Passport™

Passport EDH (Fiserv®/ First Data™) V11.23.01.* Implementation Guide for PA-DSS V3.2

MDE-5523E

Computer Programs and Documentation

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

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

Applause™ Media System	Gilbert™	PAM™	Tank Monitor™
CIM™	G-SITE™	PAM™ 1000	TCR™
C-PAM™	G-SITE Link™	PAM™ 5000	The Advantage Series™
Eclipse™	G-SITE Lite™	Passport™	Titan™
Ecometer™	Highline™	SMART™ Connect	Trimline™
ECR™	Horizon™	SMART™ CRIND	Ultra-Hi™
e-CRIND™	InfoScreen™	SMART™ Meter	ValueLine™
EMC™	Making Things Better™	SmartPad™	
FlexPay™	Multiline™	Super-Hi™	

Registered trademarks

CRIND®	Performer®
Dimension® Series	Transac®
Encore®	Transac® System 1000
Gilbarco®	TRIND®
Legacy®	VaporVac®
MPD®	

Service mark

GOLDSM

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.

PEI PETROLEUM EQUIPMENT INSTITUTE

Table of Contents

1 – Introduction 1-1

1.1 Purpose . . . 1-1
1.2 PA-DSS vs. PCI DSS . . . 1-1
1.3 Related Documents . . . 1-1
1.4 Abbreviations and Acronyms . . . 1-2
1.5 Common Terms . . . 1-4
1.6 Supported Hardware . . . 1-4

2 – System Security 2-1

2.1 Overview . . . 2-1
2.2 Setup Account Information . . . 2-1
2.3 Security Manager Login Process . . . 2-1
2.3.1 Accessing Security Manager via System Maintenance . . . 2-2
2.3.2 Accessing Security Manager via Support Console . . . 2-3
2.3.3 Security Manager Login . . . 2-4
2.4 Using Security Manager . . . 2-5
2.4.1 Entry Error . . . 2-5
2.4.2 Process Error . . . 2-6
2.4.3 System Working . . . 2-6
2.4.4 Main Security Manager Window . . . 2-7

3 – User Names and Passwords 3-1

3.1 User Management . . . 3-1
3.1.1 Adding a User . . . 3-2
3.1.2 Removing a User . . . 3-4
3.1.3 Resetting a User . . . 3-5
3.1.4 Changing the Current User Password . . . 3-7
3.1.5 Password Expiration and Invalid Login . . . 3-9
3.2 User Name and Password Best Practices . . . 3-9
3.2.1 PCI DSS Requirements . . . 3-9

4 – Reports and Data Retention 4-1

4.1 Overview . . . 4-1
4.2 Secure Report Password . . . 4-1
4.2.1 Setting the Secure Report Password . . . 4-2
4.2.2 Retrieving Secure Reports . . . 4-4
4.3 Data Retention . . . 4-5

5 – Remote Access to the EDH 5-1

5.1 Overview . . . 5-1
5.1.1 General Requirements . . . 5-1
5.2 Enabling Remote Access to the EDH . . . 5-2
5.3 Disabling Remote Access to the EDH . . . 5-4
5.4 Enabling Remote Support from the CWS . . . 5-5
5.5 Extend Secure Remote Access . . . 5-8

5.6 Enhanced Remote Support Passwords 5-8
5.6.1 Configuring Passport to Enable Remote Support Passwords 5-9
5.6.2 Using Support Console with Enhanced Remote Support Passwords Enabled 5-10
5.6.3 Using System Maintenance with Enhanced Remote Support Passwords Enabled 5-13

6 – Software Updates 6-1

6.1 Overview. 6-1
6.2 Onsite Software Updates 6-1
6.3 Remote Software Updates 6-1
6.4 Accessing and Verifying Software Updates 6-1

7 – Managing System Security 7-1

7.1 Overview. 7-1
7.2 Security Manager - System Management 7-1
7.3 System Management Options 7-2
7.3.1 Key Management 7-2
7.3.2 Secure Report Password 7-4
7.3.3 System Security 7-5
7.3.4 Security Manager Report 7-8
7.3.5 Configuring Date and Time 7-12
7.3.6 Configuring Audit Log. 7-13
7.3.7 Gilbarco Secure Access 7-15
7.3.8 Server Alert Configuration 7-15
7.3.9 Hot Fix Configuration 7-16
7.4 BIN Range Trapping. 7-17
7.5 Security Audit Log 7-17
7.5.1 Printing Current or Previous Audit Log. 7-18
7.5.2 Audit Data Requirements 7-18
7.6 Secure Data Storage Management 7-19
7.6.1 Secure Data Storage 7-19
7.6.2 Secure Delete Tool 7-19
7.7 Access to Clear Text PAN 7-20
7.8 Physical Security 7-20
7.8.1 EDH Physical Security 7-20
7.8.2 Physical Security - Other Merchant Systems 7-20
7.9 Replacing Hardware 7-21
7.10 Troubleshooting 7-21

8 – Network Time Synchronization 8-1

9 – Audit Log Definition 9-1

9.1 Audit Log Structure. 9-1
9.1.1 File Header. 9-1
9.1.2 Section Separator 9-1
9.1.3 End of File Separator 9-2
9.1.4 Audit Log Section 1 (Windows Event Log). 9-2
9.1.5 Audit Log Section 2 (Secure Delete Log). 9-2

9.2 Audit Log Examples 9-3
9.2.1 All Individual Access to Cardholder Data 9-3
9.2.2 All Actions Taken by an Individual with Root or Administrative Privileges 9-3
9.2.3 Access to All Audit Trails 9-4
9.2.4 Invalid Logical Access Attempts 9-4
9.2.5 Use of Identification and Authentication Mechanisms 9-5
9.2.6 Initialization of Audit Logs 9-5
9.2.7 Creation and Deletion of System Level Objects 9-6

10 – Supported Hardware and Software 10-1

11 – Software Versioning Methodology 11-1

11.1 Versioning Methodology 11-1
11.2 PA-DSS Version Mapping 11-1

12 – Prohibited Interfaces 12-1

12.1 Wireless Technologies 12-1
12.2 Direct Internet Connection 12-1
12.3 Transmission of Data over Public Networks 12-2
12.4 Email and Messaging Technologies 12-2

13 – Network Communication Requirements 13-1

14 – System Services 14-1

Index Index-1

This page is intentionally left blank.

1 – Introduction

1.1 Purpose

This manual provides the required information to install and operate the Passport™ Enhanced Dispenser Hub (EDH) in compliance with the Payment Application Data Security Standard (PA-DSS) version 3.2.

Failure to comply with the information provided in this manual can place the merchant in violation of PA-DSS and possibly Payment Card Industry Data Security Standard (PCI DSS) compliance.

1.2 PA-DSS vs. PCI DSS

PA-DSS is a series of requirements that apply to a payment application that stores, processes, or transmits cardholder data as part of the transaction process. The EDH falls under this requirement; therefore, must comply with PA-DSS. Many of the requirements under PA-DSS are handled automatically by the EDH; however, there are certain requirements that must be maintained by the merchant to run in a compliant manner. Each of the merchant requirements will be covered in this manual.

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 the overall payment environment is operated and maintained in a manner compliant with PCI DSS.

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

1.3 Related Documents

Document Number	Title	GOLD℠ Library
MDE-4834	Passport System Recovery Guide for Passport V8.02+	Passport
MDE-5025	Passport Point of Sale V9+ System Reference Manual	Passport
MDE-5543	Passport V20.0X Upgrade Instructions for Systems Operating on V10.10, V11.01, V11.02, V11.04, or 12.0X	Passport
MDE-5544	Passport V20.0X Software Installation Manual for PX60/PS65 Hardware	Passport
MDE-5589	Passport V21.0X Software Installation Manual for PX60 Hardware	Passport

1.4 Abbreviations and Acronyms

Term	Description
AC	Action Center
API	Application Programming Interfaces
ASC	Authorized Service Contractor
ASU	Automated Software Upgrade
AuthIP	Authenticated Internet Protocol
AV	Audio Video
BFE	Base Filtering Engine
BITS	Background intelligent Transfer Service
BOS	Back Office System
COM	Component Object Model
CRIND®	Card Reader in Dispenser
CWS	Cashier Workstation
DB	Database
DCOM	Distributed COM
DEK	Data Encryption Key
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EDH	Enhanced Dispenser Hub
EFS	Encrypting File System
FD	Function Discovery
HID	Human Interface Devices
HTTP	Hypertext Transfer Protocol
HTTPS	Secure HTTP
ICS	Internet Connection Sharing
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
iSCSI	Internet SCSI
KEK	Key Encryption Key
KTM	Kernel Transaction Manager
LAN	Local Area Network
LPD	Line Printer Daemon
LPR	Line Printer Remote
LSA	Local Security Authority
MNSP	Managed Network Service Provider
MSDTC	Microsoft® Distributed Transaction Coordinator
MWS	Manager Workstation
NAP	Network Access Protection
NCD	Network Computing Device
NetBT	NetBIOS over TCP/IP

Term	Description
NFS	Network File System
NTFS	New Technology File System
PA-DSS	Payment Application Data Security Standard
PCA	Program Compatibility Assistant
PCI DSS	Payment Card Industry Data Security Standard
PnP	Plug and Play
PNRP	Peer Name Resolution Protocol
POS	Point of Sale
PSS	Platform Support Service
QoS	Quality-of-Service
qWave	Quality Windows® Audio Video Experience
RD	Remote Desktop
RDCS	Remote Desktop Configuration service
RIP	Routing Information Protocol
RPC	Remote Procedure Call
RSA	Rivest Shamir Adleman
SAM	Security Accounts Manager
SENS	System Event Notification Service
SFTP	Secure File Transfer Protocol
SMI	Security Manager Interface
SNMP	Simple Network Management Protocol
SSDP	Simple Services Discovery Protocol
SSTP	Secure Socket Tunneling Protocol
SZR	Secure Zone Router
TAPI	Telephony API
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UPnP	Universal PnP
URL	Uniform Resource Locator
VPN	Virtual Private Network
WIA	Windows Image Acquisition
WinRM	Windows Remote Management
WMI	Windows Management Instrumentation
WPAD	Web Proxy Auto-Discovery
WPF	Windows Presentation Foundation
WS-D	Web Services - Discovery
WSCSVC	Windows Security Center Service
WUA	Windows Update Agent
XML	EXtensible Markup Language

1.5 Common Terms

Term	Description
Admin, Administrative User, Admin User	Interchangeable references to users performing high-level Security Manager functions.
Cashier, User	Interchangeable references to any personnel using POS to perform sales.
Enhanced Dispenser Hub	The black box that contains the payment, network, forecourt control sub-systems, PIN Pad functions, and secure data from the Passport POS systems.
Merchant, Operator, Manager	Interchangeable references to any site personnel, such as owners, operators, or store managers, performing Passport management and setup functions of the EDH equipment with the Authorized Service Contractor (ASC).
Manager Workstation, MWS, Server, MWS/Server	Server where store and fuel setup/programming, maintenance, management functions, and report printings are performed.
Selected	Options that are enabled, active, activated, or checked (☑).
Cashier Workstation, CWS, Terminal, POS register	Interchangeable references to where sales and non-sales transactions are performed by a cashier.

1.6 Supported Hardware

The Passport PA-DSS certification was performed using Gilbarco® hardware and software. Failure to use Gilbarco hardware and software may invalidate the Passport system's PA-DSS compliance and can impact the merchant's overall PCI DSS compliance.

2 – System Security

2.1 Overview

The Security Manager application was created to enable overall management of security on the EDH. The merchant uses this application to manage access to the EDH as well as additional merchant-owned portions of the system's security.

Note: Security Manager provides access to sensitive information and must be used only by the merchant. The Username and Password are confidential information that only the merchant may possess. The ASC should not have access to this information. The merchant must enter the username and password and print the Security Manager Report as part of setup.

2.2 Setup Account Information

A single Admin account is available on the system. This account is available during installation and is as follows:

Username: Admin
Password: Admin

Before the system can be used to process payment transactions, it will force changing of the password to a strong password of this account. Further, selection of a strong password for the Admin account and all user accounts is enforced and maintained once system security is enabled.

It is the responsibility of the Merchant to assign the Admin password to a single individual, per PCI DSS requirements, as group or shared passwords are not allowed. For Merchants with more than one administrator, additional admin level users can be added as required.

Additional details on use of the Administrative User account are provided later in this manual.

2.3 Security Manager Login Process

Passport supports two methods of access to Security Manager:

- System Maintenance
- Support Console

For more information on these two methods, refer to "2.3.1 Accessing Security Manager via System Maintenance" on page 2-2 and "2.3.2 Accessing Security Manager via Support Console" on page 2-3.

2.3.1 Accessing Security Manager via System Maintenance

To access Security Manager via System Maintenance, proceed as follows:

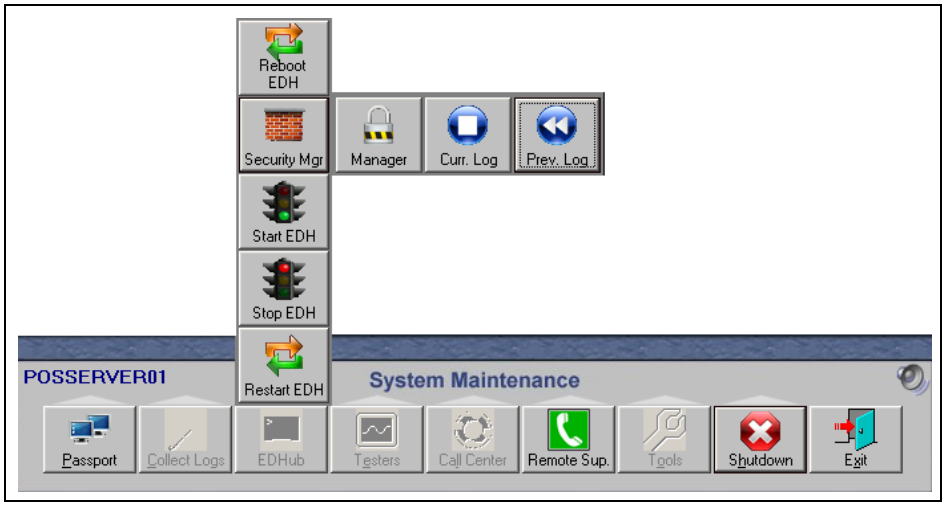
1 Press the **Ctrl**, **Alt**, and **P** keys on the Passport keyboard simultaneously. The System Maintenance login screen opens.

Figure 2-1: System Maintenance Login Screen

2 Enter **Gilbarco** in the User Name field.

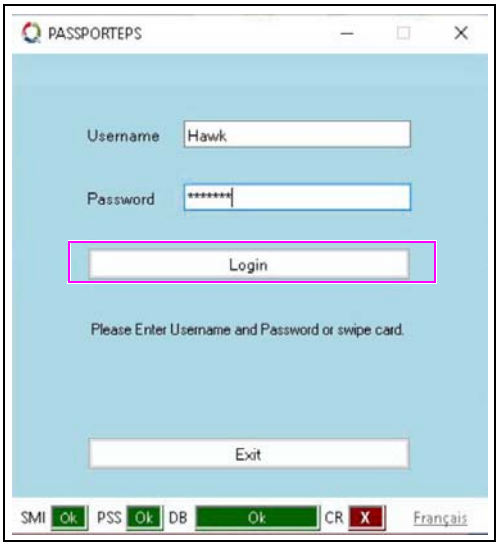
3 Enter **Passport** in the Password field. The System Maintenance toolbar appears.

Figure 2-2: EDH Menu



4 Navigate to **EDHub** > **Security Mgr** > **Manager**. The Security Manager Login window opens.

Figure 2-3: Security Manager Login Window

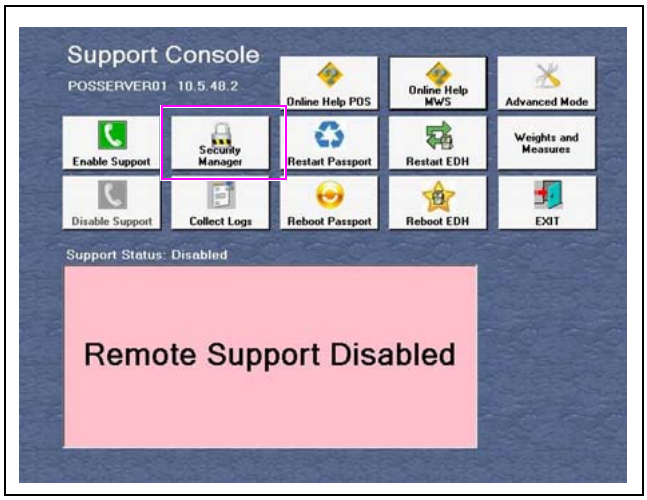


2.3.2 Accessing Security Manager via Support Console

Gilbarco added the Support Console to aid sites in accessing various support functions in Passport quickly and easily. The method used to access Support Console depends upon whether you are at the Manager Workstation (MWS) or the Cashier Workstation (CWS).

1 To access Support Console at the MWS, select the **Help** key in the upper right corner of the screen. To access Support Console at the CWS, at stores running Passport V20.03 or earlier, navigate to **More** > **More** > **Tools**, and then select **Support**. At stores running Passport V20.04 or later, select the Telephone icon at the top of the CWS screen.
The Support Console screen opens.

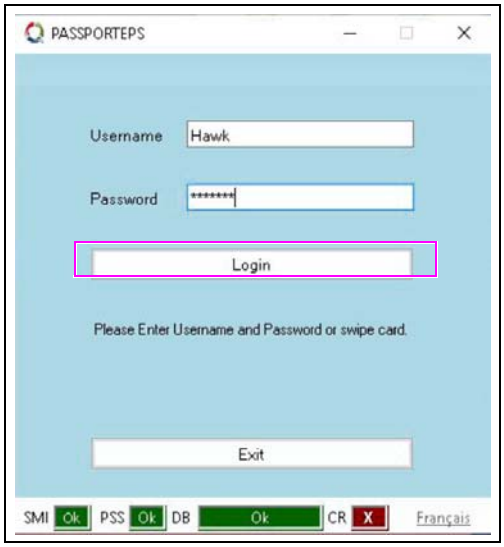
Figure 2-4: Support Console Menu



2 Select the **Security Manager** icon.

3 The Security Manager Login window opens.

Figure 2-5: Security Manager Login Window



2.3.3 Security Manager Login

Note: Security Manager logs each attempt to log into Security Manager (including unsuccessful attempts) into the security audit log.

On the Security Manager Login window, to access the EDH successfully:
- Security Manager Interface (SMI) status window must display **OK**.
- Platform Support Service (PSS) status window must display **OK**.
- Database (DB) status window must display **OK**.

To log into Security Manager, proceed as follows:

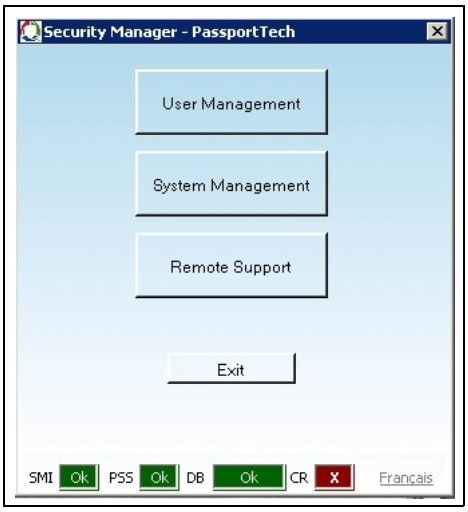
While connecting to the EDH, the key in the middle of the Security Manager Login window displays **Please wait - Connecting to EDH**. The user must wait until the key name changes to **Login** before entering details in the User Name and Password fields.

1 Enter a valid Username in the **Username** field.

2 Enter a valid Password in the **Password** field (see Figure 2-5).

3 Select **Login**. The Security Manager - Admin window opens.

Figure 2-6: Security Manager - Admin Window



2.4 Using Security Manager

Security Manager displays a series of windows and prompts to guide the user through a selected function.

Note: The figures provided in this section are examples only.

2.4.1 Entry Error

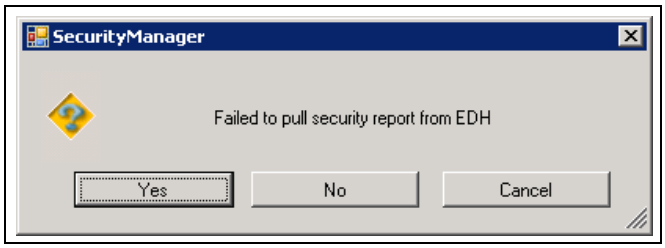
Any errors or instructions for an incorrect entry, or entry that Security Manager cannot validate, display in red on the Security Manager window.

Figure 2-7: Entry Error Example

2.4.2 Process Error

The following error message box opens for a failed process or procedure. Click **Yes** to clear the error.

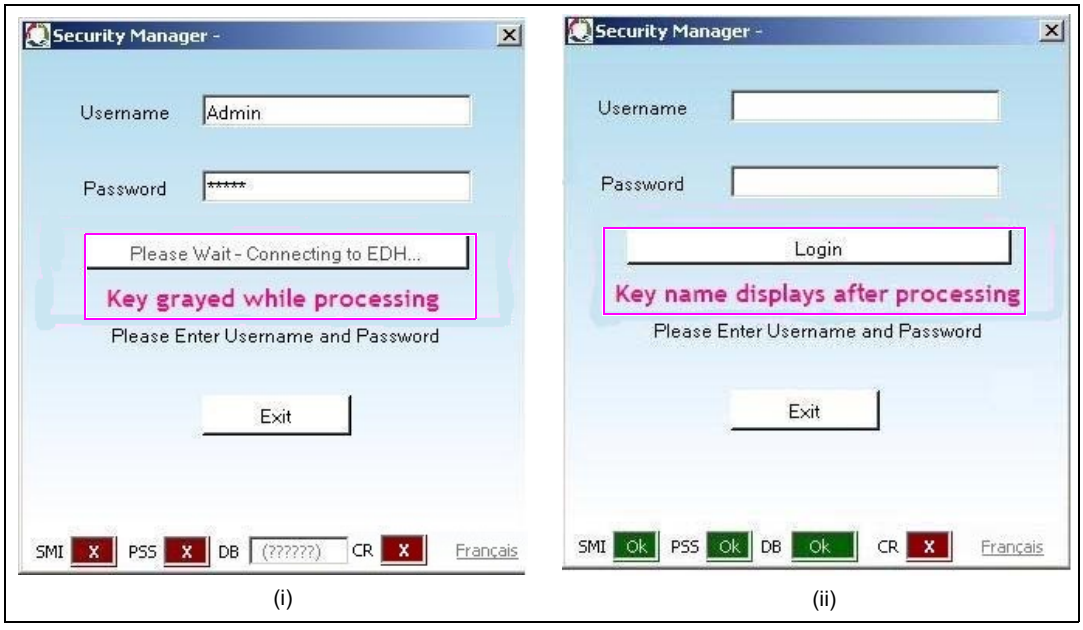
Figure 2-8: Process Error Example



2.4.3 System Working

After an entry is made or a process is started, some keys or areas of the window may be grayed out while the system is processing. The user must wait until the process is complete. The grayed areas display clearly when they become active and ready for the user's next entry or to continue the process being performed.

Figure 2-9: System Working Examples

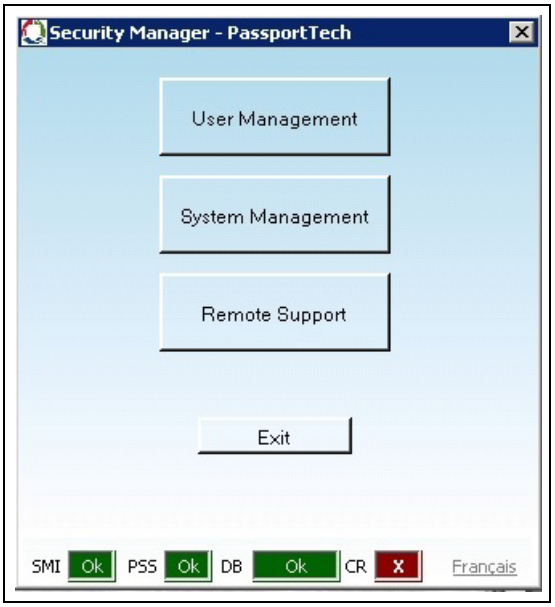


2.4.4 Main Security Manager Window

Security Manager has three main functions:

- User Management
- System Management
- Remote Support

Figure 2-10: Main Security Manager Window



The sections that follow describe each of these functions in detail.

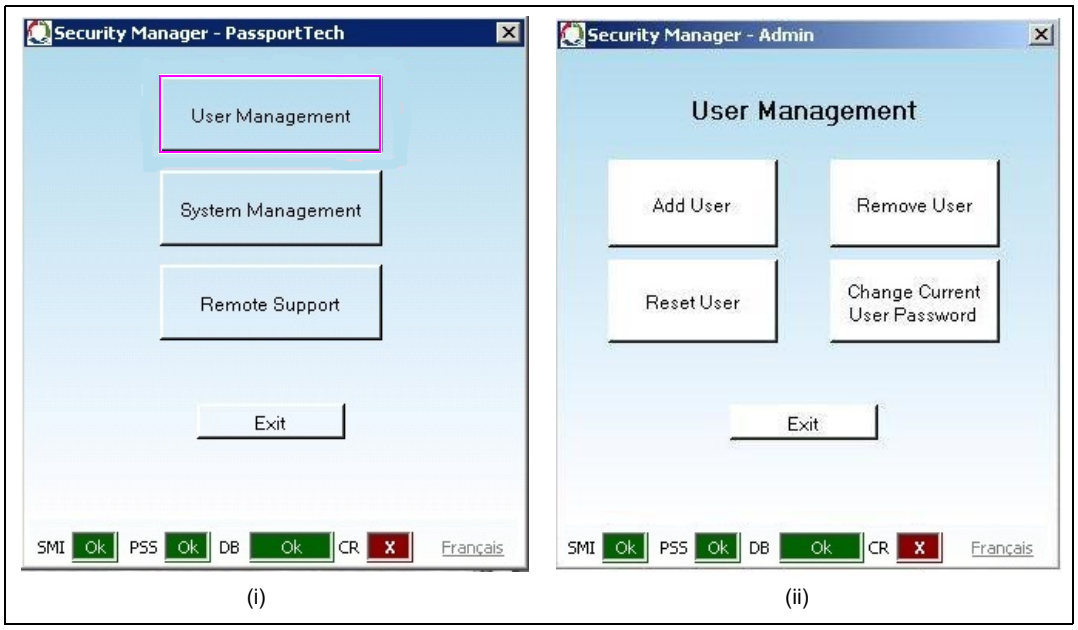
This page is intentionally left blank.

3 – User Names and Passwords

3.1 User Management

The merchant is responsible for managing User Names and Passwords on all systems within the merchant's network. This section describes how the User Management functions within Security Manager can be used to manage access to the EDH. Additionally, some best practices are included on how User Names and Passwords should be managed on any devices connected to the merchant network.

Figure 3-1: User Management



Four basic functions are provided for managing User Names and Passwords. All functions are available to users with Administrator access. Only the **Change Current User Password** function is available to non-Administrator users. If a User Name with user-level access selects any of the other functions, the following error message displays, in **red** letters, centered between the bottom row of keys and the **Exit** key:

Unauthorized User - Access Denied

Selecting the **Exit** key returns the user to the main Security Manager window.

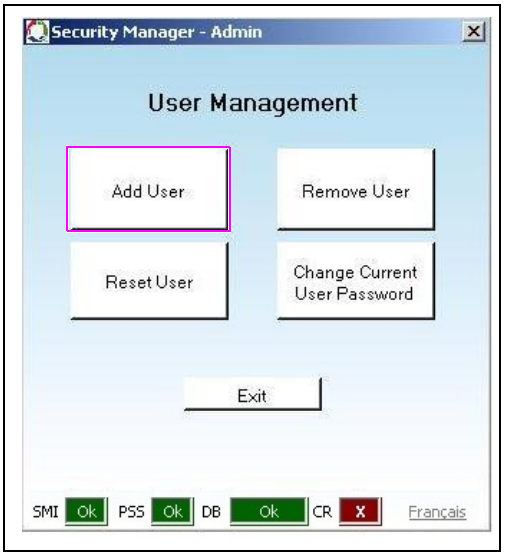
3.1.1 Adding a User

To add a new user to Security Manager, proceed as follows:

1 From the Security Manager main window, select **User Management**. The User Management window opens.

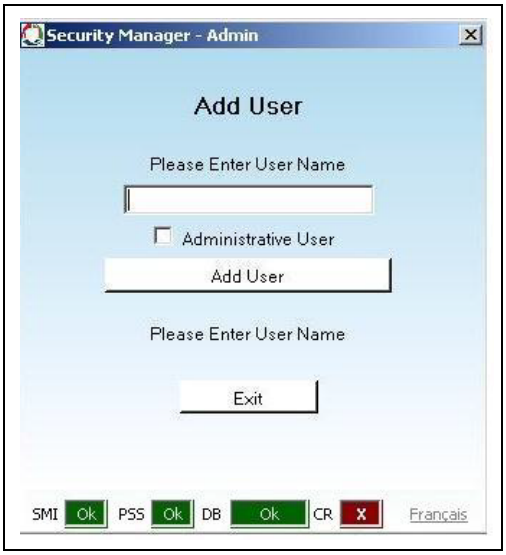
*Note: The **Add User** function can be accessed only by an Administrator-level user.*

Figure 3-2: User Management - Add User



2 From the User Management window, click **Add User**. The Add User window opens.

Figure 3-3: Add User



3 Enter the new **User Name**.

4 Select the **Administrative User** check box if the user is to be assigned as an Administrator. An Administrator-level user has access to all Security Manager functions.
Notes: 1) User Name is an alphanumeric field with minimum of seven and maximum of 20 characters.
*2) The **Administrative User** check box is cleared by default.*

3 Select **Add User**. The initial password is the value keyed in the **User Name** field and must be changed by the new user the first time the new user logs into Security Manager. This can be done by selecting the **Change Current User Password** function.

IMPORTANT INFORMATION

- A User Name cannot be added if it already exists. If an attempt is made to add an already existing User Name, Security Manager displays the error message: **"Error - User Name Already Exists."**
- Users can be added only when the system is secure (security-enabled). If an attempt is made to add a user before the system is secure, Security Manager displays the error message: **"Error - It is required that the system be Hardened (Security Enabled) in order to add more users."**
- Security Manager logs an entry in the Security Audit Log when a User Name is added. The log entry includes the following information:
  - User Name that added the new user
  - User Name added and notation if Administrative User was selected
  - Date/Time
  - Terminal at which the new user was added
- A unique User Name must be assigned to each user. Group User Names are not permitted under PCI DSS.
- For more information on managing User accounts, refer to "3.2 User Name and Password Best Practices" on page 3-9.

3.1.2 Removing a User

Removing a User Name immediately disables the user's access to Security Manager.
Note: Only an Administrator-level user can access the Remove User function.

To remove a user, proceed as follows:

1 From the Security Manager main window, select **User Management**. The User Management window opens.

Figure 3-4: User Management - Remove User

2 From the User Management window, select **Remove User**. The Remove User window opens.

Figure 3-5: Remove User

3 Enter the **User Name**.

4 Select **Remove User**.

IMPORTANT INFORMATION
• Security Manager logs an entry to the Security Audit Log when a User Name is removed. The log entry includes the following information: - User Name that removed the user - User Name removed - Date/Time - Terminal at which the user was removed • A User Name cannot be removed if it does not exist. If an attempt is made to remove a User Name that does not exist, Security Manager displays the error message: **"Error - User Name Does Not Exist."** • The merchant must manage User Name removals in accordance with PCI DSS. • For more information on managing User accounts, refer to "3.2 User Name and Password Best Practices" on page 3-9.

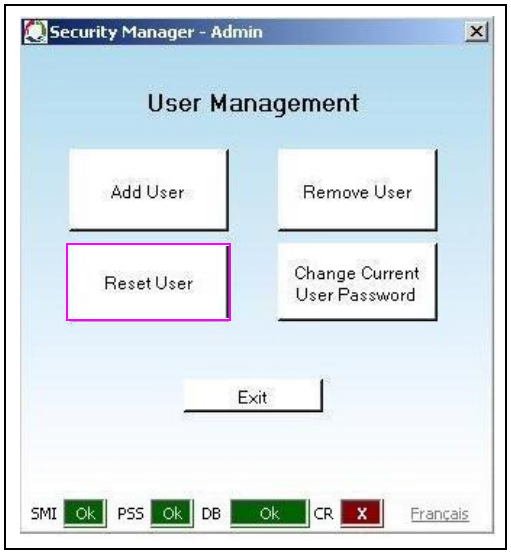
3.1.3 Resetting a User

The Reset User function is used when a user forgets his password and needs to create a new one.
Note: Only an Administrator-level user may access the Reset User function.

To reset a user password, proceed as follows:

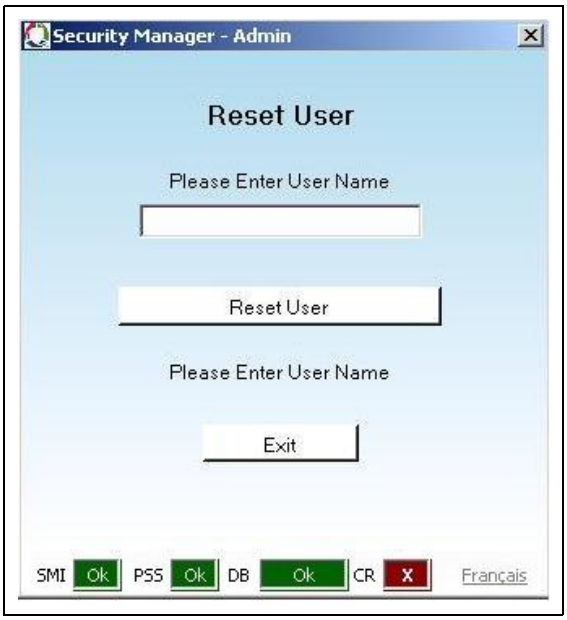
1 From the Security Manager main window, select **User Management**. The User Management window opens.

Figure 3-6: User Management - Reset User



2 From the User Management window, select **Reset User**. The Reset User window opens.

Figure 3-7: Reset User



3 Enter the **User Name**.

4 Select **Reset User**. Security Manager resets the user's password to the User Name. The user must select the **Change Current User Password** function at the next Security Manager login.

IMPORTANT INFORMATION

- Security Manager adds an entry to the Security Audit Log when a User Name is reset. The log entry includes the following information:
  - User Name that reset the user
  - User Name reset
  - Date/Time
  - Terminal at which the user was reset
- The Admin user is protected and cannot be reset.
- A User Name password cannot be reset if the User Name does not exist. If an attempt is made to reset the password of a User Name that does not exist, Security Manager displays the error message: **"Error - User Name Does Not Exist."**
- The merchant must manage User Name removals in accordance with PCI DSS.
- For more information on managing User accounts, refer to "3.2 User Name and Password Best Practices" on page 3-9.

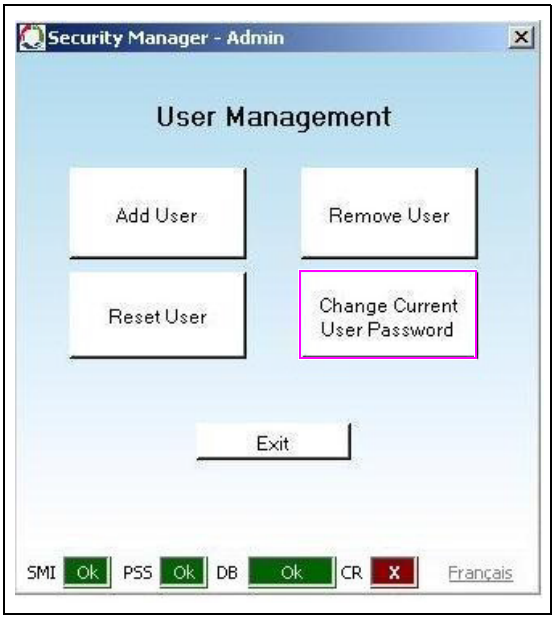
3.1.4 Changing the Current User Password

The Change Current User Password function is used to allow the user to update the password after adding a new user or resetting the password.
Note: The new password must not match any of the previous four passwords for that user.

To change the password of the user currently logged onto Security Manager, proceed as follows:

1 From the Security Manager main window, select **User Management**. The User Management window opens.

Figure 3-8: User Management - Change Current User Password



2 From the User Management window, select **Change Current User Password**. The Change Password window opens.

Figure 3-9: Change Password

3 Enter the new password in the **Enter New Password** field. Security Manager masks each user keystroke with *.

4 Enter the new password again in the **Re-Enter Password** field. Security Manager masks each user keystroke with *.

5 Select **Change Password**.

IMPORTANT INFORMATION

- The values the user keys in the **Enter New Password** and **Re-Enter Password** fields must match. If they do not, Security Manager displays the error message: **"Error - Passwords do not match."**
- The new password must not match any of the previous four passwords for that user. If the new password does match one of the previous four passwords, Security Manager displays the error: **"Error: Changing user password failed. Most likely this is because the new password matched the current password or the last one used."**
- The new password must be at least seven characters in length and contain at least one digit. Security Manager accepts special characters, as well.
- Security Manager adds an entry to the Security Audit Log when a user's password is changed. The log entry includes the following information:
  - User Name that changed the password
  - Date/Time
  - Terminal at which the password was changed
- The merchant must manage passwords in accordance with PCI DSS.
- For more information on managing User accounts, refer to "3.2 User Name and Password Best Practices" on page 3-9.

3.1.5 Password Expiration and Invalid Login

All passwords will expire after 90 days. Users attempting to log into Security Manager after the 90-day period, will be allowed to login; however, the only function that is permitted is **Change User Password.**

Entry of six consecutive invalid passwords will result in the user account being locked for 30 minutes. After the 30-minute lockout period, the user may attempt to login again.

3.2 User Name and Password Best Practices

The following are best practices for using and managing Usernames and Passwords:

- Merchants must not use Administrator-level usernames and passwords for payment application login IDs. (For example, do not use the "sa" account for payment application access to the database.).
- Merchants must assign secure authentication to default Username and Password accounts, disabled or not used. This secure authentication practice applies even if the default accounts will not be used.

3.2.1 PCI DSS Requirements

The PCI DSS requirements for managing User Names and Passwords are listed in this section.

These requirements apply to Security Manager and other devices connected to the merchant network, including the Passport MWS/Server, BOS, Loyalty systems, etc. Failure to maintain compliant settings for User Names and Passwords may result in PCI DSS non-compliance.

Requirement
Assign all users a unique User Name before allowing them access to the system.
For authentication purposes, use either a unique 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 a password reset.
Set first-time passwords to a unique value and require them to be changed after the first use.
Immediately revoke access for a terminated user.
Remove or disable inactive user accounts at least every 90 days.
Communicate password procedures and policies to all users who have access to cardholder 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 passwords containing both numeric and alphabetic characters.
Do not allow an individual to submit a new password that is the same as any of the last four previously used passwords.

This page is intentionally left blank.

4 – Reports and Data Retention

4.1 Overview

According to PCI DSS requirements, all reports that display or print unmasked customer account number information must be secured properly both on the EDH and in paper form after printing. Customer account information is stored and secured in encrypted form in a database on the EDH. The EDH provides the ability to generate Secure Reports for the merchant to use for transaction reconciliation. The merchant can configure the amount of time this data is retained.

This section provides information on how to retrieve and print Secure Reports.

4.2 Secure Report Password

To retrieve or print secure report information from the EDH, select **Secure Report** from the **Reports** menu on the Passport MWS and enter the Secure Report Password when prompted. The Secure Report Password is configured within the System Management function of Security Manager.

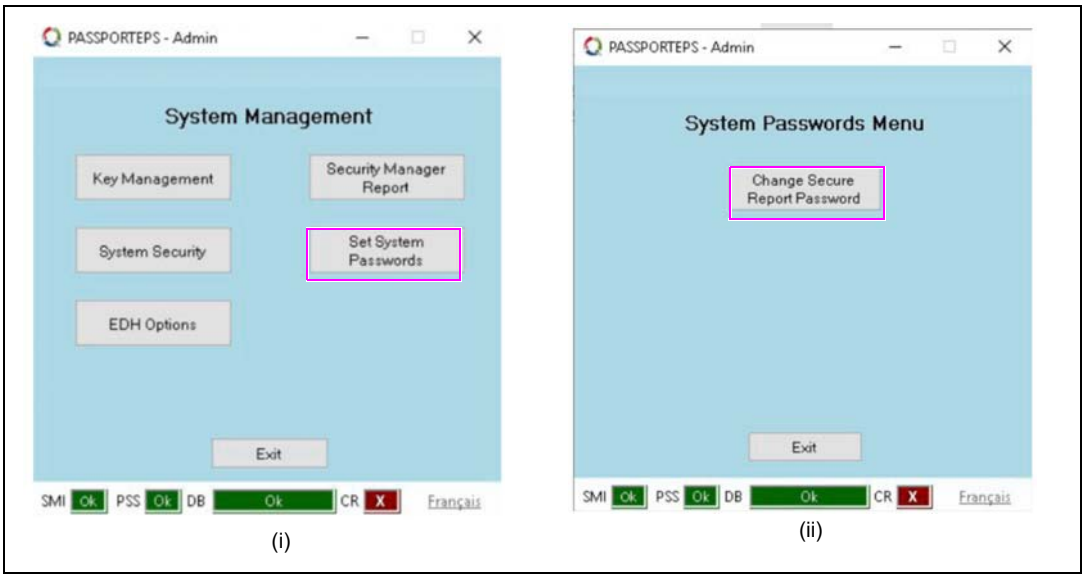
IMPORTANT INFORMATION
The default Secure Report Password during installation is **PDFPassword**. During installation of the EDH, the merchant must select a new Secure Report Password.

4.2.1 Setting the Secure Report Password

To set the Secure Report Password, proceed as follows:

1 From the Security Manager main window, select **System Management > Set System Passwords**. The System Passwords Menu window opens.
Note: Only an Administrator-level user can access Secure Report Password.

Figure 4-1: System Management Window



2 Select **Change Secure Report Password**. The Change Secure Report Password window opens.

Figure 4-2: Change Secure Report Password Window

3 Enter the new password in the **Enter New Password** field. Security Manager masks each user keystroke with *.

4 Enter the new password again in the **Re-Enter Password** field. Security Manager masks each user keystroke with *.

5 Select **Change Password**. Security Manager validates the new password and returns to the System Management screen.

IMPORTANT INFORMATION

- The values that user enters in the **Enter New Password** and **Re-Enter Password** fields must match. If they do not, Security Manager displays the error message: **"Error - Passwords do not match."**
- The new password must be at least seven characters in length and contain at least one digit. Security Manager accepts special characters, as well.
- Security Manager adds an entry to the Security Audit Log when a user's password is changed. The log entry includes the following information:
  - User Name that changed the password, along with indication if the user is an Administrator-level user
  - Date/Time
  - Terminal at which the password was changed
- The merchant must manage passwords in accordance with PCI DSS.
- For more information on managing user accounts, refer to "3.2 User Name and Password Best Practices" on page 3-9.

4.2.2 Retrieving Secure Reports

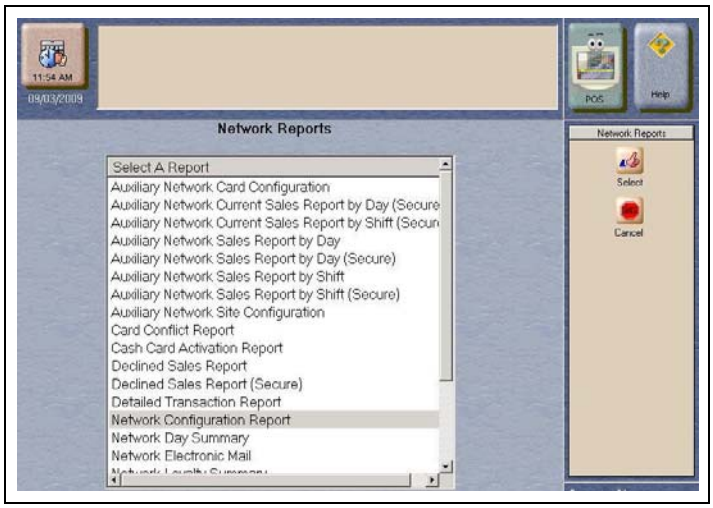
PCI DSS allows for the secured printing of unmasked account number information only in cases where needed for business purposes. Passport displays secure versions of network reports with "(Secure)" appended to the report name in **MWS** > **Reports** > **Network**.

The requirements for each payment network are different; therefore, the list of network reports approved to print vary by payment network. Refer to the relevant Network Addendum for a description of specific secure reports supported by Passport.

To retrieve a secure report, proceed as follows:

1 From the MWS main menu, navigate to **Reports** > **Network**. The Network Reports window opens.

Figure 4-3: Network Reports



Note: Passport displays secure reports in the Network Reports menu list, denoted by "(Secure)" appended to the report name.

2 Select the secure report and click **Select** displayed in the right side bar of the Network Reports window. The Period Selection screen opens.

3 Select the reporting period and click either **Print Preview** or **Print**. The Password entry dialog box opens with a prompt to enter a Document Open Password.

Figure 4-4: Password Entry Prompt

4 Enter the Secure Report Password in the **Enter Password** field.

5 Click **OK** to view or print the report or click **Cancel** to terminate the process and remove the Password entry dialog box.

IMPORTANT INFORMATION
Security Manager allows the user up to three attempts to enter the correct password. If the user enters the correct password, the report displays (**Print Preview** key selected) or prints (**Print** key selected); otherwise, Security Manager denies access to the report. For more information on Passport Reports, refer to the relevant Network Addendum.

4.3 Data Retention

The merchant is responsible for determining how long the EDH retains Secure Report information, as well as managing printed versions of secure reports in accordance with PCI DSS requirements. Per PCI DSS requirements, the merchant must:

- Keep cardholder data storage to a minimum
- Develop a data retention and disposal policy
- Limit storage volume and retention period to that required for business, legal, and regulatory purposes
- Data that is no longer needed must be securely deleted:
  - Data managed by the Passport system will be securely deleted automatically based on configured retention policies and Payment Host processing rules. If manual secure deletion is required, refer to "7.6.2 Secure Delete Tool" on page 7-19 for instructions.
  - Printed data must be disposed of in accordance with PCI DSS requirements.

These requirements apply to data retained on the EDH database and printed on secure reports. After the merchant determines the necessary data retention period, the period may be configured on the Passport MWS.

Note: Some payment networks mandate specific data retention periods, which are not configurable by the merchant. For more information on configuring retention periods, refer to the relevant Network Addendum.

This page is intentionally left blank.

5 – Remote Access to the EDH

5.1 Overview

PCI DSS has specific requirements for remote access into the merchant's network environment. This section describes the general requirements along with the specific requirements for accessing the EDH.

IMPORTANT INFORMATION

- If the nature of the support activity requires that the merchant provide the PassportTech or PassportServices password information over the phone, confirm that a support call was initiated from the merchant to Gilbarco. This password information must never be given over the phone if the call originated from somewhere other than the merchant.
- If the password information is provided, System Security must be rolled to ensure new passwords are generated. Refer to the Roll Security option detailed in "7.3.3 System Security" on page 7-5.

5.1.1 General Requirements

A merchant must:

- Incorporate two-factor authentication for remote access into the network environment.
  - Methods supported, but not limited to, include Virtual Private Network (VPN) and Rivest Shamir Adleman (RSA) Token.
  - No Merchant configuration is required to enable support for two-factor authentication.
- Enable vendor access only when required and disable access when no longer needed per PCI DSS.
- Utilize user name and password best practices when managing remote access accounts per PCI DSS, ensuring all users have a unique Username and Password; for more information, refer to the "3.2 User Name and Password Best Practices" on page 3-9.
- Implement appropriate firewall equipment to ensure security of the merchant network. PCI DSS mandates encryption of all remote connections. The following are examples of remote access security features:
  - Change default settings in the remote access software. For example, change default passwords and use unique passwords for each customer.
  - Allow connections only from specific (known) IP/MAC addresses.
  - Use strong authentication and complex passwords for login IDs, per PCI DSS.
  - Enable encrypted data transmission per PCI DSS requirements.
  - Enable account lockout after a certain number of unsuccessful login attempts per PCI DSS requirements.
  - Configure the system to enable a remote user to establish a VPN connection through a firewall before access is allowed.
  - Enable the login function.
  - Restrict access to customer passwords to authorized reseller/integrator personnel.
  - Establish customer passwords according to PCI DSS requirements.

5.2 Enabling Remote Access to the EDH

Remote access to the EDH is provided from within the merchant network from either the Passport MWS or Server or over a secured connection the merchant makes available. Passport does not allow enabling remote access to the EDH through the CWS.

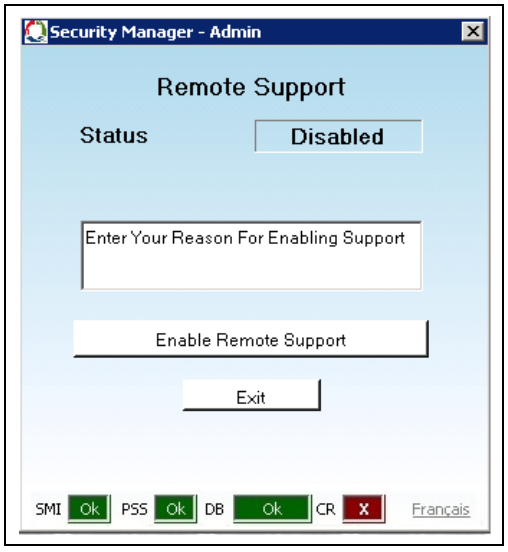
IMPORTANT INFORMATION
Direct remote access to the EDH from outside the merchant network is not supported and, if configured, could violate the merchant's PCI DSS compliance.

Remote access to the EDH is enabled through Security Manager by using System Maintenance or Support Console. For information on accessing Security Manager, refer to "2-System Security" on page 2-1.

To enable remote access to the EDH, proceed as follows:

1 From the Security Manager main window, select **Remote Support**. The Security Manager Remote Support window opens.

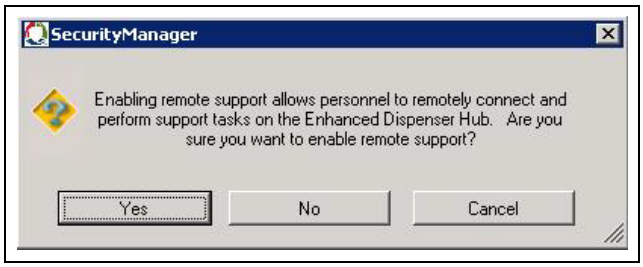
Figure 5-1: Remote Support Window



Note that the **Status** field is set to Disabled.

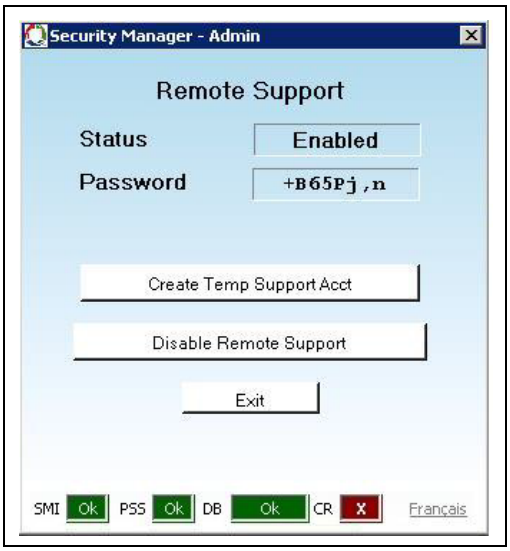
2 Enter text describing the reason for enabling Remote Support into the text box below the **Status** field and then select **Enable Remote Support**. A warning message is displayed.

Figure 5-2: Remote Support Warning Message



3 Perform one of the following:
- To discontinue enabling Remote Support, select **No** or **Cancel**. The Remote Support window continues to display Disabled in the **Status** field. Selecting **Exit** causes the Remote Support window to close and the Security Manager main window to display. Selecting **Exit** again causes the Security Manager main window to close.
- To enable Remote Support, select **Yes**. Security Manager changes the **Status** field to Enabled and generates a temporary password (displayed in the **Password** field) if the user has Administrator-level credentials.

Figure 5-3: Remote Support Enabled



IMPORTANT INFORMATION

- To prevent unauthorized access to the EDH, the merchant must know the person requesting a temporary password for remote access and why remote access is necessary before creating a temporary support account.
- Security Manager logs an entry in the Security Audit Log each time Remote Support is enabled or disabled.
- In the event a user forgets to disable Remote Support, Security Manager automatically disables Remote Support after being enabled for more than 24 hours.

4 To create a Temporary Support Account, select **Create Temp Support Acct.** Security Manager generates and displays a temporary password in the Password field. Technical support uses this password to access the EDH remotely for dial-in support.

Figure 5-4: Password Created for Remote Support

5.3 Disabling Remote Access to the EDH

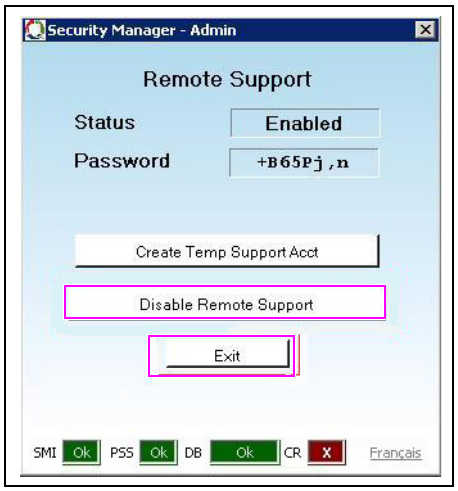
After the Gilbarco Call Center or Technical Support personnel confirm that Remote Support is no longer required, the merchant can disable Remote Support to the EDH.

To disable Remote Support, proceed as follows:

1 Log into **Security Manager**. Refer to "2.3 Security Manager Login Process" on page 2-1.

2 Select **Remote Support**. The Remote Support window opens.

Figure 5-5: Disable Remote Support



Note that the **Status** field is set to Enabled.

3 Select **Disable Remote Support**. When Security Manager disables Remote Support, the **Status** field changes to Disabled.

4 Select **Exit**. The Security Manager main window opens.

5 Select **Exit** to close the Security Manager window.

5.4 Enabling Remote Support from the CWS

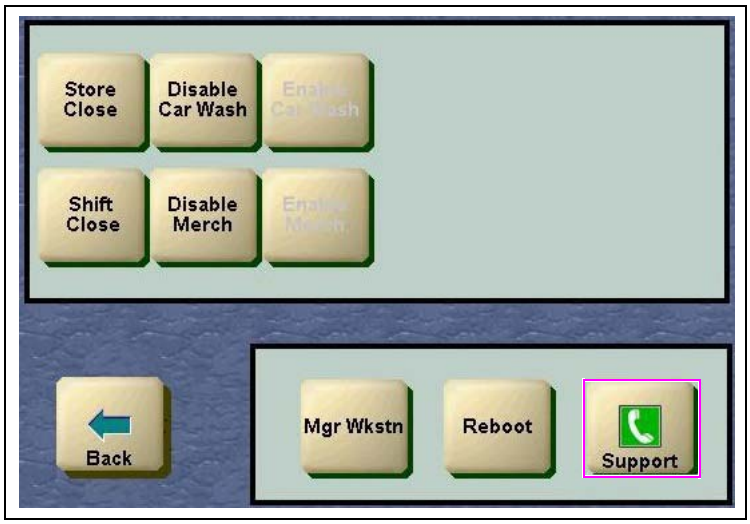
The Remote Support tool allows a cashier, without a keyboard to perform the **Ctrl, Alt,** and **P** key sequence, to enable remote support for a Gilbarco Call Center or Technical Support agent to access the Passport system.

Note: This function must be accessed only when instructed by a Gilbarco Call Center or Technical Support agent.

To access Remote Support from the CWS, proceed as follows:

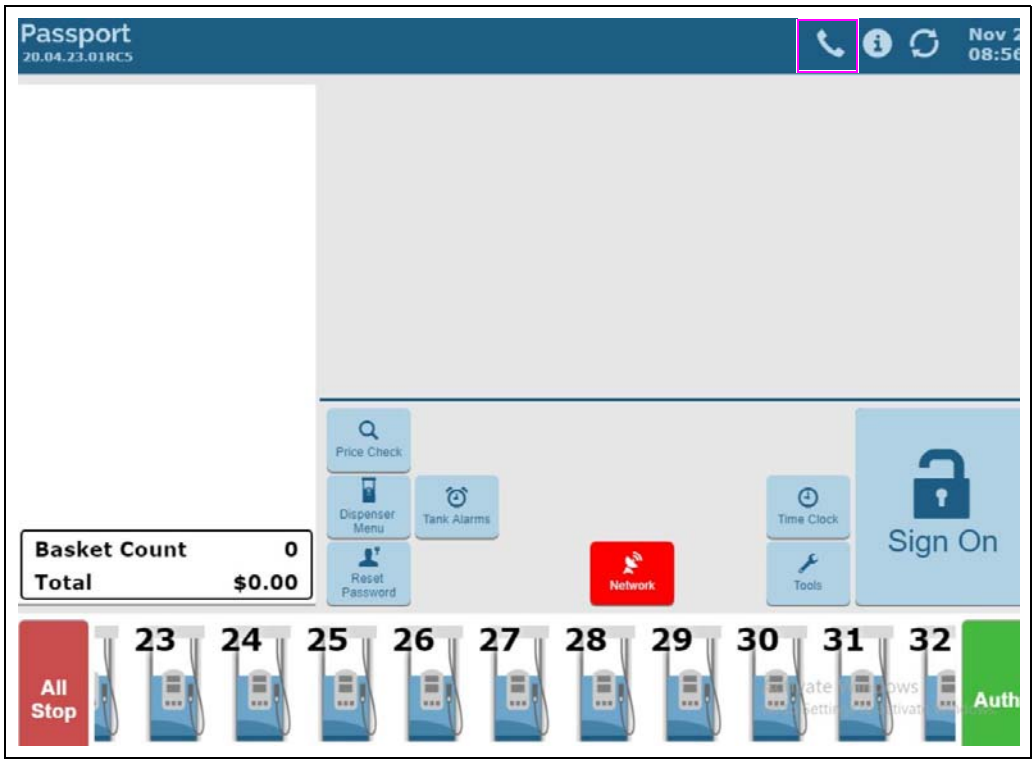
1 At sites running Passport V20.03 or earlier, from the CWS idle screen, navigate to **More** > **More** > **Tools** and select **Support**.

Figure 5-6: Tools Window



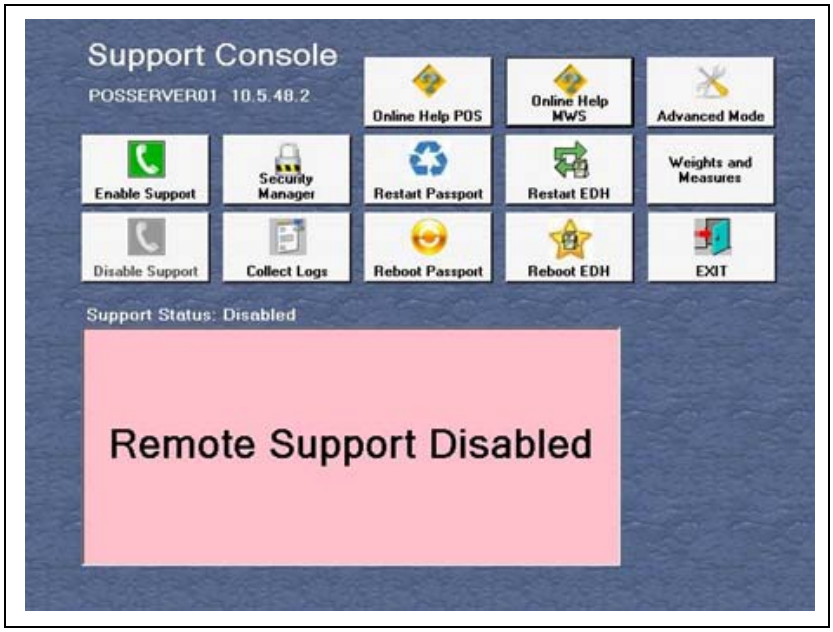
At sites running Passport V20.04 or later, select the **Telephone** icon at the top of the CWS screen.

Figure 5-7: Telephone Icon on CWS Screen



The Support Console screen opens with **Remote Support Disabled** displayed at the bottom.

Figure 5-8: Support Console - Remote Support Disabled



2 Select **Enable Support**. When remote support is enabled, the **Enable Support** key changes to "Extend Support" to allow the site to extend the amount of time that remote support will be enabled, and the **Disable Support** key turns red indicating the Passport system is ready for remote access. Gilbarco Call Center or Technical Support personnel may access the Passport system (see Figure 5-9 and Figure 5-10).

Figure 5-9: Support Console - Remote Support Enabled

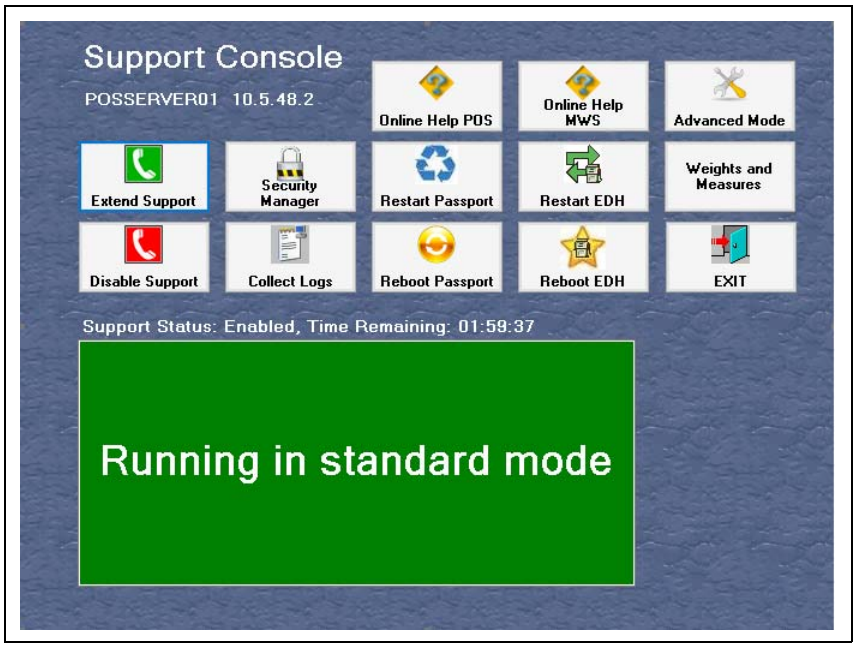
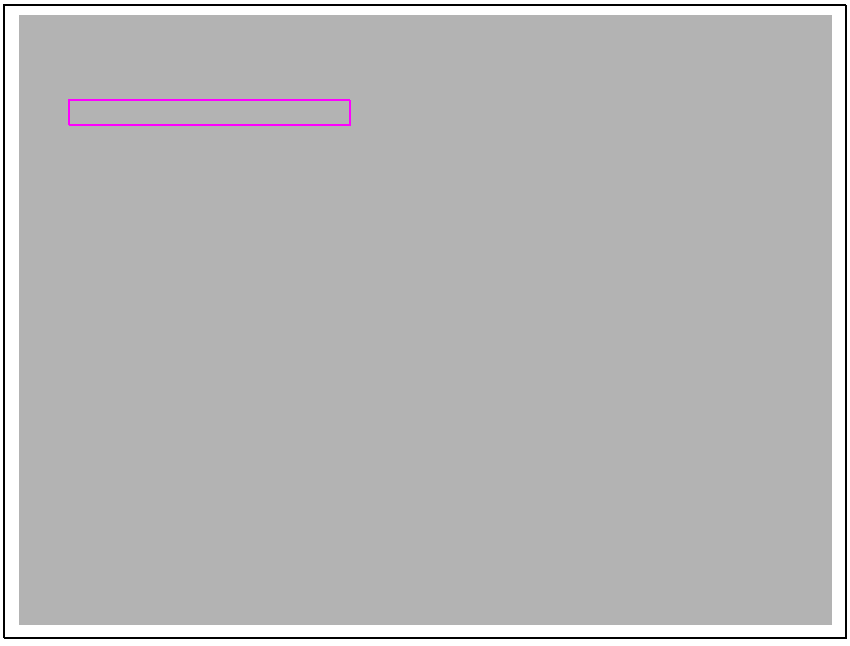


Figure 5-10: Support Console - Remote Support Enabled - Secure Zone Router (SZR)



3 When the Gilbarco Call Center or Technical Support agent completes the work, select **Disable Support** and then select **Exit**.

5.5 Extend Secure Remote Access

The merchant can configure the Passport system to extend secure remote access to the Help Desk at all times, thereby eliminating the need to have site personnel select the Enable Support button to enable remote access.

IMPORTANT INFORMATION
When configured, the PCI DSS requirement to enable/disable remote support as required is no longer enforced by the Passport system and must be handled as part of the broader Merchant network controls.

To configure this option, proceed as follows:

1 From the MWS main screen, select **Set Up > Store > Store Options**.

2 Select the **Password** tab (see Figure 5-11 on page 5-9).

3 Select **Extend Secure Remote Access for Helpdesk at all times**.

4 Restart the MWS/CWS to make Extend Secure Remote Access configuration active.

*Note: When Passport is configured to **Extend Secure Remote Access for Helpdesk at all times** and **Enable Enhanced Remote Support Passwords** is not selected:*
*1) Selecting **Enable Support** at sites using a non-Acumera Managed Network Service Provider (MNSP) is not required.*
*2) For Gilbarco access to Acumera sites, selecting **Enable Support** is required to build the remote access tunnel.*

5.6 Enhanced Remote Support Passwords

For new installations and systems being upgraded from versions prior to Passport V11.02, support for Enhanced Remote Support Passwords is available.

This section describes how to configure Passport to use the enhanced remote support passwords and how a Gilbarco Call Center or Technical Support agent interacts with personnel at the store.

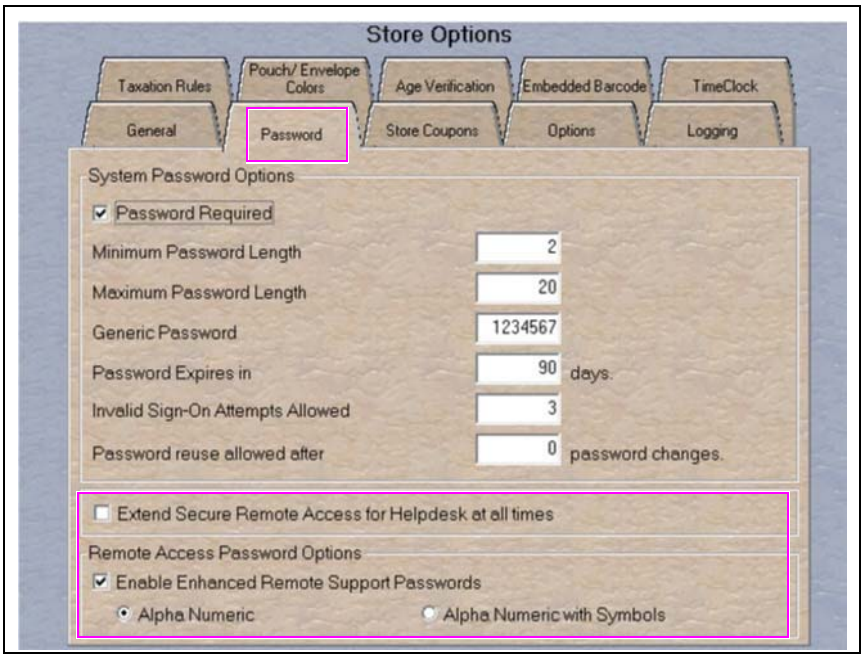
5.6.1 Configuring Passport to Enable Remote Support Passwords

To enable enhanced remote support passwords, proceed as follows:

1 From the MWS main screen, navigate to **Set Up** > **Store** > **Store Options**. The Store Options configuration screen opens.

2 Select the **Password** tab.

Figure 5-11: Store Options - Password Tab



3 In the Remote Access Password Options, select **Enable Enhanced Remote Support Passwords**. Passport automatically enables the Alpha Numeric radio button. The following table contains the Remote Access Password Options fields and their descriptions:

Field	Description
Enable Enhanced Remote Support Passwords	Checkbox; when checked, Passport generates strong unique passwords for remote access to the Passport system.
Alpha Numeric	When enabled, Passport generates Remote Support passwords containing letters and numbers. Accessible only after **Enable Enhanced Remote Support Passwords** field is enabled. Default when **Enable Enhanced Remote Support Passwords** field is enabled. This setting causes Passport to generate an 8-character strong alpha numeric remote support password.
Alpha Numeric with Symbols	When enabled, Passport generates Remote Support passwords containing letters, numbers, and symbols. Symbols set includes the following: ! @ # $ % ^ &

4 Select **Save** to save all Store Options and exit.

5.6.2 Using Support Console with Enhanced Remote Support Passwords Enabled

After enabling enhanced remote support password options, the Support Console screen starts using the options as configured in the **MWS** > **Set Up** > **Store** > **Store Options** > **Password** tab.

The Support Console screen contains a Remote Support section. By default, remote support is disabled.

Figure 5-12: Support Console Screen - Remote Support Disabled

If **Enable Enhanced Remote Support Passwords** is set, when the Passport user selects **Enable Support**, the Support Console screen opens with remote support in enhanced mode. The content of the Support Console screen depends upon the configuration saved in the **MWS** > **Set Up** > **Store** > **Store Options** > **Password** tab.

Figure 5-13 and Figure 5-14 illustrate the Support Console screen contents if the Alpha Numeric option is set.

Figure 5-13: Enhanced Remote Support - Alpha Numeric Mode

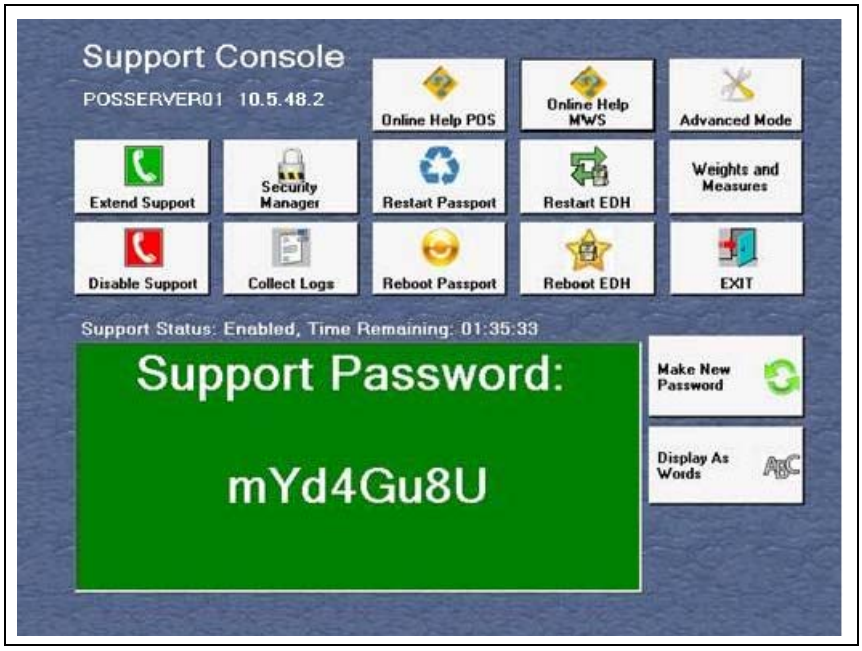
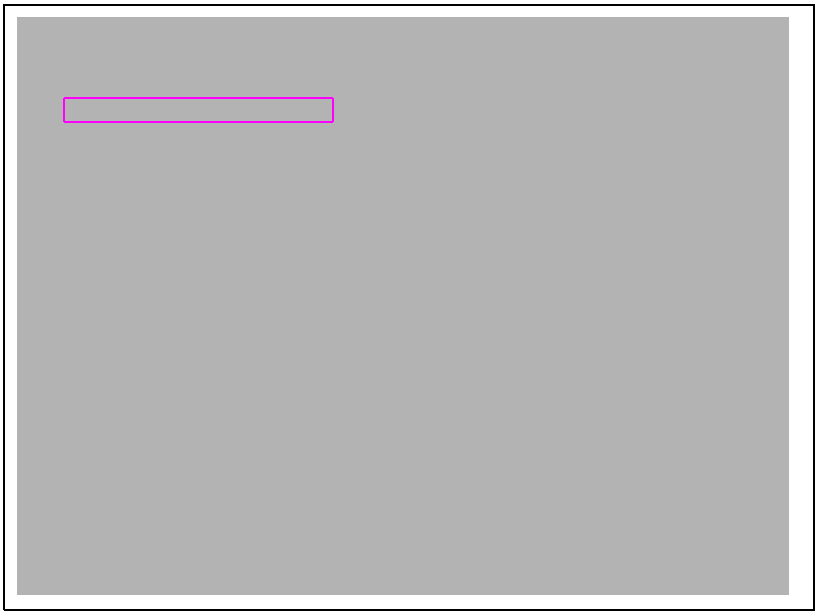


Figure 5-14: Enhanced Remote Support - Alpha Numeric Mode with SZR



In Alpha Numeric and Alpha Numeric with Symbols modes, the Support Console screen displays the 8-character support password, the amount of time that remote support will remain enabled, as well as the **Make New Password** and **Display As Words** keys. The **Make New Password** key allows the Passport user to generate a different remote support password, which may be helpful if the user and the Gilbarco Call Center or Technical Support agent are having difficulty communicating the current remote support password. The **Display As Words** key causes the remote support password to be displayed in words that the Passport user can read to the Gilbarco Call Center or Technical Support agent, making it easier to communicate the remote support password.

Figure 5-15 and Figure 5-16 illustrate the remote support password displayed as words.

Figure 5-15: Enhanced Remote Support Password Displayed as Words (Alpha Numeric)

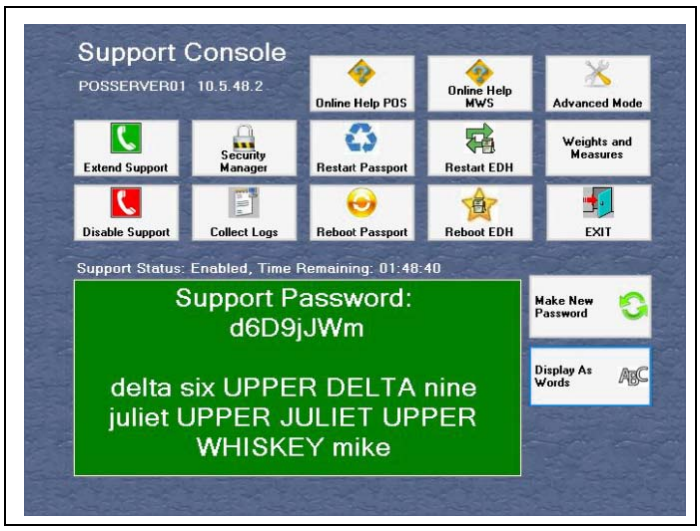
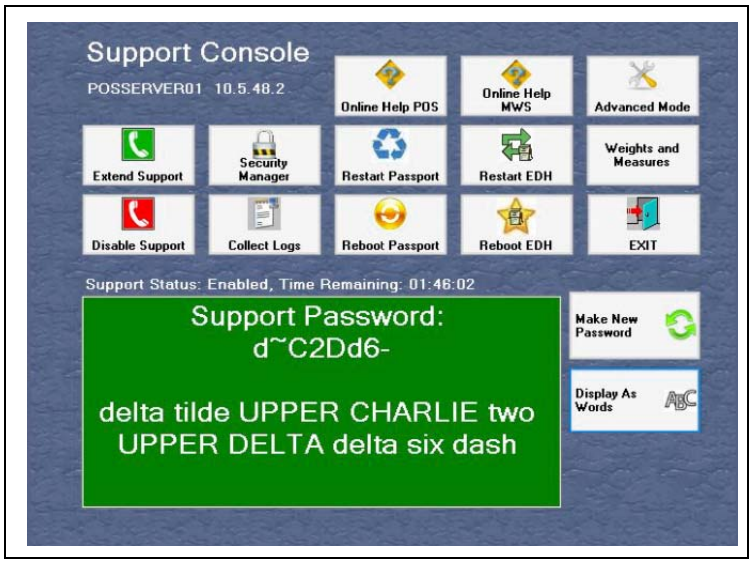


Figure 5-16: Enhanced Remote Support Password Displayed as Words (Alpha Numeric with Symbols)



5.6.3 Using System Maintenance with Enhanced Remote Support Passwords Enabled

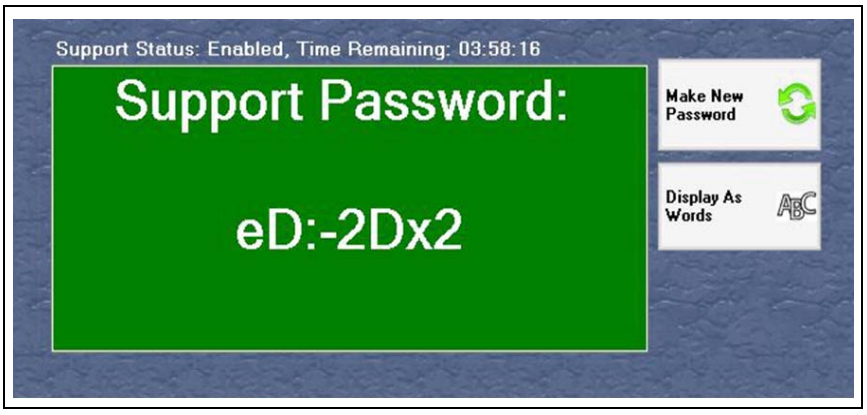
After enabling enhanced remote support password options, the System Maintenance bar begins using the options as configured in the **MWS** > **Set Up** > **Store** > **Store Options** > **Password** tab. When the Passport user selects **Remote Sup.** from the System Maintenance bar, the remote support options appear on the System Maintenance bar similar to their appearance on the Support Console.

If **Enable Enhanced Remote Support Passwords** is not set, when the Passport user selects **Remote Sup**., the password screen does not appear on the System Maintenance bar and the bar indicates standard mode is running.

Figure 5-17: System Maintenance in Standard Mode

Figure 5-18 illustrates a detail of the System Maintenance bar when the Passport user selects the **Remote Sup.** option with **Enable Enhanced Remote Support Passwords** set and configured for Alpha Numeric with Symbols.

Figure 5-18: System Maintenance in Enhanced Support Mode



This page is intentionally left blank.

6 – Software Updates

6.1 Overview

The EDH software can be updated onsite or remotely through a network connection. All updates to the EDH are provided from within the merchant network, either through the Passport MWS/Server or over a secured connection provided by the merchant.

6.2 Onsite Software Updates

The merchant is responsible for ensuring all onsite updates to the EDH are performed by authorized personnel and for limiting physical access to equipment per PCI DSS requirements.

Software updates are applied locally by the Passport MWS/Server and do not require remote access to the EDH. The Automated Software Upgrade (ASU) functionality provided in the EDH is responsible for handling software updates from the Passport MWS/Server, validating the software, and performing the installation.

6.3 Remote Software Updates

Direct remote software updates to the EDH are not performed. Any remote software update is accomplished by remote download to the Passport Server/MWS, where the update is then locally processed, including any EDH software updates.

Note: All remote connections to the merchant network and Passport system must be secured as per guidelines specified in "5-Remote Access to the EDH" on page 5-1.

6.4 Accessing and Verifying Software Updates

Official software updates are provided by Gilbarco directly, or from Gilbarco authorized Distributors and Service Contractors. While the EDH provides for protection against unknown or invalid software, to ensure valid updates are installed, Merchants should only accept software updates from official sources.

Merchants with service agreements are notified by Gilbarco when software updates are released. If a service agreement is not in place, Merchants can contact their Gilbarco Distributor or Service Contractor for information on the latest updates.

This page is intentionally left blank.

7 – Managing System Security

7.1 Overview

In addition to the features mentioned in other sections, the EDH supports a number of specific security functions and requirements. This section describes each of them in detail.

7.2 Security Manager - System Management

The System Management functions available within Security Manager provide access to security-specific functions on the EDH and are available only to users with Administrator access.

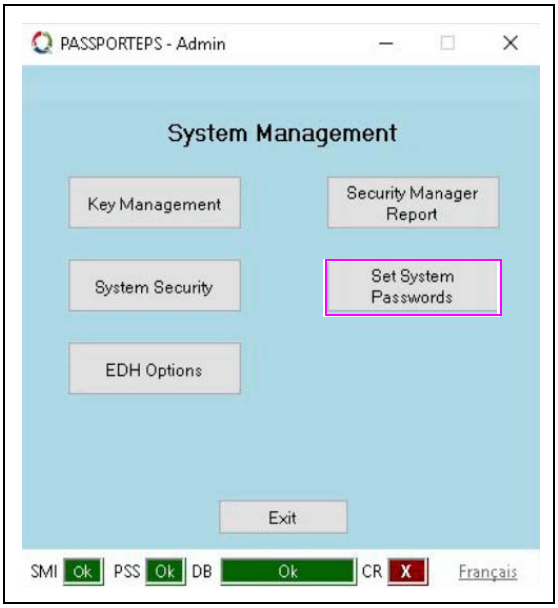
To access System Management, proceed as follows:

1 Log into **Security Manager** (for more information, refer to "2.3 Security Manager Login Process" on page 2-1).

Figure 7-1: Security Manager - System Management

2 Select **System Management**. The System Management window opens.

Figure 7-2: System Management Window



7.3 System Management Options

System Management provides the following functions or options:

- Key Management
- System Security
- EDH Options
- Security Manager Report
- Set System Passwords

7.3.1 Key Management

The Key Management function provides the merchant the ability to change (roll) the Key Encryption Key (KEK) and the Data Encryption Key (DEK) manually. In addition to rolling the encryption keys, the merchant can choose to restore the Key Storage Device Password to the secure compact flash drive (iButton®).

PCI defines the following two criteria in which a forced key rotation would be required:

- The integrity of the key is weakened
- Key compromise is known or suspected

IMPORTANT INFORMATION
• The EDH automatically rolls the KEK every 180 days. • The EDH automatically rolls the DEK every 30 days.

⚠ CAUTION

The iButton must be installed correctly in the EDH for the Key Management and Password Restoration processes to occur. If the iButton is removed, damaged, or incorrectly installed, these critical processes fail.

From the System Management window, select **Key Management**. The Manage Keys window opens.

Figure 7-3: Manage Keys Window

7.3.1.1 Roll Data Encryption Key (DEK)

From the Manage Keys window, select **Roll Data Encryption Key (DEK)**. While the EDH performs the roll DEK process, the Manage Keys window turns gray and the option or function keys are inaccessible. When the process is complete, all option or function keys are accessible.

7.3.1.2 Roll Key Encryption Key (KEK)

From the Manage Keys window, select **Roll Key Encryption Key (KEK)**. While the EDH performs the roll KEK process, the Manage Keys window turns gray and the option or function keys are inaccessible. When the process is complete, all option or function keys are accessible.

7.3.1.3 Restore Key Storage Device Password

To restore the Key Storage Device Password, proceed as follows:

1 From the Manage Keys window, select **Restore Key Storage Device Password**. The Restore Key Storage Device Password window opens.

Figure 7-4: Restore Key Storage Device Password Window

2 From the merchant's Security Manager Report, locate the **Key Storage Device Password** and enter it in the **Enter the Key Storage Device password** field.

3 Select **Restore Password**. While the EDH is restoring the Key Storage Device Password, the Restore Key Storage Device window turns gray and all option or function keys are inaccessible.

When the process is complete, all option or function keys are accessible.

7.3.1.4 Key Management Best Practices

The EDH handles all key management activities as part of the standard operation of the system. Merchants are not required to perform any key management activities manually or access any key material on the system.

Merchants utilizing cryptographic keys in other systems, must manage those keys in compliance with PCI requirements, including the following:

- Restrict access to keys to the fewest number of custodians necessary
- Store keys securely in the fewest possible locations and forms

7.3.2 Secure Report Password

For information on the Secure Report Password function, refer to "4-Reports and Data Retention" on page 4-1.

7.3.3 System Security

The System Security function is used to activate and deactivate security on the EDH. During the installation of the EDH, the merchant is required to activate System Security.

Figure 7-5: System Security Window

7.3.3.1 Enabling System Security

Note: Various terms are used interchangeably for enabling System Security, such as activating or hardening. This manual uses enabling.

Enabling System Security is a process performed to initiate all security features of the EDH. When System Security is enabled, the EDH defaults to a PA-DSS compliant mode and allows network transactions to be performed.

Before System Security can be enabled, the merchant must perform the following tasks:

- Change the default Security Manager Administrator Password
- Change the default Secure Report Password

To enable System Security, proceed as follows:

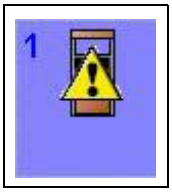
1. Log into Security Manager using a valid User Name and Password.
2. From the Security Manager main window, select **System Management**.
3. Select **System Security**.
4. Select **Enable System Security**. The Activation Complete window opens.
5. Select **OK** to return to the System Management main window.

7.3.3.2 System Security and Network Transactions

If System Security is not enabled and a network payment card is swiped or entered, the following messages appear:

- For inside transactions, the CWS or POS displays the message "Sale Denied: System Security not enabled." The transaction must be tendered with an alternate non-network tender or a transaction void performed.
- For outside transactions, the CRIND device displays "No Card Pay Now". If configured for it, the cashier can authorize the CRIND to allow the customer to dispense fuel and go inside to pay with an alternate, non-network tender, such as Cash.
- Inside on the CWS or POS, the forecourt area displays a yellow exclamation point over the fueling position indicating an error.

Figure 7-6: Forecourt Fueling Position Error Icon



- When the cashier selects the corresponding dispenser number of the CRIND in error, and selects the **Diag** key, the Diag screen displays the message "Sale Denied: system Security not enabled." in the **CRIND** field. Selecting the **Clear Errors** key deletes the error.

7.3.3.3 Disabling System Security

Disabling System Security disables all security features of the EDH, rendering Passport unusable. In addition, disabling System Security purges all financial data from the EDH, including all pending network transactions and all Secure Report information.

Per PCI DSS requirements, disabling System Security renders all cryptographic material irretrievable.

⚠ CAUTION

- Disabling System Security could result in lost transactions, and must be performed with a Gilbarco ASC onsite to save financial and diagnostic data and properly deactivate security.
- Disabling System Security must only be used when decommissioning the hardware. The system is unusable and will require reimaging.

Before disabling System Security, perform the following:

1. Ensure there are no transactions in Store and Forward.
2. Perform a Passport Store Close (**MWS** > **Period Close** > **Store Close**).
3. Print all period reports and secure reports.
4. Collect Back Office data.

To disable System Security, proceed as follows:

1 Log into Security Manager using a valid User Name and Password.

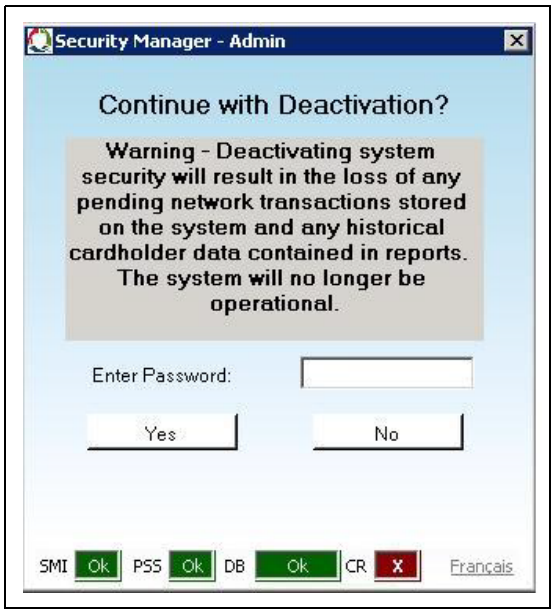
2 Select **System Management.**

3 Select **System Security**. The System Security window opens with the **Status: Enabled**.

Figure 7-7: System Security Window with Status: Enabled

4 Select **Disable System Security**. A warning window opens.

Figure 7-8: Disable System Security Warning



5 Perform one of the following:
- Select **No** to stop the disable process.
- Select **Yes** to continue. A confirmation prompt box is displayed.

Figure 7-9: Confirmation Prompt Box

- Select **No** or **Cancel** to stop the disable process.
- Select **Yes** to continue the disable process.

The Disable System Security process completes. The message "Deactivation Complete. OK" is displayed.

6 Select **OK**. The System Security window opens.

7.3.4 Security Manager Report

The Security Manager Report provides the merchant with a printed copy of the information maintained by Security Manager. This report contains sensitive information; therefore, must be secured per the merchant's PCI DSS data retention policies.

7.3.4.1 Security Report Dual Control (Split-Report)

The Security Manager Report is split into two separate reports, in order to provide dual control of the passwords printed on the report. Two authorized users must be designated by the Merchant. When an authorized user is signed in and selects the **Security Manager Report** key, the Security Manager Report window displays with two officer keys.

IMPORTANT INFORMATION
The ASC must not retain or have access to the Security Manager Report. The report can be printed only from the MWS.

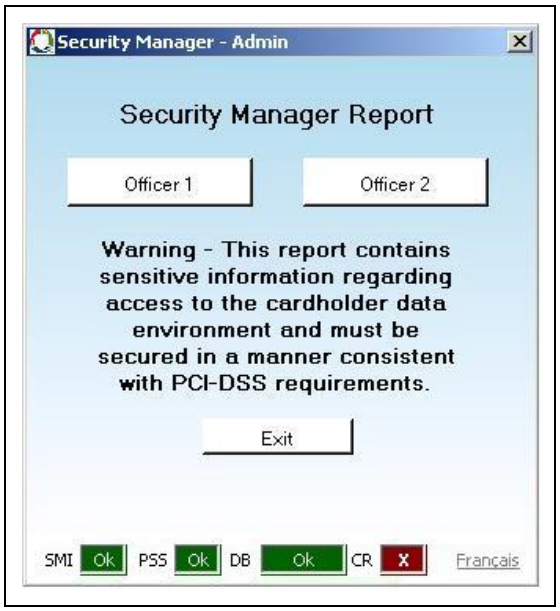
7.3.4.2 Printing the Security Manager Report

To print the report, proceed as follows:

Note: The user must be a Secure Report authorized user.

1 One of the authorized officers must log into Security Manager and navigate to **System Management** > **Security Manager Report**. The Security Manager Report window opens.

Figure 7-10: Security Manager Report Window



2 One of the authorized officers selects **Officer 1**. Half of the report prints automatically on the Passport report printer.

3 The other authorized officer must log into Security Manager and navigate to **System Management** > **Security Manager Report**. The Security Manager Report window opens.

4 The other authorized officer selects **Officer 2**. The second half of the report prints.

5 Select **Exit**. The System Management window returns.

7.3.4.3 Automatic Prompt for Printing the Security Manager Report

Security Manager recognizes Administrator-level setting changes as they occur and automatically prompts for printing a new Security Manager Report. This ensures the site has the most current Security Manager Report and saves the user steps by not requiring a manual selection of the **Security Manager Report** function.

Changes to the following Administrator-level settings cause Security Manager to prompt the user to print the Security Manager Report:

- Changing the User Name Admin password
- Manually rolling KEK
- Restoring the Key Storage Device Password
- Enabling System Security

When the user selects the **Exit** key from the Security Manager main window, the **Configuration has changed** window prompts the user to print the Security Manager Report. The user may take one of two actions:

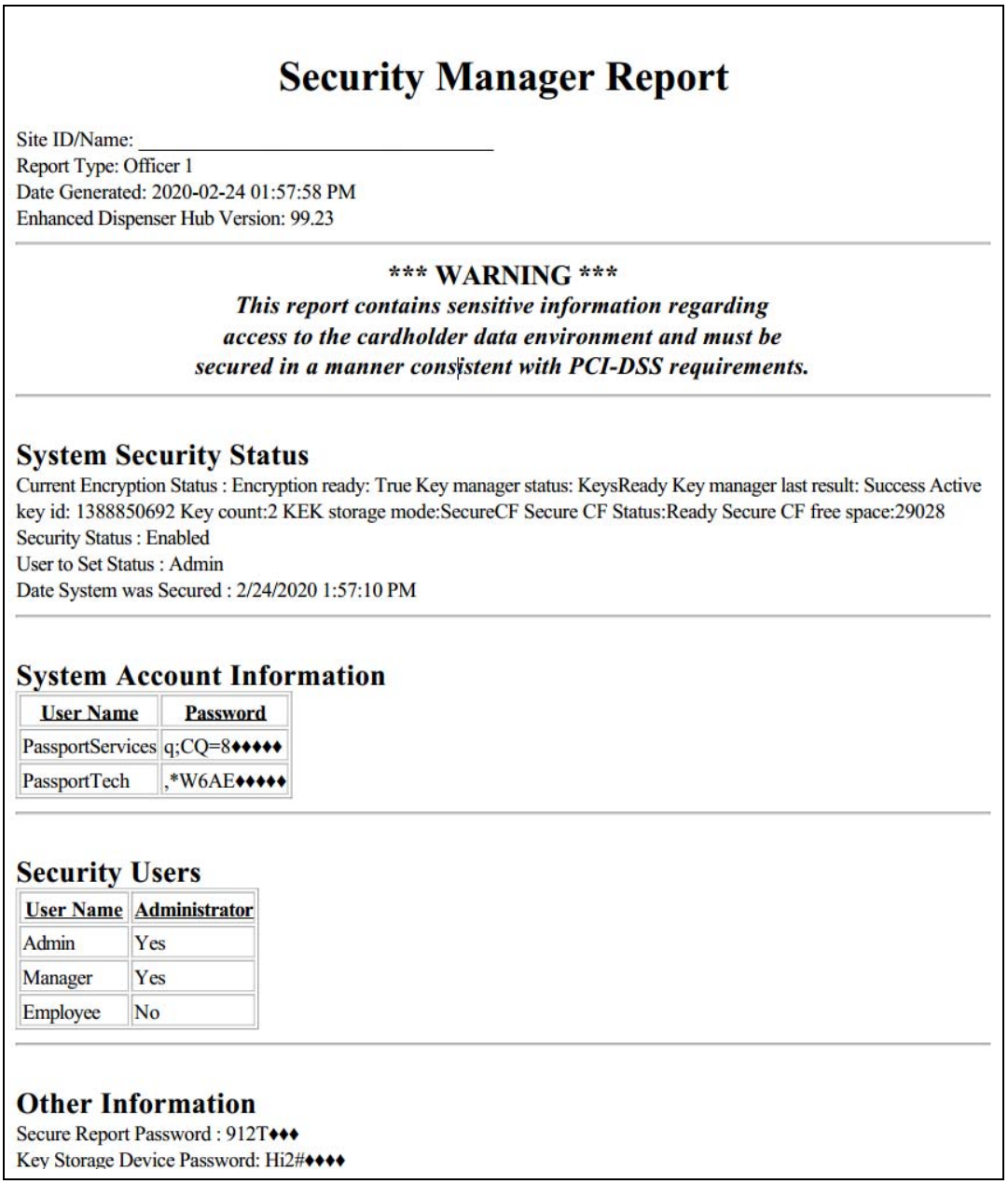
- Select **Yes** to continue to print the Security Manager Report.
- Select **No** to exit Security Manager.

7.3.4.4 Security Manager Report Samples

The following samples illustrate the format and content of the Security Manager Report.

The Security Manager Report must be stored in a secure location and only accessed by individuals authorized by the Merchant.

Figure 7-11: Sample Security Manager Report - Officer 1



Security Manager Report

Site ID/Name: _____
Report Type: Officer 1
Date Generated: 2020-02-24 01:57:58 PM
Enhanced Dispenser Hub Version: 99.23

***** WARNING *****

This report contains sensitive information regarding access to the cardholder data environment and must be secured in a manner consistent with PCI-DSS requirements.

System Security Status

Current Encryption Status : Encryption ready: True Key manager status: KeysReady Key manager last result: Success Active key id: 1388850692 Key count:2 KEK storage mode:SecureCF Secure CF Status:Ready Secure CF free space:29028
Security Status : Enabled
User to Set Status : Admin
Date System was Secured : 2/24/2020 1:57:10 PM

System Account Information

User Name	Password
PassportServices	q;CQ=8♦♦♦♦♦
PassportTech	,*W6AE♦♦♦♦♦

Security Users

User Name	Administrator
Admin	Yes
Manager	Yes
Employee	No

Other Information

Secure Report Password : 912T♦♦♦
Key Storage Device Password: Hi2#♦♦♦♦

Figure 7-12: Sample Security Manager Report - Officer 2

Security Manager Report

Site ID/Name: _____
Report Type: Officer 2
Date Generated: 2020-02-24 01:58:12 PM
Enhanced Dispenser Hub Version: 99.23

***** WARNING *****

This report contains sensitive information regarding access to the cardholder data environment and must be secured in a manner consistent with PCI-DSS requirements.

System Security Status

Current Encryption Status : Encryption ready: True Key manager status: KeysReady Key manager last result: Success Active key id: 1388850692 Key count:2 KEK storage mode:SecureCF Secure CF Status:Ready Secure CF free space:29028
Security Status : Enabled
User to Set Status : Admin
Date System was Secured : 2/24/2020 1:57:10 PM

System Account Information

User Name	Password
PassportServices	♦♦♦♦♦♦u4+bE
PassportTech	♦♦♦♦♦♦wtc5)

Security Users

User Name	Administrator
Admin	Yes
Manager	Yes
Employee	No

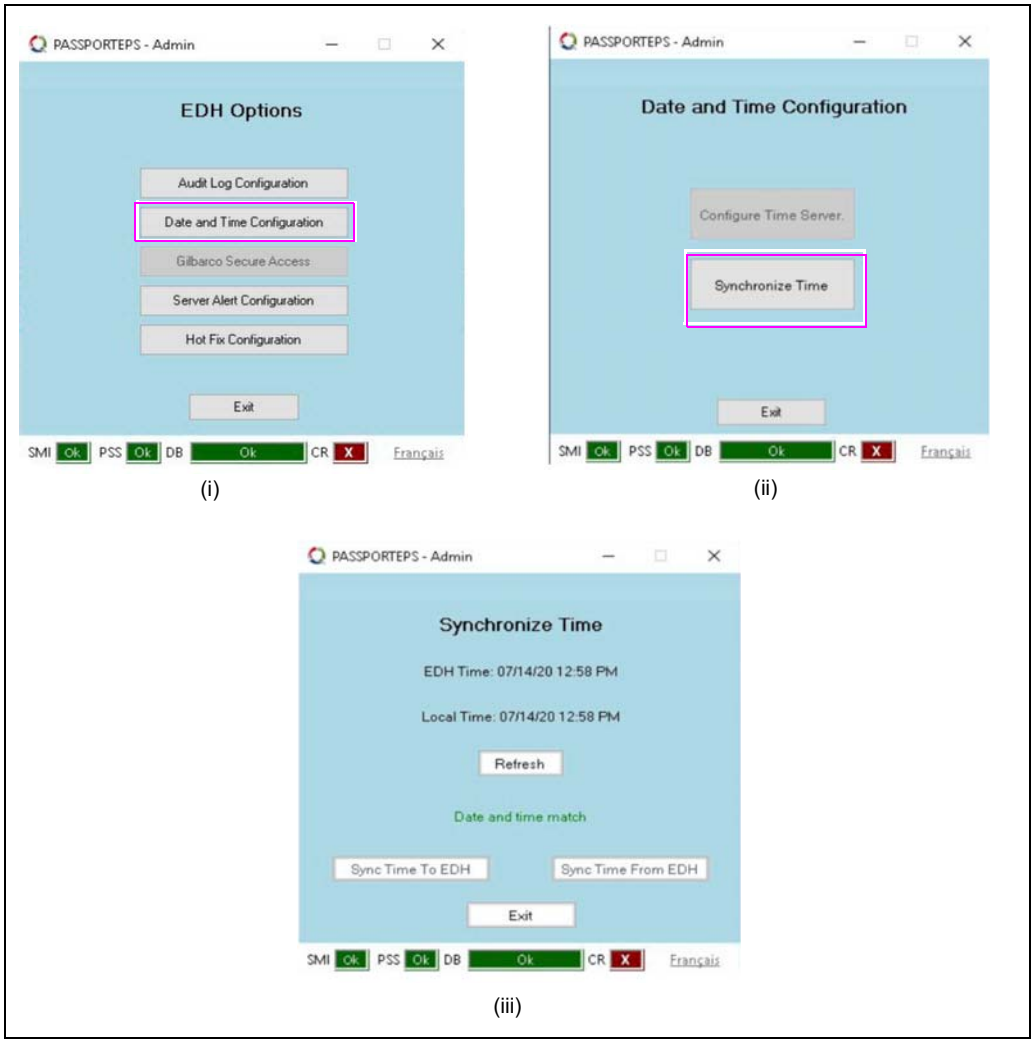
Other Information

Secure Report Password : ♦♦♦♦ech
Key Storage Device Password: ♦♦♦♦7Q(z

7.3.5 Configuring Date and Time

The Administrator-level user can select the Date and Time Configuration option on the System Management, EDH Options window, and then select **Synchronize Time** to perform manual synchronization of the time between the Passport EDH and the Passport Server.

Figure 7-13: Date and Time Configuration

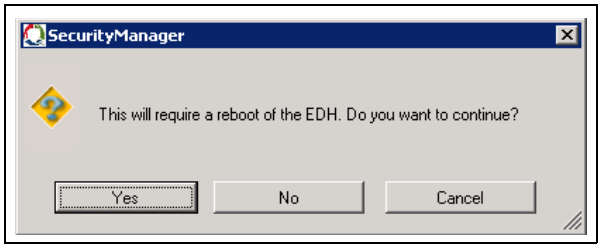


The normal operating mode is for the system to provide for automatic time synchronization. Manual synchronization should be performed only if the system time was changed incorrectly and needs to be adjusted. The current time on the EDH and the current time on the Passport server are displayed along with a status line indicating the current state. The Sync Time To EDH and Sync Time From EDH buttons are available for selection only if there is a difference in the Date, Time, or Time Zone.

7.3.5.1 Sync Time to EDH

Selecting the Sync Time To EDH option will change the time on the EDH to match the Local Time. Certain types of time changes may require the EDH to reboot to complete the action. If an EDH reboot is required, the following window opens.

Figure 7-14: Time Sync EDH Reboot Confirmation



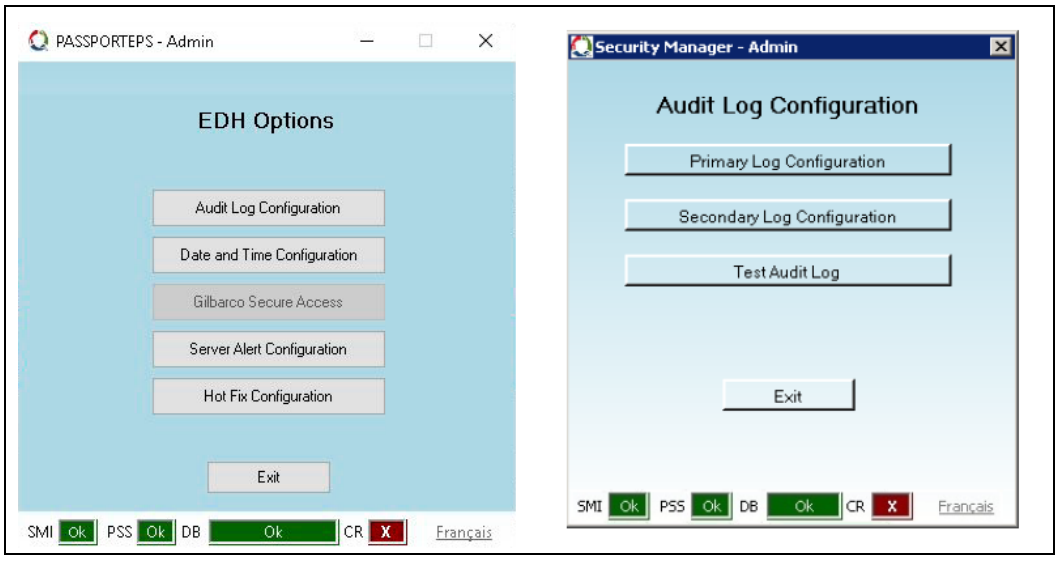
7.3.5.2 Sync Time from EDH

Selecting the Sync Time From EDH option will change the Local Time to match the time on the EDH.

7.3.6 Configuring Audit Log

The Administrator-level user can select the Audit Log Configuration option on the System Security window to configure scheduled transmission of the EDH Audit Log to a primary and secondary location to facilitate centralized logging. The transmission mechanism is via Secure File Transfer Protocol (SFTP) and is configured as per the instructions that follow.

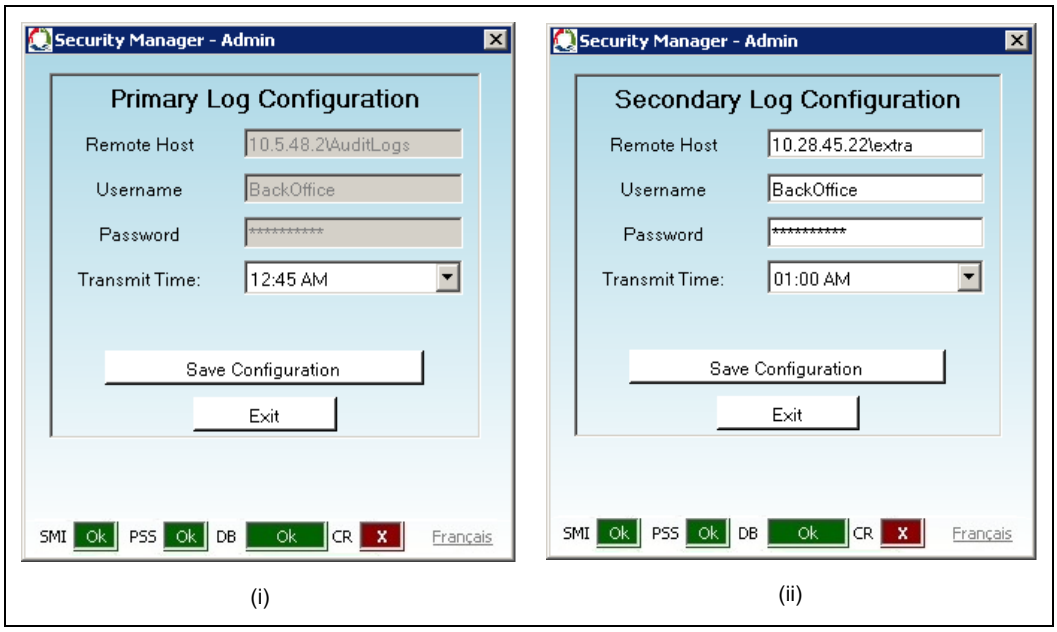
Figure 7-15: Audit Log Configuration



7.3.6.1 Primary Log Configuration and Secondary Log Configuration

Selecting the Primary Log Configuration option or the Secondary Log Configuration option will result in one of the following windows being displayed.

Figure 7-16: Primary and Secondary Log Configuration Example



7.3.6.1.1 Primary Log Configuration

The primary audit log location is defined as the Passport server audit log directory and cannot be changed by the merchant. For the primary location, the only editable option is “Transmit Time”. The Transmit Time drop-down list has 15-minute increments between midnight and 6:00 A.M. with some times excluded for performing system background tasks. The Transmit Time can also be set to DISABLED. Setting this option to DISABLED results in no audit logs being posted to the Passport Server. This option could be used for merchants who only want audit logs to be sent to the secondary location.

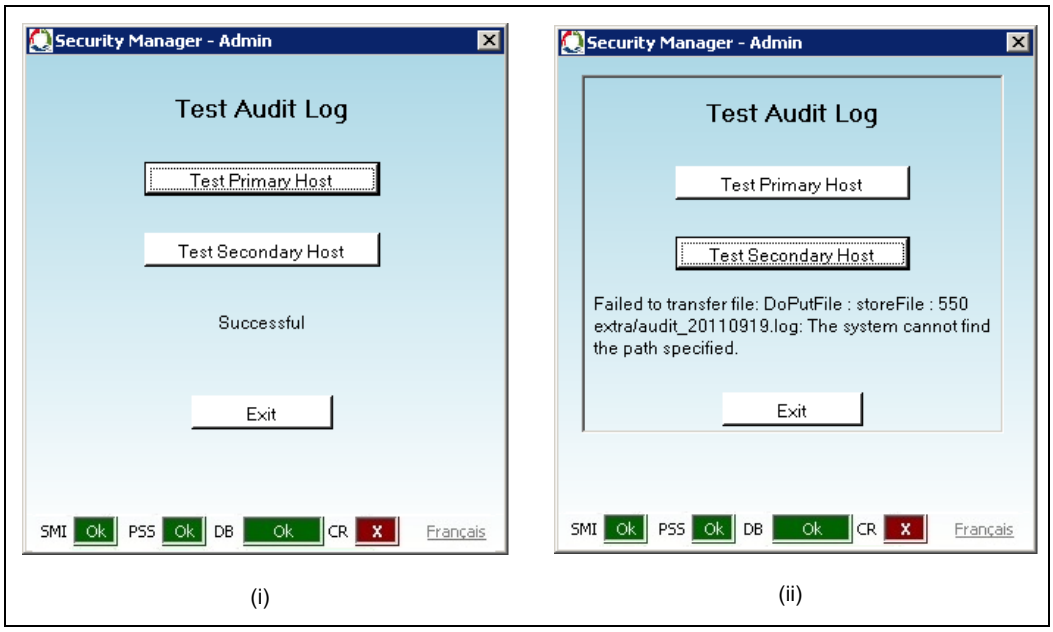
7.3.6.1.2 Secondary Log Configuration

The Secondary Log Configuration screen allows configuration of a second location to post audit logs. The merchant provides the Remote Host IP Address and directory where the audit logs are to be posted. The Username and Password are also configured here. The Transmit Time drop-down list has 15-minute increments between midnight and 6:00 A.M. with some times excluded for performing system background tasks. The Transmit Time can also be set to DISABLED. Setting to DISABLED results in no audit logs being posted to the secondary location.

7.3.6.2 Test Audit Log

Selecting the Test Audit Log option will result in one of the following windows being displayed.

Figure 7-17: Test Audit Log Example



Selecting either Test Primary Host or Test Secondary Host will transmit the prior day's audit log to the selected host (Primary or Secondary). Figure 7-17 shows examples of a successful and a failed test.

7.3.7 Gilbarco Secure Access

The Gilbarco Secure Access function on the System Management, EDH Options window does not apply to this Passport version.

7.3.8 Server Alert Configuration

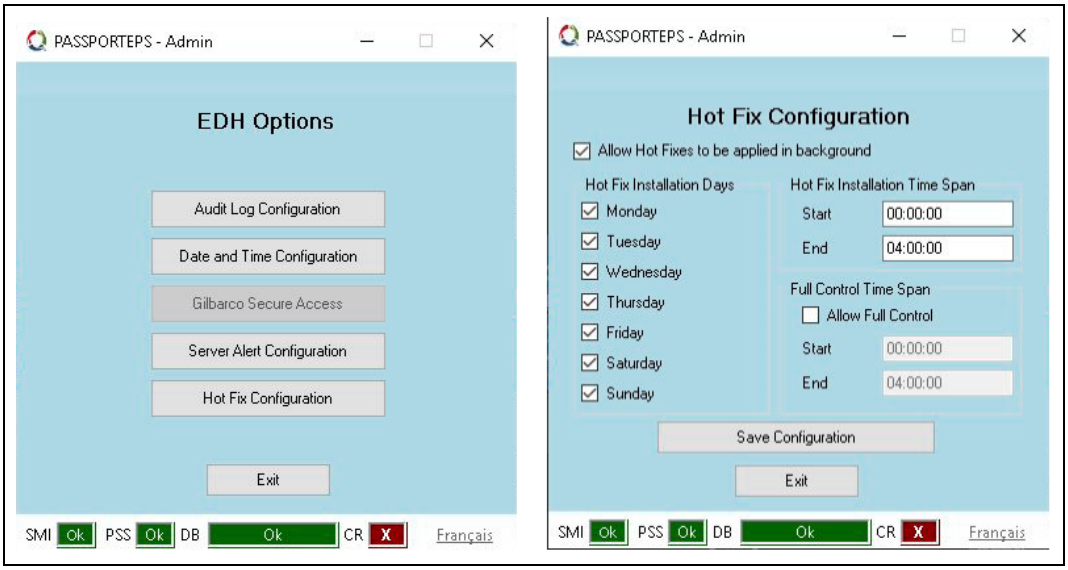
The Server Alert Configuration function on the System Management, EDH Options window does not apply to this Passport version.

7.3.9 Hot Fix Configuration

An Administrator-level user can select the Hot Fix Configuration option on the System Management, EDH Options window to override the default configuration for installing Windows OS security hot fixes. Hot fixes are special installation packages that are available separately from application media.

By default, hot fixes apply silently in the background between midnight and 4:00 A.M. on any day of the week. If a reboot is required, the hot fix application pauses and waits for the machine in question to be restarted, usually by the weekly watchdog process, before continuing. The Hot Fix Configuration window allows the merchant to override these default actions.

Figure 7-18: Hot Fix Configuration



Field	Description
Allow Hot Fixes to be applied in background	When selected, hot fixes will be applied in the background during the configured time periods. When not selected, hot fixes will be applied as part of the next Passport software package installation, thereby extending the software package installation time. Field is selected by default. *Note: Gilbarco recommends that hot fixes be allowed to apply in the background.*
Hot Fix Installation Days	Day(s) on which installation of hot fixes may occur. All days are selected by default.
Hot Fix Installation Time Span	Time span in which installation of hot fixes may occur. Default settings are Start time of 00:00:00 (midnight) and End time of 04:00:00.
Allow Full Control	If selected, the hot fix installation process will have full control to trigger any required reboots. If not selected, the hot fix application process will pause if a reboot is required and wait for the machine in question to be restarted, typically by the weekly watchdog process. Field is not selected by default. *Note: Gilbarco recommends that Allow Full Control be selected only at sites that do not trade 24 hours per day as it could interrupt trade.*
Full Control Time Span Start, End times	Time period in which any reboot required by the hot fix installation process may occur, when Allow Full Control is selected.

7.4 BIN Range Trapping

As part of PA-DSS compliance, Passport will only allow payment cards (American Express®, Discover®, Visa®, MasterCard®, and so on) to be used for payment. If a payment card is used at a Loyalty prompt driven by Passport's Generic Loyalty, a second card swipe for Mannatec®, or attendant token, Passport displays Invalid Card on the CWS. The cashier must select another card type.

Following are the card types on which BIN range trapping and decline occur:

Card Type	Prefixes	Account # Length
American Express	34, 37	15
Discover Card	6011, 622126-622925, 644-649, 65	16
JCB®	3528-3589	16
MasterCard	51-55	16
Visa	4	16
Diners Club International®	36	14

7.5 Security Audit Log

The EDH provides a Security Audit Log to help the merchant meet PCI DSS requirements. The EDH maintains the previous 90 days audit data.

The Security Audit Log can be accessed in the following four ways:

- The merchant can print the Security Audit Log for the current or previous day from the EDHub menu within System Maintenance.
- The merchant can print an audit log for any of the previous 90 days from the EDH dashboard.
- Audit logs from the last seven days are available in the Passport MWS/Server XMLGateway directory for remote collection of logs.
- If configured, audit logs are pushed remotely to the configured server at the chosen time of day.

IMPORTANT INFORMATION
PCI DSS requires that the merchant review logs daily and maintain one year of audit data.

7.5.1 Printing Current or Previous Audit Log

The Security Audit Log for the current and previous calendar day is available through Security Manager in System Maintenance. To print the Security Audit Log, proceed as follows:

1 From the MWS main screen, press the **Ctrl**, **Alt**, and **P** keys on the Passport keyboard simultaneously. The System Maintenance Login window opens.

2 Enter **Gilbarco** in the User Name field.

3 Enter **Passport** in the Password field.

4 Select **Login**. The System Maintenance tool bar appears.

5 Select **EDHub**.

6 Select **Security Mgr**.

7 To print current or today's audit log, select **Curr. Log**. To print the previous day's audit log, select **Prev. Log**. The report prints automatically on the Passport MWS report printer.

IMPORTANT INFORMATION
The audit log can only be printed from the MWS.

7.5.2 Audit Data Requirements

Per PCI DSS requirements, the following data must be included in the audit logs.

IMPORTANT INFORMATION
Failure to retain required audit log data will result in non-compliance with PCI DSS.

Implement audit trails of a system's components to reconstruct the following:

- All individual accesses to cardholder data
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of the audit logs
- Creation and deletion of system-level objects

Record the following audit trail entries for all system components for each event:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource

For information on the contents of the audit log, refer to the "9-Audit Log Definition" on page 9-1.

7.6 Secure Data Storage Management

Once System Security has been enabled, the EDH automatically handles all operations related to secure data management, including encryption/decryption key management.

In situations where all secure data must be deleted, such as decommission, Merchants must follow the instructions provided in "7.3.3.3 Disabling System Security" on page 7-6.

In the event the system is non-operational, the following information can be used to ensure all secure data is removed from the system.

7.6.1 Secure Data Storage

The EDH uses an embedded database, in combination with the iButton, for all storage of secure data.

The iButton must be physically destroyed in order to remove the stored data.

Data in the embedded database can be removed either by physical destruction of the EDH hard drive, or by using a secure delete tool to manually delete the database from the hard drive.

7.6.2 Secure Delete Tool

Gilbarco provides a Secure Delete Tool bundled with the Passport application. This tool is used by Passport for secure deletion of files during normal operation; however, this tool can also be used in situations where secure manual deletion of data is required.

In general, the EDH handles the secure deletion of data automatically; however, in cases where a manual secure deletion of data is required, Gilbarco provides instructions to the ASC on how to use the Secure Delete Tool for the specific case in question.

The Secure Delete Tool is called sdelete. It is a command line utility that supports a number of options. In a given use, it allows for the secure deletion of one or more files and directories. It can also be used to cleanse free space on a logical disk. Sdelete accepts wild card characters as part of the directory or file specifier.

Usage: sdelete [-p passes] [-s] <file or directory>
sdelete [-p passes] [-z|-c] [drive letter]

where:

-c	Zero free space (good for virtual disk optimization)
-p passes	Specifies number of overwite passes
-s	Recurse subdirectories
-z	Cleanse free space

IMPORTANT INFORMATION

The merchant must not use the Secure Delete Tool without the assistance of the ASC or Gilbarco support personnel. For more information on the Secure Delete Tool, refer to *MDE-4834 Passport V8.02+ System Recovery Guide*.

7.7 Access to Clear Text PAN

Per PA-DSS requirements all access to clear text PAN must be limited to individuals with a legitimate business need.

Passport supports clear text PAN only as part of the Secure Report function. For information on how to access and manage Secure Reports, refer to "Reports and Data Retention" on page 4-1.

In all other cases where PAN is displayed or printed, such as manual entry, receipts, and standard reports, a masked PAN is used.

7.8 Physical Security

7.8.1 EDH Physical Security

The merchant is responsible for ensuring that the EDH and sensitive cardholder data is secure. Opportunities for individuals to have access to this device and data must be restricted; otherwise, the merchant may be found in violation of PCI DSS.

7.8.2 Physical Security - Other Merchant Systems

Merchants are required to control access to any PCs, servers, and databases containing payment applications or unmasked cardholder data. In addition to restricting physical access, unique user IDs/Passwords and PCI DSS compliant secure authentication must be used.

EDH Secure Reports may contain unmasked cardholder data. Merchants using EDH Secure Reports on other systems must be compliant with the PCI DSS controls listed in this section.

7.9 Replacing Hardware

IMPORTANT INFORMATION
Secure removal of cardholder data stored in previous installations of payment applications as well as decommissioned EDH hardware is required for PCI DSS Compliance.

There are three EDH hardware replacement situations in which sensitive data must be considered:

- Replacing the EDH hard drives
- Replacing the EDH compact flash card
- Replacing the entire EDH device

When replacing the hard drive or the compact flash card, the replaced device must be destroyed physically before leaving the merchant location to ensure no sensitive data is accessible.

When replacing the entire EDH device, the merchant must disable system security using the Security Manager **System Security** function (refer to "7.3.3 System Security" on page 7-5). Disabling security ensures no sensitive data remain on the EDH device. Migration and re-encryption of cardholder data from previous versions of Passport to the EDH is not supported.

7.10 Troubleshooting

The EDH can log diagnostic information for troubleshooting purposes. Although none of the Passport Logs contain unmasked cardholder data, PCI DSS guidelines require the following actions to be taken when troubleshooting issues at a merchant location, when sensitive data is going to be gathered.

- Logging must be enabled only for the period of time needed to gather the information.
- Logging must be disabled once data is gathered.
- Logging that was enabled and might contains sensitive data must be securely deleted when it is no longer required.

If it is required to modify logging to gather sensitive information, Gilbarco will distribute additional guidelines on logging of sensitive information. In such case, only the data required to solve a specific problem should be collected. All sensitive data must be stored encrypted in a specific location with limited access and must be securely deleted immediately after its use.

This page is intentionally left blank.

8 – Network Time Synchronization

The Passport EDH is capable of synchronizing the date and time of the system with a network time server should it be required for Merchant PCI DSS compliance.

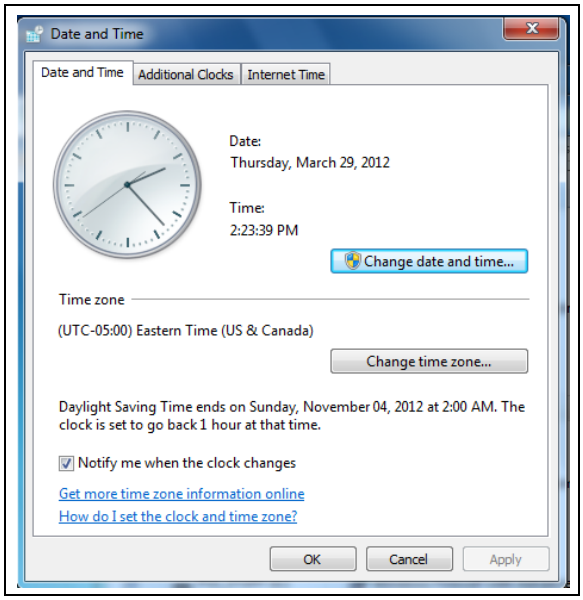
To configure the EDH, proceed as follows:

IMPORTANT INFORMATION
Many payment network applications synchronize the date and time of the EDH to the payment host. Prior to making changes, the merchant must confirm with the payment network that enabling time synchronization will not disrupt transaction flow.

1 Create a Temporary Support Account and log in to the EDH using Remote Desktop.

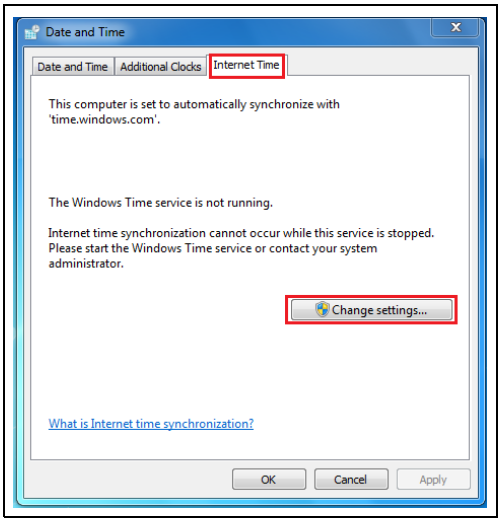
2 Access Date and Time settings.

Figure 8-1: Date and Time Settings



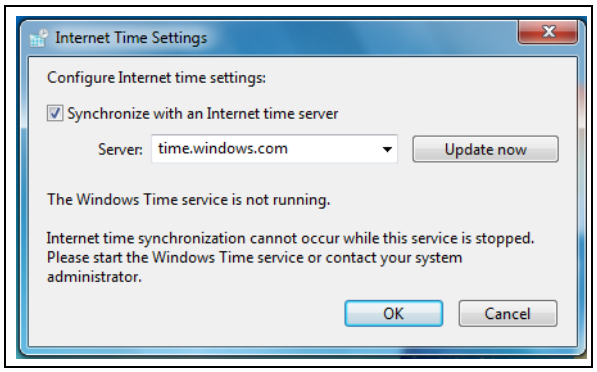
3 Select the **Internet Time** tab and from the **Internet Time** tab click **Change settings**.

Figure 8-2: Internet Time Tab



4 The **Internet Time Settings** screen opens. Select the **Synchronize with an Internet time server** check box.

Figure 8-3: Internet Time Settings



5 Enter your time server information in the **Server** box or select one of the system provided time servers from the drop-down list.

6 Select **Update now** to start synchronization.

7 After the synchronization is complete, select **OK** until you have exited out of Date and Time settings.

8 Reboot the EDH and allow it to restart and login normally.

In addition to the provided steps, the router must be modified to permit the EDH to access the time server. For sites using an Acumera Secure Zone Router, dial 1-800-743-7501, and select Option **3** and then Option **1** to have the SZR updated by Acumera. Otherwise contact the MNSP for the site to have the change applied.

9 – Audit Log Definition

9.1 Audit Log Structure

The Passport audit log is a standard text file consisting of two separate sections, each containing a different type of log data.

The overall file structure contains the following elements:

- File Header
- Audit Log Section 1 (Windows Event Log)
- Section Separator
- Audit Log Section 2 (Secure Delete Log)
- End of File Separator

9.1.1 File Header

The file header contains the following information:

- Title
- The Software version of the EDH
- The date and time that the audit log was generated

Figure 9-1: Example Audit Log Header

```
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
* Passport EDH Security Log
* EDH Version: 08.20
* Date/Time Generated: 03/29/2016   12:01 AM
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
```

9.1.2 Section Separator

A section separator is added between each of the sections to help with file parsing.

Figure 9-2: Section Separator

```
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
```

9.1.3 End of File Separator

An end of file separator has been added to denote the end of the audit log file to help with file parsing.

Figure 9-3: End of File Separator

9.1.4 Audit Log Section 1 (Windows Event Log)

Section 1 of the audit log is the primary audit log section and contains data on all events, except those specifically related to router logs and secure delete actions. The data in this section is recorded in standard Windows event log format.

Figure 9-4: Windows Event Log Entry Example

```
3/28/2016   11:20:37 AM Security    audit success     Logon/Logoff
      PASSPORTEPS Security    Successful Logon: User Name:  NETWORK SERVICE
      Domain:           NT AUTHORITY      Logon ID:         (0x0,0x3E4) Logon
Type: 5     Logon Process:    Advapi      Authentication Package: Negotiate
      Workstation Name:       Logon GUID: {00000000-0000-0000-0000-
000000000000} NETWORK SERVICE NT AUTHORITY (0x0,0x3E4) 5 Advapi   Negotiate
{00000000-0000-0000-0000-000000000000}
```

9.1.5 Audit Log Section 2 (Secure Delete Log)

Section 2 of the audit log contains all log data generated by the secure delete process.

Figure 9-5: Secure Delete Log Entry Example

```
03/28/16 18:50:19 User 'PassportServices' attempting to delete
'D:\gilbarco\upgrade\tempdata_20120328172201.xml'
03/28/16 18:50:19 Calling "c:\WINDOWS\SYSTEM32\sdelete -s -p 3
"D:\gilbarco\upgrade\tempdata_20120328172201.xml""


SDelete - Secure Delete v1.51
Copyright (C) 1999-2005 Mark Russinovich
Sysinternals - www.sysinternals.com
SDelete is set for 3 passes.
D:\gilbarco\upgrade\tempdata_20120328172201.xml...deleted.
03/28/16 18:50:19 Completed with error code: 0
```

9.2 Audit Log Examples

This section contains examples detailing how to map the Passport Audit logs to the specific PCI DSS requirements.

PCI DSS requirements define the actions which require log entries and the data elements required to be logged for each of the actions.

The following audit log examples and the corresponding table entries provide information on how to identify key elements from the audit log output.

9.2.1 All Individual Access to Cardholder Data

User Identification	Event Type	Date Time	Success or Failure	Origination of Event	Identity or name of affected data, system component, or resource
TestUser	Roll Encryption Key	3/14/2016 2:50:12PM	Key maintenance was successful	10.5.48.2	SMIService

3/14/2016 2:50:12 PM Application Warning PASSPORTEPS SMIService User 'TestUser' is attempting to log in from [10.5.48.2] User 'TestUser' is attempting to log in from [10.5.48.2]

3/14/2016 2:50:12 PM Application Information PASSPORTEPS SMIService user TestUser was valid and is trying to perform RollEncryptionKey user TestUser was valid and is trying to perform

3/14/2016 2:50:18 PM Application Information PASSPORTEPS SMIService Key maintenance was successful. Key maintenance was successful.

9.2.2 All Actions Taken by an Individual with Root or Administrative Privileges

User Identification	Event Type	Date Time	Success or Failure	Origination of Event	Identity or name of affected data, system component, or resource
TestUser	Enable Remote Support	3/14/2016 12:01:11 PM	successfully enabled remote support	10.5.48.2	SMIService

3/14/2016 12:01:11 PM Application Warning PASSPORTEPS SMIService User 'TestUser' is attempting to log in from [10.5.48.2] User 'TestUser' is attempting to log in from [10.5.48.2]

3/14/2016 12:01:23 PM Application Information PASSPORTEPS SMIService User 'TestUser' is attempting to Enable Remote Support. User 'TestUser' is attempting to Enable Remote Support.

3/14/2016 12:01:23 PM Application Information PASSPORTEPS SMIService User 'TestUser' has successfully enabled remote support User 'TestUser' has successfully enabled remote support

9.2.3 Access to All Audit Trails

User Identification	Event Type	Date Time	Success or Failure	Origination of Event	Identity or name of affected data, system component, or resource
PassportTech	Delete	3/14/2016 5:06:24 PM	An object was deleted	PASSPORTEPS	SYSLOG_20120314.log

3/14/2016 5:06:24 PM Security Audit Success File System PASSPORTEPS Microsoft-Windows-Security-Auditing An attempt was made to access an object.Subject: Security ID: S-1-5-21-1361863599-3206297125-1509950785-1001 Account Name: PassportTech Account Domain: PASSPORTEPS Logon ID: 0x75509Object: Object Server: Security Object Type: File Object Name: D:\Gilbarco\Logs\AuditLogs\SYSLOG_20120314.log Handle ID: 0x58Process Information: Process ID: 0x110 Process Name: C:\Windows\System32\cmd.exeAccess Request Information: Accesses: DELETE Access Mask: 0x10000 S-1-5-21-1361863599-3206297125-1509950785-1001 PassportTech PASSPORTEPS 0x75509 Security File D:\Gilbarco\Logs\AuditLogs\SYSLOG_20120314.log 0x58 %%1537 0x10000 0x110 C:\Windows\System32\cmd.exe

3/14/2016 5:06:24 PM Security Audit Success File System PASSPORTEPS Microsoft-Windows-Security-Auditing An object was deleted.Subject: Security ID: S-1-5-21-1361863599-3206297125-1509950785-1001 Account Name: PassportTech Account Domain: PASSPORTEPS Logon ID: 0x75509Object: Object Server: Security Handle ID: 0x58Process Information: Process ID: 0x110 Process Name: C:\Windows\System32\cmd.exe Transaction ID: {00000000-0000-0000-0000-000000000000} S-1-5-21-1361863599-3206297125-1509950785-1001 PassportTech PASSPORTEPS 0x75509 Security 0x58 0x110 C:\Windows\System32\cmd.exe {00000000-0000-0000-0000-000000000000}

9.2.4 Invalid Logical Access Attempts

User Identification	Event Type	Date Time	Success or Failure	Origination of Event	Identity or name of affected data, system component, or resource
TestUser	Log in	3/14/2016 2:47:22 PM	User TestUser Failed Validation	10.5.48.2	SMIService

3/14/2016 2:47:22 PM Application Warning PASSPORTEPS SMIService User 'TestUser' is attempting to log in from [10.5.48.2] User 'TestUser' is attempting to log in from [10.5.48.2]

3/14/2016 2:47:22 PM Application Warning PASSPORTEPS SMIService ValidateCredentials : User TestUser failed validation. ValidateCredentials : User TestUser failed validation.

9.2.5 Use of Identification and Authentication Mechanisms

User Identification	Event Type	Date Time	Success or Failure	Origination of Event	Identity or name of affected data, system component, or resource
TestUser	Log in	3/14/2016 2:47:22 PM	User TestUser Failed Validation	10.5.48.2	SMIService

3/14/2016 2:47:22 PM Application Warning PASSPORTEPS SMIService User 'TestUser' is attempting to log in from [10.5.48.2] User 'TestUser' is attempting to log in from [10.5.48.2]

3/14/2016 2:47:22 PM Application Information PASSPORTEPS SMIService Executing usp_VaultIsUserLocked user: TestUser Executing usp_VaultIsUserLocked user: TestUser

3/14/2016 2:47:22 PM Application Information PASSPORTEPS SMIService IsUserLockedOut : User TestUser lockedout=[FALSE] retval=[False] IsUserLockedOut : User TestUser lockedout=[FALSE] retval=[False]

3/14/2016 2:47:22 PM Application Warning PASSPORTEPS SMIService ValidateCredentials : User TestUser failed validation. ValidateCredentials : User TestUser failed validation.

9.2.6 Initialization of Audit Logs

User Identification	Event Type	Date Time	Success or Failure	Origination of Event	Identity or name of affected data, system component, or resource
PASSPORTEPS	Delete	6/19/2016 12:00:03 AM	Audit Success	PASSPORTEPS	event20120521.log

6/19/2016 12:00:03 AM Security Audit Success File System PASSPORTEPS Microsoft-Windows-Security-Auditing An attempt was made to access an object.Subject: Security ID: S-1-5-18 Account Name: PASSPORTEPS$ Account Domain: WORKGROUP Logon ID: 0x3e7Object: Object Server: Security Object Type: File Object Name: D:\Gilbarco\Logs\AuditLogs\event20120521.log Handle ID: 0x500Process Information: Process ID: 0x5d4 Process Name: C:\Passport\tools\EventLogMonitor.exeAccess Request Information: Accesses: DELETE Access Mask: 0x10000 S-1-5-18 PASSPORTEPS$ WORKGROUP 0x3e7 Security File D:\Gilbarco\Logs\AuditLogs\event20120521.log 0x500 %%1537 0x10000 0x5d4 C:\Passport\tools\EventLogMonitor.exe

9.2.7 Creation and Deletion of System Level Objects

User Identification	Event Type	Date Time	Success or Failure	Origination of Event	Identity or name of affected data, system component, or resource
TestUser	Roll Encryption Key	3/14/2016 2:50:12 PM	Key maintenance was successful	PASSPORTEPS	SMIService

3/14/2016 2:50:12 PM Application Information PASSPORTEPS SMIService User TestUser is attempting to Roll the Encryption Key User TestUser is attempting to Roll the Encryption Key

3/14/2016 2:50:18 PM Application Information PASSPORTEPS SMIService Key maintenance was successful. Key maintenance was successful.

3/14/2016 2:50:18 PM Application Information PASSPORTEPS SMIService RollEncryptionKey overall result=[True] RollEncryptionKey overall result=[True]

10 – Supported Hardware and Software

The Passport PA-DSS certification was performed using Gilbarco hardware and software in conjunction with supported indoor PIN Pad hardware. Failure to use approved hardware and software may invalidate the Passport system's PA-DSS compliance and can impact the merchant's overall PCI DSS compliance.

The following table lists the hardware and software that are valid for use in a PA-DSS certified Passport installation.

Note: Only hardware and software relevant to PA-DSS certification is listed. Any hardware and software not in scope for PA-DSS certification, such as Back Office PC are not included.

Device	Application Version
Passport EDH	• 11.23.01.01 • 11.23.02.01 • 11.23.04.01 • 11.23.06.01 • 11.23.07.01
Passport MWS/CWS	• 20.01.23.XX • 20.02.23.XX • 20.04.23.XX • 21.02.23.XX • 21.03.23.XX
VeriFone® MX915 PIN Pad	N/A
Gilbarco FlexPay™ II Payment Terminal	N/A
Gilbarco FlexPay IV Payment Terminal	N/A
Wayne iX Pay™ SPM	N/A
Ingenico® ipp320	N/A
Ingenico isc250	N/A
Cryptera EPP 1.x/2.x	N/A

The merchant is responsible for ensuring that only payment terminals approved under their PCI DSS certification are deployed as part of the Passport install.

This page is intentionally left blank.

11 – Software Versioning Methodology

11.1 Versioning Methodology

The Passport EDH consists of Core components that are shared by all payment networks, and network-specific components that drive specific business rules of the payment network.

The Passport EDH version number is composed of the following elements:

- HH - Major Version Number. This portion of the version number increments any time the scope of changes, defined for a specific release, exceeds the threshold for a “low impact” change, as defined by PCI.
- CC - Customer Indicator. Denotes the particular customer/processor associated with the release.
- LL - Minor Version Number. This portion of the version number increments any time the scope of changes, defined for a specific release, exceeds the threshold for a “no impact” change, but is not significant enough to require a major version change.
- * - Wildcard used to denote “no impact” changes.

This results in an EDH version number of the following format:

- 11.XX.01.* - This denotes Version 11, Revision 01, of Customer/Processor XX.

11.2 PA-DSS Version Mapping

The following table contains information linking the PA-DSS certified Passport EDH version information to applicable Passport EDH configurations for Passport V20.01. To obtain this information for subsequent Passport versions, select **INFO** on the MWS.

PA-DSS Version Number	Passport EDH Version
11.23.01.0000	11.23
11.23.01.0001	11.23

This page is intentionally left blank.

12 – Prohibited Interfaces

12.1 Wireless Technologies

The EDH does not require the use of wireless technologies. Implementation of the EDH in a wireless environment violates the product's PA-DSS compliance and could result in a violation of the merchant's PCI DSS compliance.

IMPORTANT INFORMATION
The merchant or ASC must not install the EDH in a wireless environment. A merchant who chooses to install a wireless environment must install and configure a secure firewall to isolate cardholder data per PCI DSS requirements. The merchant must also change all wireless default encryption keys, passwords and Simple Network Management Protocol (SNMP) community strings upon installation and any time anyone with knowledge of the keys or passwords leaves the company or changes positions. Merchants using wireless networks are advised to follow industry best practices [for example, Institute of Electrical and Electronics Engineers (IEEE) 802.11.i] to provide strong encryption for authentication and transmission.

12.2 Direct Internet Connection

PCI DSS prohibits any direct Internet connection to the payment environment.

The EDH does not support a direct Internet connection. Implementing the EDH with a direct connection to the Internet violates the product's PA-DSS compliance and the merchant's PCI-DSS compliance.

IMPORTANT INFORMATION
The merchant or ASC must not install the EDH with a direct Internet connection. A merchant who chooses to support direct Internet connectivity at the location must secure the connection by firewall and configure according to PCI DSS requirements.

12.3 Transmission of Data over Public Networks

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

IMPORTANT INFORMATION
The merchant or ASC must not install the EDH in an environment where sensitive data is transmitted directly from the EDH over a public network. If a merchant chooses to transmit sensitive data over a public network, the use of secure encryption transmission technology, that is IP security (IPsec), VPN, or Transport Layer Security (TLS), is required.

A merchant who supports public network connections must refer to PCI DSS requirements for information to properly transmit data over public networks.

12.4 Email and Messaging Technologies

Passport does not transmit cardholder data using end-user messaging technologies (email, SMS, instant messaging, and so on).

IMPORTANT INFORMATION
PCI DSS requirements prohibit transmission of unencrypted cardholder data using email or other end-user messaging technologies.

13 – Network Communication Requirements

The following tables detail the services and ports used by the EDH to communicate across network zones.

Protocol	Port(s)	Description
Automated Software Update	5802	Used to update software on the EDH.
Gilbarco File Transfer Service	5810	Used to transfer logs and reports from the EDH to the Manager Workstation.
Gripps	7000/7001	Primary interface between the EDH and Manager Workstation for communications.
Microsoft Proprietary	49152 49153 49154 49155	Diagnostic interfaces used to support shutdown, as well as, task and event viewing.
Fiserv Payment Interface	Customer and Implementation Dependent	Primary protocol used for transaction processing to the payment processor

This page is intentionally left blank.

14 – System Services

The following table details the System Services utilized on the Passport EDH. All services are system managed and do not require any user configuration or maintenance.

Service	Description
ActiveX Installer (AxInstSV)	Provides User Account Control validation for the installation of ActiveX controls from the Internet and enables management of ActiveX control installation based on Group Policy settings. This service is started on demand and if disabled the installation of ActiveX controls will behave according to default browser settings.
Adaptive Brightness	Monitors ambient light sensors to detect changes in ambient light and adjust the display brightness. If this service is stopped or disabled, the display brightness will not adapt to lighting conditions.
Application Experience	Processes application compatibility cache requests for applications as they are launched.
Application Identity	Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced.
Application Information	Facilitates the running of interactive applications with additional administrative privileges. If this service is stopped, users will be unable to launch applications with the additional administrative privileges they may require to perform desired user tasks.
Application Layer Gateway Service	Provides support for third-party protocol plug-ins for Internet Connection Sharing (ICS).
Application Management	Processes installation, removal, and enumeration requests for software deployed through Group Policy. If the service is disabled, users will be unable to install, remove, or enumerate software deployed through Group Policy. If this service is disabled, any services that explicitly depend on it will fail to start.
ASU	(Gilbarco) Automated Software Upgrade
ASP.NET State Service	Provides support for out-of-process session states for ASP.NET. If this service is stopped, out-of-process requests will not be processed. If this service is disabled, any services that explicitly depend on it will fail to start.
Background Intelligent Transfer Service (BITS)	Transfers files in the background using idle network bandwidth. If the service is disabled, then any applications that depend on BITS, such as Windows Update or MSN® Explorer, will be unable to automatically download programs and other information.
Base Filtering Engine	The Base Filtering Engine (BFE) is a service that manages firewall and IPsec policies and implements user mode filtering. Stopping or disabling the BFE service will significantly reduce the security of the system. It will also result in unpredictable behavior in IPsec management and firewall applications.
Bit9 Agent	Monitors system activity to keep your computer safe from unwanted and potentially malicious software.
BitLocker Drive Encryption Service	BitLocker Drive Encryption Service (BDESVC) hosts the BitLocker Drive Encryption service. BitLocker Drive Encryption provides secure startup for the operating system, as well as full volume encryption for OS, fixed or removable volumes. This service allows BitLocker to prompt users for various actions related to their volumes when mounted, and unlocks volumes automatically without user interaction. Additionally, it stores recovery information to Active Directory, if available, and, if necessary, ensures the most recent recovery certificates are used. Stopping or disabling the service would prevent users from leveraging this functionality.
Block Level Backup Engine Service	The WBENGINE service is used by Windows Backup to perform backup and recovery operations. If this service is stopped by a user, it may cause the currently running backup or recovery operation to fail. Disabling this service may disable backup and recovery operations using Windows Backup on this computer.
Bluetooth® Support Service	The Bluetooth service supports discovery and association of remote Bluetooth devices. Stopping or disabling this service may cause already installed Bluetooth devices to fail to operate properly and prevent new devices from being discovered or associated.

Service	Description
BranchCache	This service caches network content from peers on the local subnet.
Certificate Propagation	Copies user certificates and root certificates from smart cards into the current user's certificate store, detects when a smart card is inserted into a smart card reader, installs the smart card Plug and Play (PnP) minidriver if needed.
Client for NFS	Enables this computer to access files on Network File System (NFS) shares.
CNG Key Isolation	The CNG key isolation service is hosted in the Local Security Authority (LSA) process. The service provides key process isolation to private keys and associated cryptographic operations as required by the Common Criteria. The service stores and uses long-lived keys in a secure process complying with Common Criteria requirements.
COM+ Event System	Supports System Event Notification Service (SENS), which provides automatic distribution of events to subscribing Component Object Model (COM) components. If the service is stopped, SENS will close and will not be able to provide logon and logoff notifications. If this service is disabled, any services that explicitly depend on it will fail to start.
COM+ System Application	Manages the configuration and tracking of COM+-based components. If the service is stopped, most COM+-based components will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.
Computer Browser	Maintains an updated list of computers on the network and supplies this list to computers designated as browsers. If this service is stopped, this list will not be updated or maintained. If this service is disabled, any services that explicitly depend on it will fail to start.
Credential Manager	Provides secure storage and retrieval of credentials to users, applications, and security service packages.
Cryptographic Services	Provides four management services: Catalog Database Service, which confirms the signatures of Windows files and allows new programs to be installed; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from this computer; Automatic Root Certificate Update Service, which retrieves root certificates from Windows Update and enable scenarios such as TLS; and Key Service, which helps enroll this computer for certificates. If this service is stopped, these management services will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.
DCOM Server Process Launcher	The DCOMLAUNCH service launches COM and Distributed COM (DCOM) servers in response to object activation requests. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the DCOMLAUNCH service running.
Desktop Window Manager Session Manager	Provides Desktop Window Manager startup and maintenance services.
Dynamic Host Configuration Protocol (DHCP) Client	Registers and updates IP addresses and Domain Name System (DNS) records for this computer. If this service is stopped, this computer will not receive dynamic IP addresses and DNS updates. If this service is disabled, any services that explicitly depend on it will fail to start.
Diagnostic Policy Service	The Diagnostic Policy Service enables problem detection, troubleshooting and resolution for Windows components. If this service is stopped, diagnostics will no longer function.
Diagnostic Service Host	The Diagnostic Service Host is used by the Diagnostic Policy Service to host diagnostics that need to run in a Local Service context. If this service is stopped, any diagnostics that depend on it will no longer function.
Diagnostic System Host	The Diagnostic System Host is used by the Diagnostic Policy Service to host diagnostics that need to run in a Local System context. If this service is stopped, any diagnostics that depend on it will no longer function.
Dialog Box Filter	Prevents dialogs and windows from blocking or interfering with the primary user interface.
Disk Defragmenter	Provides Disk Defragmentation Capabilities.
Distributed Link Tracking Client	Maintains links between New Technology File System (NTFS) files within a computer or across computers in a network.
Distributed Transaction Coordinator	Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. If this service is stopped, these transactions will fail. If this service is disabled, any services that explicitly depend on it will fail to start.

Service	Description
DNS Client	The DNS Client service (dnscache) caches DNS names and registers the full computer name for this computer. If the service is stopped, DNS names will continue to be resolved. However, the results of DNS name queries will not be cached and the computer's name will not be registered. If the service is disabled, any services that explicitly depend on it will fail to start.
EDH	(Gilbarco) Starts the Gripps service and NGCrind, monitors the Gripps service and Fuel Subsystems, and Stop Gripps and Fuel when Stopped. Also ensures System Recovery and the EdhSQLStartMonitor has run at start.
Encrypting File System (EFS)	Provides the core file encryption technology used to store encrypted files on NTFS file system volumes. If this service is stopped or disabled, applications will be unable to access encrypted files.
EventLogMonitor	(Gilbarco) Event Log Monitor writes Windows Events to a text file included in Audit Logging.
Extensible Authentication Protocol	The Extensible Authentication Protocol (EAP) service provides network authentication in such scenarios as 802.1x wired and wireless, VPN, and Network Access Protection (NAP). EAP also provides Application Programming Interfaces (APIs) that are used by network access clients, including wireless and VPN clients, during the authentication process. If you disable this service, this computer is prevented from accessing networks that require EAP authentication.
Fiserv/First Data Hardware Detection	Provides notifications for AutoPlay hardware events.
Function Discovery Provider Host	The FDPHOST service hosts the Function Discovery (FD) network discovery providers. These FD providers supply network discovery services for the Simple Services Discovery Protocol (SSDP) and Web Services - Discovery (WS-D) protocol. Stopping or disabling the FDPHOST service will disable network discovery for these protocols when using FD. When this service is unavailable, network services using FD and relying on these discovery protocols will be unable to find network devices or resources.
Function Discovery Resource Publication	Publishes this computer and resources attached to this computer so they can be discovered over the network. If this service is stopped, network resources will no longer be published and they will not be discovered by other computers on the network.
GDSSVC	Gilbarco Deployment Service used for Deployment and Diagnostics.
GIAFramework	(Gilbarco) GIA Publish/Subscribe Framework
Gilbarco Secure CF Card Manager	(Gilbarco) Manager of iButton Encryption Services
GilbarcoScheduler	(Gilbarco) System Task/Job Scheduler
Gripps	(Gilbarco) Generic Retail Payment Processor System.
Group Policy Client	The service is responsible for applying settings configured by administrators for the computer and users through the Group Policy component. If the service is stopped or disabled, the settings will not be applied and applications and components will not be manageable through Group Policy. Any components or applications that depend on the Group Policy component might not be functional if the service is stopped or disabled.
GVR Diag	Gilbarco Diagnostics Service
GVRFTS	Gilbarco File Transfer Service
Health Key and Certificate Management	Provides X.509 certificate and key management services for the NAPAgent. Enforcement technologies that use X.509 certificates may not function properly without this service.
HomeGroup Listener	Makes local computer changes associated with configuration and maintenance of the homegroup-joined computer. If this service is stopped or disabled, your computer will not work properly in a homegroup and your homegroup might not work properly. It is recommended that you keep this service running.
HomeGroup Provider	Performs networking tasks associated with configuration and maintenance of homegroups. If this service is stopped or disabled, your computer will be unable to detect other homegroups and your homegroup might not work properly. It is recommended that you keep this service running.

Service	Description
Human Interface Device Access	Enables generic input access to Human Interface Devices (HID), which activates and maintains the use of predefined hot buttons on keyboards, remote controls, and other multimedia devices. If this service is stopped, hot buttons controlled by this service will no longer function. If this service is disabled, any services that explicitly depend on it will fail to start.
IKE and AuthIP IPsec Keying Modules	The IKEEXT service hosts the Internet Key Exchange (IKE) and Authenticated Internet Protocol (AuthIP) keying modules. These keying modules are used for authentication and key exchange in IPsec. Stopping or disabling the IKEEXT service will disable IKE and AuthIP key exchange with peer computers. IPsec is typically configured to use IKE or AuthIP; therefore, stopping or disabling the IKEEXT service might result in an IPsec failure and might compromise the security of the system. It is strongly recommended that you have the IKEEXT service running.
Indexing Service	Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.
Interactive Services Detection	Enables user notification of user input for interactive services, which enables access to dialogs created by interactive services when they appear. If this service is stopped, notifications of new interactive service dialogs will no longer function and there might not be access to interactive service dialogs. If this service is disabled, both notifications of and access to new interactive service dialogs will no longer function.
Internet Connection Sharing	Provides network address translation, addressing, name resolution and/or intrusion prevention services for a home or small office network.
IP Helper	Provides tunnel connectivity using IPv6 transition technologies (6to4, ISATAP, Port Proxy, and Teredo), and Internet Protocol-Secure Hypertext Transfer Protocol (IP-HTTPS). If this service is stopped, the computer will not have the enhanced connectivity benefits that these technologies offer.
IPsec Policy Agent	Internet Protocol security (IPsec) supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. This service enforces IPsec policies created through the IP Security Policies snap-in or the command-line tool “netsh ipsec”. If you stop this service, you may experience network connectivity issues if your policy requires that connections use IPsec. Also, remote management of Windows Firewall is not available when this service is stopped.
Keyboard Filter	Controls keystroke filtering and mapping.
KtmRm for Distributed Transaction Coordinator	Coordinates transactions between the Microsoft Distributed Transaction Coordinator (MSDTC) and the Kernel Transaction Manager (KTM). If it is not needed, it is recommended that this service remain stopped. If it is needed, both MSDTC and KTM will start this service automatically. If this service is disabled, any MSDTC transaction interacting with a Kernel Resource Manager will fail and any services that explicitly depend on it will fail to start.
Link-Layer Topology Discovery Mapper	Creates a Network Map, consisting of PC and device topology (connectivity) information, and metadata describing each PC and device. If this service is disabled, the Network Map will not function properly.
LPD Service	Enables client computers to print to the Line Printer Daemon (LPD) service on this server using TCP/IP and the Line Printer Remote (LPR) protocol.
Microsoft .NET Framework NGEN v2.0.50727_X86	Microsoft .NET Framework NGEN
Microsoft .NET Framework NGEN v4.0.30319_X86	Microsoft .NET Framework NGEN
Microsoft iSCSI Initiator Service	Manages Internet Small Computer System Interface (iSCSI) sessions from this computer to remote iSCSI target devices. If this service is stopped, this computer will not be able to log in or access iSCSI targets. If this service is disabled, any services that explicitly depend on it will fail to start.
Microsoft Software Shadow Copy Provider	Manages software-based volume shadow copies taken by the Volume Shadow Copy service. If this service is stopped, software-based volume shadow copies cannot be managed. If this service is disabled, any services that explicitly depend on it will fail to start.

Service	Description
Multimedia Class Scheduler	Enables relative prioritization of work based on system-wide task priorities. This is intended mainly for multimedia applications. If this service is stopped, individual tasks resort to their default priority.
Net.Msmq Listener Adapter	Receives activation requests over the net.msmq and msmq.formatname protocols and passes them to the Windows Process Activation Service.
Net.Pipe Listener Adapter	Receives activation requests over the net.pipe protocol and passes them to the Windows Process Activation Service.
Net.Tcp Listener Adapter	Receives activation requests over the net.tcp protocol and passes them to the Windows Process Activation Service.
Net.Tcp Port Sharing Service	Provides ability to share TCP ports over the net.tcp protocol.
Netlogon	Maintains a secure channel between this computer and the domain controller for authenticating users and services. If this service is stopped, the computer may not authenticate users and services and the domain controller cannot register DNS records. If this service is disabled, any services that explicitly depend on it will fail to start.
Network Access Protection Agent	The NAP agent service collects and manages health information for client computers on a network. Information collected by NAP agent is used to make sure that the client computer has the required software and settings. If a client computer is not compliant with health policy, it can be provided with restricted network access until its configuration is updated. Depending on the configuration of health policy, client computers might be automatically updated so that users quickly regain full network access without having to manually update their computer.
Network Connections	Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.
Network List Service	Identifies the networks to which the computer has connected, collects and stores properties for these networks, and notifies applications when these properties change.
Network Location Awareness	Collects and stores configuration information for the network and notifies programs when this information is modified. If this service is stopped, configuration information might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Network Store Interface Service	This service delivers network notifications (e.g. interface addition/deleting, etc.) to user mode clients. Stopping this service will cause loss of network connectivity. If this service is disabled, any other services that explicitly depend on this service will fail to start.
Offline Files	The Offline Files service performs maintenance activities on the Offline Files cache, responds to user logon and logoff events, implements the internals of the public API, and dispatches interesting events to those interested in Offline Files activities and changes in cache state.
Peer Name Resolution Protocol	Enables serverless peer name resolution over the Internet using the Peer Name Resolution Protocol (PNRP). If disabled, some peer-to-peer and collaborative applications, such as Remote Assistance, may not function.
Peer Networking Grouping	Enables multi-party communication using Peer-to-Peer Grouping. If disabled, some applications, such as HomeGroup, may not function.
Peer Networking Identity Manager	Provides identity services for the PNRP and Peer-to-Peer Grouping services. If disabled, the PNRP and Peer-to-Peer Grouping services may not function, and some applications, such as HomeGroup and Remote Assistance, may not function correctly.
Performance Logs & Alerts	Performance Logs and Alerts Collects performance data from local or remote computers based on preconfigured schedule parameters, then writes the data to a log or triggers an alert. If this service is stopped, performance information will not be collected. If this service is disabled, any services that explicitly depend on it will fail to start.
Plug and Play	Enables a computer to recognize and adapt to hardware changes with little or no user input. Stopping or disabling this service will result in system instability.
PnP-X IP Bus Enumerator	The PnP-X bus enumerator service manages the virtual network bus. It discovers network connected devices using the SSDP/WS discovery protocols and gives them presence in PnP. If this service is stopped or disabled, presence of Network Computing Device (NCD) devices will not be maintained in PnP. All pnpx based scenarios will stop functioning.

Service	Description
PNRP Machine Name Publication Service	This service publishes a machine name using the PNRP. Configuration is managed via the netsh context ‘p2p pnrp peer’.
Portable Device Enumerator Service	Enforces group policy for removable mass-storage devices. Enables applications such as Windows Media Player and Image Import Wizard to transfer and synchronize content using removable mass-storage devices.
Power	Manages power policy and power policy notification delivery.
Print Spooler	Loads files to memory for later printing.
Problem Reports and Solutions Control Panel Support	This service provides support for viewing, sending and deletion of system-level problem reports for the Problem Reports and Solutions control panel.
Program Compatibility Assistant Service	This service provides support for the Program Compatibility Assistant (PCA). PCA monitors programs installed and run by the user and detects known compatibility problems. If this service is stopped, PCA will not function properly.
Protected Storage	Provides protected storage for sensitive data, such as passwords, to prevent access by unauthorized services, processes, or users.
Quality Windows Audio Video Experience	Quality Windows Audio Video Experience (qWave) is a networking platform for Audio Video (AV) streaming applications on IP home networks. qWave enhances AV streaming performance and reliability by ensuring network Quality-of-Service (QoS) for AV applications. It provides mechanisms for admission control, run time monitoring and enforcement, application feedback, and traffic prioritization.
Remote Access Auto Connection Manager	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.
Remote Access Connection Manager	Manages dial-up and VPN connections from this computer to the Internet or other remote networks. If this service is disabled, any services that explicitly depend on it will fail to start.
Remote Desktop Configuration	Remote Desktop Configuration service (RDCS) is responsible for all Remote Desktop Services and Remote Desktop (RD) related configuration and session maintenance activities that require SYSTEM context. These include per-session temporary folders, RD themes, and RD certificates.
Remote Desktop Services	Allows users to connect interactively to a remote computer. Remote Desktop and Remote Desktop Session Host Server depend on this service. To prevent remote use of this computer, clear the check boxes on the Remote tab of the System properties control panel item.
Remote Desktop Services UserMode Port Redirector	Allows the redirection of Printers/Drives/Ports for RDP connections.
Remote Procedure Call (RPC)	The RPCSS service is the Service Control Manager for COM and DCOM servers. It performs object activations requests, object exporter resolutions and distributed garbage collection for COM and DCOM servers. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the RPCSS service running.
Remote Procedure Call (RPC) Locator	In Windows 2003 and earlier versions of Windows, the RPC Locator service manages the RPC name service database. In Windows Vista™ and later versions of Windows, this service does not provide any functionality and is present for application compatibility.
Remote Registry	Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.
RIP Listener	Listens for route updates sent by routers that use the Routing Information Protocol version 1 (RIPv1).
Routing and Remote Access	Offers routing services to businesses in local area and wide area network environments.

Service	Description
RPC Endpoint Mapper	Resolves RPC interfaces identifiers to transport endpoints. If this service is stopped or disabled, programs using RPC services will not function properly.
Secondary Logon	Enables starting processes under alternate credentials. If this service is stopped, this type of logon access will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Secure Socket Tunneling Protocol Service	Provides support for the Secure Socket Tunneling Protocol (SSTP) to connect to remote computers using VPN. If this service is disabled, users will not be able to use SSTP to access remote servers.
Security Accounts Manager	The startup of this service signals other services that the Security Accounts Manager (SAM) is ready to accept requests. Disabling this service will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to fail to start correctly. This service should not be disabled.
Security Center	The Windows Security Center Service (WSCSVC) monitors and reports security health settings on the computer. The health settings include firewall (on/off), antivirus (on/off/out of date), antispyware (on/off/out of date), Windows Update (automatically/manually download and install updates), User Account Control (on/off), and Internet settings (recommended/not recommended). The service provides COM APIs for independent software vendors to register and record the state of their products to the Security Center service. The Action Center (AC) User Interface (UI) uses the service to provide systray alerts and a graphical view of the security health states in the AC control panel. NAP uses the service to report the security health states of clients to the NAP Network Policy Server to make network quarantine decisions. The service also has a public API that allows external consumers to programmatically retrieve the aggregated security health state of the system.
Server	Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Simple TCP/IP Services	Supports the following TCP/IP services: Character Generator, Daytime, Discard, Echo, and Quote of the Day.
Smart Card	Manages access to smart cards read by this computer. If this service is stopped, this computer will be unable to read smart cards. If this service is disabled, any services that explicitly depend on it will fail to start.
Smart Card Removal Policy	Allows the system to be configured to lock the user desktop upon smart card removal.
SMIService	(Gilbarco) Secure Management Interface
SNMP Service	Enables Simple Network Management Protocol (SNMP) requests to be processed by this computer. If this service is stopped, the computer will be unable to process SNMP requests. If this service is disabled, any services that explicitly depend on it will fail to start.
SNMP Trap	Receives trap messages generated by local or remote SNMP agents and forwards the messages to SNMP management programs running on this computer. If this service is stopped, SNMP-based programs on this computer will not receive SNMP trap messages. If this service is disabled, any services that explicitly depend on it will fail to start.
Software Protection	Enables the download, installation and enforcement of digital licenses for Windows and Windows applications. If the service is disabled, the operating system and licensed applications may run in a notification mode. It is strongly recommended that you not disable the Software Protection service.
SPP Notification Service	Provides Software Licensing activation and notification.
SQL Active Directory Helper Service	Enables integration with Active Directories.
SQL Server (MSSQLSERVER)	Provides storage, processing and controlled access of data, and rapid transaction processing.
SQL Server Agent (MSSQLSERVER)	Executes jobs, monitors Structured Query language (SQL) Server, fires alerts, and allows automation of some administrative tasks.
SQL Server Browser	Provides SQL Server connection information to client computers.

Service	Description
SQL Server VSS Writer	Provides the interface to backup/restore Microsoft SQL server through the Windows Volume Shadow Copy Service (VSS) infrastructure.
SSDP Discovery	Discovers networked devices and services that use the SSDP discovery protocol, such as UPnP devices. Also announces SSDP devices and services running on the local computer. If this service is stopped, SSDP-based devices will not be discovered. If this service is disabled, any services that explicitly depend on it will fail to start.
StartProcSvc	(Gilbarco) Startup Processor for ASU Services.
Superfetch	Maintains and improves system performance over time.
SyslogServer	SYSLOG server which saves log entries to an SQL database.
SysRecoverySvc	Starts the System Recovery application and exits on completion.
System Event Notification Service	Monitors system events and notifies subscribers to COM+ Event System of these events.
Task Scheduler	Enables a user to configure and schedule automated tasks on this computer. The service also hosts multiple Windows system-critical tasks. If this service is stopped or disabled, these tasks will not be run at their scheduled times. If this service is disabled, any services that explicitly depend on it will fail to start.
TCP/IP NetBIOS Helper	Provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution for clients on the network, therefore enabling users to share files, print, and log on to the network. If this service is stopped, these functions might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Telephony	Provides Telephony API (TAPI) support for programs that control telephony devices on the local computer and, through the LAN, on servers that are also running the service.
Telnet	Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet clients, including UNIX-based and Windows-based computers. If this service is stopped, remote user access to programs might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Themes	Provides user experience theme management.
Thread Ordering Server	Provides ordered execution for a group of threads within a specific period of time.
TPM Base Services	Enables access to the Trusted Platform Module (TPM), which provides hardware-based cryptographic services to system components and applications. If this service is stopped or disabled, applications will be unable to use keys protected by the TPM.
UPnP Device Host	Allows Universal PnP (UPnP) devices to be hosted on this computer. If this service is stopped, any hosted UPnP devices will stop functioning and no additional hosted devices can be added. If this service is disabled, any services that explicitly depend on it will fail to start.
User Profile Service	This service is responsible for loading and unloading user profiles. If this service is stopped or disabled, users will no longer be able to successfully logon or logoff, applications may have problems getting to users' data, and components registered to receive profile event notifications will not receive them.
Virtual Disk	Provides management services for disks, volumes, file systems, and storage arrays.
Volume Shadow Copy	Manages and implements Volume Shadow Copies used for backup and other purposes. If this service is stopped, shadow copies will be unavailable for backup and the backup may fail. If this service is disabled, any services that explicitly depend on it will fail to start.
WebClient	Enables Windows-based programs to create, access, and modify Internet-based files. If this service is stopped, these functions will not be available. If this service is disabled, any services that explicitly depend on it will fail to start.
Windows Audio	Manages audio for Windows-based programs. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.
Windows Audio Endpoint Builder	Manages audio devices for the Windows Audio service. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.
Windows Backup	Provides Windows Backup and Restore capabilities.

Service	Description
Windows Biometric Service	The Windows biometric service gives client applications the ability to capture, compare, manipulate, and store biometric data without gaining direct access to any biometric hardware or samples. The service is hosted in a privileged SVCHOST process.
Windows CardSpace	Securely enables the creation, management, and disclosure of digital identities.
Windows Color System	The WcsPlugInService service hosts third-party Windows Color System color device model and gamut map model plug-in modules. These plug-in modules are vendor-specific extensions to the Windows Color System baseline color device and gamut map models. Stopping or disabling the WcsPlugInService service will disable this extensibility feature, and the Windows Color System will use its baseline model processing rather than the vendor's desired processing. This might result in inaccurate color rendering.
Windows Defender	Protection against spyware and potentially unwanted software.
Windows Driver Foundation - User-mode Driver Framework	Manages user-mode driver host processes.
Windows Error Reporting Service	Allows errors to be reported when programs stop working or responding and allows existing solutions to be delivered. Also allows logs to be generated for diagnostic and repair services. If this service is stopped, error reporting might not work correctly and results of diagnostic services and repairs might not be displayed.
Windows Event Collector	This service manages persistent subscriptions to events from remote sources that support WS-Management protocol. This includes Windows Vista event logs, hardware and IPMI-enabled event sources. The service stores forwarded events in a local Event Log. If this service is stopped or disabled event subscriptions cannot be created and forwarded events cannot be accepted.
Windows Event Log	This service manages events and event logs. It supports logging events, querying events, subscribing to events, archiving event logs, and managing event metadata. It can display events in both XML and plain text format. Stopping this service may compromise security and reliability of the system.
Windows Firewall	Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.
Windows Font Cache Service	Optimizes performance of applications by caching commonly used font data. Applications will start this service if it is not already running. It can be disabled, though doing so will degrade application performance.
Windows Image Acquisition (WIA)	Provides image acquisition services for scanners and cameras.
Windows Installer	Adds, modifies, and removes applications provided as a Windows Installer (*.msi) package. If this service is disabled, any services that explicitly depend on it will fail to start.
Windows Licensing Monitoring Service	This service monitors the Windows software license state.
Windows Management Instrumentation	Provides a common interface and object model to access management information about operating system, devices, applications and services. If this service is stopped, most Windows-based software will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.
Windows Media Player Network Sharing Service	Shares Windows Media Player libraries to other networked players and media devices using UPnP.
Windows Modules Installer	Enables installation, modification, and removal of Windows updates and optional components. If this service is disabled, install or uninstall of Windows updates might fail for this computer.
Windows Presentation Foundation Font Cache 3.0.0.0	Optimizes performance of Windows Presentation Foundation (WPF) applications by caching commonly used font data. WPF applications will start this service if it is not already running. It can be disabled, though doing so will degrade the performance of WPF applications.

Service	Description
Windows Remote Management (WS-Management)	Windows Remote Management (WinRM) service implements the WS-Management protocol for remote management. WS-Management is a standard web services protocol used for remote software and hardware management. The WinRM service listens on the network for WS-Management requests and processes them. The WinRM Service needs to be configured with a listener using winrm.cmd command line tool or through Group Policy in order for it to listen over the network. The WinRM service provides access to Windows Management Instrumentation (WMI) data and enables event collection. Event collection and subscription to events require that the service is running. WinRM messages use Hypertext Transfer Protocol (HTTP) and HTTPS as transports. The WinRM service does not depend on IIS but is preconfigured to share a port with IIS on the same machine. The WinRM service reserves the /wsman URL prefix. To prevent conflicts with IIS, administrators should ensure that any websites hosted on IIS do not use the /wsman URL prefix.
Windows Time	Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Windows Update	Enables the detection, download, and installation of updates for Windows and other programs. If this service is disabled, users of this computer will not be able to use Windows Update or its automatic updating feature, and programs will not be able to use the Windows Update Agent (WUA) API.
WinHTTP Web Proxy Auto-Discovery Service	WinHTTP implements the client HTTP stack and provides developers with a Win32 API and COM Automation component for sending HTTP requests and receiving responses. In addition, WinHTTP provides support for auto-discovering a proxy configuration via its implementation of the Web Proxy Auto-Discovery (WPAD) protocol.
WMI Performance Adapter	Provides performance library information from WMI providers to clients on the network. This service only runs when Performance Data Helper is activated.
Workstation	Creates and maintains client network connections to remote servers using the SMB protocol. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Index

A
accessible 7-3
account lockout 5-1
administrator access 3-1
alphanumeric field 3-3
appended 4-4
Authorized Service Contractor 1-4

B
best practices 3-1
black box 1-4

C
cardholder data 1-1
Change Password 3-8
characters 4-3
compliance 1-1
compliant mode 7-5
consecutive invalid passwords 3-9
create 3-5

D
data retention 4-5
data retention period 4-5
data storage 4-5
default accounts 3-9
devices 3-9
Document Open Password 4-4

E
End of File Separator 9-1
Enhanced Dispenser Hub 1-1

F
File Header 9-1
financial data 7-6
format 7-10
fueling position 7-6

I
identify 9-3
IMPORTANT 7-3, 7-6
IP/MAC addresses 5-1

K
keystroke 3-8

L
lockout period 3-9
log entry 3-5
Loyalty systems 3-9

M
merchant network 3-1, 6-1

N
non-network tender 7-6
non-sales transactions 1-4

O
onsite updates 6-1

P
PA-DSS compliance 1-4
Passport Audit logs 9-3
Payment Application Data Security Standard 1-1
payment network 4-4
Period Selection 4-4
Platform Support Service 2-4
procedure 2-6

R
regulatory purposes 4-5
relevant network addendum 4-4
Remote Support 2-7
removals 3-5
requirements 1-1
Reset User 3-6
retention period 4-5
retrieve 4-1
router logs 9-2

S
Section Separator 9-1
secure authentication 3-9
secure delete process 9-2
Secure Report Password 4-1
Security Audit Log 3-5
Security Manager 2-1
Security Manager Interface 2-4
Security Manager Report 2-1
security-enabled 3-3
storage volume 4-5
support 2-3
Support Console 2-3
System Maintenance 2-2
System Maintenance login 2-2
System Management 2-7

T
Technical Support 5-7
terminate the process 4-5
two-factor authentication 5-1

U
unauthorized access 5-3
update 3-7
User Management 2-7
user-level access 3-1

V
validate 2-5
validates 4-3
vendor access 5-1
Virtual Private Network 5-1

7300 West Friendly Avenue • Post Office Box 22087
Greensboro, North Carolina 27420
Phone (336) 547-5000 • http://www.gilbarco.com • Printed in the U.S.A.
MDE-5523E Passport EDH (Fiserv®/First Data™) V11.23.01. Implementation Guide for PA-DSS V3.2 · May 2022*