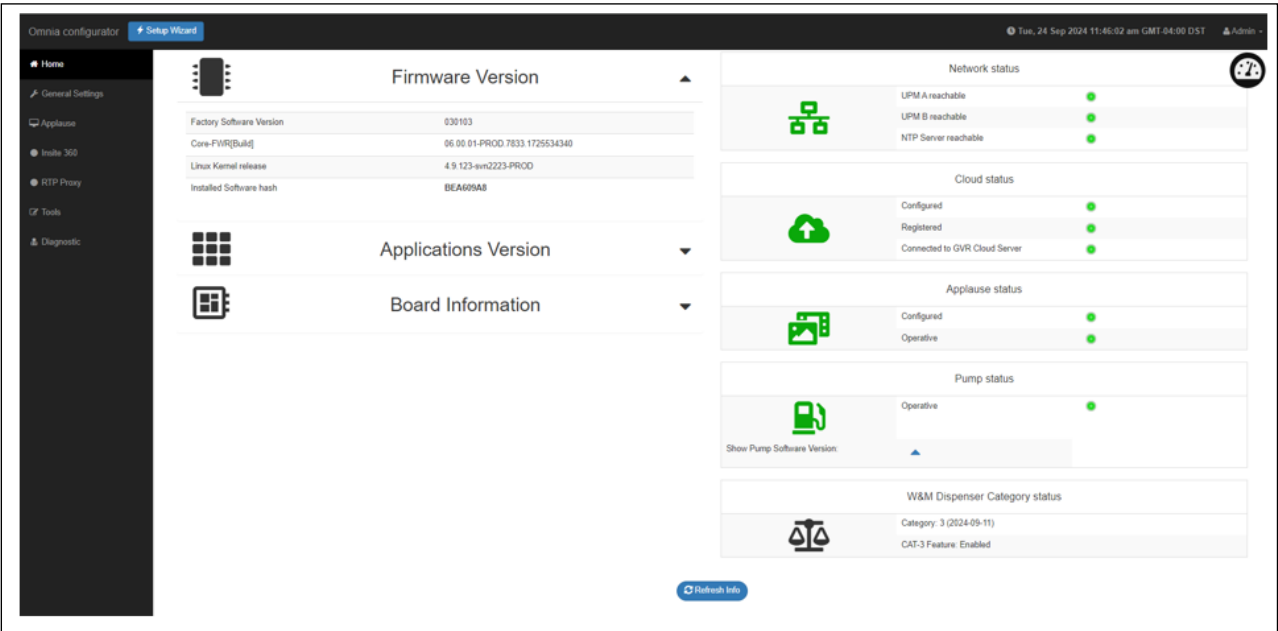
- 3 Open the file named “OmniaConfig.txt”. This text file contains all of the information about the Omnia configuration.
- 4 Open the file “OmniaSession-YYYYMMDDhhmmss.txt”. This text file includes information about operations performed during the Maintenance session (until the USB drive was attached to the Omnia).
- 5 Check the files to validate the configuration and maintenance operations performed.

This page is intentionally left blank.

7 – Troubleshooting

Open the Omnia Home page to view the status of all connections at the bottom of the page.

Figure 7-1: Omnia Home Page

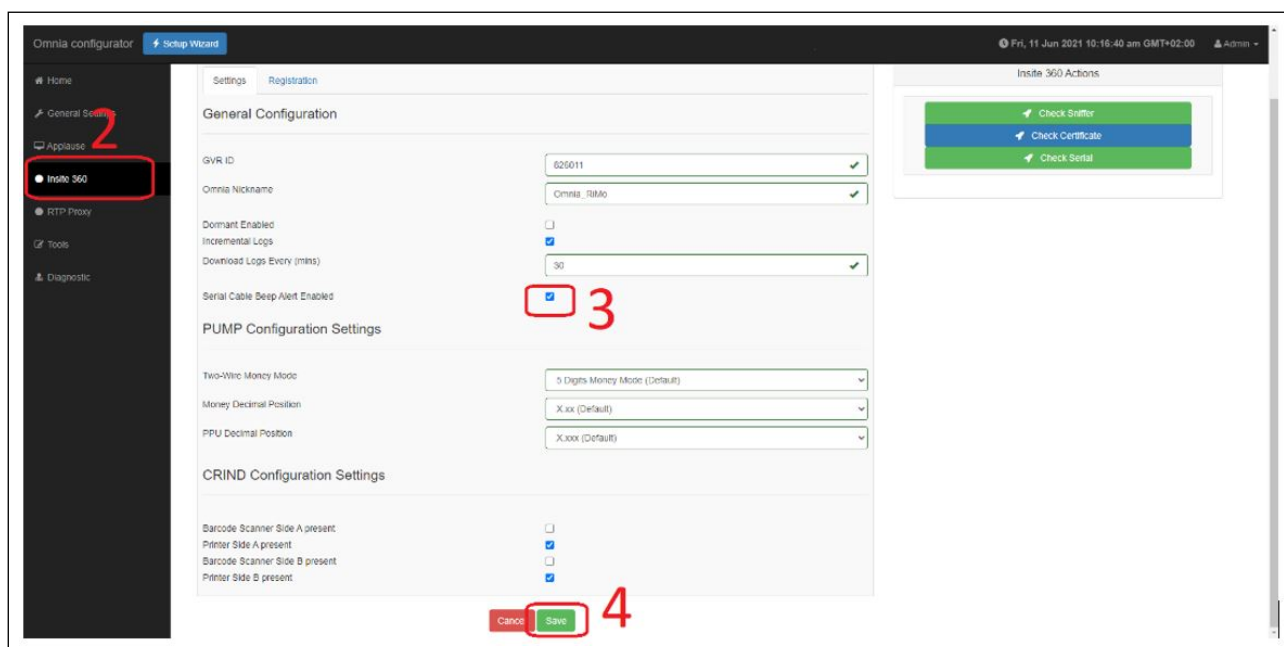


Enabling and Disabling the Beeper Alarm from the Web UI

To enable or disable the beeper alarm from the Web UI, proceed as follows:

- 1 Log in to the Web UI.
- 2 Click **Insite 360** on the left menu.
- 3 Select or clear the check box for **Serial Cable Beep Alert Enabled**.
Note: If you try to disable the alarm with the cable connected, the beep alert will re-enable automatically after approximately 5 seconds.
- 4 Click **Save**.

Figure 7-2: Enabling or Disabling the Beeper Alarm

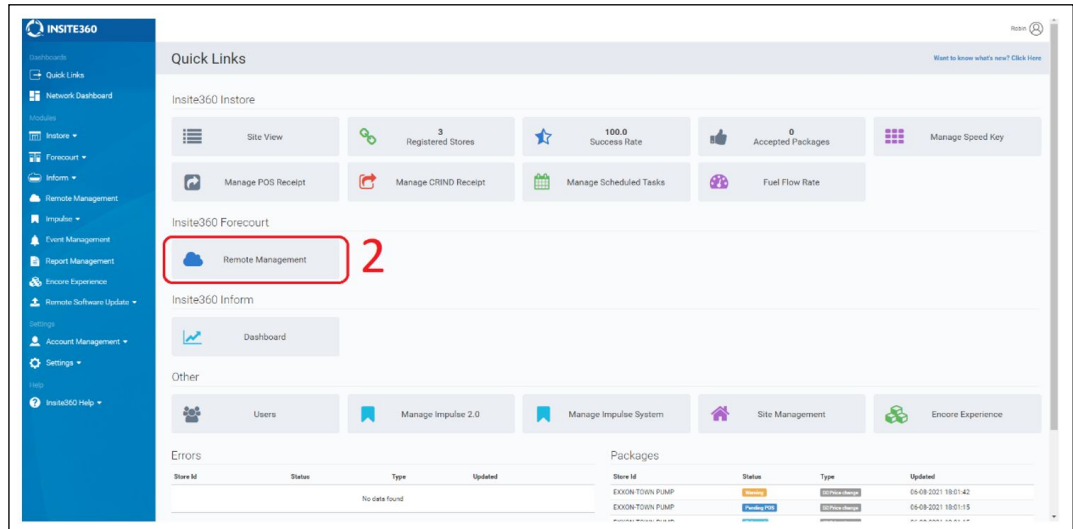


Enabling and Disabling the Beeper Alarm from Insite360

To enable or disable the beeper alarm from Insite360, proceed as follows:

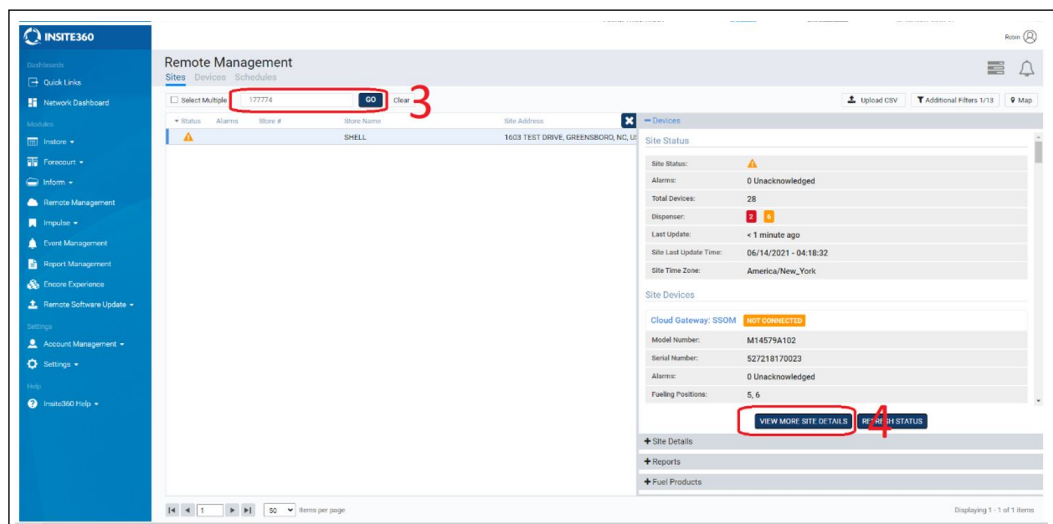
- 1 Log in to Insite360.
- 2 Click **Remote Management**.

Figure 7-3: Selecting Remote Management



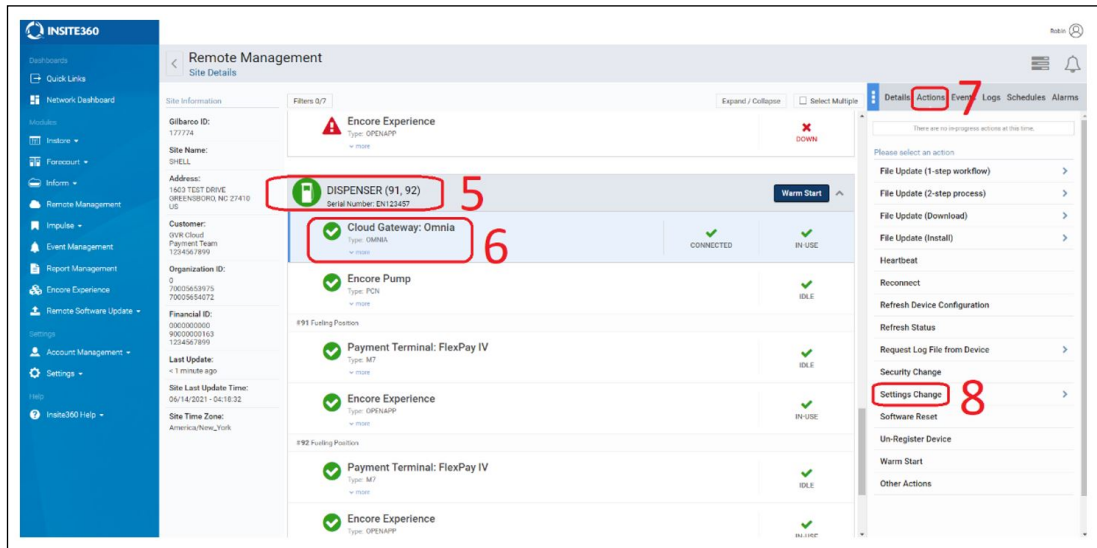
- 3 Search for the Site ID.
- 4 Click **VIEW MORE SITE DETAILS**.

Figure 7-4: Selecting Site Details



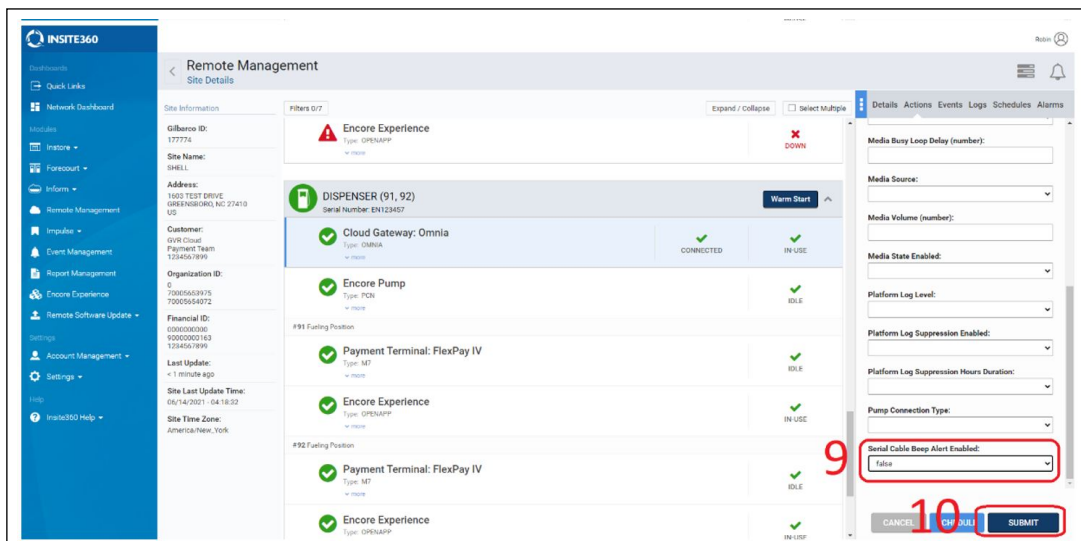
- 5 Select the correct fueling position.
- 6 Select **Cloud Gateway: Omnia**.
- 7 Click **Actions**.
- 8 Click **Settings Change**.

Figure 7-5: Selecting Actions and Changing Settings



- 9 Set Serial Cable Beep Alert Enabled to True/False.
- 10 Click **Submit**.

Figure 7-6: Setting the Serial Cable Beep Alert



11 Click **Events**.

12 Verify that the actions are correctly submitted.

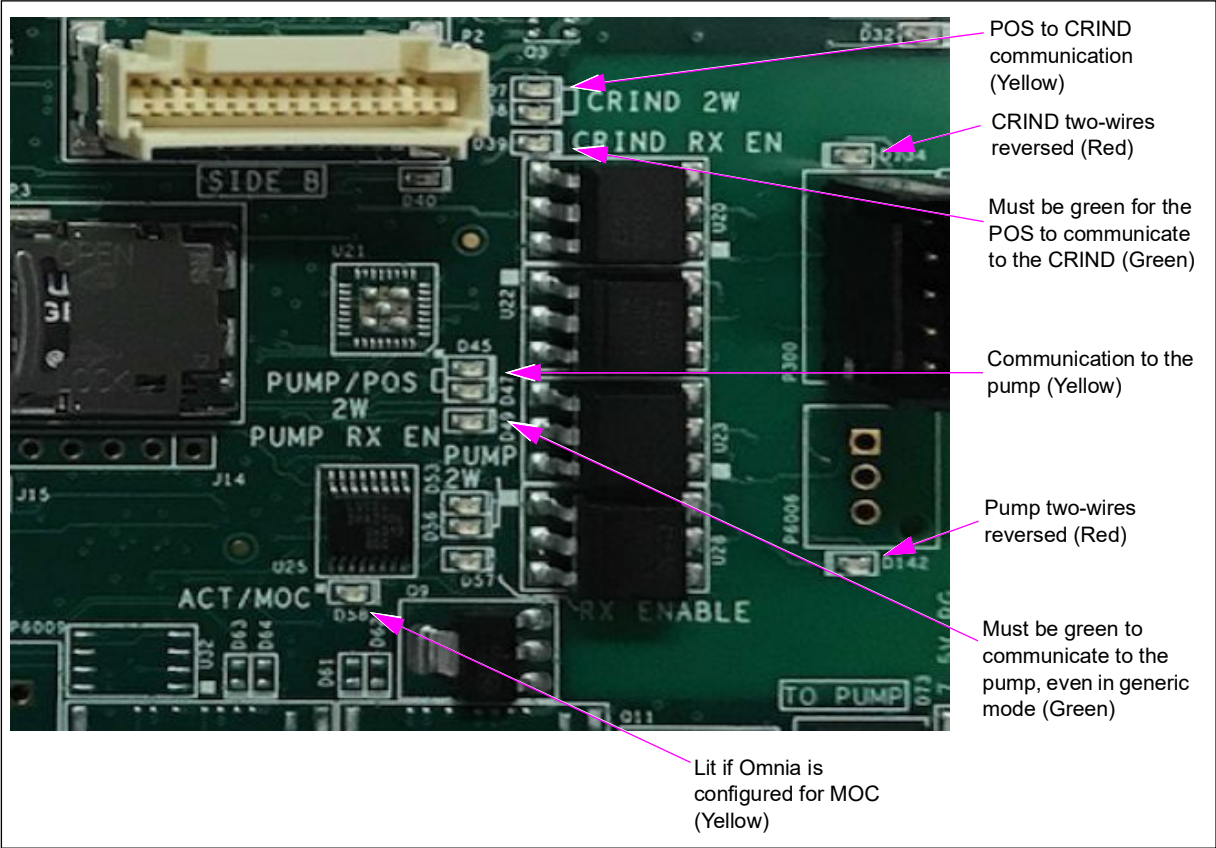
Figure 7-7: Selecting Events

The screenshot displays the Insite360 Remote Management interface. On the left is a navigation sidebar with options like Dashboard, Quick Links, Network Dashboard, Modules, Inform, Remote Management, Impulse, Event Management, Report Management, Encore Experience, Remote Software Update, Settings, Account Management, and Insite360 Help. The main area is titled 'Remote Management Site Details' and shows site information for 'Gibraltar' (ID: 177774, Site Name: SHELL). Below this is a list of components and their status: 'Encore Experience' (DOWN), 'DISPENSER (91, 92)' (CONNECTED), 'Cloud Gateway: Omnia' (CONNECTED), 'Encore Pump' (IDLE), 'Payment Terminal: FlexPay IV' (SOLE), 'Encore Experience' (IN-USE), 'Payment Terminal: FlexPay IV' (IDLE), and 'Encore Experience' (IN-USE). On the right, a 'Details' panel is open, showing a list of events. A red box highlights the 'Events' tab and a specific 'Settings Change' event with the message 'Command Result: SUCCESS'.

Connection Board Light Emitting Diodes (LEDs)

The following section of the board will help diagnose communication problems.
The Omnia intercepts POS-to-Pump communication for non-Passport POS.

Figure 7-8: Connection Board



LED		Color	Function	Behaviour
CRIND 2W	D37	Yellow	POS to CRIND communication	Not lit or solid if using CRIND over IP (CoIP) or EMV. Blinks on when POS transmits to any CRIND via two-wire.
	D38	Yellow	CRIND to POS communications	Blinks on when CRIND A or B side replies to POS via two-wire.
CRIND RX EN (D39)		Green	CRIND receiver is enabled	Green after boot cycle.
D134		Red	CRIND two-wires reversed	Lit if two-wire connection is reversed.
PUMP/POS 2W	D45	Yellow	Pump Data between Omnia and POS.	Not lit or solid if POS is Passport. Blinks on when POS transmits to any pump via 2W.
	D47	Yellow		Not lit or solid if POS is Passport. Blinks on when pump A or B side replies to POS via 2W.

LED		Color	Function	Behaviour
PUMP RX EN (D49)		Green	Enables POS-to-Pump data on Omnia.	Green after boot cycle.
Omnia to PUMP 2W	D53	Yellow	Pump Data between Omnia and Pump.	For Passport, blinks after Omnia boots and tried to talk to the pump. For any other POS, it mimics D45.
	D56	Yellow		Blinks when pump responds to Omnia (Passport) or the POS (other POS). For any other POS, it mimics D47.
D142		Red	Pump two-wires reversed	Lit if two-wire connection to the pump is reversed.
RX ENABLE (D57)		Green	Pump-to-Omnia receiver is enabled.	Lit if PUMP RX EN and CRIND RX EN Green LEDs are lit.
ACT/MOC (D58)		Yellow	MOC or Generic	Lit if MOC. Following each reboot, the ACT/MOC LED will light briefly and then, after a few seconds, returns to the state programmed in the Omnia web configuration.

Pump Serial Cable Disconnect Alarm

This section explains the Pump serial cable disconnect alarm designed to diagnose and report the disconnection of the serial cable to the pump.

Omnia has an alarm that gives an audible and visible feedback in case the serial cable to the pump is left disconnected.

The system will report a disconnected pump serial cable in case:

- Omnia is registered to Insite360
- Pump type is rtp-serial or ZModem

The system reports the disconnection of the serial cable by:

- Audible beep
- Banner on Web UI
- Event sent to Insite360

The beep alarm is a repeated sequence of 3-second beep followed by 5 second of silence.

ASC can disable the audible feedback both from the Web UI and Insite360 by setting the “Serial Cable Beep Alert Enabled” parameter to false. The default value for the parameter is true. After the cable is connected, the beeper alarm is re-enabled automatically after approximately 5 seconds.

When the beep is disabled, the banner on the Web UI and Insite360 events remains visible to alert the ASC about the wrong serial connection.

PIP3 Connections

Ensure that the loopback jumper is in place on the B side of the PIP3.

Figure 7-9: PIP3 Loopback Connector

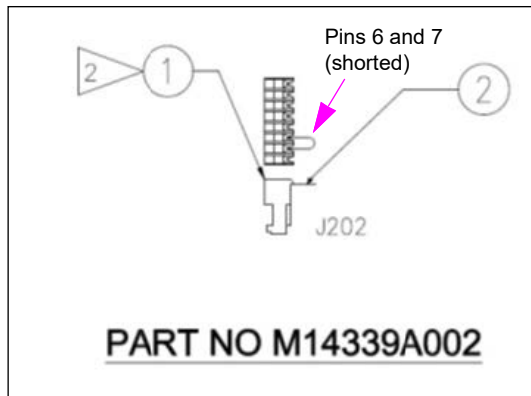
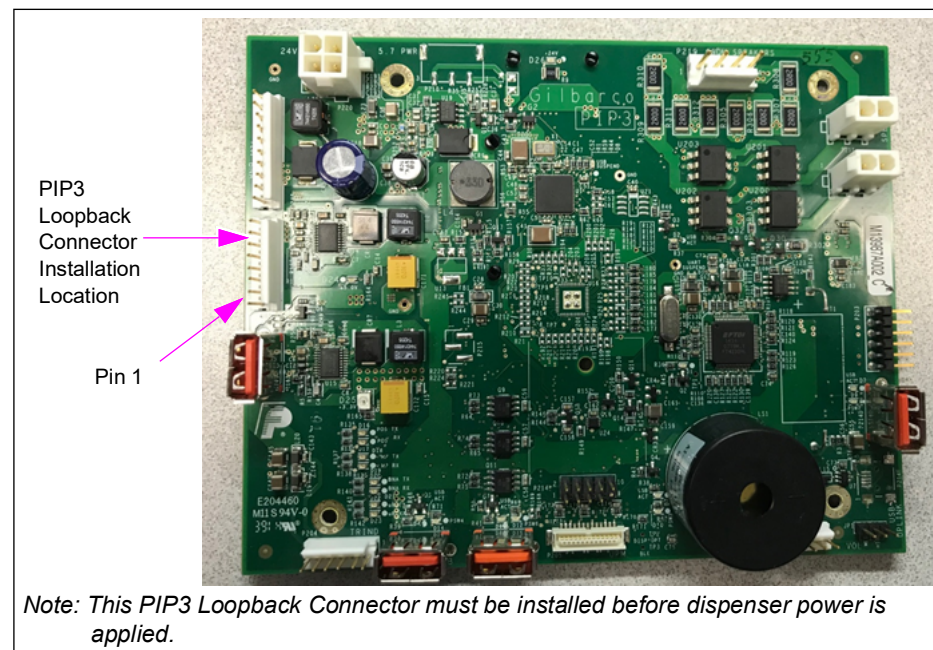


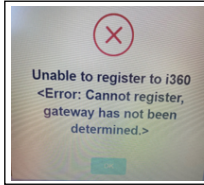
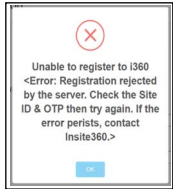
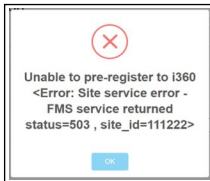
Figure 7-10: Loopback Connector Location on PIP3 (B Side Only)



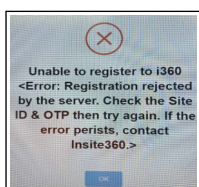
Pins	Connection Status
1-5	Open
6 and 7	Shorted <i>Note: If a M14339A002 is not available, you can use 0.1-inch jumper.</i>
8	Open

Insite360 Forecourt Dispenser Troubleshooting

Insite360 Forecourt Dispenser Troubleshooting			
Component	Symptom	Probable Cause	Steps to Resolve
Registration	The registration process has resulted in a "KO" error	- The "save configuration" process is still performing tasks in background- registration task was attempted too soon after the "save configuration" was performed. - No internet connection - Wrong SSoM configuration (duplicate IDs, IPs, wrong GVR ID, etc.)	- Click the OK button, wait for three minutes and repeat the registration process several times. - If you get the same error message at least three consecutive times, then troubleshoot based on the error message received.
	Pre-Registration KO- "EAI AGAIN" Error (see screenshot)	Duplicate IP Addresses or Local IDs	Check SSoM configuration and verify no duplicate local IDs or IP addresses.
	Pre-Registration KO- "EPROTO" ERROR	Expired Certificate	Update SSoM software to the latest approved version and attempt registration again.
1.7.10 upgrade and potential loss of communication	Lost communication to POS, maintain communication with Insite360 after updating SSoM from 1.7.10 to latest software or SSoM replacement with 3.2.4.	UPM is not programmed correctly and requires the correct default gateway: 172.16.100.254 and subnet: 255.255.255.0.	In the UPM Secure Menu (Orange screen), update the default gateway to 172.16.100.254 and subnet: 255.255.255.0.

Insite360 Forecourt Dispenser Troubleshooting			
Component	Symptom	Probable Cause	Steps to Resolve
	Pre-Registration KO	Even though you may get a successful Internet test, this could be a case where the IT department did not whitelist our URLs properly.	Run connectivity tests such as Telnet, tracer, or on-board diagnostics off SSoM/Omnia if running the latest SW.
	Pre-Registration KO- {}	Site may be blocking one of the SSoM URLs	Run connectivity tests such as Telnet, tracer, or on-board diagnostics of SSoM/Omnia if running the latest SW.
	Pre-Registration KO- "unable to find customer for device"	Provisioning problem or the wrong GVR ID was programmed in SSoM/Omnia	• Verify the correct GVR ID is programmed into the Omnia/SSoM. • Call TAC to contact provisioning team to resolve issue.
	Pre-Registration KO "Etimedout","errno"; "Etimed out"; "syscall"; "connec"	No Connection to internet or network	Verify SSoM/Omnia config, IP addresses, network rules, IP address access granted on network, etc. Use Telnet and/or TraceRT troubleshooting tools to confirm internet connectivity. If Telnet passes, possible bad SSoM/Omnia- Replace hardware.
			
	Pre-Registration "E not found"	No Connection to internet or network	Verify SSoM config, IP addresses, network rules, IP address access granted on network, etc. Use Telnet and/or TraceRT troubleshooting tools to confirm internet connectivity. If Telnet passes, possible bad SSoM/Omnia- Replace hardware.
			
			

Insite360 Forecourt Dispenser Troubleshooting			
Component	Symptom	Probable Cause	Steps to Resolve
	Registration KO- "Error: Exec Error (1)	Internal devices not communicating to SSoM/Omnia. Wrong IP addresses programmed either on the SSoM/Omnia or device itself, Physical connection to devices, or wrong SW version on CRINDs.	Check the virtual LEDs on the "Home" tab at the bottom of the page of the Omnia/SSoM Web UI (v2.1.2 and later) to see which device is not communicating with SSoM/Omnia. If all device LEDs are green, then it could be a network connectivity issue. Ensure that all Gilbarco Host names are whitelisted (transfer.gilbarco.com, registration.gilbarco.com, and device.gilbarco.com). Ensure that the DNS settings are correct. Use Telnet and/or TraceRT troubleshooting tools to confirm internet connectivity. If Telnet passes, possible bad SSoM/Omnia. Replace hardware.
	Registration error "Cannot update registration information. Contact support-Registration cannot be completed. Try unregistering and register back again"	Duplicate IP Addresses, Local IDs or fueling positions	Check SSoM/Omnia configuration and verify no duplicated local IDs, IP addresses or fueling positions on the site.
	Registration KO- "Code", "ENOTFOUND", "errno", "ENOTFOUND", "syscall", "get add	Site internet connectivity issue	Check jumper position J3 on DCM2.x based on connection type (BRCM2 vs CAT5) P304 port. Ensure that the URLs are whitelisted properly. Use network diagnostic tools on latest version of SSoM or Omnia. Use Telnet and/or TraceRT troubleshooting tools to confirm internet connectivity. If Telnet passes, possible bad SSoM/Omnia. Replace hardware.
	Pre-Registration KO- "System error: contact application support team"	Incorrect SMS setup of site, possible issue with GEO Codes (site coordinates Log/Lat)	Call TAC to escalate to provisioning team to resolve issue.
	Pre-Registration KO- Device type was not found in SMS- error=get_phantom_device_from_fms. Unable to find phantom serial for the device_type=SSOM and site Id=xxxxxx+null-null	Site is not setup properly in SMS	Call TAC to escalate to provisioning team to resolve issue.
	Dispenser was successfully registered but it is not showing on Portal	Dispenser registered to wrong site, check GVR ID Delay in devices populating to portal dashbd - view site devices from the Device tab, if not showing check site details and GVR ID used to register Possible registration server glitch	Call TAC.
	Registration Failure: "Duplicate Record"	I360 Database Issue	Call TAC to escalate to Gilbarco Cloud engineering.



Insite360 Forecourt Dispenser Troubleshooting			
Component	Symptom	Probable Cause	Steps to Resolve
	After registering SSoM or Omnia to I360 successfully, all the devices go into a "not connected" state on IS360 (orange status)	Omnia- Either date and time is programmed wrong or device server is not whitelisted. SSoM device server not whitelisted	Check date and time of Omnia. Ensure that the device.gilbarco.com is whitelisted in the site's network router.
	Omnia registration error "Org.freesdesktop.Dbus.error.noreply"	Database error	Reload Omnia software.
De-Registration	De-Registration Fails from the SSoM WebApp with message "Error in de-registration: ECONNRESET"	Cloud connectivity issues	Resolve any site connectivity issues and try again; call Gilbarco Helpdesk to deregister device if issue is related to hardware problems.
DCM2.2	CRIND screen stuck in "starting application" mode		Check the connections for P303 on DCM2.2 and P1109 on the PCN. Verify the jumper setting at J6 (it should be set to position B-45mA).
SSoM UI	Can't get logged into the SSoM Application	Wrong IP address and port typed (:61084) in browser Static IP address of laptop wrong IP address of SSoM has changed or was configured wrong No power to SSoM or SSoM locked-up Defective cable Old version of web browser SSoM Application Failure	Ensure that the IP address is entered properly and port ID (:61084) for SSoM is included at the end of the address (i.e., 172.16.100.254:61084). Ensure the laptop IP address is on the same IP scheme as the SSoM; i.e., set laptop IP address to 172.16.100.15 if SSoM IP is set to 172.16.100.254. To reset SSoM back to factory default (172.16.100.254), see Appendix B "Reset Network Configuration to Factory Values". Observe LEDs; the ACT LED on CCP should be blinking or solid on. Try another CAT5 cable (ensure that it is seated properly in both the DCM2.x and laptop). Use latest version of web browser; Chrome is preferred.
SSoM Registration	"Check Internet" failed test	Older versions of SSoM software reached out to Google (8.8.8.8 IP) for this test, it is possible that Google is being blocked by firewall- Try to register device and troubleshoot according to the error message presented by registration failure Homeplug jumper missing on DCM2.1 (if site is using BRCM2) SSoM configured improperly Router rules and firewalls not allowing network traffic to internet No power to DCM or there is a communication cable connection issue on units using FlexPay Connect v1 (DCM to DCM2.1 connection)	For FlexPay Connect v2, verify that the HomePlug jumper is installed. Verify SSoM configuration (static IP, gateway and DNS) is correct; confirm with site IT personnel. Routers (firewall, routing rules, physical connections, etc.) are configured properly and IT personnel has verified settings. Internet Service Provider is online and active. For FlexPay Connect v1 sites; verify that the DCM has power and is connected properly to the DCM2 via CAT5 cable to port P304A. If it is connected and still no internet, power cycle DCM and/or dispenser and retest. Use network diagnostic tools on latest version of SSoM or Omnia. Use Telnet and/or TraceRT troubleshooting tools to confirm internet connectivity. If Telnet passes, possible bad SSoM/Omnia. Replace hardware.

Insite360 Forecourt Dispenser Troubleshooting			
Component	Symptom	Probable Cause	Steps to Resolve
zModem	"Check zModem" test failed on SSoM UI	zModem cable (defective, not seated properly, not connected) PCN software doesn't meet minimum requirements 3.3.19 Bad PCN or serial port.	Ensure the zModem cable is properly connected to the CCP (P315) and on the PCN P1111. Try new zModem cable. Update PCN software (meets minimum requirements). <i>Note: If you service the PCN and the zModem cable is removed, ensure that you reconnect zModem cable or else many Remote Management features will not work. This will include replacing the PCN or using the laptop port (P1111) for pulling logs or downloading software, etc.</i>
SSoM/Omnia	All SSoMs unknown/not connected in Cloud	Site's Internet Service Provider offline Recent changes to firewall rules and settings BRCM2 or site router Issue Direct Ethernet switch or router issue Certificate within SSoM application expired If this occurs immediately after registration check date and time on Omnia UI	Check access to internet from other devices at the site. Check functionality of BRCM2 and system routers and ensure connections are good. If site has direct Ethernet to dispensers, then check main network switch or router. If this occurs immediately after registration, check date and time on Omnia UI. Escalate to PSS if certificate expiration is suspected.
Remote RKL Failure	KBPK Key in TR34 Cannot Be Stored: AP (0x6c)	Bad UPM Replace UPM	
Contactless Card Reader	Contactless Card Reader (UX410) not functioning (DCM2.2 only)		Verify that the VLAN Jumper (J5) is installed on the FlexPay II unit only and card readers are connected to the proper RJ45 port.
PCN	The Check Serial Interface test fails from the SSoM UI or the PCN is not responding to Insite360 commands.		Verify ZMODEM cable is connected at P315 and on P1111 at the PCN (excludes E300 and The Advantage Series).

Omnia Encore Dispenser Troubleshooting

Omnia Encore Dispenser Troubleshooting			
Component	Symptom	Probable Cause	Steps to Resolve
Applause Media System (working prior to Omnia installation)	Applause Media System does not display on any units after installing the Omnia dispenser.	- Applause Media System Site Server IP address does not match the new IP scheme at dispensers. - Applause Site Server IP addresses or media configuration set incorrectly in the CRIND programming router configuration. - Applause Media not turned ON in Omnia Media programming.	1 Check the following Applause setting on the Media page in the Omnia programming: • External IP addresses for CRINDs • Applause Server IP in Omnia config • Applause Site Server and routers 2 Power cycle the Applause Media System Site Server. 3 Check the side jumper on PIP 3.
Omnia Applause Media configuration is not set properly	Applause Media System is not displayed at a specific fueling position after installing Omnia dispenser.	- Media configuration (M7) set incorrectly in the CRIND programming. - Terminal ID and Pump Monitor ID set incorrectly in the Omnia configuration. - CRIND IP address and gateway for Applause Media System Site Server is set incorrectly.	1 Check the following Applause setting on the Media page in the Omnia programming: • In the Media Configuration page, verify that Applause is turned ON. External IP addresses for CRINDs. • Applause Server IP in Omnia config • Applause Site Server, and routers 2 Power cycle the Applause Media System Site Server. 3 Check the side jumper on PIP3. 4 Verify that Omnia connection module is selected in the UPM. 5 Run Media Utility test from the Media Configuration page.
	Applause Media System does not display after replacing the UPM.	IP address is not auto-set properly by the CRIND.	1 Check UPM software version. 2 Check that Communication module is set to Omnia. 3 Check CRIND configuration.
Omnia FlexPay IV unit	During startup of an Omnia FlexPay IV unit, the communication to the back room halts. A message "Starting Application" may appear on the CRIND Screen. Seems as if the download from the POS never started (or halted early on).	The jumper is not installed properly on the Side B PIP.	1 With the Omnia PIP, verify that the jumper is installed on the B Side PIP. 2 On PIP3 when used with Omnia, verify the "Loopback Connector" is installed on Side B PIP3 at the P202 Connector (The loopback connector comes in the Omnia Kit). 3 In MOC setting, "Start Application" could mean that the CRIND is not communicating with the Pump. Check P1109 on PCN and P303 on Omnia.
Omnia through Onboard web page	- Cannot update software on Omnia through Onboard web page. - Omnia time and date is lost (This could become a problem parsing logs to investigate problems).	Battery jumper on Omnia PCB not installed properly.	1 The battery jumper on the Omnia PCB should be installed from the factory on crates and kits in the J3 (pins 17 and 18 position - top jumper in the J3 bank). 2 Set date and time on the board.

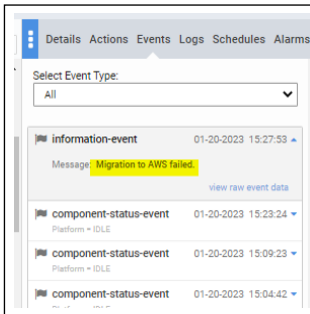
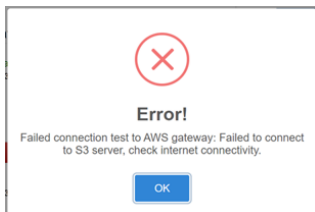
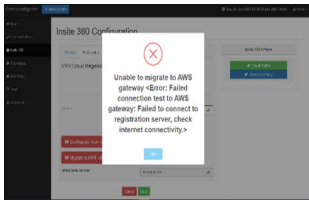
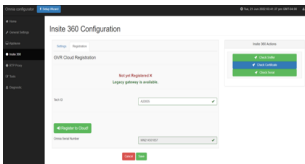
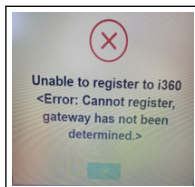
Omnia Encore Dispenser Troubleshooting			
Component	Symptom	Probable Cause	Steps to Resolve
POS on CRIND	No communication to the POS (CRIND or pump).	The wrong two-wire cable may have been used in the installation. The unit or kit is shipped with three two-wire cables (one for MOC and one for Generic, and an additional cable if there is no DCM3 to intercept the connection).	1 Verify that the correct cable was used. M11961A003 is for MOC; M11961A004 is used for Generic. In environments without a DCM3, add the M02993A005 cable to close the connection. 2 Verify the web app configuration for MOC and GENERIC setting.
	On sites with Commander POS, the POS application download freezes (or halts) midway through the download.	CRIND not set to 9600 Baud Rate at the UPM, and at the Commander POS.	Verify 9600 Baud Rate is set at the Commander and in the UPM.
Card Reader on CRIND	Card Reader is in an Error State (either the text "Card Reader Error" is displayed on the CRIND Screen, or a red "X" is displayed over the card reader) after setting the Omnia parameter in the UPM's Device Configuration "Communication Module" setting.	Card Reader IP settings are incorrect.	1 The card reader must be set to its default IP setting 172.16.100.2 (for both Side A and B) when Omnia is configured in the UPM. This is accomplished by assigning the default IP address in the green screen of the UPM (press the button on the UX300 Card Reader). <i>Note: For Omnia, the UPMs are automatically set to 172.20.100.1/3, and the Card Readers remain at their factory Default Setting of 172.16.100.2 (both sides). The different IP Scheme is possible because of the Omnia's VLAN routing and dedicated ports.</i>
	Can't set card reader to default setting after Omnia installed. Usually occurs on Side B.	Can't reach card reader because proper sequence was not followed during kit upgrade.	1 Connect Side B card reader in the yellow UX300B port on the Omnia board. 2 In the Device Config menu, confirm that the Omnia parameter is set. 3 Reboot after Omnia settings. 4 Select <2> Device Configuration. 5 Select <2> VFI Device Configuration. 6 Press the button on the UX300 card reader and assign the default IP address 172.16.100.2. 7 Exit. The UPM reboots, and then the UPM updates the card reader. Wait until this process completes.
Card Reader Errors	Display shows a card with a red "X" through it and one of the following error codes:		
		CR 00	CR not Configured.
			1 Set the UPM programming Card Reader to VFI Manual. 2 Power off, and then power on the unit.

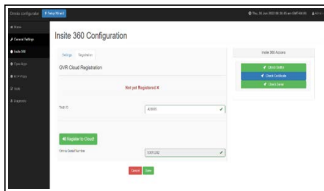
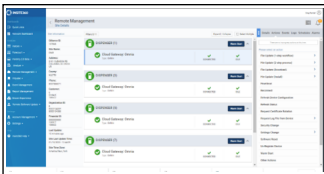
Omnia Encore Dispenser Troubleshooting			
Component	Symptom	Probable Cause	Steps to Resolve
	CR 02	CR disconnected.	1 Power off, power on unit. 2 Check the cable. 3 Assign an IP address to the Card Reader. a From the UPM, in the System Menu, press <2> Device Configuration . b In the Device Config menu, press <2> VFI Device Configuration . c In the VFI Device Config menu, press <1> VFI Device IP Assignment and follow the prompts.
	CR 03	CR tampered.	Lost keys. Replace CR.
	CR 05	CR dismounted.	Perform the activation procedure.
	CR 08	CR driver error.	Replace CR.
	After upgrading UPMs to version xxx or later and installing the Omnia board, the side A card reader goes through its upgrade and works, but the side B card reader does not go through its upgrade and is inoperative.	Proper sequence was not followed during kit upgrade.	To recover the side B card reader: 1 Connect side B card reader in the right Omnia port. 2 Check if Omnia parameter is set into device config menu. 3 Reboot after making Omnia settings. 4 Select <2> Device Configuration . 5 Select <2> VFI device configuration . 6 Go through the card reader button push process. It should discover the card reader and assign the card reader to 172.16.100.2. 7 Exit and allow the UPM to reboot. On rebooting, the UPM should begin updating the card reader. ALLOW THIS PROCESS TO COMPLETE.
	Card reader errors or UPMs not communicating properly. Sales go into POS from the wrong side. Various unusual symptoms with UPMs and card readers.	CAT5 cable connection not correct.	1 Verify the CAT5 cables on the Omnia PCB. 2 Verify that the RJ45 ports on Omnia are dedicated and color coded due to VLAN. 3 Verify that top row is Side A, and bottom row is Side B. UPMs use the blue CAT5 cables and UX300s use yellow CAT5 cables. 4 Verify proper CAT5 connections. 5 Ensure that the CRIND IDs are set correctly.

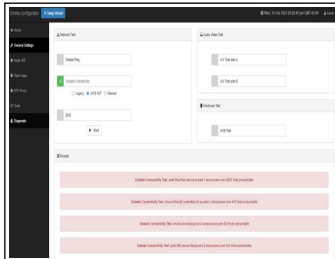
Omnia Encore Dispenser Troubleshooting			
Component	Symptom	Probable Cause	Steps to Resolve
Insite360 Units	Cannot register the unit to GVR Cloud, but the Internet connectivity passes test.	Firewall blockers within the site network.	1 Check for firewall blockers within the site's network (may require Site IT assistance). 2 Verify all 3 Gilbarco URLs can be hit from the back room. 3 To register Omnia to Insite360 Forecourt, the site must allow access to the 3 URLs (device.gilbarco.com, registration.gilbarco.com, and transfer.gilbarco.com) for registration to occur. Ensure that these websites are white-listed. 4 Verify proper site connectivity in the back room (router configurations, etc.). <i>Note: You can connect your laptop to the BRCM2 or BRCM2.1 or connect at Service Port on Omnia PCB. Ensure to make proper settings to your laptop. For example, the Default Gateway to back room, etc. must be set.</i>
	Internet connectivity test does not pass.	Site connectivity issues.	1 Check high-speed connection to the back room. 2 If the connectivity LEDs appear correct, double-check the gateway settings and primary DNS. 3 Move laptop to back room switch or to a free BRCM or BRCM2 port and try to connect to the Internet (example Google). 4 If everything fails, ensure that the site is allowing the required external Internet connections.
Pump Control Node	PCN not reachable on Insite360 Forecourt. Cannot remotely perform PCN resets, pull logs, etc. from the pump portion of Insite360.	ZMODEM connection improper.	Verify the ZMODEM connection from Omnia P315 to PCN Laptop Port P1111. This cable must be connected and reconnected after any service is performed on the unit.
Omnia PCB	Omnia PCB not able to register through Secure Zone Router.	Firewall access.	Verify that the MAC addresses of each device have been provided to the site IT personnel to allow them through the firewall.
	Can't Reach the Omnia programming web page from the BRCM 2.X (Back Room).		Use 10.5.55.71:3000 to get to the Omnia Configuration Page (72, 73, 74, etc.) from the BRCM2 or BRCM2.1. <i>Note: The External IP Address could be customer specified, and not the recommended default 10.5.55.XX value. Two-wire Over IP must be enabled in Omnia General settings page.</i>
Card Reader	Cannot ping the card reader IP address from service port on the Omnia PCB.	Not able to ping the UX300 Card Readers at 172.16.100.2 due to VLAN Omnia Segmenting.	The UX300 Card Readers cannot be pinged at 172.16.100.2 due to VLAN Omnia Segmenting. The VLAN/Laptop Static IP setting along with the default UX300 does not allow to ping the UX300s. We can ping the UPM CRIND IP addresses 172.20.100.1/3 from the service port.

Omnia Encore Dispenser Troubleshooting			
Component	Symptom	Probable Cause	Steps to Resolve
Remote Management	Cannot warm start dispenser remotely.	ZMODEM cable connection.	Check if the ZMODEM cable is properly connected.
	Omnia date and time is not automatically updated via Cloud.	Firewall access.	1 Check for firewall blockers within the site's network (may require Site IT assistance). 2 Verify that all of the NTP URLs can be reached from the back room: • 0.debian.pool.ntp.org • 1.debian.pool.ntp.org • 2.debian.pool.ntp.org • 3.debian.pool.ntp.org
	Alarms for remote door sensors are not visible in Insite360.	1 ZMODEM cable connection. 2 Pump connection type set incorrectly.	1 Ensure that the ZMODEM cable is properly connected. 2 From Insite360 Configuration page, ensure that Pump Serial Interface is set to RTP - Serial.

AWS IoT Registration and Migration Troubleshooting

AWS IoT Registration and Migration Troubleshooting			
Component	Symptom	Probable Cause	Steps to Resolve
Migration From Insite360	Failed to migrate after migration attempt	Navigate to the Events Tab 	No URLs or improperly whitelisted AWS URLs, or not pre-registered (Pre-registration is performed by Gilbarco).
Migration from WebUI (Omnia or SSoM)	Failed to migrate after migration attempt	 	Failure due to AWS whitelisting issue, but could be network connectivity if the device is not currently connected to Legacy Gateway (Not connected state on I360 dashboard). Not pre-registered by Gilbarco could also apply.
Registration from Omnia/SSoM WebUI	AWS Registration failure (not available)	 	Due to no URLs or whitelisting issue or connectivity issue (from Omnia/SSoM UI) If the message on the Insite360 Registration page shows "Legacy Gateway is available" or "No Gateway available" then there is a AWS URL issue or connectivity issue. Test connectivity by running ping test on the Diagnostic Page. Check with site's IT dept to confirm URLs are in place and set properly.

AWS IoT Registration and Migration Troubleshooting			
Component	Symptom	Probable Cause	Steps to Resolve
Registration from Omnia/SSoM WebUI	Registration failure (From Omnia/SSoM UI) AWS Gateway is available, but fails to register.		Due to provisioning issue, wrong GVR ID used, or OTP entered incorrectly (capital letters must be used). Ensure that the Omnia/SSoM serial number prefix is capitalized and contains no spaces when entering into the ASC App. Verify that One Time Password is entered properly (ensure Caps Lock key is not on). Get another OTP, and verify that site was provisioned properly (Gilbarco must confirm this; check the Site Management to verify that site is in I360; verify provisioning via test links; verify GVR ID). Finally, verify that the GVR ID was entered correctly in WebUI.
Registration from Omnia/SSoM WebUI	Registration to AWS is not available (no Gateway available message option)		Due to wrong Omnia/SSoM Software, Registration Page message shows "Not yet registered", AWS compatible SW is not loaded. Install the Omnia 05.06 or SSoM 4.5.0 or higher to gain access to the AWS servers.
Registration from Omnia/SSoM WebUI	Registration failure.	• Message returns "Device already registered in the Cloud". • Gilbarco did not remove old device from AWS IoT dashboard in I360. • Duplicate fueling positions are detected.	De-register the device from Insite360 and try again. Also, check if using the same FP of another device that is already registered. Verify using the correct GVR ID.
Registration from Omnia/SSoM WebUI	Registering in Dormant Mode does not show any devices besides Omnia.		Disable the dormant mode, and then re-enable it after the device is updated on the dashboard.
Failure to register from AWS IoT Gateway.	"Unable to register to i360. Registration rejected by server" message is displayed.	Dispenser de-registration process must occur at both the dispenser and Insite360. De-register action at the dispenser only removes the communication certificates.	Contact Gilbarco TAC to de-register the dispenser on Insite360. Wrong GVR ID - Ensure that the correct GVR ID is being used; remove the old GVR ID, re-enter and then save configuration, and try to register again. OTP wrong - OTP entered incorrectly, Retry OTP at least 3 times, get new OTP, and ensure that the prefix letters in serial are in all caps when entering in the OTP tool. If device was previously registered to AWS - Contact Gilbarco to de-register the device from Insite360. Site Provisioning is not complete - Contact Gilbarco and request to check the Provisioning status.

AWS IoT Registration and Migration Troubleshooting			
Component	Symptom	Probable Cause	Steps to Resolve
WebUI	During the software install/ AWS Migration, it was found that after the SW updates, the WebUI connectivity LED was showing RED indicating no connectivity to the I360 Portal. The LED should be green when unit is properly connected. After investigation, it was found that I360 was in fact connected even though LED status was Red.	The LED is labeled "Connected to GVR Cloud Server"	Refresh the browser connected to WebUI. If problem persists, restart the Omnia Device (Initiate reboot through the Tools Page of the WebUI)
WebUI	Cannot connect to Device WebUI with laptop browser.	-	Make sure Laptop is set to proper IP Scheme Clear cache on laptop Switch to a different browser (Problems have been seen using Microsoft Edge), Try Chrome
I360 Portal	I360 portal shows device not connected when device is connected. WebUI was showing Green LED Status, yet site was showing not connected on the I360 Portal.	-	Perform a "refresh status" or "refresh device config" command on the Actions Tab on the device to re-sync Device to I360 Refresh Status - This command requests immediate current status of each device/component Refresh Device Configuration - This command requests full configuration of each device and component (i.e. SW Version, Programming, etc.)
Software Downloads via I360	Cannot download software to device (or any resource files)	-	Potential Customer IT Issue - URL whitelisting issue or Network configuration.
Log Pull (Uploads) via I360	Unable to pull logs (uploads) from devices. WebUI diagnostics pass.	-	Potential Customer IT Issue - URL whitelisting issue or Network configuration. If connected to AWS, the time of the Omnia must be within 10 mins of site time; if not, it cannot retrieve logs. Ensure that the Omnia has access to NTP servers to keep the time accurate.
Diagnostics	General Migration and First Time Registrations Failures		Verify Device Configuration and run Diagnostics Test.

De-Registration from AWS IoT Gateway

De-Registration from the AWS IoT Gateway is a two-step process:

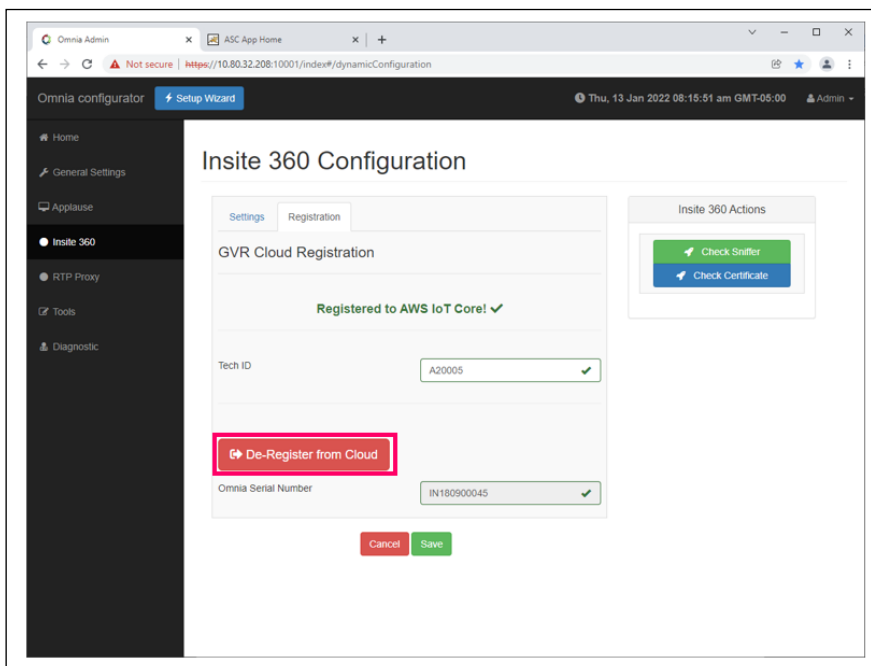
- De-Register the dispenser at the local dispenser registration screen.
- Un-Register the dispenser at the Remote Management portal.

The order of the two steps is not important, but both need to be completed. De-Registration from the dispenser removes the communication certificates inside the dispenser. The dispenser will be listed (not connected) in the I360 Remote Management portal. The second step is Un-Register the dispenser at the Remote Management portal (this action only removes the dispenser from the Remote Management portal). If the De-Registration locally at the dispenser was not performed, the dispenser will think that it is still registered but the AWS IoT Gateway will deny the connection. The step to Un-Register at the Remote Management portal completes the De-Registration action.

To De-Register a Dispenser from the AWS IoT Gateway:

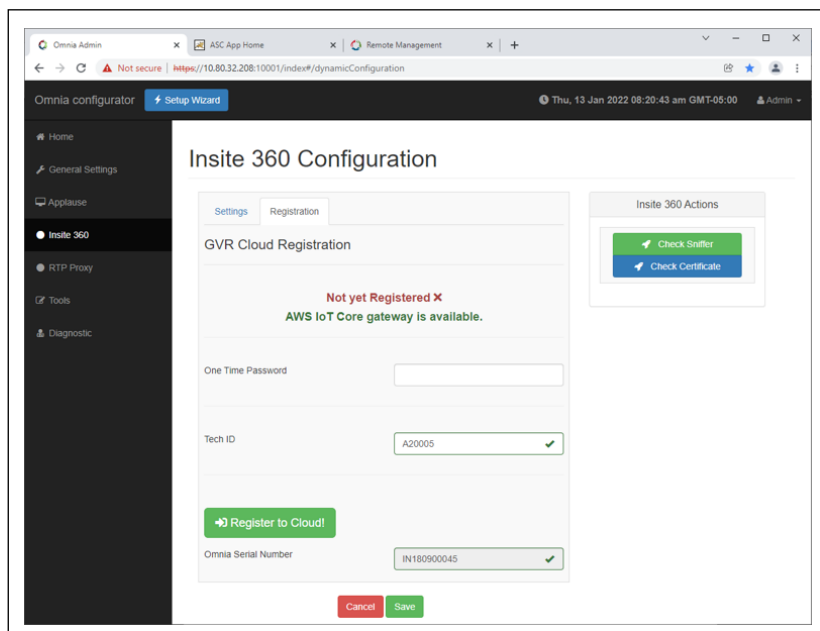
- 1 From the Insite 360 Configuration page, click **De-Register from Cloud**.

Figure 7-11: GVR Cloud Registration - De-Register from Cloud



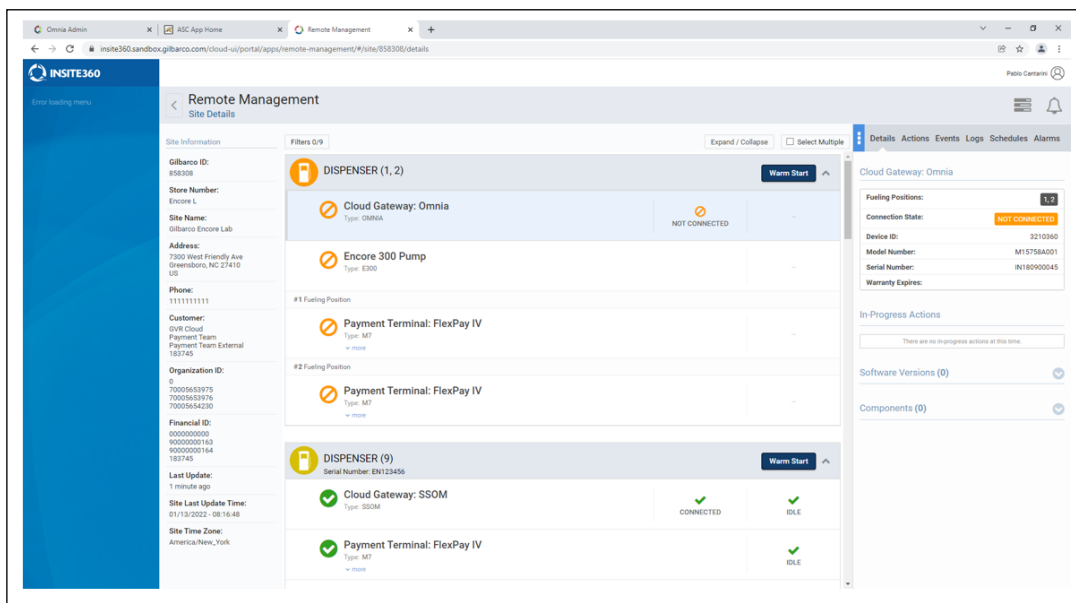
- 2 The messages “Not Yet Registered” and “AWS IoT Core gateway is available” are displayed.

Figure 7-12: AWS IoT Core Gateway Message



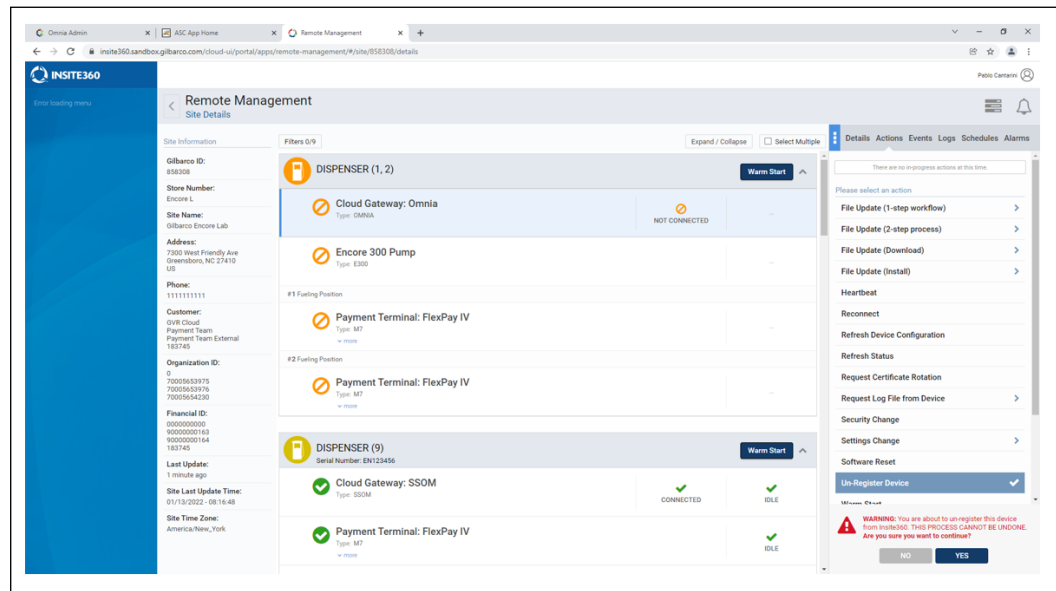
- 3 From the Insite 360 Remote Management portal, go to the Dispenser that you want to Un-Register. The Cloud Gateway: Omnia device will display as “Not Connected” if the Omnia was de-registered from the Cloud only from the Omnia UI, but not the Insite 360 Forecourt portal.

Figure 7-13: Remote Management - Cloud Gateway: Omnia Device



- 4 In the right pane, select **Actions > Un-Register Device**, and click **Yes**.

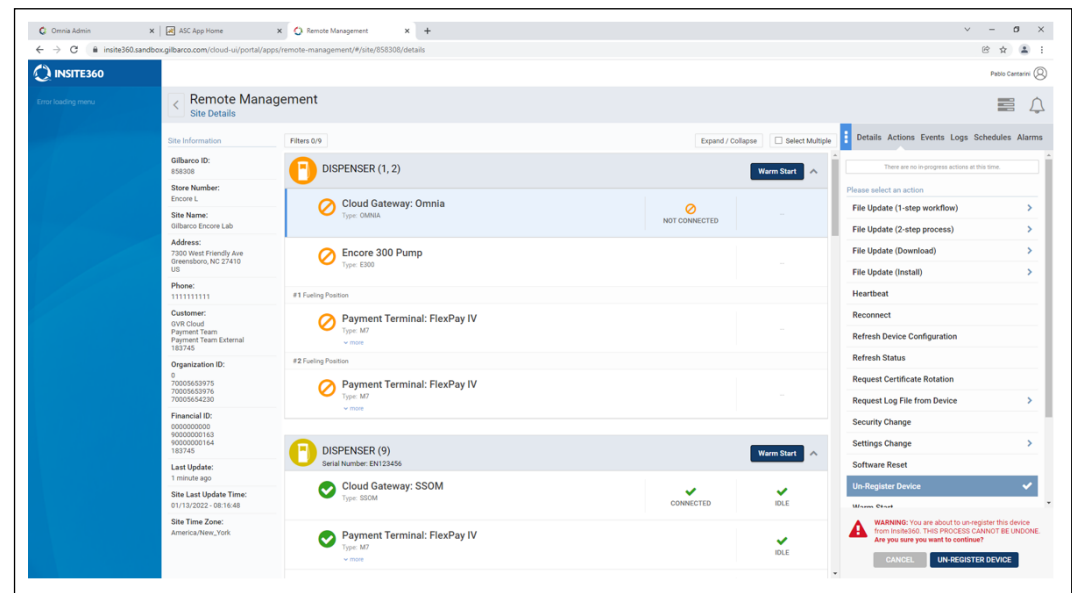
Figure 7-14: Remote Management - List of Actions



- 5 Click **UN-REGISTER DEVICE** to confirm.

Note: To register a device after de-registration, call TAC at 1-800-743-7501.

Figure 7-15: Remote Management - Un-Register Device - Confirm



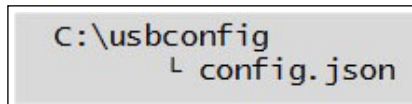
The dispenser is de-registered from the AWS Gateway and un-registered from Insite 360.

Retrieving the Omnia Network Configuration

The default IP address for the Omnia is 172.20.100.254. If it has been changed, you can use the following procedure to retrieve the current IP address:

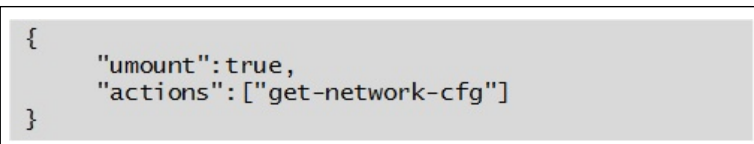
- 1 Create a folder on your Windows desktop with the name “usbconfig”. Create a sub-folder within it, with the name “config.json”.

Figure 7-16: usbconfig Folder



- 2 Using a text editor, such as Windows Notepad, type the following command exactly as shown in [Figure 7-17](#).

Figure 7-17: Command



- 3 Save the file as config.json to the Windows desktop.
- 4 Copy and paste the config.json file into the usbconfig folder.
- 5 Copy the usbconfig folder and its content to the root directory of an empty, FAT-formatted Universal Serial Bus (USB) stick.
- 6 Plug the USB stick into the USB J6301 of Omnia.

The board will automatically detect the USB storage and will create a file on it with the current networking configuration.

- 7 When the operation is completed successfully, the red LED under USB J6301 blinks. If an error is detected, the red LED turns solid ON.

Note: The results are stored in the following location: usbconfig\network-config-SERIALNUMBER.txt. The SERIALNUMBER is the serial number of the Omnia.

Resetting the Network Configuration to Factory Values

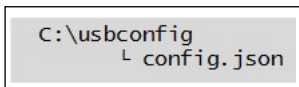
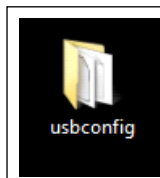
IMPORTANT INFORMATION



The procedure described below will modify the networking settings of the Omnia, potentially making the dispenser or the entire site temporarily inoperative!
Execute the procedure only under direction and supervision of Gilbarco Help Desk.

- 1 Create a folder on the Windows desktop with the name “usbconfig”. In that, create a file with the name “config.json”.

Figure 7-18: Creating Folder



- 2 Using an editor of your choice (for example, Windows Notepad), type the following command exactly as shown in [Figure 7-19](#).

Figure 7-19: Command

```
{
  "umount": true,
  "actions": ["network"]
}
```

- 3 Save the file as config.json to the Windows desktop.
- 4 Copy and paste the config.json file into the “usbconfig” folder.
- 5 Copy the usbconfig folder and its content in the root directory of an empty, FAT-formatted, USB drive.
- 6 Plug the USB drive into the USB connector of the Omnia.

The Omnia board automatically detects the file and command on the USB drive (reboot is not required) and then resets the network settings back to factory default Omnia IP address (172.20.100.254). The process takes no longer than 2 minutes. When the operation has finished, D28-D32 LEDs will be ON.

After completing the procedure, you can access the configuration web application using the default IP parameters and apply any changes to the Omnia configuration.

- 7 Reconfigure the PC network configuration as follows:
 - **IP:** 172.16.100.15
 - **Netmask:** 255.255.255.0
- 8 Connect a PC with a browser to service port.
- 9 Open a browser and type **http://172.20.100.254:3000/** in the address field.
- 10 Apply changes to the Omnia configuration as needed. Configure the Omnia network as follows:

External Omnia IP address for Side A

Address: 10.5.55.71

Netmask: 255.255.255.0

External Omnia IP address for Side B

Address: 10.5.55.72

Netmask: 255.255.255.0

Internal Omnia IP address

Address: 172.20.100.254

Netmask: 255.255.255.0

Note: Netmask should be 255.255.255.0

Note: If the process was successful, a log file of the change will be automatically copied to the `usbconfig`.

The network configuration should be as shown in [Figure 7-20](#).

Figure 7-20: Network Configuration

```
auto lo
iface lo inet loopback

auto eth0
allow-hotplug eth0
iface eth0 inet static
address 10.5.55.71
netmask 255.255.255.0

auto eth0:0
allow-hotplug eth0:0
iface eth0:0 inet static
address 10.5.55.72
netmask 255.255.255.0

auto eth1
allow-hotplug eth1
iface eth1 inet static
address 172.16.100.254
netmask 255.255.255.0
```

Note: The log file of the operation is located in the folder “usbconfig”.

- 11 Restore your PC network configuration.

Appendix A: Site Network Survey

The following questions are intended to be submitted to the customer or its IT consultants to collect information required for a proper networking configuration.

- 1 Is the customer dictating its own IP scheme for the forecourt? YES ☐ NO ☐

If YES:

- a What is the subnet intended for the dispenser's net and what is the range of available IP addresses?

First available IP	Last available IP	Netmask
_____ . _____ . _____ . _____	_____ . _____ . _____ . _____	_____ . _____ . _____ . _____

Ensure that the number of available IP addresses match the following requirements:

- Two IP addresses per dispenser (1 if dispenser is single sided)
- One IP address for the BRCM2 or BRCM2.1
- One IP address for Applause Media System Site Server (if present)

- b What is the default gateway of the site?

Default Gateway
_____ . _____ . _____ . _____

- c What is the primary DNS server IP address?

Primary DNS IP
_____ . _____ . _____ . _____

- d Does the customer's main router have one available Ethernet port to connect the BRCM2 or BRCM2.1? YES ☐ NO ☐

If the answer is NO, it might be necessary for the customer to buy an additional switch.

- 2 Does the customer restrict the access to the DNS server out to Internet? YES ☐ NO ☐

IF THE ANSWER IS YES, THE CUSTOMER MUST BE REQUIRED TO ALLOW ACCESS AT LEAST TO THE FOLLOWING:

ercsh.gilbarco.com (Port: 25201)
erkl.gilbarco.com (Port: 5001)
device.gilbarco.com (Port: 443)
registration.gilbarco.com (Port: 443)
transfer.gilbarco.com (Port: 443)

- 3 Does the customer enforce any MAC filtering or Port Security policy in the site net?
YES ☐ NO ☐

If the answer is YES, it may be required that you know in advance the MAC addresses of every Omnia to be installed on the site.

- 4 Is the Site running Applause? YES ☐ NO ☐

If YES:

- a Is the Applause Media System Site Server directly connected with the customer site router or is it connected to an intermediate router (normally Cisco RV042)?

☐ MAIN ROUTER ☐ RV042

- b What is the IP address of the Applause Media System Site Server?

Applause IP Address

_____._____._____._____

- c Is Applause Media System Site Server configured to use single NIC or dual NIC?

If the answer is dual NIC, convert the Applause system to a single NIC configuration, which may require an additional router (RV042 Firewall Router).

SINGLE NIC ☐ DUAL NIC ☐

- 5 Draw a simple sketch of the site network topology.
- 6 Notify the site IT personnel that User Datagram Protocol (UDP) port 123 must remain open; the Omnia platform requires the NTP access to the following locations:
- 0.debian.pool.ntp.org
 - 1.debian.pool.ntp.org
 - 2.debian.pool.ntp.org
 - 3.debian.pool.ntp.org

Contact IT personnel to verify that the site router allows the connection to these servers. If an NTP intercept is enabled on the router, the router must provide an answer to a time request from Omnia in less than 100 ms to avoid a loop in which the time keeps changing on the Omnia device.

- 7 Ensure that the network rules allow access to the following addresses defined in the [Pre-Installation Checklist](#) on [page 3-2](#).

Appendix B: FlexPay IV Applause® TV on Invenco Cloud Services (ICS) Migration

The FlexPay IV Applause Media System sites operating on Applause site servers will be migrated to the cloud-based platform, Invenco Cloud Services (ICS). As a result of this migration, the existing site server hardware will no longer be required. For more information, refer to “[Migration Instructions](#)” on [page B-3](#).

Software Requirements

*Note: To download Software, go to **Extranet** > **Technical Resources** > **Laptop Tool and Software**.*

The following are the required software versions:

- Encore Experience software version 6.00BR2
- OmniaICS_Package1_04.0.0014
- OmniaICS_Package2_01.00.02.03_DefaultPOS
- OmniaICS_Package3_01.00.02.03_VerifonePOS (For Verifone POS only)

Site Survey, Dispenser, and POS Requirements

A site survey must be performed to ensure successful migration to the ICS networks. The site survey form can be accessed using the following link:

<https://app.smartsheet.com/b/form/fa87517ce08f423c83c25945d19e3146>

After the site survey is completed, the technician must ensure that sites meet the following qualifications before continuing with the migration.

- 1 Dispensers must be Gilbarco Encore 500S/700S with FlexPay IV and Omnia.
- 2 Sites must not include a mix of SSoM and Omnia.
- 3 The POS brand must be Passport, NCR, or Verifone®.
Note: Passport Version 11 or older is not supported with this migration.
- 4 MNSP must be informed of addresses to whitelist for ICS and Insite360 connectivity.
- 5 Site must be provisioned by onboarding team and ready for ICS and Insite360 registration.
- 6 All dispensers must be registered to Insite360.
- 7 CRIND display resolution must be one of the following:
 - M14004AXXX VGS (640x480)
 - M19045A001 SVGS (800x600)
 - M15899B001 15.6” Display (1366x768)

Insite360 Forecourt Whitelisting/End Point Requirements for AWS-IoT and Invenco/ICS

Technicians must work with the site's MNSP to whitelist all the addresses listed in the [“Installation Checklists” on page 3-1](#), and referenced below for Insite360 and ICS connections.

AWS IoT URLs

- aatnflk6u65sn-ats.iot.us-east-1.amazonaws.com (ports 443, 8443, 8883)
- cfvuav3n0omj9.credentials.iot.us-east-1.amazonaws.com (ports 443, 8443, 8883)
- device-download-prod.s3.amazonaws.com (ports 443, 8443, 8883)
- s3.amazonaws.com/prod.i360.device.fileupload/* (ports 443, 8443, 8883)
- omnia-checkin.prod.insite360.gilbarco.com (Port 443)

NTP Server Destinations (Destination Port = 123, Protocol = UDP)

- 0.debian.pool.ntp.org
- 1.debian.pool.ntp.org
- 2.debian.pool.ntp.org
- 3.debian.pool.ntp.org

GSTV/ICS Media

- https://icsapiprod.applause.gilbarco.com (Port 443), or
- *applause.gilbarco.com

*Note: Use the wildcard URL (*applause.gilbarco.com) if possible, this will future proof the connection if we add URLs later. If wildcards are prohibited, use option <https://icsapiprod.applause.gilbarco.com/>.*

Migration Instructions

IMPORTANT INFORMATION

The Encore Experience software must be installed in the order as instructed using the following steps for successful installation.

For migration instructions, proceed as follows:

- 1 Install the Encore Experience software V6.00BR2 onto the Omnia.
- 2 Select **Yes**, and **reboot** when the Encore Experience software installation is complete.
- 3 Register the dispenser to the Insite360 cloud and ensure that it is successfully registered.
- 4 Install OmniaICS_Package1_04.0.0014 or latest available version onto the Omnia.
- 5 Select **Yes**, and **reboot** when the OmniaICS_Package1_04.0.0014 installation is complete.
- 6 Install OmniaICS_Package2_01.00.02.03_DefaultPOS or latest available version onto the Omnia.
- 7 If POS is Verifone, install the OmniaICS_Package3_01.00.02.03_VerifonePOS or latest available version package. If not, go to step 8.
- 8 Log into the Omnia Configuration and click **Open Apps**. Select the configuration for the **Media State Enable** field as follows and set **Volume** to “70” (see [Figure B-1](#)).
 - Disabled - for Passport POS
 - Enabled - for Generic POS

Figure B-1: Open Apps Configuration

The screenshot displays the 'Open Apps Configuration' interface within the Omnia configurator. The left sidebar shows navigation options: Home, General Settings, Insite 360, Open Apps (selected), RTP Proxy, Aspector Tool v2 1.3, Tools, and Diagnostics. The main configuration area includes the following settings:

- Media State Enabled:** A dropdown menu set to 'Enabled'.
- Idle Loop Delay:** A text input field set to '10'.
- Idle Loop Delay From Busy:** A text input field set to '10'.
- Busy Loop Delay:** A text input field set to '5'.
- Volume:** A dropdown menu set to '70'.
- Server:** A text input field set to '10.5.55.66'.
- JavaScript Console:** A dropdown menu set to 'Disabled'.
- Side A:**
 - Pump ID:** A text input field set to '7'.
- Side B:**
 - Pump ID:** A text input field set to '11'.

At the bottom of the configuration area are two buttons: 'Cancel' (red) and 'Save' (green).

- 9 Ensure that the dispenser is connected to ICS and media is playing (during fueling) by contacting the Invenco by GVR Onboarding team (at 866-606-8966). The Onboarding team will validate the connection and inform the technician of the results. If the connection is not working, the Onboarding team will instruct the technician on next steps.
- 10 Disconnect the existing physical Applause site server and leave the server at the site.

Troubleshooting

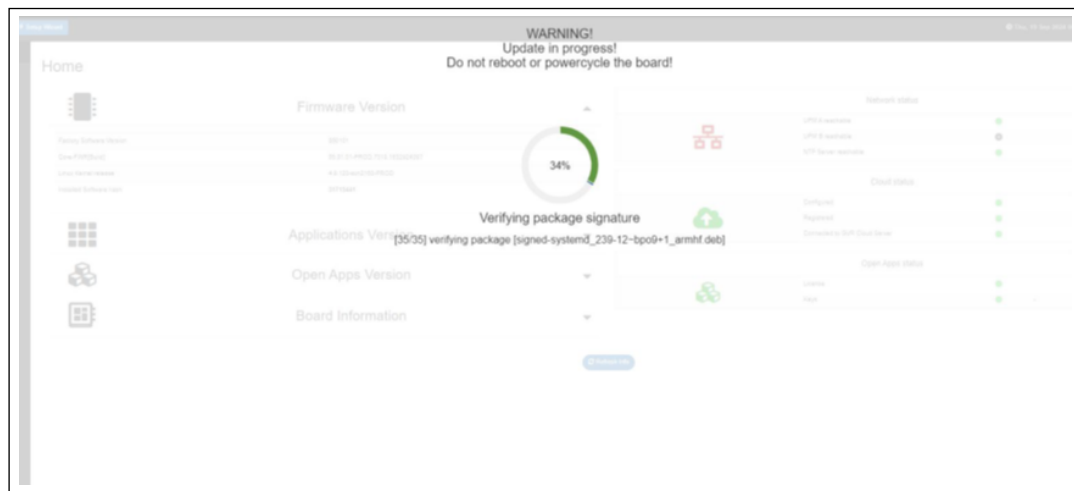
IMPORTANT INFORMATION

Do not use the Encore Experience Removal Tool to remove the Encore Experience and the Omnia ICS packages. In the event that the Encore Experience and Omnia ICS packages must be removed, use the Omnia ICS Removal Tool that is available on the Extranet. Instructions are included in the Omnia ICS Removal Tool package.

Message “Warning! Update in progress! Verifying package signature”

If the above message is displayed when accessing the Omnia Configurator, warmstart the dispenser to clear the message. This is due to software that has been staged (downloaded) from Insite360 to the Omnia but is yet to be installed.

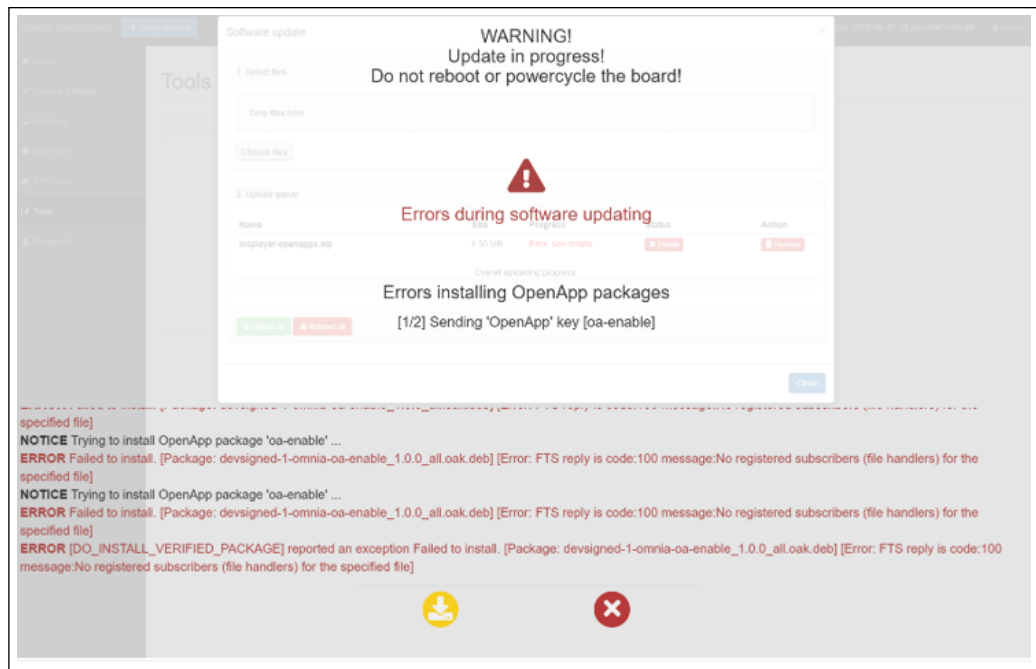
Figure B-2: Warning Message - Update in Progress!



“Errors during software updating - Errors installing OpenApp packages”

If this error message is displayed during the installation of the OmniaICS_Package2_01.00.02.03_DefaultPOS, this indicates that the Encore Experience software has not been installed. Install the Encore Experience software, and then reinstall the OmniaICS_Package2_01.00.02.03_DefaultPOS.

Figure B-3: Warning Message - Errors During Software Updating



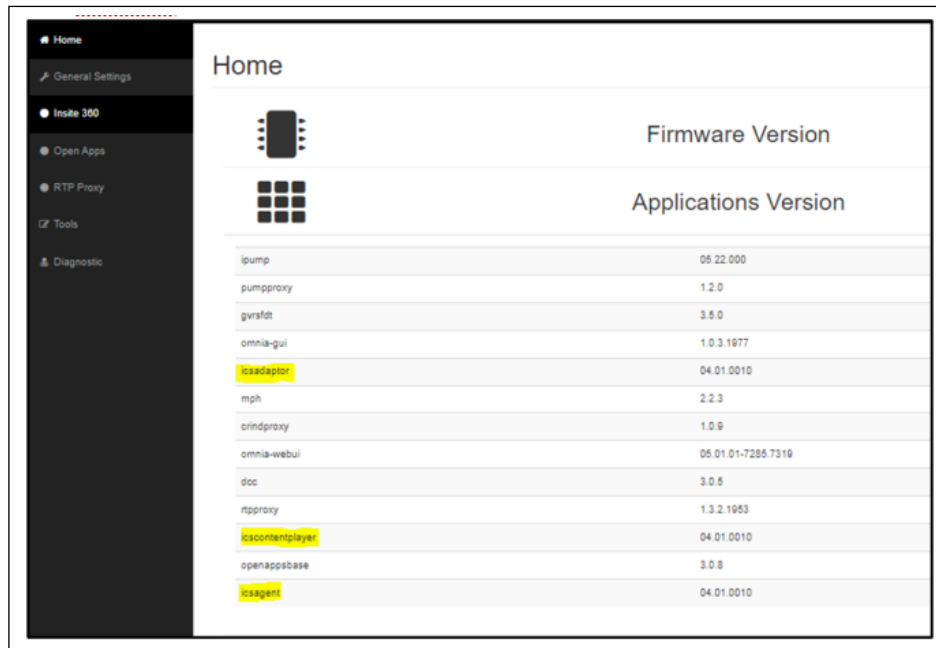
Note: When Encore Experience is successfully installed on the Omnia, the Applause Configuration is removed, and the Open Apps Configuration is added to the Omnia Configurator in the left navigation panel.

Verify Omnia is Ready to Connect to ICS and Installation is Successful

Connect to the Omnia Configurator. From the Home page, proceed as follows:

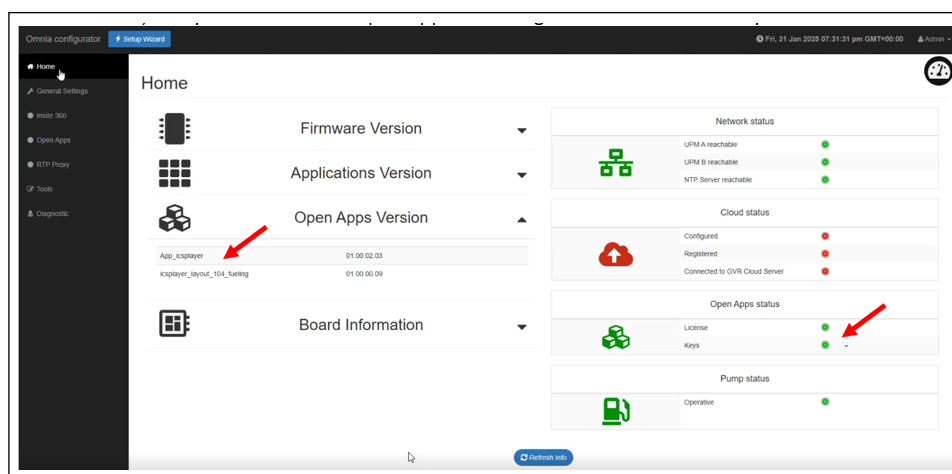
- 1 Expand the **Applications Version** and verify that the following fields are shown:
 - icsadaptor
 - icscontentplayer
 - icsagent

Figure B-4: Applications Version



- 2 Expand the **Open Apps Version** and verify that the **App_icsplayer** and **icsplayer_layout_104_fueling** were installed. Also, verify that the LEDs in Open Apps status are green for License and Keys.

Figure B-5: Open Apps Version



Appendix C: Legacy Gateway

Registering Omnia to Insite360 Forecourt

Ensure that the Network Rules are set to allow the following URLs, which are applicable to all versions of Omnia Software:

- **registration.gilbarco.com**
- **transfer.gilbarco.com**
- **device.gilbarco.com**

To register Omnia to Insite360 Forecourt, proceed as follows:

- 1 Click the **Registration** tab.
- 2 Enter a valid Tech ID number in the ASC ID field, and then click **Register Omnia to SODA!** for registration.

Figure B-1: Pre-registration to Gilbarco Cloud In Progress

The screenshot shows the 'Insite 360 Configuration' window. The 'Registration' tab is active. Under 'GVR Cloud Registration', it says 'Not yet Registered X'. There are two input fields: 'Tech ID' with the value 'A20005' and 'Omnia Serial Number' with the value '15739150'. A large green button with a cloud icon and the text 'Register to Cloud!' is prominently displayed. To the right, a sidebar titled 'Insite 360 Actions' contains three buttons: 'Check Internet', 'Check Serial', and 'Check Installer'. At the bottom of the main window are 'Cancel' and 'Save' buttons.

A dialog box opens to indicate success or failure.

Figure B-2: Indicating Success or Failure

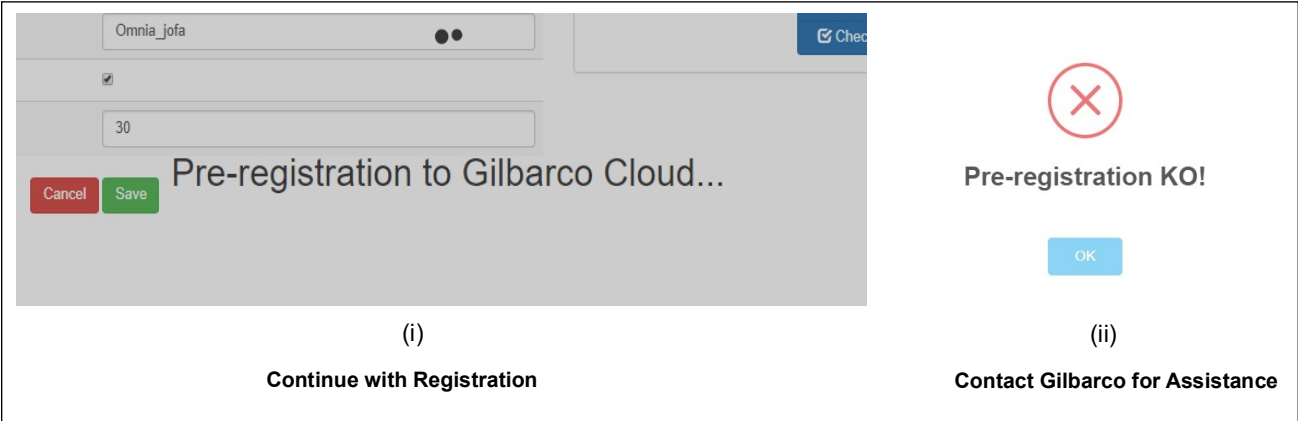
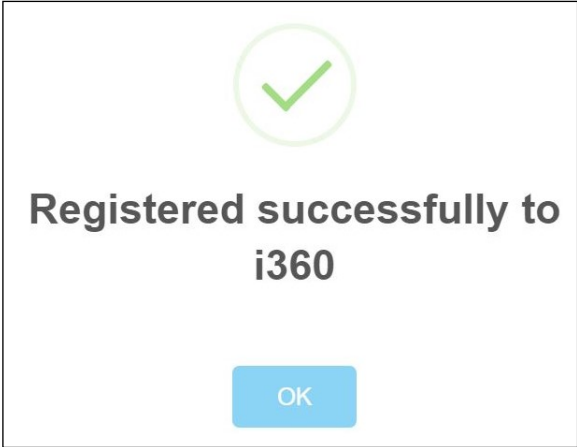


Figure B-3: Registration OK



If the registration is unsuccessful, a dialog box as shown in [Figure B-4](#) opens after 1-2 minutes.

Figure B-4: Registration KO (Failure) Message

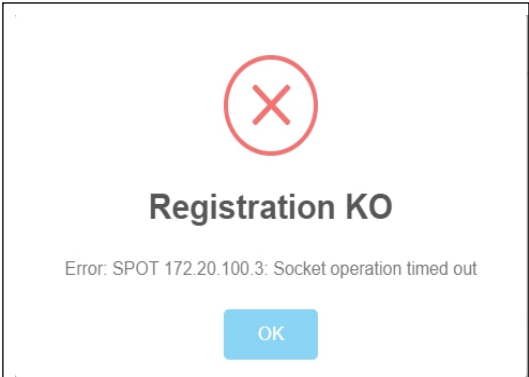
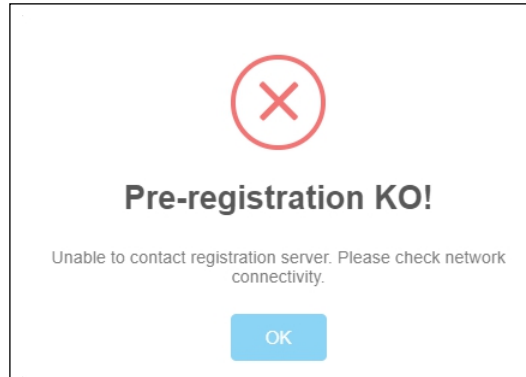


Figure B-5: Pre-registration KO (Failure) Message

If the registration is unsuccessful after multiple attempts, refer to [“Troubleshooting”](#) on [page 7-1](#).

Completing the Programming

To complete the programming, proceed as follows:

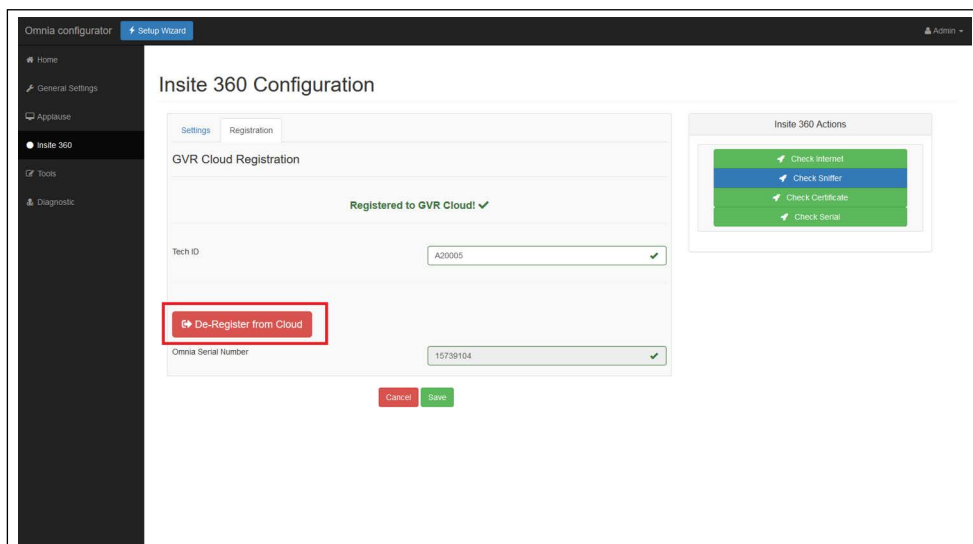
- 1 Exit the Omnia Configurator.
- 2 Re-establish two-wire communication to the POS.
Note: Depending on the POS, a purge may be required. Then, download the POS application.
- 3 Test the unit operation and open the fueling positions for use.

De-registering Omnia from Insite360 Forecourt

To unregister dispenser from Insite 360 Cloud, proceed as follows:

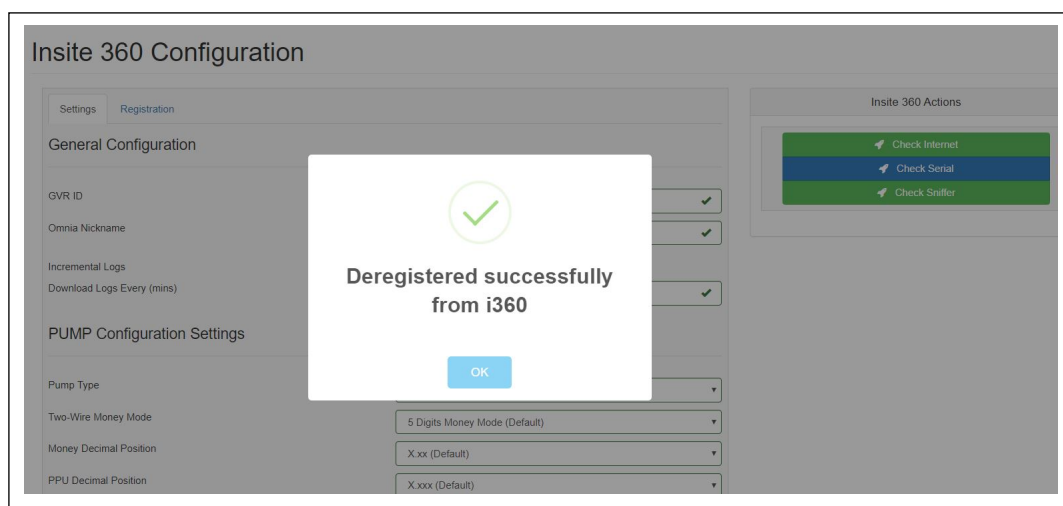
- 1 Within the Omnia webpage application, click the **Registration** tab.
- 2 Select **De-Register** and Wait for the de-register success message.

Figure B-6: De-Register



Note: De-register the Omnia PCB before replacing. Re-register after service.

Figure B-7: De-registration Success Message

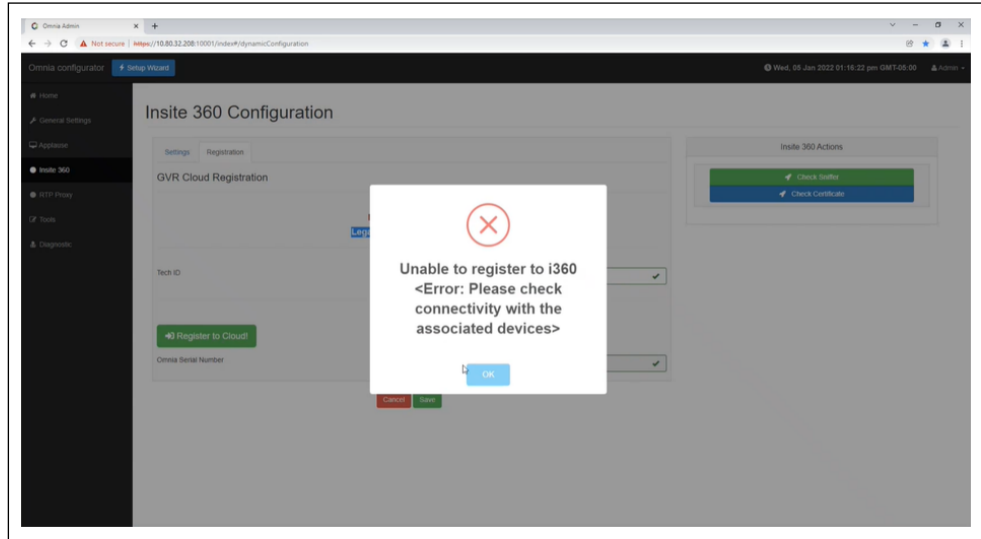


GVR Cloud Registration Error Cases

The following section shows errors related to Registration and describes possible causes and actions to take for resolution.

1 Problem: Failure to register to Legacy Gateway.

Figure B-8: Legacy Gateway Registration Error



Possible Cause: One of the internal devices (UPM of GSoM of Programmed) is not communicating to the Omnia at the time of the registration attempt.

Action: Check connectivity to the UPM/GSoM. Verify the physical connection, IP scheme, and IP addresses in both the Omnia and UPM/GSoM.

2 Problem: Failure to De-register from Legacy Gateway.

Possible Causes: Unable to reach Legacy servers; Legacy servers are not online.

Action: Call Insite 360 or check network status of the customer site.

This page is intentionally left blank.

Index

A

Alert symbol 2-1
Applause Media System Site Server A-1

B

Barricading 2-1
BOM 3-1

C

Caution warnings 2-1
Checklists 3-1

D

Danger warnings 2-1
DCM2.1 5-1

E

Electrical
 Shut-off 2-1
Emergency
 Electrical shut-off 2-1
Evacuation 2-1
Explosions
 Preventing 2-1
External 5-6, 5-18

F

Fires
 Preventing 2-1
FlexPay Connect v2 3-1

I

Insite360 Cloud 1-1

N

Netmask A-1

P

Pre-Installation Checklist 3-1
Primary 5-6, 5-18

R

Remote Management Help Desk 3-2

S

Safety Information
 Alert symbol 2-1
 Barricading 2-1
 Emergency electrical shut-off 2-1
 Evacuation 2-1
 NFPA regulations 2-1
 Preventing explosions and fires 2-1
 Regulations 2-1
 Replacement parts 2-1
 Safety symbols 2-1
 Shut-off 2-1
 Signal words 2-1
 Warning words 2-1
Safety symbols 2-1
Shut-off 2-1
 Emergency electrical 2-1
Signal words
 Safety 2-1
Site Network A-1

W

Warning words 2-1
Warnings 2-1
Windows XP 1-6

