CFN Series

CFN III Fuel Management System PA-DSS Implementation Guide

Version 3.6

MDE-4870A

Computer Programs and Documentation

All Gasboy computer programs (including software on diskettes and within memory chips) and documentation are copyrighted by, and shall remain the property of, Gasboy. 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 Gasboy.

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.

Approvals

Gasboy, Greensboro, is an ISO 9001:2000 registered facility.

Underwriters Laboratories (UL):

UL File#	Products listed with UL
MH4314	All dispensers and self-contained pumping units
MH10581	Key control unit, Model GKE-B Series
	Card reader terminals, Models 1000, 1000P
	Site Controller, Model 2000S CFN Series
	Data entry terminals, Model TPK-900 Series
	Fuel Point Reader System

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 Compliance (CoC):

Gasboy 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 #	CoC#	Product	Model #
95-179	Dispenser	9100 Retail Series, 8700 Series, 9700 Series	91-019	Dispenser	9100 Commercial Series	05-002	Atlas	8700K, 8800K, 9100K, 9200K, 9800K
95-136	Dispenser	9800 Series	91-057	Controller	1000 Series FMS, 2000S-CFN Series			

Patents

Gasboy products are manufactured or sold under one or more of the following US patents:

Dispensers

5,257,720

Point of Sale/Back Office Equipment

D335,673

Additional US and foreign patents pending.

Trademarks

Non-registered trademarks

Atlas™
Consola™
Infinity™

Registered trademarks

ASTRA®
Fuel Point®
Gasboy®
Keytrol®
Slimline®

Additional US and foreign trademarks pending.

Other brand or product names shown may be trademarks or registered trademarks of their respective holders.

This document is subject to change without notice.
E-mail: literature@gasboy.com · Internet: http://www.gasboy.com

PETROLEUM EQUIPMENT INSTITUTE PEI

Table of Contents

1 – Introduction

Purpose

This document provides information required to install and operate the CFN III in a manner compliant with Payment Application - Data Security Standard (PA-DSS) version 1.2.

Failure to comply with the information in this document could put the merchant in violation of PA-DSS and possibly Payment Card Industry (PCI-DSS) compliance.

Related Documents

Document Number	Document Title	GOLD Library
PA-DSS – Requirements Version 1.2		
MDE-4739	CFN III PCI Secure Controller Software Installation/Upgrade	CFN Series Networks, Card Handlers, and Pump Interface
MDE-4871	CFN III Manager's Manual for Windows® XP Embedded Version 3.6	CFN Series Controllers and POS
MDE-4872	CFN III Configuration Manual for Windows XP Version 3.6	CFN Series Controllers and POS
MDE-4873	CFN Series Site Controller III Start-up Manual for CFN III Version 3.6 and Later	CFN Series Controllers and POS

PA-DSS and PCI-DSS

PA-DSS is a series of requirements that apply to any payment application that stores, processes, or transmits card holder data as part of the transaction process. CFN III falls under this requirement and therefore must comply with PA-DSS. Many of the requirements under PA-DSS are handled automatically by CFN III. However, there are certain requirements that must be maintained by the merchant in order to run in a compliant manner. Each of the merchant requirements will be covered in this document.

PCI-DSS is a series of requirements that apply to the entire payment environment at a merchant location. PA-DSS covers only a portion of that environment. It does not cover all aspects of PCI-DSS. It is the responsibility of the merchant to ensure that their overall payment environment is operated and maintained in a manner compliant with the PCI-DSS.

For more information on specific requirements of PCI-DSS or PA-DSS, refer to the PCI Security Standards Council website http://www.pcisecuritystandards.org.

Certification Status

CFN III version 3.6A was evaluated by K3DES in July 2009, and certified as compliant under PA-DSS version 1.2.

Abbreviations and Acronyms

Term	Description
ASC	Authorized Service Contractor
CFN	Cash Flow Network
DES	Data Encryption Standard
PA-DSS	Payment Application - Data Security Standard
PCI-DSS	Payment Card Industry - Data Security Standard
PIN	Personal Identification Number
POS	Point Of Sale
SC	Site Controller
TIP	Transaction In Process
USB	Universal Serial Bus

2 – Getting Started

Physical Security

The merchant is responsible for ensuring that the CFN III is physically secure.

System Security

Physical access to the Site Controller system must be limited to only those that use the Site Controller. If modular Profit Point POS systems are used, then the Site Controller is best controlled in a locked back room, with restricted access. If using Integral Profit Point POS system, the system must only be accessible by those using the system. If it is not possible to maintain the system in a secure area, the area must have adequate coverage by available security cameras so that unauthorized access can be recorded and used to determine any cause of physical security breaches.

System Report and Other Logs

Though the system log is secure from exposing any sensitive card information, it is a good practice to keep the log printer in a secure area. It is possible that some bank host systems require card account information to be listed on a report or log for back office purposes. When the reports are used for holding account information it is the responsibility of the site manager or store owner to secure the reports from unauthorized access.

Installations and Upgrades

To upgrade the CFN payment system from a non-compliant version of 3.4 or earlier, to a secure PCI-compliant version, refer to MDE-4739 CFN III PCI Secure Controller Software Installation/Upgrade Instructions.

The integrity of software upgrades is guaranteed because only software created by Gasboy® will operate on the CFN III board set. Software created without the unique Gasboy development system will typically fail checksum. However, in the event that the software passes that test, the system will not boot or operate.

Purge Transaction Records

After the installation is complete, the embedded payment controller transaction table must be purged of any information left in memory, which may retain previous card information. This is a mandatory procedure in order to meet PCI requirements and cannot be skipped. This process must be executed before the site is allowed to start processing card data. It would be best to proceed with this process right after the table sizing is finalized.

To remove the non-secure information, proceed as follows:

1. In the SC3 window, log on to the Payment System as an administrator user with an administrator permission level.
2. Type **FIX TRAN;I** and press **Enter**.
3. Type **RESET TRAN;I** and press **Enter**.
4. Type **RESTORE TRAN FROM TRANWIPE.DTA** and press **Enter**. If the message, “Transaction physical record too large” is displayed on the screen, it is harmless, ignore the message. After this command is executed, the transaction table will be wiped of any information (system is unusable at this time).
5. Type **FIX TRAN;A** and press **Enter**. This command will renumber and correctly set up the cleaned transaction table. The table is now ready for accepting secure card data.

Delete System Security Keys

To securely delete the System security keys, format the RAM drive.

1. Type **FORMAT R:** and press **Enter**.
2. Type **autoexec** and press **Enter**.

Re-encrypting Historic Data

CFN III does not support maintaining historic data before the upgrade. All transactions must be settled before the upgrade begins.

User Accounts

Overview

PCI PA-DSS requirement 8 mandates the use of unique user IDs and secure authentication for administrative access, access to card holder data, and access to PCs with payment applications.

The merchant is responsible for managing User Names and Passwords on all systems within their network.

Removing System Defaults

The system is provided with some defaults to assist the install or upgrade process. However, to meet the PCI requirements the default passwords must be changed, providing a secure system.

CFN III User Passwords and Permission Levels

Note: Contact Gasboy Technical Support if you do not know the CFN III Manager password.

Upgrading from a non-secure version will result in the removal of previous passwords. For more information on obtaining a password, refer to MDE-4739 CFN III PCI Secure Controller Software Installation/Upgrade Instructions.

Manager permission level access must not be granted for passwords that are used by general CFN users. CFN general users and managers must meet the minimum password requirements listed in "Appendix A: PCI Password Requirements" on page A-1. A unique CFN User ID must be used for every individual that will be accessing the CFN system.

Windows XPE Users and Passwords

The Windows XP Embedded (XPE) PC is set up for three users - "Administrator", "guest", and "gasboy". The "guest" user is disabled and must not be enabled. The "gasboy" user is a hybrid user and the account type for the "gasboy" user must not be modified or the system will not meet PCI PA-DSS requirement 8.

The "Administrator" user is the Windows system administrator and, as default, is set up without a password. On completion of the system install and the embedded payment system configuration, the "Administrator" user password must be set. This administrator account must be assigned to one individual only and only that individual must know the password. The password is set up by logging onto the Windows XPE as the "Administrator" user, through the Control Panel "User Accounts".

If other employees require administrative rights to Windows XP, such as access to Audit logs for backup, then additional administrative level users must be created for each individual. These accounts can be created by logging onto the Windows XPE as an administrator user, accessing the Control Panel "User Accounts", and adding a user.

For PCI password requirements, refer to "Appendix A: PCI Password Requirements" on page A-1.

Screen Saver

To ensure that only the intended individual has access to the system, a password-protected screen saver must be used for each Administrative level user account.

1. Log on to the system using an Administrative level user account.
2. Right-click on the desktop.
3. Select **Properties**.
4. Select **Screen Saver** tab in the Display Properties box.
5. Select any option other than "None" from the list of options for Screen Saver.
6. Set the wait time to 5 minutes.

7 Select **On resume, password protect**.

8 Click **OK**.

9 Repeat step 1 to 8 for each Administrative level user account.

Administrator Desktop

The newly created administrator user's desktop will not look exactly like the default "Administrator" user's. To change to default settings, proceed as follows:

To change the settings for the Control Panel, proceed as follows:

1 Click on **Start** > **Settings** > **Control Panel**.

2 Select **Switch to classic view**.

To change the settings for the Start Menu, proceed as follows:

1 Click on **Start** > **Settings** > **Control Panel** > **Taskbar and Start Menu Properties** > **Start Menu**.

2 Select **Classic Start Menu**.

To change the settings for the desktop icons, proceed as follows:

1 Right-click on the desktop and select **Properties** > **Display Properties** > **Desktop**.

2 Select **Customize Desktop**.

3 Clear the options My Documents, My Network Places, and Internet Explorer icons.

To resize the SC3 Window to default settings, proceed as follows:

1 Right-click title bar of SC3 window.

2 Select **Properties**.

3 Set Window Size - Height to 26.

Remote Access

Two-factor authentication is required for remote access into the CFN III system by employees, administrators, and third-party.

Passwords and access by vendors for remote maintenance must be enabled only when explicitly required, and must be disabled thereafter. Best practice is to only enable this access when access to the system has been requested by the vendor. Remote access is provided only to users with permission level 9 or lower. Remote access is not provided for users with permission level 10 or higher.

Disabling and Enabling Remote Access

Remote access is disabled by setting the remote port channel to “None” in Sys_par page 8. Instructions for setting this are documented in MDE- 4872 CFN III Configuration Manual for Windows XP Version 3.6.

CFN III Key Management

System Keys are required to protect card holder data against disclosure and misuse. The following must be implemented to meet PCI requirements:

- Strong keys must be generated, which are a mix of lower case letters, upper case letters, and numerical data.
- The Master key and Pass key must be initially loaded by two separate personnel.
  Note: A key custodian is a person who holds, maintains, controls, stores, and protects the keys required by the CFN III system. Such keys encrypt and protect customer card data.
- Keys are to be stored in a secure manner preventing unauthorized personnel from access.
- Any old keys are to be destroyed to prevent unauthorized access.
- Keys are to be changed on a periodic basis as required. Keys must be changed at least once a year to maintain PCI compliance.
- Keys must be changed if there is any known or suspected compromise to the system.
- Each key-custodian must sign a key-custodian form or document, which states that he or she understands and accepts the responsibilities of key custodianship. Such a document, for key custodianship, is to be produced, maintained, and controlled by the accessor company.

The CFN III system provides a menu for setting and loading the security keys. For additional information, refer to MDE-4873 CFN Series Site Controller III Start-up Manual for CFN III Version 3.6 and Later.

Audit Trail

CFN III creates an automated audit trail to meet the PCI requirements.

The audit journal contains information about system access, system actions executed, and programs executed. The audit file contains the user ID, action taken by the user, the security level of the user, and the channel device location of the user. This information is required to allow traceability of user actions and must be protected to meet PCI requirements.

The audit journal is enabled by enabling journal.log in sys_par. Disabling this audit feature will result in the system not being PCI-DSS compliant.

The disk journal in sys_par, item 10 must be set to “Yes”. New installs will already be defaulted to run the disk journal. The journal is used to create system access audit information and must be set to “Yes” to meet the PCI requirements.

Services

Windows XPE is set up with restricted services. The Windows XPE system is not set up as a general PC computer and must be used only for the purpose of housing the CFN embedded payment controller. Microsoft® Windows XPE license states that an Windows XPE system cannot be used as a general purpose PC. For example, the restrictions would include general software such as Microsoft Word, Microsoft Excel®, or other general applications.

Windows XPE system does not support networking and does not have the functionality for wireless connections or other type of networking. The configuration of Windows XPE serial and USB ports is for connecting to local equipment only. Using the serial or USB ports for any other purpose may not meet the PCI security requirements. USB ports can be utilized to download audit and other files to a separate smart or thumb drive.

3 – Recurring Operations

Data Retention

The PCI PA-DSS requirement 3.1 defines the data retention requirements.

Note: The merchant is responsible for determining the duration to retain the secure information by the CFN III.

- Keep card holder data storage to a minimum.
- Develop a data retention and disposal policy.
- Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes.
- Set the size of the transaction file small enough to ensure that the system will over write the oldest transaction before the end of your defined retention period. For instructions on setting the size of your transaction table, refer to MDE-4872 CFN III Configuration Manual for Windows XP Version 3.6.

In the event that the transaction data is not over written in the defined period, the transaction memory must be purged as described in "Purge Transaction Records" on page 3.

User Accounts

Refer to "Appendix A: PCI Password Requirements" on page A-1.

Audit Trail

This Audit Log information is required to allow traceability of user actions and must be protected to meet the PCI requirements. This information must be reviewed daily by the merchant. It is required that at least 90 days of audit information resides on the system and the administrator/owner is to retain at least one year of audit information, offline, and in a secure location. New audit information is to be copied to removable media for downloading and protecting on a regular basis.

The Audit Log must remain enabled.

This page is intentionally left blank.

4 – Maintenance and Troubleshooting

Software Updates

The merchant is responsible for ensuring that all onsite updates to the CFN III are performed by authorized personnel.

Merchant responsibilities for physical access to equipment are defined in PCI-DSS requirement 9.

The integrity of software upgrades is guaranteed because only software created by Gasboy will operate on the CFN III board set. Software created without the unique Gasboy development system will typically fail checksum. However, in the event that the software passes that check, the system will still not boot or operate.

CFN III does not support remote Software Updates.

Troubleshooting

Gathering Sensitive Data

CFN III does not require the collection of sensitive data for troubleshooting.

Sensitive information, such as Magnetic Stripe Data, Card Validation Codes, PINs, or PIN Block Data must:

- Only be collected to solve a specific problem and the data must be limited to only what is required to resolve the problem.
- Be stored in specific, known locations with limited access.
- Be encrypted while it is stored.
- Be securely deleted immediately upon resolving the issue.

Note: Sensitive information must not be transferred by e-mail.

Backup Password

CFN III supports a one-time backup password for use when the standard passwords have been lost.

For obtaining and using the Backup password, refer to MDE-4871 CFN III Manager's Manual for Windows XP Embedded Version 3.6.

Updating Windows XPE

To remain PCI-DSS compliant, Windows XPE must be updated with the latest security patches.

1. From an internet-connected computer visit the Microsoft web site and locate the security patches.
   http://www.microsoft.com/technet/security/bulletin/summary.mspx
2. Download the required security patches and save the files to a CD or USB thumb drive.
3. Log on to CFN III as an administrator user and insert the CD or USB thumb drive.
4. Use explorer to view the files and double-click on each file to install the updates.

5 – Prohibited Interfaces

Wireless Technologies

CFN III does not require the use of wireless technologies. Modification of CFN III to be installed in a wireless environment violates the product's PA-DSS compliance and could result in a violation of the merchant's PCI-DSS compliance.

Merchants and Authorized Service Contractors (ASCs) must not install the CFN III in a wireless environment.

Direct Internet Connection

PCI-DSS requirement 1.3 prohibits any direct internet connection to the payment environment.

CFN III does not support a direct internet connection. Implementing CFN III with a direct connection to the internet violates the product's PA-DSS compliance and the merchant's PCI-DSS compliance.

Merchants and ASCs must not install the CFN III with a direct internet connection.

Transmission of Data over Public Networks

CFN III does not support the transmission of sensitive data over public networks. Implementing CFN III in an environment where data is transmitted directly from the CFN III over a public network violates the product's PA-DSS compliance and the merchant's PCI-DSS compliance.

Merchants and ASCs must not install CFN III in an environment where sensitive data is transmitted directly from the CFN III over a public network.

This page is intentionally left blank.

Appendix A: PCI Password Requirements

The following password controls must be followed to meet minimum PCI PA-DSS requirement 8:

- Assign all users a unique User Name before allowing them access to the system.
- For authentication purposes use either a Password/Passphrase or two-factor authentication (such as token or smart card).
- Control addition, deletion, and modification of User Names and passwords.
- Verify user identity before performing password resets.
- Set first-time passwords to a unique value and require them to be changed after the first use.
- Immediately revoke access for any terminated or temporary users.
- Remove/disable inactive or unnecessary user accounts at least every 90 days.
- Communicate password procedures and policies to all users who have access to card holder data.
- Do not use group, shared, or generic accounts and passwords.
- Change user passwords at least every 90 days.
- Require a minimum password length of at least seven characters.
- Use “Strong” passwords containing a combination of lower case letters, upper case letters, and numeric. A strong password must be unique and not consist of common names or places.
- Do not allow an individual to submit a new password that is the same as any of the last four passwords used.

This page is intentionally left blank.

Glossary

Dispenser
A fueling dispenser that consists of a card reader, display, pump, and optionally a printer.

Master Key
Main security key used to protect card information.

Merchant
Refers to the owner and operator of the CFN equipment.

Pass Key
Secondary Key required to either protect card information or a key used to obtain a backup password from Gilbarco® Technical Support.

Payment Card
A Credit or Debit Card used for payment.

POS
Point Of Sale system, or computer used to process electronic transactions at the POS.

TIP
Transaction In Process record used in the Site Controller memory for maintaining on going sales information.

Trans Record
Transaction Record held in the Site Controller memory used to retain sales information.

Two-factor Authentication
Authentication requiring two separate forms of identification check, to ensure that the security cannot be breached by breaking a single check point.

7300 West Friendly Avenue · Post Office Box 22087
Greensboro, North Carolina 27420
Phone 1-800-444-5529 · http://www.gasboy.com · Printed in the U.S.A.
MDE-4870A CFN III Fuel Management System PA-DSS Implementation Guide Version 3.6 · June 2010