Point of Sale
# Table of Contents

**GETTING STARTED** .................................................................................................................. 1  
Technical Support ......................................................................................................................... 1  
Point-of-Sale Overview .................................................................................................................... 2  
Point-of-Sale Devices ....................................................................................................................... 3  
  Receipt Printer ............................................................................................................................ 3  
  Cash Drawer ............................................................................................................................... 4  
  Verifone MX830 Payment device ............................................................................................... 5  
  Signature Pad ............................................................................................................................. 6  
  Customer Display ....................................................................................................................... 6  
  Weigh Scale ............................................................................................................................... 6  
  Barcode Scanner ......................................................................................................................... 6  

**PCI COMPLIANCE REQUIREMENTS** ......................................................................................... 9  
1 Payment Systems Security .......................................................................................................... 9  
  1.1 Introduction .......................................................................................................................... 9  
  1.2 Why you need to be concerned about this ......................................................................... 9  
  1.3 The PCI Data Security Standard ......................................................................................... 9  
2 Merchant and Requirements for Compliance ...................................................................... 11  
3 EBMS® PCI Security Practices ............................................................................................... 12  
4 Securely implementing EBMS® ........................................................................................... 12  
  Merchant Applicability .............................................................................................................. 12  
  4.1.1 Previous Versions ........................................................................................................... 12  
  Merchant Applicability .............................................................................................................. 12  

**TOUCH SCREEN POS SYSTEM** .......................................................................................... 21  
Overview ........................................................................................................................................ 21  
Configure POS Profiles .................................................................................................................. 22  
Programmable Buttons .................................................................................................................. 25  
Using the POS station ...................................................................................................................... 28  
Processing Credits and Returns .................................................................................................... 30  

**BAR CODES** ........................................................................................................................... 31  
Entering Bar Codes within EBMS .................................................................................................. 31  
  Bar codes for inventory items ...................................................................................................... 31  
Scanning Bar Codes ...................................................................................................................... 35  

**MOBILE SCANNER SOLUTION** ............................................................................................ 37  
Mobile Scanner Solution ............................................................................................................... 37  

**PAYMENT CARD PROCESSING** .......................................................................................... 39  
Processing Credit Cards using a Credit Card Gateway ............................................................... 39  
Troubleshooting PAYware PC .................................................................................................... 42  
For PAYware PC Administrators .................................................................................................. 43  

**ADVANCED TOOLS** ............................................................................................................... 47  
Sync Tool Overview ..................................................................................................................... 47  
On-Screen Keyboard .................................................................................................................... 48  

INDEX ............................................................................................................................................ 49
Getting Started

Technical Support

Welcome to the instructional manual for the E-Commerce module within EBMS. In the sections following, explanations and examples of the available features within the E-Commerce Module will be explained. If you need to reach our staff for further help, contact us using the information below:

Eagle Software
5351 Lincoln Highway, Suite 9
Gap, PA 17527
(717) 442-3247 x2
(717)-442-1096 fax
www.EagleBusinessSoftware.com
Email: Support@EagleBusinessSoftware.com

Manual Revision 7.4.214.565 July 2012
Point of Sale

Point-of-Sale Overview

The Eagle Business Software (EBMS) contains many powerful Point-of-Sale (POS) tools. These options are used to create invoices or sales receipts at the time of sale. Payment options such as cash, check, debit, and credit cards payments are processed within the POS window. The EBMS software contains three primary windows to process POS transactions:

1. The standard EBMS Invoice and SO Window: This option is documented within the main documentation (volume 1).
   - Review the Sales > Sales Orders section for more details on creating sales orders
   - Review the Sales > Invoices section for more details on creating and processing sales invoices
   - Review the Sales > Customer Payments Section for more details on processing payments

2. The Touch Screen POS System: This POS option is used primarily as a cash register replacement. This option can be used for a remote location, a multi-lane store, or any store that requires quick checkout options.
   - Review the following Touch Screen POS System > Overview section of this manual for more details.

3. The Online E-commerce web: This powerful browser based option can be used for retails sales or online ordering for distributors and wholesales sales.
   - Review the E-commerce documentation for more details on creating the POS option for the web.

Credit cards, Debit cards, and other specialty cards can be used as payments within each one of these POS options. The system uses the Verifone Payware PC software so the user can interface to a variety of merchant accounts and card programs. Review the Processing Credit Cards using a Credit Card Gateway section for more details on Payware PC service and setup.

The POS software systems of EBMS interface with a number of POS hardware devices such as cash drawers, receipt and invoice printers, bar code scanners, payment devices etc. These devices can be configured for individual POS stations. Review the Point-of-Sale Devices section for more details on configuring these hardware options.
Point-of-Sale Devices

Technology such as barcode scanners, cash drawers, and receipt printers can be interfaced within the EBMS software to create a powerful point-of-sale solution. Product and bin labels containing barcodes can be printed directly from the EBMS software. Electronic signature pads, credit card processing, customer pole displays, and weigh scales are some additional devices supported by EBMS.

EBMS does interface with a Touch Screen point-of-sale station. This POS station is an excellent cash register replacement. The combination of touch screen hardware and the easy-to-use POS software makes the system easy to operate for non-technical users. Review the separate Point-Of-Sale for Touch Screen software section for details on the setup instructions and user details for this option.

Receipt Printer

Install the receipt printer driver within MS Windows before configuring the report. Select Sales > Options from the main EBMS menu and click on the Reports tab.

Set receipt settings as shown above. Review the Sales > Invoices > Printing a Sales Invoice or Payment Receipt section for more details on these settings.
NOTE that all the settings within the Devices tab of Sales > Options are stored within the MS Windows registry of each individual computer.

The device settings must be set for each computer system or POS station.

Cash Drawer

The EBMS system supports serial cash drawers, USB cash drawers, and cash drawers connected to a receipt printer. The recommended configuration is the serial cash drawer. Open the following EBMS Devices tab within the computer that is attached to a cash drawer. Select Sales > Options from the main EBMS menu and click on the Device tab as shown below:

Select the Connect to device / file option when the cash drawer is connected to a printer or other device. Enter the device id. For example: LPT1 for printers connected to the primary printer port.

Select the Connect to serial port option when cash drawer is connected to a serial port. Set the appropriate serial port settings:
Set the appropriate **Control string** that is used to open the cash drawer. This is the control string that is sent to the device or serial port to open the cash drawer. Use a backward slash (\) and a 3 digit ASCII number. For example: `\027P\000\025\250` will open the cash drawer for Epson printers.

### Verifone MX830 Payment device

The Verifone MX830 payment device is a secure method of processing credit card and debit card payments. The device is a combination of a credit card swipe device, Debit card keypad, and signature pad.

Select MX830 from the Verifone device drop down options and click on the **Port Settings** button. Set the following settings:
Point of Sale

The **Signature Pad** selection will be disabled when the MX830 **Verifone device** is selected.

Set the appropriate **Signature Size** for the MX830 device.

**Signature Pad**

The only **Signature Pad** option at the time of this documentation was the MX830. Note that some legacy pads are supported. Contact your EBMS support technician for details on the signature pad settings.

**Customer Display**

**Weigh Scale**

**Barcode Scanner**

The EBMS software can support a variety of bar codes and bar code scanners. Keyboard wedge scanners and serial port scanners are both support. The Serial port scanner is recommended because of reliability and speed. All bar code scanners must be properly programmed to interface with the EBMS software. Review the [Bar Codes > Scanning Bar Codes](#) section for details on configuring and scanner setup.
PCI Compliance

Requirements

1 Payment Systems Security

1.1 Introduction

In order to address the growing national and international concern for securing credit card information, Visa began to develop standards and announced the Cardholder Information Security Program (CISP) in April, 2000. These standards became required in June, 2001, for all entities that store, process or transmit Visa cardholder data.

Since that time, other credit card companies have become involved, and a new group called the Payment Card Industry Security Standards Council was formed to standardize security requirements across the entire credit card industry. The result is a new security standard called Payment Card Industry Data Security Standard (PCI-DSS or simply "PCI") which is designed to ensure standardized compliance for multiple associations.

This document is provided to guide users of EBMS® into becoming and remaining PCI compliant.

1.2 Why you need to be concerned about this

Credit Card companies are requiring compliance with PCI standards for every entity that is involved in the storage, processing, or transmission of credit card information. Failure to comply can result in denial or revocation of your organization’s ability to process credit cards.

Furthermore, as these standards have become widely recognized, non-compliance places your organization at risk of legal and/or civil consequences if credit card information becomes compromised.

Compliance with PCI standards is necessary whether or not you use EBMS® to process transactions “online.” Even if you use a POS terminal or other method to process transactions, and simply retain information in EBMS®, you must be concerned about proper use of the program to maintain security and confidentiality of customer data.

As of October 1, 2008, Credit Card Processors and Bank Card Acquirers must only accept level 3 and 4 merchants that are PCI-DSS compliant or that utilize PA-DSS compliant applications.

Beginning October 1, 2009, all payment applications which are not PA-DSS compliant will be de-certified.

Beginning July 1, 2010, Credit Card Processors and Bank Card Acquirers must ensure that merchants and agents use only PA-DSS compliant applications.

1.3 The PCI Data Security Standard

The "PCI-DSS" is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.
To learn more about PCI, visit www.pcisecuritystandards.org.

The standard must constantly evolve in order to remain viable in today’s rapidly changing internet and computing environment. Thus, the PCI-DSS will be reviewed at least every 24 months, and can be updated at any time.

EBMS® version 7.4 has been certified as compliant under the Payment Application Data Security Standard (PA-DSS) 1.2. The PA-DSS is a separate security standard that applies to software vendors that develop applications for sale to merchants to process and/or store cardholder data. Just because EBMS® has been certified as PA-DSS 1.2 compliant does not automatically make you, as a merchant, PCI compliant. It is an important and necessary step toward that goal. Payment applications validated per the PA-DSS, when implemented in a PCI-DSS-compliant manner, will minimize the potential for security breaches leading to compromises of sensitive cardholder data, and the damaging fraud resulting from these breaches, and speed you on your way to PCI compliance.
## 2 Merchant and Requirements for Compliance

There are twelve basic requirements (organized in six areas) which a merchant must meet in order to become certified as PCI-compliant. Each of these requirements, along with POS Vendor’s recommendations, is noted in this document. However, you must familiarize yourself with the details of each requirement as set forth in the PCI Data Security Standard documentation. (Refer to Section 4 “Reference” for guidance on where to get more information.) The following table lists the twelve basic requirements.

### PCI Requirements

<table>
<thead>
<tr>
<th>PCI Topic</th>
<th>Basic Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Use and regularly update anti-virus software</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to cardholder data by business need-to-know</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>12. Maintain a policy that addresses information security</td>
</tr>
</tbody>
</table>
3 EBMS® PCI Security Practices

Because it has been certified as compliant under the PA-DSS 1.2 requirements, using EBMS® as a tool will support you in meeting some of your merchant requirements to become and remain PCI-DSS compliant. However, it is important that you use the software as designed, and that you follow certain practices and procedures internally both when you install the software and as you enter transactions.

Compliance with PCI standards is necessary and you must be concerned about proper use of the program to maintain security and confidentiality of customer data. Therefore, the following sections provide guidance on how to implement and maintain the EBMS® application per PA-DSS requirements (as they relate to PCI) along with other general PCI security information.

4 Securely implementing EBMS®

4.1 Sensitive Authentication Data

Reference: PA-DSS 1.0 Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data

EBMS® version 7.4 does not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PINs or PIN block data.

EBMS® is using PA-DSS compliant Verifone PAYware PC as payment engine. This means processing transactions through Verifone PAYware PC is PA-DSS compliant. This covers the moment when Verifone PAYware PC receives the transaction and returns a response to EBMS®.

Since EBMS® version 7.4 has also been certified as compliant under the Payment Application Data Security Standard (PA-DSS) 1.2, the end-to-end transaction process beginning with entry into the EBMS® until the response from Verifone PAYware PC is returned has met the same level of compliance as Verifone PAYware PC’s PA-DSS compliance.

Refer to “Important Security Notice” section in Verifone PAYware PC’s Users Manual document on how to securely implementing Verifone PAYware PC.

Merchant Applicability

You must not, physically or digitally or in any other way, retain any sensitive payment card data. It is the merchant’s responsibility to remove any magnetic stripe data, card validation values or codes, PINs or PIN block data, cryptographic key material, or cryptograms stored by previous versions of the software. Removal of this prohibited historical data is required for PCI compliance.

4.1.1 Previous Versions

Any previous versions of EBMS® have never stored:

- full magnetic stripe, or
- PINs or PIN block data.

EBMS® version 7.1 or earlier does, however, facilitate credit cards PANs and card validation codes or values (CAV2, CID, CVC2, CVV2) storage. These must be removed. The removal of this data is required for PCI compliance.

Merchant Applicability

Users of EBMS® version 7.1 or earlier that stored credit card information in customer’s and sales invoice’s terms and have upgraded to version 7.4, need to run RemoveCCTerms.exe application. You can download it by logging in to:
http://www.eaglebusinesssoftware.com/support/login/
 PCI Compliance Requirements

RemoveCCTerms.exe will put mask values in place of the sensitive data and then delete the credit card data. This removes credit card information on customers and invoices.

If you are not sure and are now running EBMS® version 7.4, Esh Computer Center encourages you to just simply run the application.

4.1.2 Troubleshooting

EBMS® and its developers/vendor (Esh Computer Center) never collects nor stores customers’ full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), PINs or PIN block data for any debugging or troubleshooting purposes.

4.2 Protect Stored Cardholder Data

Reference: PA-DSS 2.0 Protect stored cardholder data

- All card numbers are masked on the displayed after entry and tabbing off the field. Receipts and reports generated from EBMS® also have card numbers masked.

- All sensitive cardholder data is rendered unreadable or not fully shown in EBMS® database, reports, and logs.

- EBMS® is using a feature of PA-DSS compliant Verifone PAYware PC to enable EBMS® users to store and use a reference to a specific credit card PAN and expiration date that is stored in Verifone PAYware PC’s database. This “reference” is called REF_TROUTD and can be used for payment processing. No sensitive data is exposed during the request to retrieve or to use the REF_TROUTD.

- Transmissions of transaction requests from EBMS® to Verifone PAYware PC and back to EBMS® are secured by Verifone PAYware SIM SSL (Secure Socket Layer).

4.2.1 Purge Stale Cardholder Data

EBMS® does not store cardholder data, but utilizes Verifone PAYware PC’s ability to do so in its database.

Merchant Applicability

You (merchant) must purge cardholder data after expiration of merchant-defined retention period (see PCI DSS Requirement 3.1 below). Verifone PAYware PC users manual provides guidance for you on data removal and the location of the data to be deleted.

PCI DSS Requirement 3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.

4.2.2 Securely Delete Cryptographic Material
EBMS® has not used cryptographic key material or cryptograms to encrypt cardholder in versions prior to PA-DSS compliant 7.4 version.

4.3 Secure Authentication Features

Reference: PA-DSS 3.0 Secure authentication features

4.3.1 Administrative and Privileged Access to the Application

The "out of the box" installation of the payment application (Verifone PAYware PC') facilitates the use of unique user IDs and secure authentication (defined at PCI DSS Requirements 8.1, 8.2, and 8.5.8--8.5.15) for all administrative access and for all access to cardholder data.

Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the payment application.

You are not required to create secure passwords in EBMS® since it does not store sensitive credit card information. However, you should refer to the "Password and Account settings" section Verifone PAYware PC users manual for information on how to setup secure logins in Verifone PAYware PC.

EBMS® will require a Verifone PAYware PC login to communicate. This login should be setup as a "POS" role. Create a "POS" role that can create new transactions but cannot access any sensitive credit card information. See Verifone PAYware PC users manual for setting up logins. See screenshot of Verifone PAYware PC Administration Center below to review functionality the "POS" role should or should not have access to:
4.3.2 General Non-privileged Access to the Application

Access to the computer that has Verifone PAYware PC installed must require a unique user ID and secure authentication. PCI Data Security Standard Requirements 8.1 and 8.2

Please refer to Verifone PAYware PC users manual for instructions to control access, via unique user ID and PCI DSS-compliant secure authentication, to the computer that has Verifone PAYware PC installed.

PCI DSS Requirement 8.1: Assign all users a unique ID before allowing them to access system components or cardholder data.

PCI DSS Requirement 8.2: In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:

- Password or passphrase
- Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)

PA-DSS Requirement 4.0
Point of Sale

4.0 Log payment application activity

EBMS® does not log credit card transactions. This is done in the Verifone PAYware PC software. EBMS® sends the invoice number to Verifone PAYware PC so the invoice can be referenced when viewing the credit card transaction logs. EBMS® stores the TROUTD with the payment transaction in the invoice. The TROUTD can be searched in Verifone PAYware PC to get credit card transaction details. See Verifone PAYware PC documentation for more information on logging.

4.5 Protect Wireless Transmissions

Reference: PA-DSS 6.0 Protect wireless transmissions

4.5.1 Wireless Technology Included in or with the Payment Application

Wireless technology is not required or recommended with EBMS® because of network stability and speed requirements.

Per PCI DSS Requirement 1.2.3 you must install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

4.5.2 General Use of Wireless Technology

If wireless technology is used to connect to the computer where Verifone’s Payware PC® is installed, or if a wireless local area network (LAN) is connected to or part of the Verifone’s Payware PC® cardholder data environment (for example, not clearly separated by a firewall), the PCI DSS requirements and testing procedures for wireless environments apply and must be performed as well (for example, Requirements 1.2.3, 2.1.1, and 4.1.1). Before wireless technology is implemented, a company should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission.

Wireless environments must be implemented and maintained per the following PCI DSS Requirements:

**PCI-DSS 1.2.3** Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

**PCI-DSS 2.1.1** For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.

**PCI-DSS 4.1.1** Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.
• For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.
• For current wireless implementations, it is prohibited to use WEP after June 30, 2010.

4.6 Systems Connected to the Internet

Reference: PA-DSS 9.0 Cardholder data must never be stored on a server connected to the Internet

This is not applicable because:
• EBMS® does not store cardholder data, but utilizes PA-DSS compliant Verifone PAYware PC’s ability to do so in its database.
• EBMS® is using a feature of PA-DSS compliant Verifone PAYware PC to enable EBMS® users to store and use a reference to a specific credit card PAN and expiration date that is stored in Verifone PAYware PC’s database.

4.7 Secure Remote Software Updates

Reference: PA-DSS 10.0 Facilitate secure remote software updates

See the section, “Remote Update Procedures”, in Verifone PAYware PC’s users manual for details on software updates.

4.8 Secure Remote Access to Payment Application

Reference: PA-DSS 11.0 Facilitate secure remote access to payment application

4.8.1 Two-Factor Authentication

If the Verifone PAYware PC application must be accessed remotely, remote access to the payment application must be authenticated using a two-factor authentication mechanism. EBMS® does not require this security because it does not store sensitive credit card data.

Two-factor authentication is defined as something you have (e.g. smartcard or token) and something you know (e.g. PIN or biometric). These two factors must be presented in conjunction with one another to authenticate to a network or system.

PCI DSS Requirement 8.3: Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.
4.8.2 Secure Remote Access Requirements

While we encourage secure remote access to EBMS, it is not required for PCI compliance. However, secure remote access must be followed for the connection to the Verifone PAYware PC computer. See the “Password and Account settings” section in Verifone PAYware PC’s users manual for more information.

4.9 Encrypt Sensitive Traffic over Public Networks

Reference: PA-DSS 12.0 Encrypt sensitive traffic over public networks

EBMS® does not send cardholder data over public networks. Verifone PAYware PC does send this information through the internet. Refer to Verifone PAYware PC PA-DSS users guide section “Encrypting Network Traffic” for information on safeguarding sensitive cardholder data during transmission over open, public networks.

4.10 Encrypt all Non-console Administrative Access

Reference: PA-DSS 13.0 Encrypt all non-console administrative access

13.1 Encrypt all non-console administrative access using technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

PCI-DSS Requirement 8

Assign a Unique ID to each Person with Computer Access

PCI DSS 8.1: Assign all users a unique ID before allowing them to access system components or cardholder data.

PCI DSS 8.2: In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:

- Password or passphrase
- Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)

PCI DSS 8.3: Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

PCI DSS 8.4: Render all passwords unreadable during transmission and storage on all system components using strong cryptography (defined in PCI DSS Glossary of Terms, Abbreviations and Acronyms).
PCI DSS 8.5: Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:

PCI DSS 8.5.1: Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.

PCI DSS 8.5.2: Verify user identity before performing password resets

PCI DSS 8.5.3: Set first-time passwords to a unique value for each user and change immediately after first use

PCI DSS 8.5.4: Immediately revoke access for any terminated users

PCI DSS 8.5.5: Remove/disable inactive user accounts at least every 90 days.

PCI DSS 8.5.6: Enable accounts used by vendors for remote maintenance only during the time period needed

PCI DSS 8.5.7: Communicate password procedures and policies to all users who have access to cardholder data

PCI DSS 8.5.8: Do not use group, shared, or generic accounts and passwords

PCI DSS 8.5.9: Change user passwords at least every 90-days

PCI DSS 8.5.10: Require a minimum password length of at least seven characters

PCI DSS 8.5.11: Use passwords containing both numeric and alpha characters

PCI DSS 8.5.12: Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.

PCI DSS 8.5.13: Limit repeated access attempts by locking out the user ID after not more than six attempts.

PCI DSS 8.5.14: Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.

PCI DSS 8.5.15: If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal.
PCI DSS 8.5.16: Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.
A good point-of-sale (POS) system requires a solution that is quick, easy-to-use, and flexible to meet the needs of today’s retail environment. A retail system must be reliable and fail safe to offer a customer friendly service.

The Touch Screen POS System is an easy-to-use cash register replacement. The combination of the touch screen and the simple-to-use POS software makes the system easy to operate for non-technical users.

The Touch Screen system uses a combination of bar code scanning technology and programmable buttons to enhance both the usability and speed of the check out process. The programmable buttons can be configured to identify popular items, groups of items, discounts, and other processes that are commonly used at a POS station.

- Review the Configure POS Profiles section for details on configuring each of the POS station.
- Review the Programmable Buttons section for details on configuring these user defined buttons.

The Touch Screen system is driven by the inventory management system within EBMS. Grouping products and properly identifying bar code options require proper inventory planning.

Review the Inventory Items > Adding and Deleting Inventory Folders section for more details on grouping products.

Review the Bar Code Technology > Entering Bar Codes within EBMS section for more details on assigning bar codes to inventory items.

The Touch Screen POS system in conjunction with the optional Sync tool allows the system to run independently of the main computer network or the EBMS system database. The Sync option removes the dependance of the POS system to the speed or down time of the network. This Sync technology can also be used to poll POS systems in remote sales locations. This document labels clients that are not directly connected to the EBMS data but are connected to data using the Sync tool as remote clients. Review the Advanced Tools > Sync Tool Overview for more details on this option.

Continue with the Using POS Station section for instructions on using the system.
Configure POS Profiles

The point-of-sale (POS) configuration is done within the main EBMS program. A profile must be created for each POS station before a station can be used. POS stations do not share profiles. Go to Sales > Options and click on the Point of Sale tab to view the POS Profile list:

Click on the New button to create a new POS profile or the Properties button to change an existing profile.
Enter a unique Point of Sale Station Id that identifies the specific station.

Enter the Computer Name or IP address of the POS station. The Computer Name can be found by right clicking on the Computer menu option on the Windows start menu and selecting Properties. This setting must match the computer name for the POS station to operate properly.

Enter a Description of the POS station.

Enter an optional Default Customer Id code that is loaded when the POS station is launched. Miscellaneous customers are often used in a POS environment. Review the Sales > Miscellaneous Customer section within the main documentation for more details on Miscellaneous customers. This default customer code can be kept blank to prompt the user to enter a customer code each time the POS station is started. Review the Using the POS station section for more details on setting the customer id within the POS station window.

Enter an Invoice Prefix. The invoice number will be appended to the required Invoice Prefix to create a unique transaction number. This prefix must be unique for each POS profile.

The Next Invoice Number is incremented each time a new sales transaction is created. This number should be set to the first transaction (invoice) number when the POS profile is initially setup.
Disable the Allow credit payment on this POS option to restrict the user to only positive total transaction. When this option is disabled the user can not complete a sales transaction with a total that is less than zero. This option allows management to force the cashier to log into EBMS with proper security rights to process any credits or returns.

The Warehouse option will not appear unless the optional Multiple Warehouse Module is installed. The inventory that is sold on this POS station will be deducted from the specified warehouse. Review the Inventory > Warehousing > Warehouse Overview section of the inventory documentation for more details.

Click OK to continue

Review the Programmable Buttons section for details on the Programmable Buttons tab.
Programmable Buttons

A common method used to increase the efficiency of a POS station is to program quick key buttons on the right side of the window. These programmable buttons can indicate an individual inventory item or a group of items. Subgroups (folders within EBMS) can also be attached to a programmable button. Programmable buttons can also launch programs, J-scripts for custom processes, utilities, or a series of short cut keys. Each POS station contains its own set of programmable buttons although the Copy From button can be used to copy programmable button settings from one POS station to another.

Programmable buttons are setup within the POS Setup dialog within EBMS. Go to Sales > Options and click on the Point Of Sale tab. Highlight the appropriate POS profile and click on the Properties button. Review the Configure POS Profiles section for details on creating multiple POS profiles.

Click on the Programmable Buttons tab to open the button list as shown in the example below:

Click the New button to add a button to the list. The following List explains how to create some of the most common programmable buttons:
Point of Sale

- Button for fast moving items: The following example is a programmable button that is attached to a fast moving item - DIRSHO - Dirt Shovel.

Select the **Inventory Item** button type.

Enter the specific **Inventory ID**.

Normally the **Default Quantity** should equal 1. This value is copied to the **Quantity** column when this button is selected.

Enter the **Button Name**. This button must be labeled with a unique description.

The button color will default to the color associated with the **Button** type. Click on the **Choose Button Color** and select the desired color from the color dialog as shown below:
This dialog allows the user to select from the standard color list or to create custom colors. Click OK to choose a button color.

The **Undo**, **Set to No Color**, or **Reset to Default Color of This Button Type** buttons are useful to restore color values or set the color to the POS station's background (No Color).

Disable the **Active Button** option to remove the button from the POS Station without deleting the button.
Using the POS station

The POS station dialog is launched as a separate program file rather than from the main EBMS menu. The POS station program should be configured to launch when the PC or POS station is powered up. Review the MS Windows OS manual for details on launching programs on start up.

The user should login with a specific user name and password to properly record totals and sales for specific cashiers or users. Note that a person can logout quickly and prompt a new log in by clicking on the **Logout** button on the top of the POS window as shown below.

The following POS window is opened when the POS station is launched:

The **Customer ID** will need to be entered if a default Customer ID is not set within the POS Station properties. Review the **Configure POS Profiles** section for details on entering a default customer. The **Search** button located on the upper right corner of the dialog, will open the standard customer lookup dialog if the **Customer ID** entry is highlighted. Click on the **Customer ID** entry to highlight the customer code.

Click on the programmable keys to add products to the sales list or scan items with the POS bar code scanner. Review the **Bar Codes > Scanning Bar Codes** section for more details on scanning items.

**Inventory** items can also be typed into the system using a traditional keyboard or using the digital keyboard that is distributed with the MS Windows OS. Review the **Advanced Tools > On-Screen Keyboard** section for more details.

The **Inventory** item record can be opened by clicking on **Lookup** button located above the programmable button list. A standard search dialog can be opened by click on the **Search** button.
You can change the quantity of the items that were scanned or selected from a product button using the following methods:

- Increase or decrease the quantity by clicking on the `+` or `-` button on the Window's numeric keypad. The +/- keys can be used immediately after the item is selected or by highlighting a specific product and then clicking the +/- keys.

- Click on the **Quantity** entry and key the quantity using the numeric keypad on the screen or on a standard keyboard. Note that selecting the +/- key options will move highlight the **Quantity** column.

- Set the **Default Quantity** within the programmable button dialog to default the **Quantity** when the programmable button is selected. The **Quantity** column will be highlighted within the POS window if the **Default Quantity** within the programmable button properties is set to zero.

- The **Quantity** is incremented each time the same product bar code is scanned using a bar code scanner

An item can be removed from the sales list by highlighting the item and clicking the **Remove This Item** button. Click on the **Remove All Items** to clear the entire list.

Click on the appropriate **Payment** method using one of the payment buttons shown below:

![Payment Methods](image)

Note that only the applicable payment buttons will be enabled. The **Charge** button may be disabled for cash customers. Review the **Sales > Invoices > Payment Methods and Terms** section within the main documentation for details on the payment options including split tender details.

Click the **Clear Payment** button to clear a payment and choose a new payment.

Click the **Process** button to complete the transaction.
Processing Credits and Returns

Credits and returns are processed within EBMS including the Touch Screen POS station by entering a negative quantity after selecting the item. Select the item by scanning the bar code, touching a programmable button, or entering the SKU number in the Inventory column. Normally the quantity will default to “1”. Press the negative button located on the right side on the on-screen numeric keypad as shown below. The quantity will be reduced by 1 each time the negative button is pressed. Press the button twice to change the quantity from 1 to negative one. This will create a credit within the POS system as shown below:

Note that the profile must be configured to allow processing a sale with a credit amount. Enable the Allow credit transactions on this POS option within the POS station's profile within the main EBMS software. Review the Configure POS Profiles section for more details on this option.
Bar Codes

Entering Bar Codes within EBMS

Bar code technology can greatly enhance the efficiency and accuracy of data entry. Receiving, shipping, and point-of-sale processes can be greatly improved by using existing bar codes on products or by printing new bar codes for individual items, cases, or skids.

The EBMS Bar Code Controls, Reports, and Fonts kit gives the user the ability to print bar codes onto packing lists, work orders, and other forms. Product labels can be generated containing a bar code, pricing, and/or other product information. A variety of existing bar codes can be associated with inventory products or printed directly from a label or laser printer. A bar code can be associated with each unit-of-measure setting for an inventory item. The bar code technology that has been used by large companies for years is now affordable for a small business. EBMS incorporates this technology so you can run your business efficiently.

Bar codes for inventory items

Bar codes can be associated within individual inventory items using 2 different methods:

1. A bar code such as a UPC code can be entered within the inventory item record. Open an inventory item and click on the General tab.
Point of Sale

Enter the **UPC Code** into the upper right hand corner as shown above. Note that any valid bar code (non UPC code) can be entered within this entry. This bar code identifies the **Default Selling** unit of measure recorded within the **Count** tab. Review the **Inventory Items > Changing Inventory Items** section of the inventory documentation for more details on creating or changing general inventory details.

The bar code values for other units of measure are set within the UOM dialog. Click on the **Count** tab, select a unit-of-measure form the list, and click the **Properties** button to open the following dialog:

Enter the specific **Unit of measure** bar code within the **UPC** entry and press **OK** to save.
2. The Inventory ID can be printed in a bar code 39 format as shown below. Unlike the UPC code, the bar code 39 can consist of numbers or letters and can be of varying lengths. Note that the longer the inventory item ID

A inventory ID must consist of numbers and letters. Most symbols do not properly convert into bar codes. Note that IDs that contain spaces cannot be scanned using the bar code 39 font.

The EBMS system contains many reports that contain barcode fonts. Enable the Print Bar Code option on the print dialog of the report if the optional EBMS bar code font option is installed. Note that there are many bar code labels included in the reports menu. Go to File > Reports dialog for a complete list of reports.
Scanning Bar Codes

A variety of bar code scanners can be configured to be used with the EBMS software. Scanners must be programmed to work with the EBMS software. Contact an EBMS support rep for bar code scanner programming instructions. EBMS will accommodate scanners that are setup as a keyboard wedge and scanners that are attached to a COM port. There are benefits and limitations involved with each option.

Keyboard Wedge

Limitations:

The system cannot scan products as fast as the COM port scanner option.

Benefits:

- Allows the user to use a bar code scanner to scan any code into any field within EBMS.
- Maximum flexibility for a scanner that is used for many different processes.
- Ideal for a POS environment that occasionally uses the POS scanner or stations where checkout speed is average or less.

COM Port Connection

Limitations:

Only the following items can be scanned.
- Inventory items within the sales invoice or POS station screen
- Inventory items within the expense purchase order screen
- Consumed items within the manufacturing screen
- Inventory items within the Job Costing > Inventory Transfer screen
- Inventory items within the Warehouse transfer screen
- Rental items within the rental contract screen.

Benefits:

- Can scan very rapidly
- Ideal for checkout lanes that use the scanner primarily for a single process such as point-of-sale checkout.

Many of the scanners can be programmed to use either connection type.
Mobile Scanner Solution

The Eagle Mobile Scanner solution has functionality that features Shipping, Receiving, Warehouse and Job Transfers; including editing of quantities right on the device. An intuitive interface seamlessly integrates this remote, Wi-Fi enabled, hand-held device directly with your EBMS system. The expanded keypad makes typing and modifying data easy for all users. The device also features inventory count processing to allow cycle or end-of-year counting that makes inventory tracking and ordering a snap. Include the UPC Association functionality and the bar coding and tracking of your inventory has never been this fast and easy!

Main Features

- Highly functional touch screen
- Adjust Inventory counts
- Associate item UPC codes
- Populate Sales Orders on the fly
- Handle Shipping, Receiving, Warehouse & Job Transfers
- Print reports and labels quickly and easily
- Go wherever you have Wi-Fi coverage
- Set per employee permission controls and more

Streamline processes, reduce time spent managing inventory, and dramatically cut human errors.
Payment Card Processing

Processing Credit Cards using a Credit Card Gateway

The optional credit card gateway used by EBMS is PAYware PC Payment Server. This gateway allows a user to record and process a credit card within the EBMS software. The user can choose one of the many merchant accounts that interface with PAYware PC. Verify that the credit card merchant account is compatible to the PAYware PC payment server. Go to Payware Payment Processing for a preferred merchant reseller contact information.

Contact a EBMS customer Service Rep to properly install the payment server.

The credit card gateway settings are entered within the Payment records. The Payment options are accessed by selecting Sales > Options from the main EBMS menu and clicking on the Payment tab as shown below:
Configure the following PAYware PC settings:

1. Enable the **Disable PAYware PC** option only to disable the PAYware PC option. This option must be disabled to properly process credit cards within EBMS using the PAYware PC gateway.

2. Enter the name of the computer where PAYware PC payment server is installed into the **Computer name or IP Address** entry. This setting must be updated if the IP address or computer name changes.

3. Enter the PAYware PC **Port** value located within the PAYware PC management client.

4. Click on the **Credentials Settings** button to set the user credentials. This is a management setting that should only be accessed by the manager.

5. The **Report path** is an optional location setting to identify the location for reports exported to a file. This option may be disabled in the current version.

Click on a **Payment Name** record that reflects a credit card payment type using Payment PC Charge. Click on the **Properties** button to open the properties button.
The **Payment Name** identifies the payment type.

Enable the **Active** option.

Enter the following PAYware PC settings. Enter the settings for each department or warehouse if multiple records show as displayed above.

1. Set the appropriate **Cash Account**. Review the [Sales > Customer payments > Cash Accounts, Deposits, and Reconciling Cash](#) section for more details on setting the cash accounts.

2. Enter the four-digits payment **Processor ID**.

3. Enter the correct **Merchant No**.

4. Enter the Host\Termina **Processor Type**.

5. Enter the **Settlement URL**: This setting is used if your processor is host based. This URL identifies the processor's website that is used to access the processor's credit card settlement process.

Refer to the detailed PC Charge documentation for details on installing PC Charge, configuring merchant accounts, and other details.
Troubleshooting PAYware PC

Type topic text here.
For PAYware PC Administrators

Please Note: Due to PCI DSS Requirements, Verifone’s Payware PC’s password will expire every 2 months. This will effect EBMS as you will not be able to do credit card transactions until the Password has been changed in Payware PC.

When the password for PAYware PC expires, open the PAYware PC Management Client and you will be prompted for the old password and asked to enter a new one. The default password must have at least 7 characters including 1 uppercase character, 1 number and 1 special character.

After the password is changed in the PAYware PC Management Client, you are now required change the password in EBMS under the Sales > Options > Payments tab. Go to Sales > Options > Payments tab and click on the Credentials: Settings button:

The PAYware PC Credentials must be updated to allow it to connect to the Payware PC Management Client. Change and confirm the Password to the new password that was entered in the Payware PC Management Client.
Changing the Password before it expires (recommended)

To change the password before it expires, open the Payware PC Management Client. Click the Configuration button.

Click on the View Configuration button
Shown below is a list of options used to manage the PAYware PC Management Client.

Expand the **System Services** menu and click on **User Management** to view the **User** settings.
Select a user and click on the **Edit User** button on the bottom. You will now have the option of changing your password.

**Please Note:** Whenever the Administrator Password is changed in Payware PC, the password must be changed in EBMS as shown above.
Advanced Tools

Sync Tool Overview

The Sync Tool is an EBMS option that allows the user to duplicate data on a POS station or e-commerce data center. This tool could also be used with laptops that are not connected to the main EBMS network. The Sync Tool synchronizes the remote copy of the EBMS data (normally an abbreviated version) with the main EBMS database. The Sync Tool is a popular tool used in the following environment:

Point-of-Sale system: Touch Screen POS system in conjunction with the optional Sync tool allows the system to run independently of the main computer network or the EBMS system database. The Sync option removes the dependence of the POS system to the speed or down time of the network. This Sync technology can also be used to poll POS systems in remote sales locations.

The Sync tools is used
On-Screen Keyboard

Type topic text here.
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Button.................................27</td>
<td>Bank Card Acquirers .......................11</td>
<td>Cardholder Information Security Program..11</td>
<td>Default Color...............................27</td>
<td>Eagle Mobile Scanner ....................43</td>
</tr>
<tr>
<td>Disable.........................................27</td>
<td>Bar Codes ..................................41</td>
<td>announced ..................................11</td>
<td>Reset........................................27</td>
<td>EBMS1, 2, 3, 11, 14, 23, 24, 27, 34, 37, 41, 43, 45, 49, 53</td>
</tr>
<tr>
<td>Adjust Inventory..............................43</td>
<td>Scanning ..................................41</td>
<td>Cash Account ...............................45</td>
<td>Default Customer Id.......................24</td>
<td>back ..........................................14</td>
</tr>
<tr>
<td>Administrative Access ........................14</td>
<td>Bar Codes within EBMS ...................37</td>
<td>Cash Drawer ................................31</td>
<td>Default Quantity ........................27, 31</td>
<td>connected ..................................23</td>
</tr>
<tr>
<td>Administrative and Privileged Access ......14</td>
<td>Entering ..................................37</td>
<td>Charge button ..............................31</td>
<td>Set ...........................................31</td>
<td>Contact .....................................41, 45</td>
</tr>
<tr>
<td>the Application ...............................14</td>
<td>Barcode Scanner ............................3</td>
<td>Choose Button Color ......................27</td>
<td>Default Selling ............................37</td>
<td>copy ..........................................53</td>
</tr>
<tr>
<td>Administrator Password .....................49</td>
<td>Computer Access ..........................14</td>
<td>Clear Payment button .....................31</td>
<td>Disable PAYware PC .......................45</td>
<td>implementing ................................14</td>
</tr>
<tr>
<td></td>
<td>Computer Name ...............................24</td>
<td>Computer Name .............................24</td>
<td></td>
<td>Enable ......................................45</td>
</tr>
<tr>
<td></td>
<td>Configure POS Profiles ......................24</td>
<td>Configure POS Profiles ....................24</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Credentials Settings .......................45</td>
<td>Credentials Settings .....................45</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Credit Card Gateway .......................45</td>
<td>Credit Card Gateways .....................45</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit Card Processors .....................11</td>
<td>Customer Customer Display ..............3</td>
<td>Customer ID ................................31</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>G</td>
<td>H</td>
<td>I</td>
<td>J</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EBMS Bar Code Controls ....................37</td>
<td>Bank Card Acquirers .......................11</td>
<td>General Use of Wireless Technology ....14</td>
<td>Implementing ...............................14</td>
<td>Job Costing ................................41</td>
</tr>
<tr>
<td>EBMS Devices ..................................3</td>
<td>Bar Codes ..................................41</td>
<td>Hand Shipping ..............................43</td>
<td>EBMS .........................................14</td>
<td>Job Transfers .............................43</td>
</tr>
<tr>
<td>following .....................................3</td>
<td>Scanning ..................................41</td>
<td></td>
<td>EBMS ..........................14</td>
<td></td>
</tr>
<tr>
<td>EBMS Invoice .................................2</td>
<td>Enter .......................................37</td>
<td></td>
<td>Verifone PAYware PC ....................14</td>
<td>Keyboard Wedge ..........................41</td>
</tr>
<tr>
<td>EBMS menu ...................................3, 31, 45</td>
<td>Barcode Scanner ............................3</td>
<td>Inventories ..................................24</td>
<td></td>
<td>Laptops .................................53</td>
</tr>
<tr>
<td>Edit User ......................................49</td>
<td>Credit Card Processors ...................11</td>
<td>Incremented ................................24, 31</td>
<td>Implementing ...............................14</td>
<td>Mobile Scanner Solution .................43</td>
</tr>
<tr>
<td>Encrypt Sensitive Traffic ....................14</td>
<td>Customer Customer Display ..............3</td>
<td>Inventory ID ...............................27, 37</td>
<td>EBMS .........................................14</td>
<td>MS Windows OS ..........................31</td>
</tr>
<tr>
<td>Encrypting Network Traffic ................14</td>
<td>Customer ID ................................31</td>
<td>Inventory Item .............................27, 31</td>
<td>Important Security Notice ................14</td>
<td>Multiple Warehouse Module .............24</td>
</tr>
<tr>
<td>Esh Computer Center .........................14</td>
<td></td>
<td>Select ......................................27</td>
<td>Incremented ................................24, 31</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K</td>
<td>L</td>
<td>M</td>
<td>N</td>
<td>O</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keyboard Wedge .............................41</td>
<td>Laptops ......................................53</td>
<td>Main Features .............................43</td>
<td>Mobile Scanner Solution .................43</td>
<td>Multiple Warehouse Module .............24</td>
</tr>
<tr>
<td></td>
<td>Mobile Scanner Solution ..................43</td>
<td>Merchant Applicability ....................14</td>
<td>MS Windows OS ..........................31</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Review .....................................31</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
On-Screen Keyboard..............................54
Payment Application............................14
  Secure Remote Access..........................14
Payment Application Data Security Standard ..11, 14
Payment Card Industry Data Security Standard..11
Payment Card Industry Security Standards Council..........................11
Payment Name..................................45
Payment PC Charge...............................45
Payment Systems Security........................11
Payware PC.....................................2, 45, 48, 49
  disable.........................................45
  following......................................45
  Troubleshooting..............................48
  PAYware PC Administrators......................49
  PAYware PC Credentials........................49
  PAYware PC Management Client..................49
  connect........................................49
  PAYware PC Management Client..................49
  PAYware PC Payment Server........................45
  PAYware PC Port..................................45
  PC Charge.......................................45
  installing.....................................45
  PCI Data Security Standard.....................13
  PCI Data Security Standard Requirements 8.1........................................14
  Point Of Sale...................................27
  Point-of-Sale Devices...........................3
  Point-of-Sale Overview...........................2
  Populate Sales Orders...........................43
  Port Settings...................................3
  POS ..............................................53
    creating......................................2
    Description....................................24
    name..........................................24
    number........................................2
    use.............................................11
    uses.........................................41
  POS environ...................................24
  POS Profile list..............................24
  view.............................................24
  POS Setup dialog...............................27
  POS Station.....................................27, 31
  Using..........................................31
  Print Bar Code..................................37
  Enable..........................................37
  Process button.................................31
  Processor ID....................................45
  Programmable Buttons..........................24, 27
  Properties button............................27
  Protect Stored Cardholder Data.................27
  Protect Wireless Transmissions................14
  Public Networks................................14
  Purge Stale Cardholder Data....................14
Receipt Printer................................3
Receiving.......................................43
Reference........................................13
Remote Update Procedures.......................14
Reports..........................................3, 37, 45
Required.........................................14
  PCI.............................................14
  Verifone PAYware PC.............................14
  Requirements..................................13
  Compliance.....................................13
Reseller.........................................45
Secure Remote Access............................14
  Payment Application............................14
  Secure Remote Access Requirements...........14
  Secure Remote Software Updates..............14
  Secure Socket Layer............................14
  Securely Delete Cryptographic Material........14
  Security management...........................11
  Security standard that includes...............11
  See screenshot................................14
  Verifone PAYware PC Administration Center........14
Sensitive Authentication Data....................14
Sensitive credit................................14
Serial...........................................3
Service Rep.....................................45
  Settlement URL.................................45
  Shipping........................................43
  Signature Pad...................................3
  Signature Size..................................3
  MX830..........................................3
Smartcard.......................................14
  Software design................................14
  SSL..............................................14
  Suite...........................................1
  Support@EagleBusinessSoftware.com...........1
Sync tool.......................................23, 53
  using...........................................23
  Sync Tool Overview.............................53
  System Services menu...........................49
  Expand..........................................49
  Systems Connected.............................14
  Internet........................................14
Technical Support...............................1
Terms.............................................14
**Point of Sale**

<table>
<thead>
<tr>
<th>PCI DSS Glossary</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Payment Application</td>
<td>14</td>
</tr>
<tr>
<td>The PCI Data Security Standard</td>
<td>11</td>
</tr>
<tr>
<td>This Button Type</td>
<td>27</td>
</tr>
<tr>
<td>Touch Screen</td>
<td>3, 23</td>
</tr>
<tr>
<td>Touch Screen POS</td>
<td>23, 34, 53</td>
</tr>
<tr>
<td>Touch Screen POS System</td>
<td>2, 23</td>
</tr>
<tr>
<td>Two-Factor Authentication</td>
<td>14</td>
</tr>
</tbody>
</table>

**U**

| Unique ID                            | 14 |
| Assign                               | 14 |

**V**

| Verifone Payware PC                  | 2, 14 |
| implementing                         | 14 |
| number                               | 14 |
| part                                 | 14 |
| refer                                | 14 |
| require                              | 14 |
| uses                                 | 2 |

| Verifone PAYware PC Administration Center | 14 |
| See screenshot                        | 14 |
| Verifone PAYware PC application       | 14 |
| Verifone PAYware PC's                 | 14 |
| Verifone PAYware PC's Users Manual    | 14 |
| Verifone PAYware SIM SSL              | 14 |
| Verifone's Payware PC's               | 49 |
| View                                 | 24 |
| POS Profile list                     | 24 |
| View Configuration                   | 49 |
| Visa                                 | 11 |
| VPN                                  | 14 |

| Warehouse                            | 24, 41, 43 |
| Weigh Scale                          | 3 |
| WEP                                   | 14 |
| Wireless Technology Included          | 14 |