

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	7
1 Payment Systems Security	7
1.1 Introduction	7
1.2 Why you need to be concerned about this	7
1.3 The PCI Data Security Standard	7
2 Merchant and Requirements for Compliance.....	9
3 EBMS® PCI Security Practices.....	10
4 Securely implementing EBMS®.....	10
Merchant Applicability	10
4.1.1 Previous Versions	10
Merchant Applicability	10
TOUCH SCREEN POS SYSTEM	19
Overview	19
Configure POS Profiles	20
Programmable Buttons	23
Using the POS station.....	26
Processing Credits and Returns	28
BAR CODES	29
Entering Bar Codes within EBMS	29
Bar codes for inventory items	29
Scanning Bar Codes	33
MOBILE SCANNER SOLUTION.....	35
Mobile Scanner Solution	35
PAYMENT CARD PROCESSING	37
Payment Card Overview	37
Processing Payment Cards.....	39
Pre-authorization	39
Completing the Transaction.....	40
Settlement of Funds.....	42
Configuring EBMS for Payment Cards.....	44
Storing Credit Cards.....	48
Store Credit Card.....	48
Accessing Store Credit Card	49
Troubleshooting Credit Card Processing	51
Merchant Account Parameters.....	53
For PAYware PC Administrators.....	54

INDEX.....59

Getting Started

Technical Support

Welcome to the instructional manual for the Point-of-Sale 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 7.6 October 2012

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 retail 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 [Payment Card Processing > Processing Payment Cards](#) 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.

The screenshot shows the 'Options' dialog box with the 'Reports' tab selected. The dialog is organized into several sections for configuring report printing:

- Report to Print when Processing Sale:**
 - ☐ Use this report: INVOICE (PLAIN PAPER) [Browse]
 - ☐ Choose report when processing
 - ☒ User Specific: INVOICE RECEIPT (CONDENSED) (EP [Browse]
 - ☐ Use secondary report when processing a charge sale.
- Report to Print when Processing Charge Sale:**
 - ☒ Use this report: INVOICE (PLAIN PAPER) [Browse]
 - ☐ Choose report when processing
 - ☐ User Specific: [Browse]
 - ☐ Show the print dialog when processing an invoice.
- Report to Print as a Payment Receipt:**
 - ☐ Use this report: PAYMENT RECEIPT (PLAIN PAPER) [Browse]
 - ☒ User Specific: PAYMENT RECEIPT (EPSON) [Browse]
 - ☐ Show the print dialog when processing a payment
 - ☐ Print payment receipt report when processing invoice with credit card payment.

At the bottom of the dialog, there is a note: "Press this button to modify which reports show up on the print button menus by dragging the proper reports into the corresponding folders." followed by an 'Edit System Folders' button. The 'OK' and 'Cancel' buttons are at the bottom right.

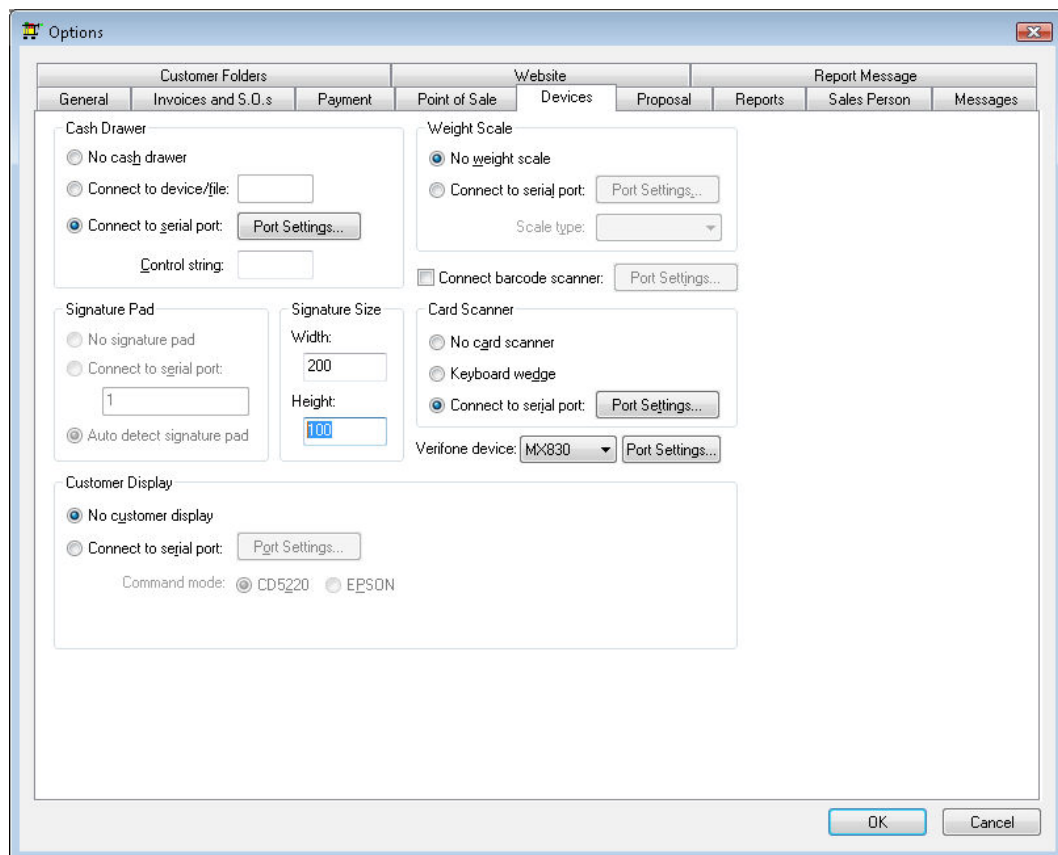
Set receipt settings as shown above. Review the [Sales > Invoices > Printing a Sales Invoice or Payment Receipt](#) section for more details on these settings.

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.

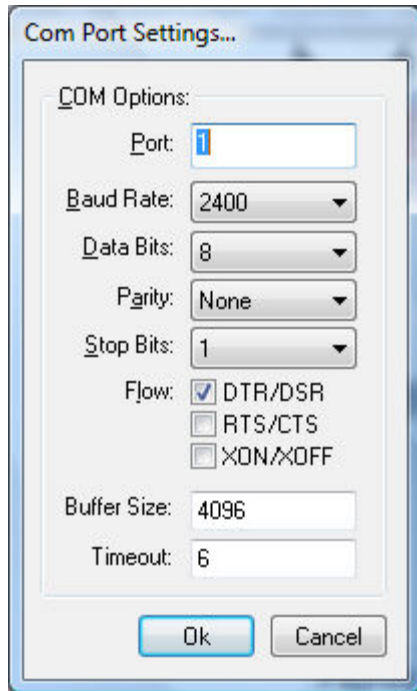
Cash Drawer

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:



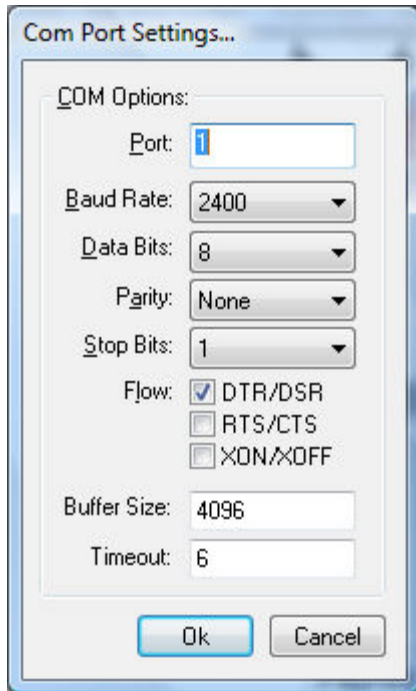
Click OK to save the serial settings.

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:



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.

Point of Sale

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

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

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/>

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

Point of Sale

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:

Users	Roles	Password Policy	Inactive Users
Administrator			
Manager			
Clerk			
PDS			

<input type="checkbox"/>	View Manager Reports
<input checked="" type="checkbox"/>	View Non-Manager Reports
<input type="checkbox"/>	Create Manager Reports
<input type="checkbox"/>	Create Non-Manager Reports
<input type="checkbox"/>	Delete Reports
<input checked="" type="checkbox"/>	Process Sale-type Transactions
<input checked="" type="checkbox"/>	Process Void Transactions
<input checked="" type="checkbox"/>	Process Refund Transactions
<input checked="" type="checkbox"/>	Process Balance Manipulation Transactions (Gift Cards)
<input type="checkbox"/>	Process Cash-Out Transactions (Gift Cards)
<input checked="" type="checkbox"/>	Process Batch/Settlement Transactions
<input type="checkbox"/>	Issue System-level Commands
<input checked="" type="checkbox"/>	View Customer Records
<input checked="" type="checkbox"/>	View Customer Contact Records
<input checked="" type="checkbox"/>	View Customer Contract/Agreement Records
<input checked="" type="checkbox"/>	View Customer Payment Account Records
<input checked="" type="checkbox"/>	Create Customer Records
<input checked="" type="checkbox"/>	Create Customer Contact Records
<input checked="" type="checkbox"/>	Create Customer Contract/Agreement Records
<input checked="" type="checkbox"/>	Create Customer Payment Account Records
<input type="checkbox"/>	Delete Customer Records
<input type="checkbox"/>	Delete Customer Contact Records
<input type="checkbox"/>	Delete Customer Contract/Agreement Records
<input type="checkbox"/>	Delete Customer Payment Account Records
<input type="checkbox"/>	Allow Override of SAF Transactions

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.

Point of Sale

PCI DSS 8.5.16: Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.

Touch Screen POS System

Overview

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 of the Inventory documentation for more details on grouping products.

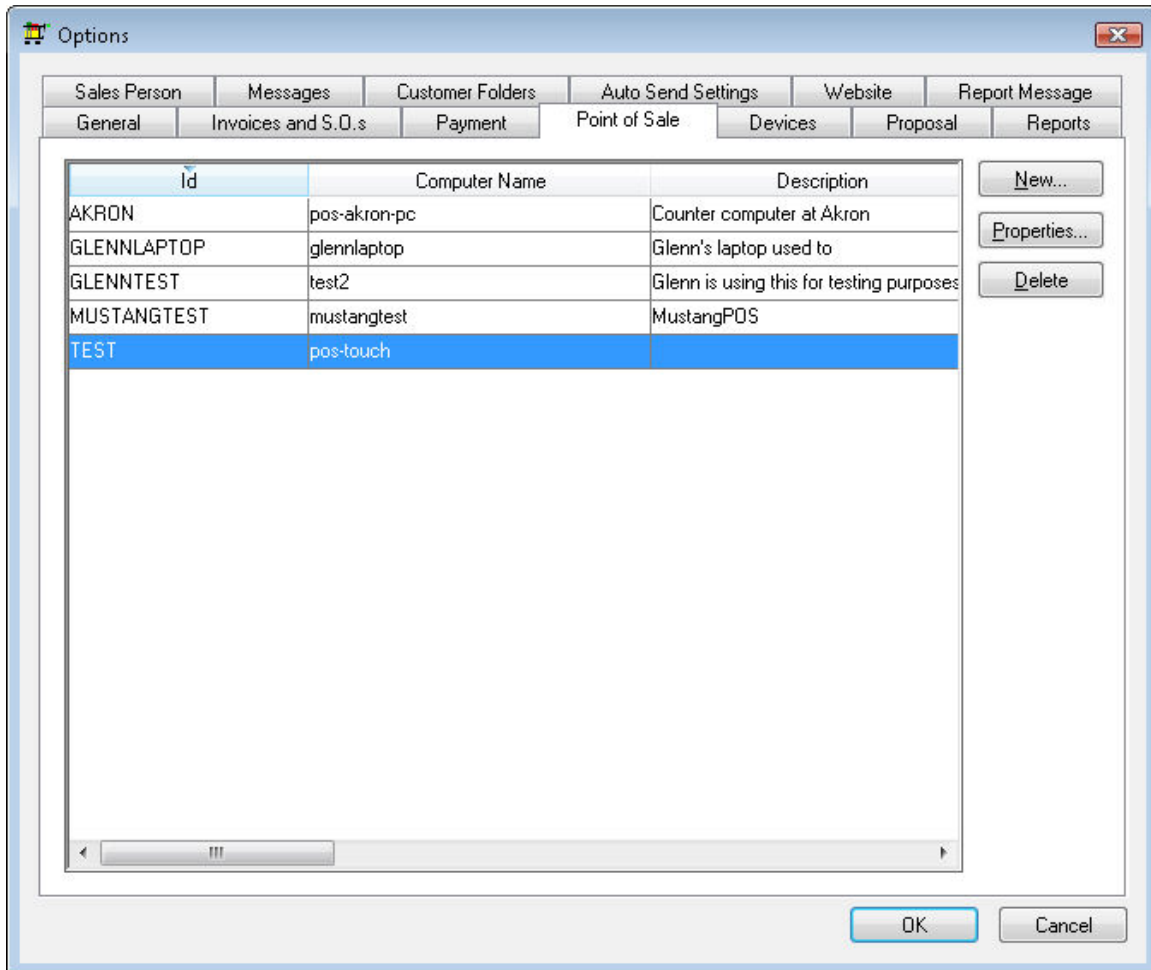
Review the [Bar Code Technology > Entering Bar Codes within EBMS](#) section for more details on assigning bar codes to inventory items.

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.

Point Of Sale Station

Id: POS1

General Programmable Buttons

Computer Name: Counter-POS

Description: Touch Screen POS station on front counter

Default Customer: CASH

Invoice Prefix: P

Next Invoice Number: 1008

☒ Allow credit payment on this POS

Warehouse: GENERAL

OK Cancel

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.

Point of Sale

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 [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 it's 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:

Point Of Sale Station

Id: POS1

General Programmable Buttons

Active	Button Name	Type
✓	GARDEN SUPPLIES	Inventory Folder
✓	HOME SUPPLIES	Inventory Folder
✓	PAPER SUPPLIES	Inventory Folder
✓	PAINT	Inventory Folder
✓	POWER TOOLS	Inventory Folder
✓	HAND TOOLS	Inventory Folder
✓	Dirt Shovel	Inventory Item
✓	Adjustable Wrench	Inventory Item
✓	25' Garden Hose	Inventory Item
✓	Oil Change Fee	Inventory Item
✓	Castor Dolly	Inventory Item
✓	Goingrich's Glue	Inventory Item
✓	Duct Tape	Inventory Item
✓	10' Ladder	Inventory Item

Total Number of Programmable Buttons: 24

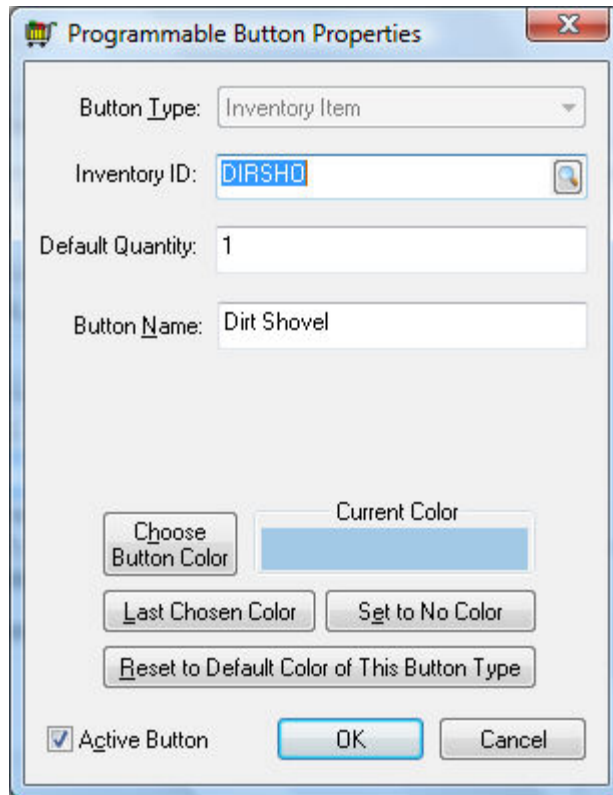
Number of Active Programmable Buttons: 24

OK Cancel

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*.



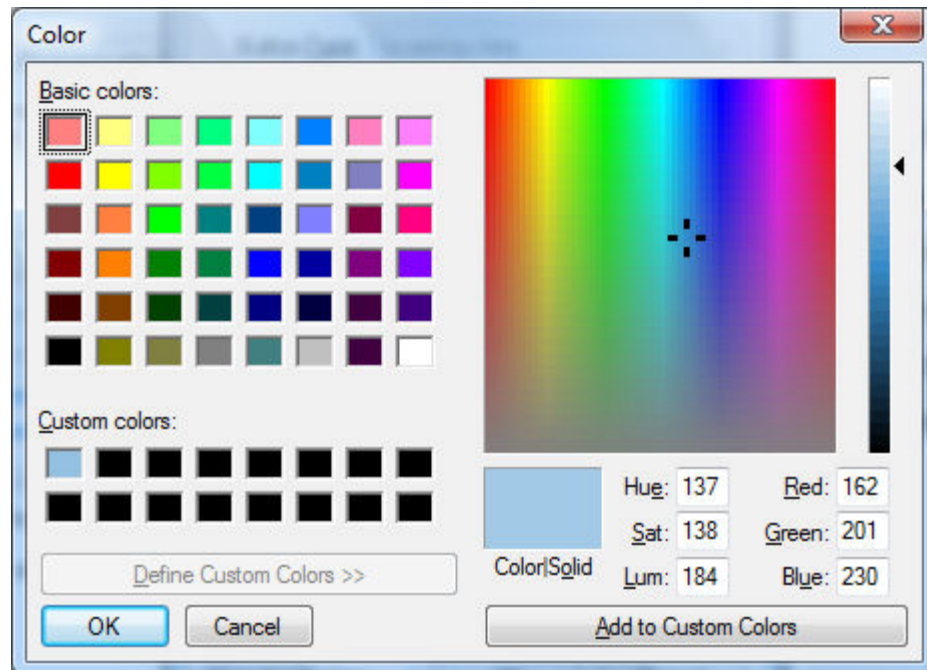
Select the **Inventory Item** button type.

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 quick 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:

EBMS Point of Sale System - Quality Hardware

File Edit Process View Help

Customer ID: CASH Cash Customer Transaction No.: P1009
Monday, September 25, 2000
Register 1
User: ADMINISTRATOR Logout

Remove This Item Remove All Items PA

Inventory	Quantity	Description	Price	Amount	G/L Account
DIRSHD	1.00	Dirt Shovel	25.56	25.56	51000-010
					51000-010
*					

Lookup Search

GARDEN SUPPLIES	HOME SUPPLIES	PAPER SUPPLIES
PAINT	POWER TOOLS	HAND TOOLS
Dirt Shovel	Adjustable Wrench	25' Garden Hose
Oil Change Fee	Castor Dolly	Goingsrich's Glue
Duct Tape	10' Ladder	Honda Air Compressor
50' Extension Cord	Shovel Blade	18 IN HONDA CHAIN SAW
10 lb. Sledge Hammer	10 Oz. can of spray paint	3 inch Paint Brush
6" Phillip's Screwdriver	Calculator	On-screen Keyboard

Payment

CASH CHECK CREDIT DEBIT VOUCHER GIFT CARD CHARGE CLEAR PAYMENT

Subtotal: \$25.56
% Discount: 7 8 9 Back-space
Tax: \$1.53
Total Amount: \$27.09
Change: \$0.00

Total Paid: \$0.00 Balance: \$27.09

PROCESS

0 . Enter

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 7 or later OS.

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:




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.

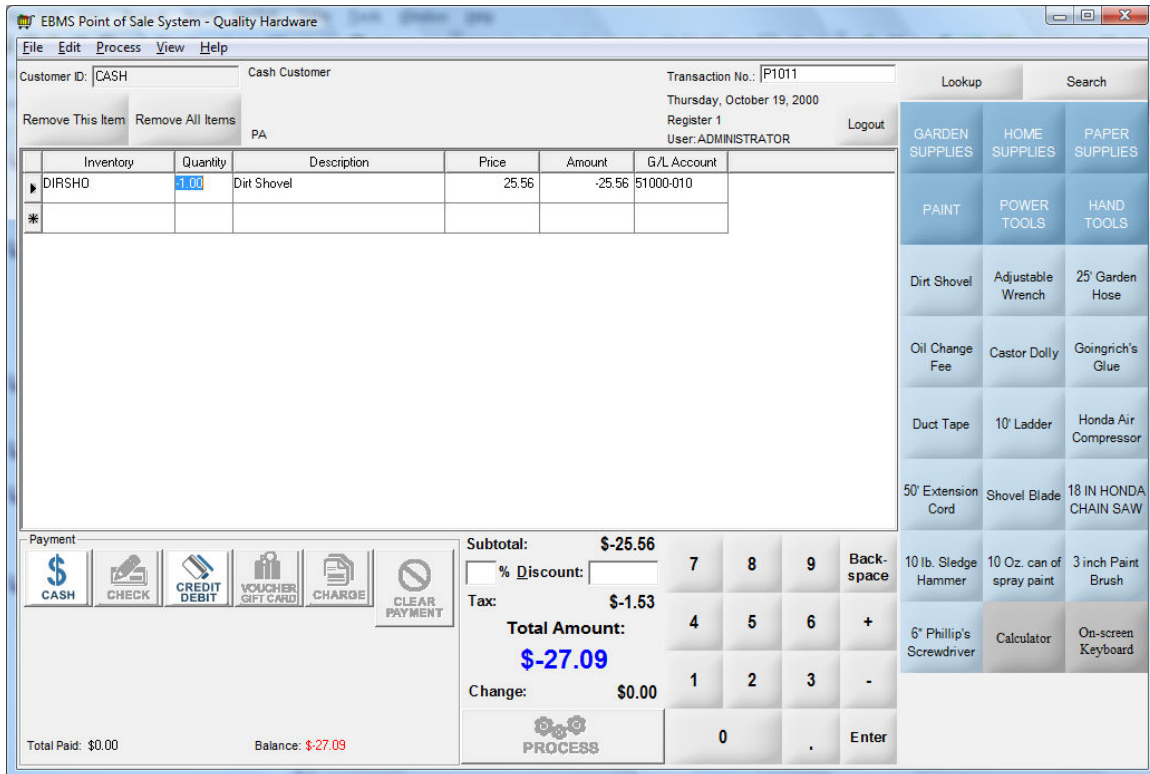
Click the **Clear Payment** button to clear a payment and choose a new payment.

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:



The screenshot displays the EBMS Point of Sale System interface. The main window is titled "EBMS Point of Sale System - Quality Hardware". It features a menu bar with "File", "Edit", "Process", "View", and "Help". The interface is divided into several sections:

- Customer Information:** Customer ID: CASH, Cash Customer, Transaction No.: P1011, Thursday, October 19, 2000, Register 1, User: ADMINISTRATOR, Logout.
- Buttons:** Remove This Item, Remove All Items, PA.
- Inventory Table:**

Inventory	Quantity	Description	Price	Amount	G/L Account
DIRSHO	-1.00	Dirt Shovel	25.56	-25.56	51000-010
*					
- Payment Section:**
 - Payment methods: CASH, CHECK, CREDIT DEBIT, VOUCHER/GIFT CARD, CHARGE, CLEAR PAYMENT.
 - Subtotal: \$-25.56
 - % Discount: 7, 8, 9, Back-space
 - Tax: \$-1.53
 - Total Amount: \$-27.09
 - Change: \$0.00
 - Buttons: 4, 5, 6, +, 1, 2, 3, -, 0, ., Enter
- Lookup/Search Section:**
 - Buttons: GARDEN SUPPLIES, HOME SUPPLIES, PAPER SUPPLIES, PAINT, POWER TOOLS, HAND TOOLS.
 - Items listed: Dirt Shovel, Adjustable Wrench, 25' Garden Hose, Oil Change Fee, Castor Dolly, Goingsrich's Glue, Duct Tape, 10' Ladder, Honda Air Compressor, 50' Extension Cord, Shovel Blade, 18 IN HONDA CHAIN SAW, 10 lb. Sledge Hammer, 10 Oz. can of spray paint, 3 inch Paint Brush, 6" Phillip's Screwdriver, Calculator, On-screen Keyboard.
- Bottom Status Bar:** Total Paid: \$0.00, Balance: \$-27.09, PROCESS button.

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.

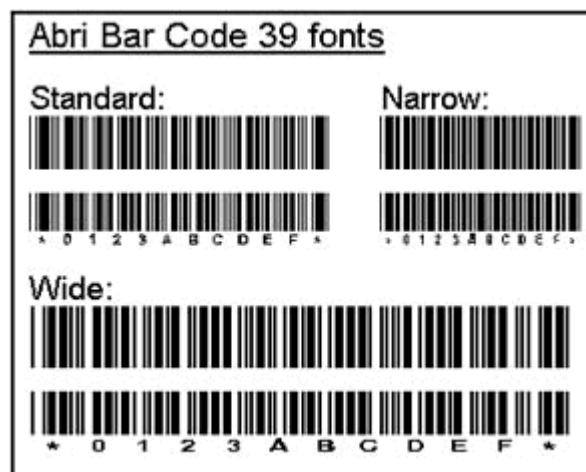
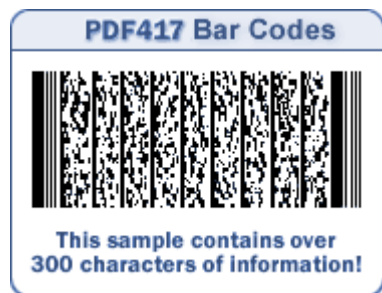
Bar Codes

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. This feature allows the user to scan

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

Inventory\Products\Garden Supplies\Dirt Shovel

Item: DIRSHO Warehouse: All Folder: Garden Supplies

General Purchasing Pricing Count Components Accessories Advanced Website 2000 1999 1998

Description: Dirt Shovel Show on invoice: ☒

Entry Date: 08/20/1998 Thu UPC Code: 123456789012

Gross Weight: 6.50 Type: Location: B

☐ Weigh Item On Entry ☒ Taxable

Manufacturer ID: QUABUI Quality Built Part No: Web: Classification: Track Count Change...

Note:

Substitute Item Description

OK Cancel New Delete Print

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 from the list, and click the **Properties** button to open the following dialog:

Inventory\Products\Garden Supplies\Dirt Shovel

Item: DIRSHO Warehouse: All Folder: Garden Supplies

General Purchasing Pricing Count Components Accessories Advanced Website 2000 1999 1998

Processed: 1,023.000000

In Ordered Received

Unit of Measure Website

Unit of measure: pk

A(n) pk is larger than a(n) ea.

There are 6.0000 ea in each pk.

UPC: 234567890123

☒ Allow selling with this unit of measure

OK Cancel

Ordering Amount: Maximum: 50.00 Minimum: 20.00

Main Unit: ea Default Selling: ea

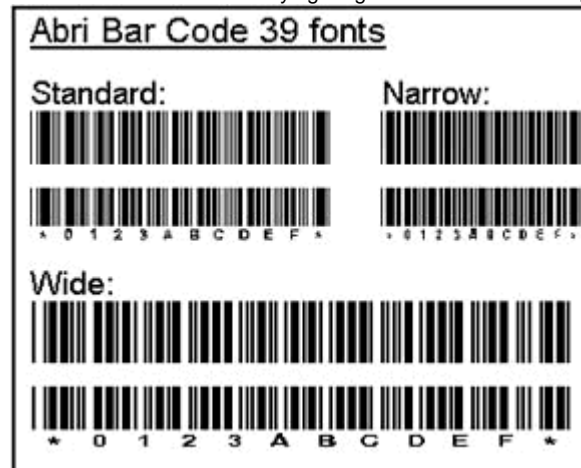
Sell	Unit	Formula
✓	pk	Multiplies by 6.0000

Add... Properties... Delete

OK Cancel New Delete Print

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



the longer the bar code.

A inventory ID must consist of numbers and letters. Most symbols do not properly convert into bar codes. Note that IDs that contain spaces can not 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.

Print - PACKING LIST [X]

Choose Printer

☒ Default Printer HP LaserJet 1200 Series PCL 5 on USB001

☐ Specific Printer HP LaserJet 1200 Series PCL 5 on USB001

Report Options

Order Number: 123456

☐ Print Customer Contacts

☒ Print Bar Code

☐ Do Not Print Logo

☐ Do Not Print Company Info

☐ Do Not Print Memo

Print

Print Preview

Print Setup

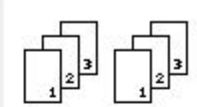
Cancel

Set Query

☐ Use Query

Orientation:

Portrait



☒ Collate

Copies: 1

Save as Default

Restore Defaults

Export...

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

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.

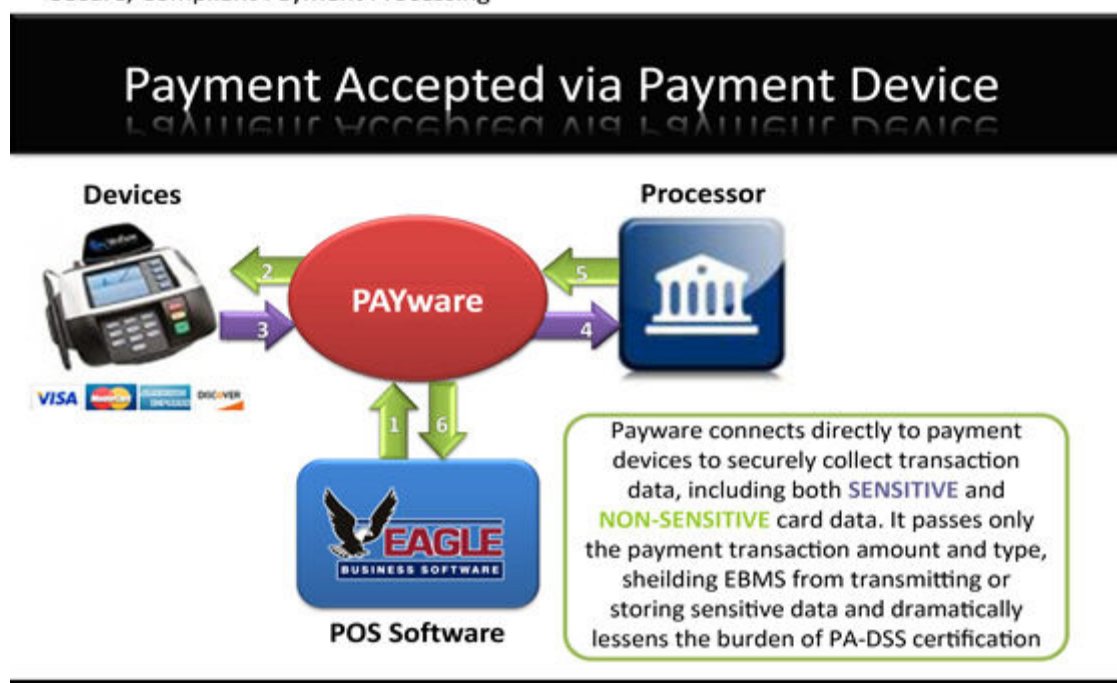
Payment Card Processing

Payment Card Overview

Payment cards such as credit, debit, and EBT cards can be processed directly from the EBMS software. This option streamlines the processing, settlement, and management of payment card processing. The secure PCI approved method of credit card storage and processing combined with the cash management tools of the EBMS software creates an efficient way of recording multiple payment methods.

The payment card module also gives the user a secure means of storing credit card information within a sales order or customer account without storing the actual credit card number. The payment card process gives the user the convenience of flexible payments without the security concerns of many applications.

Secure, Compliant Payment Processing



To find out if you are PCI-DSS Compliant contact Eagle Business Software, 717.442.3247 ext. 2

The optional credit card gateway used by EBMS is Verifone Payware. This gateway gives the user the flexibility to choose one of the many merchant accounts available for this widely used interface.

Payware gives the user the following two options to communicate credit card transactions between the EBMS software and the customer determined merchant account.

1. Payware Connect - EBMS connects directly to this online option removing the requirement for Payware hardware. This online service is an ideal solution for companies with minimal IT staff or multiple locations.
2. Payware PC - This option requires that the Payware PC software be installed on the users local area network (LAN)

Following is a list of the main Payware Payment Processing options:

- Allows the user to process credit cards and debit cards directly from the EBMS Software. Review the [Processing Payment Cards](#) section for more details.

Point of Sale

- Allows the user a wide variety of merchant accounts with the EBMS Software. Any merchant account that is verified with Verifone Payware PC or Payware Connect can communicate with the EBMS software. Review the [Merchant Account Parameters](#) section for more details.
- Separate cash accounts can be setup for multiple locations or multiple merchant accounts to simplify cash reconciliation. Review the [Configuring EBMS for Payment Cards](#) section for more details.
- Credit cards can be pre-authorized for sales orders before an order is shipped and processed
- EBMS can communicate pre-entered credit card information into a secure database. No credit card information is ever stored within the EBMS databases. Review the Storing Credit Cards section for more details.
- Allows the user to create and maintain a reliable solution that is easy to PCI Certify because of the centralized, secure payment server
- Interfaces with the Verifone Payment Device

Processing Payment Cards

The processing of payment cards may comprise of two or more steps:

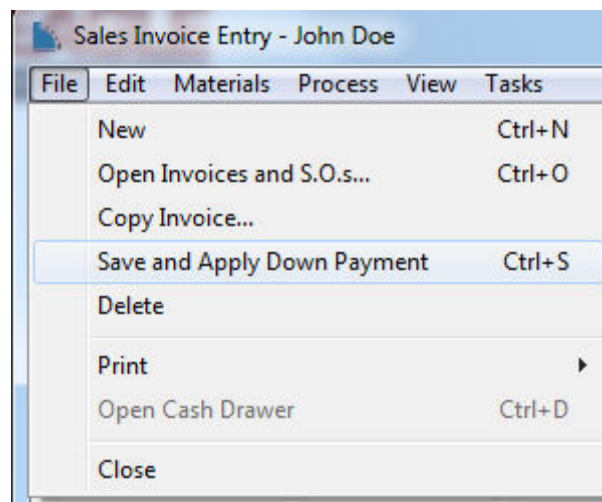
1. Optional step of pre-authorization - EBMS allows the user to authorize a payment card before the transaction is completed. This authorization step will verify that the credit card is valid and that funds are available. This step will hold the amount of funds specified on the sales order. The length of time that these funds are held varies and is based on the policy of the merchant account. The amount of the transaction can be changed until the next step is completed.
2. Completing the transaction - The payment card debit transaction is completed during this step. The amount of the transaction cannot be changed after the completion step. This step happens automatically when the EBMS sales invoice is processed. The user has the option to complete this step before the invoice is processed.
3. Settlement of funds - The final step of processing a credit card is the "end of day" batch settlement of the transactions. This step is completed using the EBMS deposit dialog. Review the [Settlement of Funds](#) section for more details.

Pre-authorization

The pre-authorization step is used most commonly for e-commerce transactions. Review the [Processing Orders > Processing Credit Cards](#) section of the e-commerce documentation for more details.

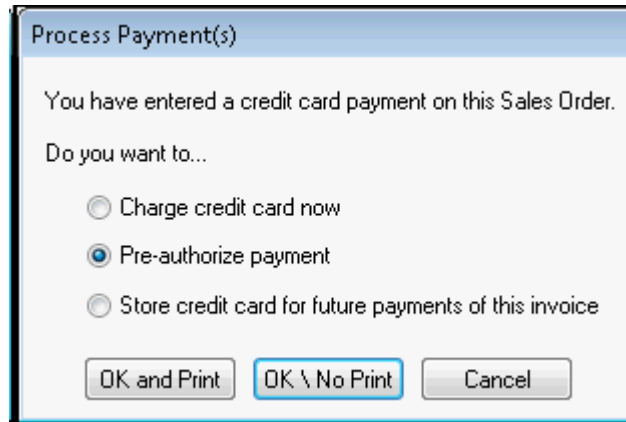
A payment card amount can be pre-authorized by completing the following steps:

1. Open a sales order - Review the [Sales > Sales Orders > Entering a Sales Order](#) section of the main documentation for more details.
2. Click on the credit card payment option and enter the credit card information. Review the [Sales > Invoices > Payment Methods and Terms](#) section of the main documentation for more details on entering payment card information.
3. Select **File > Save and Apply Down Payment** from the sales order menu as shown below:



4. Select one of the three options:
 - A. Select **Charge credit card now** to complete the credit card transaction.

- B. Select **Pre-authorize payment** to only authorize the card.
- C. Select **Store credit card for future payments of this invoice** to securely store the credit card information within the sales order for future processing. This step does not pre-authorize the card.



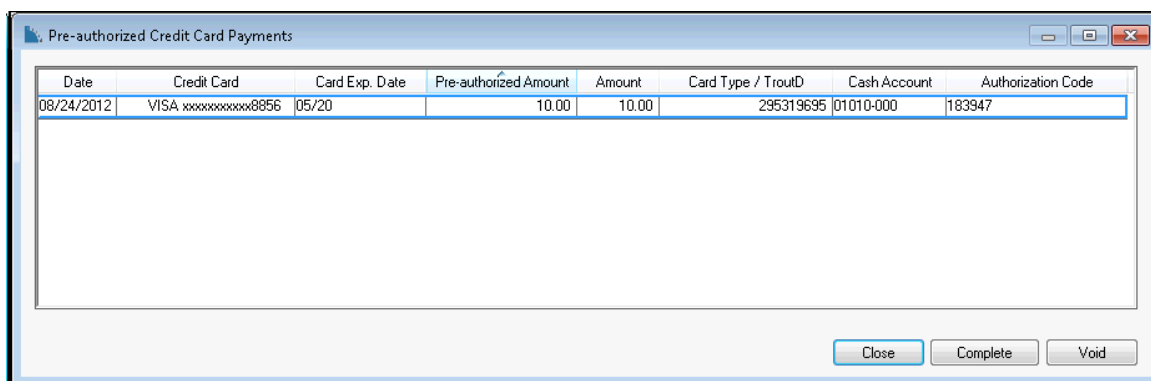
- 5. Click the **OK and Print** button to complete the process and generate a payment receipt. Click the **OK \ No Print** to process without printing a receipt.

The pre-authorizations can be viewed within the sales order by selecting **View > Pre-Authorize CC Payments** from the sales order menu.

Completing the Transaction

Select the **Credit/Debit Card** payment method when processing the sales order to complete the credit card transaction. The payment card transaction is completed automatically if the card was pre-authorized. Review the [Sales > Invoices > Payment Methods and Terms](#) section of the main documentation for more details on entering payment card information.

View the pre-authorized transactions to manually complete the transaction before the invoice is processed. Select **View > Pre-Authorize CC Payments** to view the following dialog:



Click on the **Complete** button to complete the payment card transactions. Click on the **Void** button to void the pre-authorization.

Select **View - Processed Payments** from the sales order menu to view or void completed payment card transactions as shown below:

The screenshot shows a window titled "View Payments" with a table containing the following data:

Date	Type	Reference	Amount	Cash Account	Credit Card	Authorization Code	Address Verification
07/05/2012 Thu	VISA	76068483	113.75	01010-000	VISA xxxxxxxxxx 6068	0059	Z

Below the table, a note states: "Voided payments are shown in red."

At the bottom right, there are three buttons: "Close", "Transactions..." (highlighted with a blue border), and "Void...".

Click the **Transactions** button to view the general ledger transaction detail.

Click the **Void** button to void the selected transaction. The transaction can only be voided before credit card settlement. Create a credit transaction if the original transaction can not be voided.

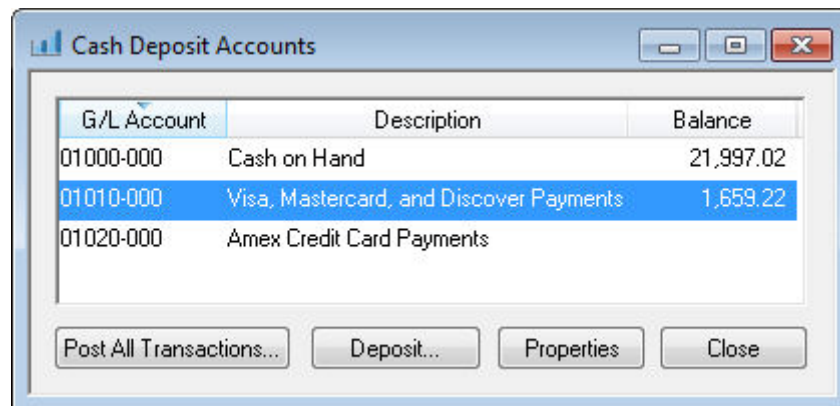
Settlement of Funds

The settlement process is used to deposit payment card payments into the companies bank account. The payment card settlement may be initiated from one of the following ways

- A. Host Settle - The settlement process is initiated by the merchant account and is often scheduled during the night.
- B. Terminal Settle - This method requires the user or the Payware software to initiate the settlement. The settlement should be scheduled or manually processed after each days sales.

The Payware settlement process will send a report via e-mail listing the transactions included in the settlement batch and deposited in the bank account. Complete the following steps to reconcile the credit card cash account.

1. Go to **Sales > Deposits** from the main EBMS menu.
2. Select the cash account that contains the credit card transactions. Note that multiple settlements based on payment card type should be separated into multiple cash accounts. Review the [Sales > Customer Payments > Cash Accounts, Deposits, and Reconciling Cash](#) section of the main documentation for more details on cash accounts.



3. Open the **Visa, Mastercard, and Discover Payments** account to deposit the **Receipts** or view the transactions as shown below:

Deposits - 01010-000 Visa, Mastercard, and Discover Payments

Show transactions up to: 07/10/2000 Mo

Receipts Paid Out

Status	Type	Date	Description	Amount	Vendor/Customer	Source	G/L Code
✓	VISA	07/10/2000	John Doe	41.34	DOEJOH	ARP	01010-000
✓	VISA	07/10/2000	John Doe	689.00	DOEJOH	ARP	01010-000
✓	MC	07/10/2000	Arden's Landscaping	812.26	6103884490	ARP	01010-000
✓	DISC	07/10/2000	Discount Paint Center	116.62	DISPAI	ARP	01010-000

Select All Unselect All

Selected Receipts

Cash:

Checks:

Other: \$1,659.22

Total: \$1,659.22

Paid Out:

Cash:

Adjustment:

Current Balance: \$1,659.22

Total Deposit: \$1,659.22

Ending Balance:

Deposit Transaction

Deposit Date: 07/10/2000 Mo

Description: Deposit

Deposit to: 01100-000 - Checking Account

OK Cancel Source Deposit and Print Deposit / No Print Adjustment... Print Wizards

- Select the transactions that are listed on the payment card settlement report.
- The amount on the **Total Deposit** should equal the total on the settlement report.
- Click on the **Deposit and Print** to complete the deposit and print a deposit slip.
- Click on the **Deposit / No Print** to complete the deposit without printing a deposit slip. Review the [Sales > Customer Payments > Cash Accounts, Deposits, and Reconciling Cash](#) section of the main documentation for more details on deposits.

Configuring EBMS for Payment Cards

The configuration of the processing software and the merchant account must be completed properly before configuring EBMS. Contact an EBMS support representative and a merchant account reseller for detailed instructions. Continue with this section after the merchant account and processing software has been selected.

EBMS allows the following two **Processing Software** options:

1. **Payware Connect** - This software connects to a hosted Payware Connect service. This option is the recommended solution since hardware is not required.
2. **Payware PC** - This software connects to the Payware PC server hosted on a computer on the user's local area network (LAN).

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:

Active	Payment Name	Cash Account	Properties...
<input checked="" type="checkbox"/>	Cash	Based on Warehouses	Based on \
<input checked="" type="checkbox"/>	Check	Based on Warehouses	Based on \
<input type="checkbox"/>	Gift Card	Based on Warehouses	Based on \
<input checked="" type="checkbox"/>	Visa	Based on Warehouses	Based on \
<input checked="" type="checkbox"/>	MasterCard	Based on Warehouses	Based on \
<input checked="" type="checkbox"/>	Discover	Based on Warehouses	Based on \
<input type="checkbox"/>	American Express	Based on Warehouses	Based on \
<input type="checkbox"/>	EBT	Based on Warehouses	Based on \
<input type="checkbox"/>	Debit	Based on Warehouses	Based on \

☐ Only allow debit card payment

Credit Card Processing Software

☒ Disable Credit Card Processing Software (not recommended)

Processing Software: PAYware Connect Credentials: Settings...

Primary URL: https://IPCharge.net/IPCHAPI/rh.aspx

Secondary URL: https://IPCharge2.net/IPCHAPI/rh.aspx

Merchant Key: X0X1XX1X-0101-01X0-010X-0X10101010

OK Cancel

Configure the following PAYware settings:

1. Enable the **Disable Credit Card Processing Software (not recommended)**. This option must be enabled to properly process credit cards within EBMS using the PAYware software.
2. Select one of the following **Processing Software** options:

- A. **Payware Connect** - Recommended
 - B. **Payware PC**
3. Click on the **Credentials Settings** button to set the user credentials. This is a management setting that should only be accessed by the manager.
 - A. Enter a **User Name** and **Password**. A unique **User Name** must be created for the EBMS software interface. Do not use the same **User Name** when logging into Payware directly.
4. Enter the following information if the **Payware Connect Processing Software** is selected:

Active	Payment Name	Cash Account	PAYware PC Client ID	Process
<input checked="" type="checkbox"/>	Cash	01000-000 - Cash/Check Undeposited		
<input checked="" type="checkbox"/>	Check	01000-000 - Cash/Check Undeposited		
<input type="checkbox"/>	Gift Card	01000-000 - Cash/Check Undeposited		
<input checked="" type="checkbox"/>	Visa	01010-000 - Credit Card Undeposited	100010001	H
<input checked="" type="checkbox"/>	MasterCard	01010-000 - Credit Card Undeposited	100010001	H
<input checked="" type="checkbox"/>	Discover	01010-000 - Credit Card Undeposited	100010001	H
<input checked="" type="checkbox"/>	American Express	01010-000 - Credit Card Undeposited	100010001	H
<input type="checkbox"/>	EBT	01010-000 - Credit Card Undeposited	100010001	H
<input checked="" type="checkbox"/>	Debit	01010-000 - Credit Card Undeposited	100010001	H

☐ Only allow debit card payment
☐ Credit Card Processing Software
☐ Disable Credit Card Processing Software (not recommended)

Processing Software: PAYware Connect Credentials: Settings...

Primary URL: https://IPCharge.net/IPCHAPI/rh.aspx

Secondary URL: https://IPCharge2.net/IPCHAPI/rh.aspx

Merchant Key: XXXXXXXXXXXXXXXXXXXXXXXXXXXX

OK Cancel

- A. Enter the **Primary URL**. The value of this field is normally set to: **https://IPCharge.net/IPCHAPI/rh.aspx**
 - B. Enter the **Secondary URL**. The value of this field is normally set to: **https://IPCharge2.net/IPCHAPI/rh.aspx**
 - C. Enter the **Merchant Key**. This value must match the Payware Connect merchant account.
5. Enter the following information if the **Payware PC Processing Software** is selected.

Point of Sale

☐ Only allow debit card payment

Credit Card Processing Software

☐ Disable Credit Card Processing Software (not recommended)

Processing Software: Credentials:

Computer name or IP address:

Port:

- A. 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.
 - B. Enter the PAYware PC **Port** value located within the PAYware PC management client.
6. Click on a **Payment Name** record that reflects a credit card payment type such as **Visa** or **Mastercard**. Click on the **Properties** button to open the following dialog:

Payment Name: ☒ Active

Company Wide

Cash Account:

PAYware PC Client ID:

Host / Terminal: ☐ Auto Settle Host ☐ Paymentech

Settlement URL:

- A. The **Payment Name** identifies the payment type.
 - B. Enable the **Active** option.
 - C. Enter the following PAYware settings. Enter the settings for each department or warehouse if multiple records show as displayed above.
 - D. 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.
 - E. Enter the four-digits payment **Processor ID**.
- B. Enter the correct **Merchant No**.

- C. Enter the Host\Terminal **Processor Type**.
- D. 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.

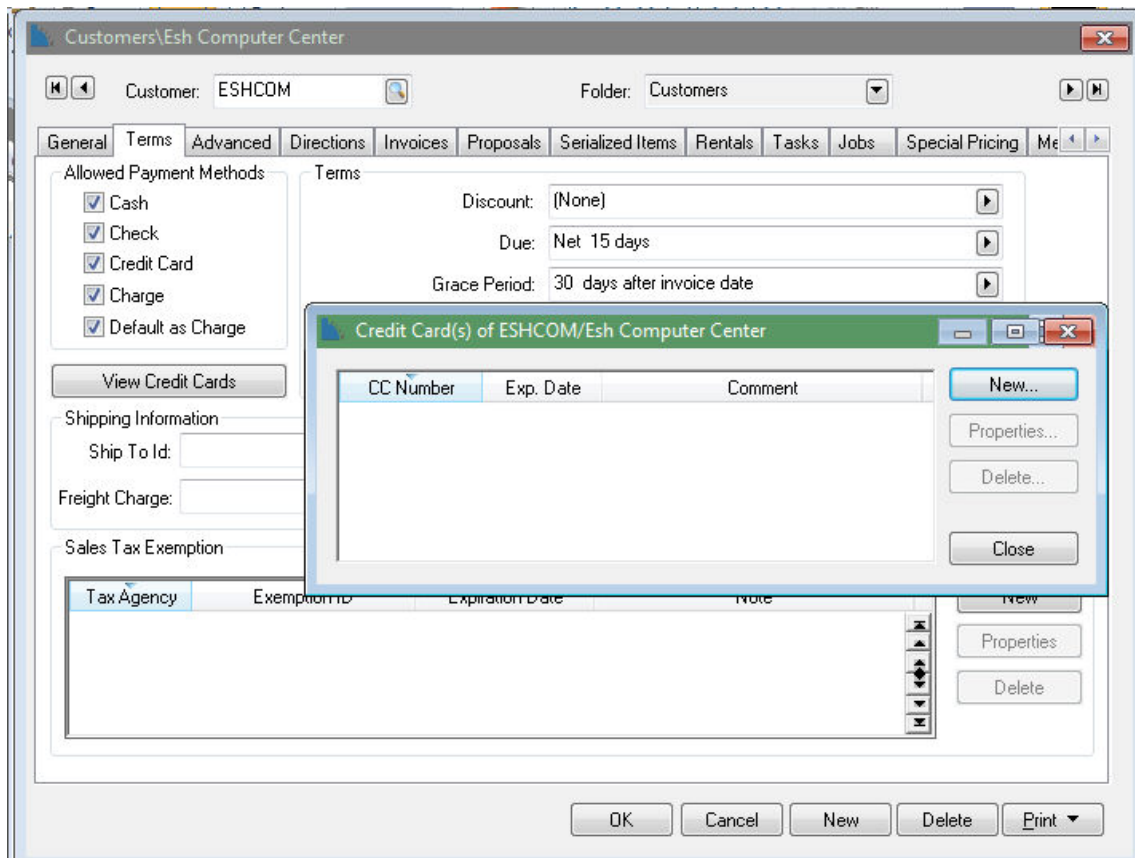
Storing Credit Cards

A customers credit card can be stored within a customer account or sales order using a secure PCI compliant method. The credit card information is passed to Verifone Payware. Verifone Payware returns a reference number and the last four digits of the credit card number. The credit card account number is never stored within the EBMS database system.

Store Credit Card

Complete the following steps to enter a customers credit card information into their account record:

1. Open the customer account number. Review the Sales > Customers > Changing Customer Information section of the main documentation for more details on the customer record.
2. Click on the **Terms** tab then click on the **View Credit Cards** button as shown below:



3. Click **New** to add a new credit card as shown below:

Enter credit card info of ESHCOM/Esh Computer Center

Credit Card Information
 Credit card number: 5XXXXXXXXXXXX1111
 Expiration date: 12/12 (MM/yy)

Address Information
 Address: 1234 Main Street
 Zip: 17529

PAYware Connect Client Id
 XXXXXXXXXXXXXXX

Comment:
 This is the company credit card authorized by John Doe

This card information is being stored within Verifone PAYware PC and is subject to the purge settings within PAYware PC Management Client.

OK Cancel

4. Enter a 16 digit **Credit card number**. Only the first and last four digits will be stored within EBMS.
5. Enter the credit cards **Expiration date**. Note that the CVV number may not be recorded before a sale is authorized.
6. Enter the billing street **Address** for the credit card.
7. Enter the **Zip** for the billing address.
8. Enter any applicable **Comments** and click **OK** to save.

All the credit card information must be re-entered if the credit card number or other information changes.

Accessing Store Credit Card

Complete the following steps to use a stored credit card within a sales invoice.

1. Open a sales invoice as shown below:

Point of Sale

Sales Invoice Entry - John Doe

File Edit Materials Process View Tasks

Customer ID: DOEJOH Invoice: 1328 Ship To: DOEJOH Date: 07/10/2000 Mon

Bill To: John Doe
99 Pine St
Willowdale PA 16633

Entry Date: 06/15/2000 Thu

Payment: **Credit / Debit Card** (highlighted with a red box)
Payment: \$733.58 Card #:
Exp. Date: / (MM/yy) CVV: VISA *****6744 Exp.:
Cash Acct.: 01000-000 - Cash on Hand

Sales Person: ADMINISTRATOR P.O./Job: Ship Date: 06/15/2000 Thu Ship Via: Price Level: Retail Warehouse: LOC B

Job ID:

	Ordered	Shipped	Inventory	Measure	Description	Price	Amount	Tax Group
	1.00	1.00			Garden Kit	200.00	200.00	Taxable
	1.00	1.00	DIRSHO	ea	Dirt Shovel	32.48	32.48	Taxable
	3.00	3.00	GARRAK		Garden Rake	55.84	167.52	Taxable
	2.00	2.00	TRABIN30		30 Gallon Trash Bin	39.00	78.00	Taxable
	1.00	1.00	MAGLIT4		Maglite 4-Cell Battery	27.00	27.00	Taxable

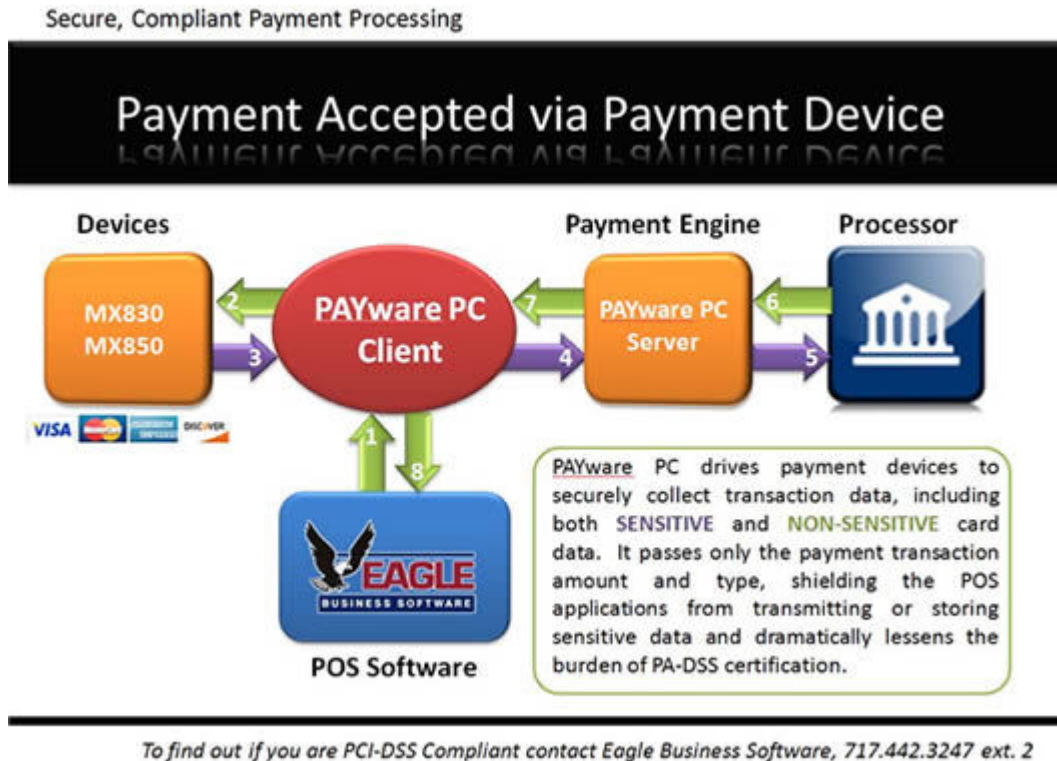
Tax Table: PA Freight: Discount: % Costs: \$454.60 S.O. Total: \$290.97 Subtotal: \$692.06
Tax: \$41.52 Finance Chg: Paid: \$733.58 Balance: \$0.00 **733.58**

Sales Order

2. Select **Credit/Debit Card** and click the down arrow to select a stored credit card as shown above. Review the [Sales > Invoices > Entering a Sales Invoice](#) section of the main documentation for more details.

Troubleshooting Credit Card Processing

PAYware accepts transaction data, including both sensitive and non-sensitive card data from manually entered information from the POS Software. It passes only the payment transaction amount and type, shielding the POS applications from transmitting or storing sensitive data and dramatically lessens the burden of PA-DSS certification.



A credit card transaction that is scanned by a payment device such as a Verifone MX Payment device is communicated directly into PAYware without interfacing with EBMS. Credit card information entered into EBMS is immediately communicated to PAYware client. The credit card transaction is then communicated to the PAYware PC server or via internet to PAYware Connect which contains the instructions to communicate to the credit card merchant account or Processor. The Processor approves the credit card transaction based on the information communicated to the processor from PAYware. Any card rejection such as insufficient funds, invalid credit card information, or any other hold on the card is determined by the credit card processor.

Review the following steps to troubleshoot credit card transactions:

- A. Try another card from the customer to see if a hold was placed on the original card or the processor is rejecting the transaction because of account issues. The credit card account may create a hold on the account causing the Processor to reject the transaction. Insufficient information or insufficient funds may also cause the processor to reject a transaction.
- B. Try a card from another bank or processor to verify that the processor is not experiencing processing issues.
- C. Verify that your internet connection is working properly. The communication between EBMS and the processor is done through a secure internet connection.
 - a. Access the same internet connection through your browser or connection tool to verify that your internet connection is operating properly.
 - b. Check any firewall settings to insure that the necessary port is not being blocked by your firewall software.

Point of Sale

- c. Note that some anti-virus or security software updates can block communication to PAYware Connect to the credit card processor.
- D. The communication between EBMS or the payment device and PAYware may be disrupted.
 - a. Log into the PAYware PC Payment Center if you are connected to PAYware PC. EBMS is connected to your PAYware PC Payment Center using your local area network (LAN). Reboot the PAYware PC Server machine on your network or have your IT staff review your LAN connections.
 - b. Log directly into PAYware Connect if you use the remote PAYware Connect service. This connection requires an internet connection. Review the notes on Step C if you cannot access PAYware Connect. Contact [PAYware Connect technical support](#) to verify that the PAYware Connect service is operating properly.
- E. Contact your EBMS support Rep for assistance if you are unable to resolve the credit card processing transaction error with the steps listed above.

Merchant Account Parameters

Eagle Business Software has partnerships with a variety of different companies to give the best variety and service possible. A merchant account must be approved by Verifone Payware in order to interface with the Eagle Business Software.

Reference the information required to configure EBMS and Payware at www.eaglebusinesssoftware.com/EBMS/Modules/MerchantAccountParameters

Select the proper form from the EBMS website and submit it to an EBMS Support Representative. Contact an EBMS Support Representative for assistance for this process.

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:

Active	Payment Name	Cash Account	PAYware PC Client ID	Proxy
<input checked="" type="checkbox"/>	Cash	Based on Warehouses	Based on Warehouses	Based on Warehouses
<input checked="" type="checkbox"/>	Check	Based on Warehouses	Based on Warehouses	Based on Warehouses
<input checked="" type="checkbox"/>	Gift Card	Based on Warehouses	Based on Warehouses	Based on Warehouses
<input checked="" type="checkbox"/>	Visa	Based on Warehouses	Based on Warehouses	Based on Warehouses
<input checked="" type="checkbox"/>	MasterCard	Based on Warehouses	Based on Warehouses	Based on Warehouses
<input checked="" type="checkbox"/>	Discover	Based on Warehouses	Based on Warehouses	Based on Warehouses
<input checked="" type="checkbox"/>	American Express	Based on Warehouses	Based on Warehouses	Based on Warehouses
<input checked="" type="checkbox"/>	EBT	Based on Warehouses	Based on Warehouses	Based on Warehouses
<input checked="" type="checkbox"/>	Debit	Based on Warehouses	Based on Warehouses	Based on Warehouses

☐ Only allow debit card payment

Credit Card Processing Software

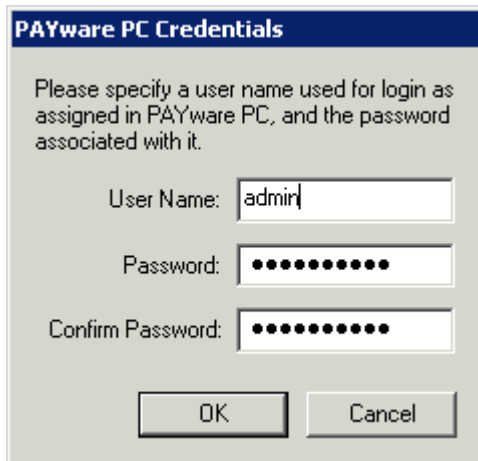
Computer name or IP address: 192.168.253.65 Credentials: **Settings...**

Proxy source port: 5500

Report path: Webms2K3VPCChargeShared

OK Cancel

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.



PAYware PC Credentials

Please specify a user name used for login as assigned in PAYware PC, and the password associated with it.

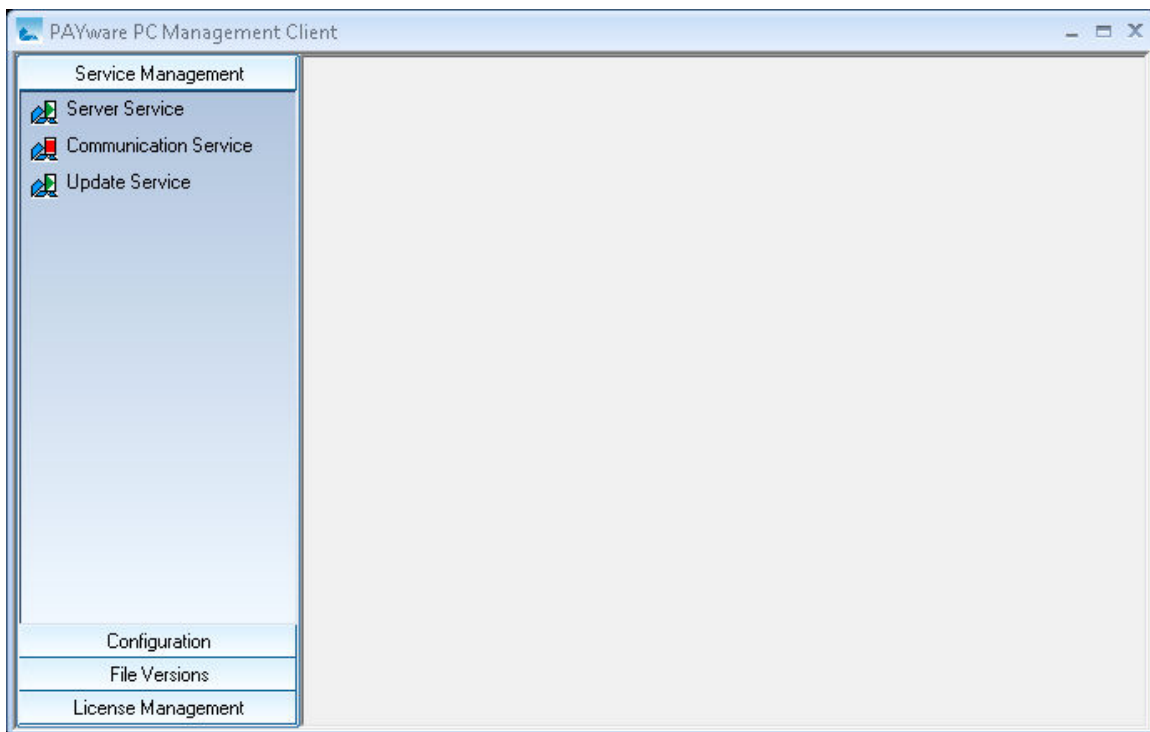
User Name:

Password:

Confirm Password:

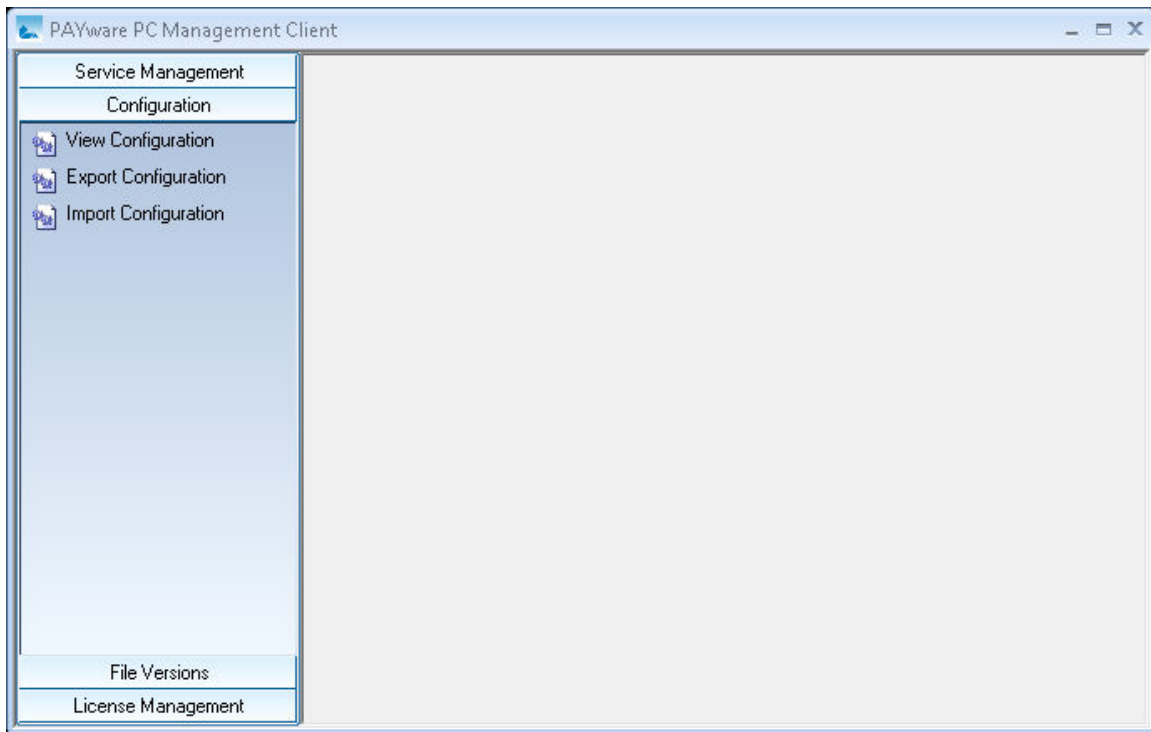
Changing the Password before it expires (recommended)

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



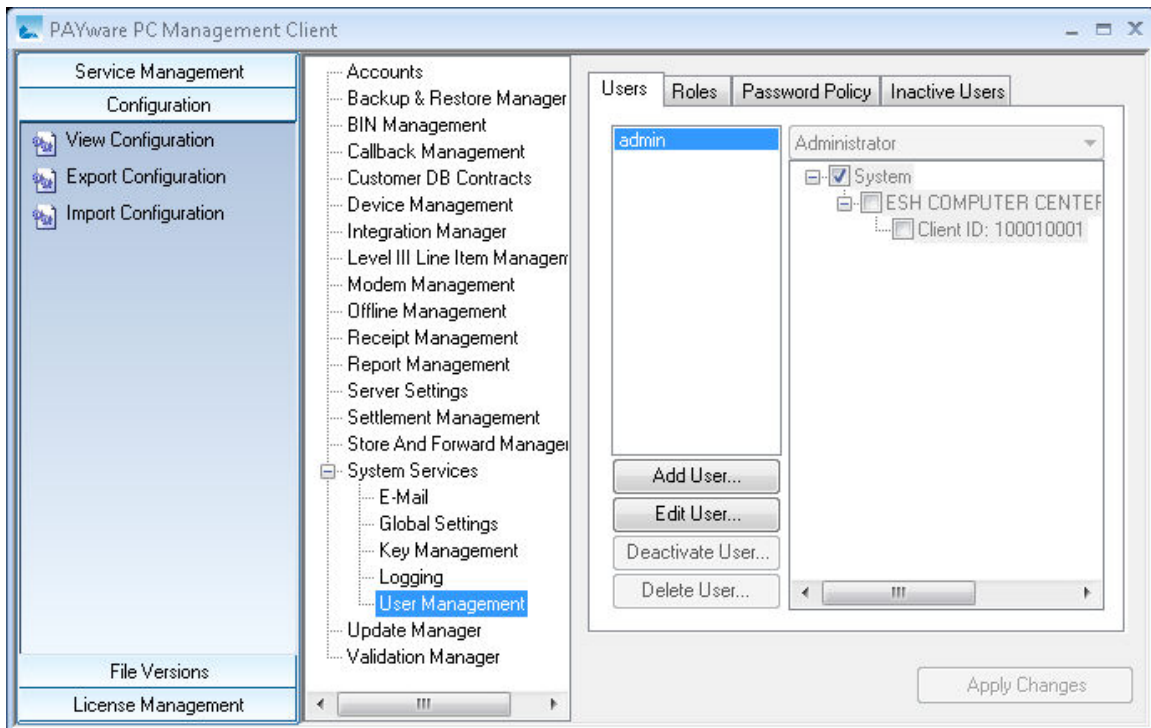
Click on the **View Configuration** button

Point of Sale

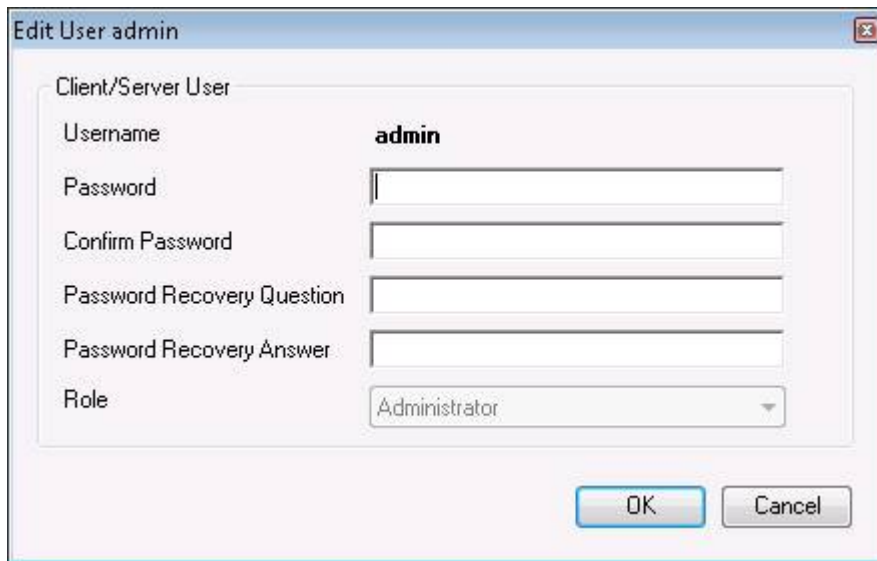


Shown below is a list of options used to manage the PAYware PC Management Client.

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.



Edit User admin

Client/Server User

Username: **admin**

Password:

Confirm Password:

Password Recovery Question:

Password Recovery Answer:

Role: Administrator

OK Cancel

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

Index

1	Computer	43
1096 fax	Computer Access.....	12
A	Computer menu	22
Acronyms.....	clicking.....	22
Active	Computer Name.....	22
Enable	Confidentiality	9, 12
Active Button.....	Configuration.....	60
Disable	Configure POS Profiles.....	22
Adjust Inventory	Confirm	60
Administrative Access	Password.....	60
Administrative and Privileged Access	Connect.....	3, 21, 57, 60
the Application	EBMS	21
Administrator Password.....	PAYware PC	57
Allow	Payware PC Management Client	60
Disable	Select	3
Enable	Contact.....	37, 43
Assign	EBMS	37, 43
Unique ID	Control	3
Attached.....	Copied.....	25
COM.....	Quantity	25
B	Copy From button	25
Bank Card Acquirers	Count	33
Bar Codes	Creating	2
Scanning	POS.....	2
Bar Codes within EBMS	Credentials.....	60
Entering	Credentials Settings.....	43
Barcode Scanner	Credit Card.....	9
Button Name.....	Credit Card Processing.....	57
C	Troubleshooting	57
Cardholder Information Security Program...9	Credit Card Processors	9
announced	Credits.....	31
Cash Account	Processing.....	31
Cash Drawer.....	Critical protective	9
Changing	Customer Display.....	3
Password	Customer ID	28
Charge button.....	CVC2	12
Choose Button Color	CVV2.....	12
Clear Payment button	D	
Clicking	Debit.....	2, 3
Computer menu	Default.....	28
Logout button	Quantity	28
Payment.....	Default Color	25
Remove This Item button.....	Reset	25
COM Port Connection	Default Customer Id	22
Commerce Module	Default Quantity	25, 28
Communicated.....	Set	28
PAYware	Default Selling.....	33
PAYware PC	identifies	33
Compliance.....	Description	22
Requirements.....	POS	22
	Devices	3
	Disable	22, 25, 43
	Active Button	25

Allow.....	22	General Use of Wireless Technology	12
PAYware PC	43	H	
Disable PAYware PC.....	43	Handle Shipping.....	39
Enable	43	Highlight.....	28
E		Quantity	28
Eagle Business Software.....	2	Host.....	43
Eagle Mobile Scanner	39	I	
Eagle Software	1	ID12, 33	
EBMS1, 2, 3, 9, 12, 21, 22, 25, 31, 33, 37,		Identifies.....	33
39, 43, 57, 60		Default Selling	33
back.....	12	IDs.....	12, 33
connected.....	21	Implementations.....	12
Contact.....	37, 43	Implementing	12
implementing.....	12	EBMS	12
maintain.....	12	Verifone PAYware PC.....	12
running	12	Important Security Notice	12
EBMS bar	33	Include	39
EBMS Bar Code Controls.....	33	UPC Association	39
EBMS Devices.....	3	Incremented	22, 28
following	3	Installing.....	43
EBMS Invoice	2	PC Charge.....	43
EBMS menu.....	3, 28, 43	Internet.....	12
Edit User	60	Systems Connected	12
Email.....	1	Introduction	9
Enable.....	31, 33, 43	Inventory	21, 31
Active	43	Inventory ID.....	25, 33
Allow.....	31	Inventory Item	25, 28
Disable PAYware PC	43	Select	25
Print Bar Code	33	Inventory Transfer.....	37
Encrypt.....	12	Invoice Prefix	22
Encrypt Sensitive Traffic.....	12	IP22, 43	
Encrypting Network Traffic	12	IP Address	43
Entering	31, 33	IPSEC	12
Bar Codes within EBMS.....	33	IT57	
SKU	31	J	
Epson printers.....	3	Job Costing	37
Esh Computer Center.....	12	Job Transfers	39
Exe application	12	K	
Expand.....	60	Keyboard Wedge	37
System Services menu	60	L	
F		Lincoln Highway.....	1
File	33	Logout button	28
Firewall	12, 57	clicking.....	28
Firewalls.....	12	Lookup button	28
Following.....	3, 12, 25, 28, 43	M	
EBMS Devices	3	Magnetic stripe.....	12
List.....	25	Main Features	39
PAYware PC	43	Maintain	12
PCI DSS Requirements	12	EBMS	12
POS window.....	28	Merchant	11
G		Merchant Applicability	12
General Non-privileged Access	12		
the Application	12		

Point of Sale

Merchant No	43	called	9
Miscellaneous	22	Payment Card Overview	41
Mobile Scanner Solution	39	Payment Cards	43
MS Windows	3, 28	Processing	43
MS Windows OS	28	Payment Name	43
Review	28	Payment PC Charge	43
Multiple Warehouse Module	22	Payment Systems Security	9
N		Payments	28, 43, 60
Name	22	clicking	43
POS	22	PAYware	57
New	25	communicated	57
New button	22	PAYware Connect	57
Next Invoice Num	22	Payware PC	2, 57, 60
No Color	25	communicated	57
Set	25	connected	57
Number	2, 12	PAYware PC	43
POS	2	disable	43
Verifone PAYware PC	12	following	43
O		PAYware PC Administrators	60
Online	2	PAYware PC Credentials	60
Options	3, 22, 25, 43, 60	PAYware PC Management Client	60
Overview	21	connect	60
P		PAYware PC Mangagement Client	60
PA	9, 12, 57	PAYware PC Payment Center	57
buden	57	PAYware PC Port	43
PA-DSS	9, 12	PAYware PC Server	57
PA-DSS 10.0 Facilitate	12	Reboot	57
PA-DSS 11.0 Facilitate	12	PC	28
PA-DSS 12.0 Encrypt sensitive traffic	12	PC Charge	43
PA-DSS 13.0 Encrypt	12	installing	43
PA-DSS 2.0 Protect	12	PCI	9, 11, 12
PA-DSS 3.0 Secure	12	relate	12
PA-DSS 6.0 Protect wireless transmissions	12	remaining	9
PA-DSS 9.0 Cardholder	12	required	12
PA-DSS Requirement 4.0	12	PCI Data Security Standard	11
PANs	12	PCI Data Security Standard Requirements	
Part	12	8.1	12
Verifone's Payware PC	12	PCI DSS	12
Passphrase	12	PCI DSS 8.1	12
Password	12, 60	PCI DSS 8.2	12
Changing	60	PCI DSS 8.3	12
confirm	60	PCI DSS 8.4	12
Password and Account	12	PCI DSS 8.5	12
Passwords to	12	PCI DSS 8.5.1	12
Payment Application	12	PCI DSS 8.5.10	12
Secure Remote Access	12	PCI DSS 8.5.11	12
Payment Application Data Security Standard	9, 12	PCI DSS 8.5.12	12
Payment Card Industry Data Security Standard	9	PCI DSS 8.5.13	12
Payment Card Industry Security Standards Council	9	PCI DSS 8.5.14	12
		PCI DSS 8.5.15	12
		PCI DSS 8.5.16	12
		PCI DSS 8.5.2	12
		PCI DSS 8.5.3	12
		PCI DSS 8.5.4	12
		PCI DSS 8.5.5	12
		PCI DSS 8.5.6	12

PCI DSS 8.5.7	12	Programmable Buttons	22, 25
PCI DSS 8.5.8	12	Properties.....	22, 33, 43
PCI DSS 8.5.9	12	selecting	22
PCI DSS Glossary	12	Properties button.....	25
Terms	12	Protect Stored Cardholder Data	12
PCI DSS Requirement 3.1.....	12	Protect Wireless Transmissions	12
PCI DSS Requirement 8.2.....	12	Public Networks	12
PCI DSS Requirement 8.3.....	12	Purge Stale Cardholder Data.....	12
PCI DSS Requirements.....	12, 60	Q	
following	12	Quantity.....	25, 28
PCI DSS Requirements 8.1	12	copied.....	25
PCI Requirements	11	default.....	28
PCI Security Practices	12	highlight	28
PCI-DSS	9	R	
PCI-DSS 1.2.3	12	RADIUS	12
PCI-DSS 2.1.1	12	Reboot	57
PCI-DSS 4.1.1	12	PAYware PC Server.....	57
PCI-DSS Requirement	12	Receipt Printer	3
Pcsecuritystandards	9	Receiving	39
Per PCI DSS Requirement 1.2.3	12	Refer	11, 12
PIN	12	Section	11
Point Of Sale.....	25	Verifone PAYware PC	12
Point-of-Sale Devices	3	Verifone PAYware PC PA	12
Point-of-Sale Overview	2	Reference	11
Populate Sales Orders	39	Relate.....	12
Port Settings	3	PCI	12
POS 2, 3, 9, 12, 21, 22, 25, 28, 31, 37, 57		Remaining.....	9
creating	2	PCI	9
Description	22	Remote Update Procedures	12
name	22	Remove All Items.....	28
number	2	Remove This Item button.....	28
shielding.....	57	clicking.....	28
use	9	RemoveCCTerms	12
uses.....	37	Reports	3, 33, 43
POS bar	28	Required	12
POS envinment.....	22	PCI	12
POS Profile list.....	22	Verifone PAYware PC.....	12
view	22	Requirements.....	11
POS Setup dialog	25	Compliance	11
POS Software.....	57	Requirements 1.2.3.....	12
POS Station	25, 28	Reset.....	25
Using	28	Default Color	25
POS Vendor's recommendations	11	Returns	31
POS window	2, 28	Review	2, 28
following	28	MS Windows OS	28
Previous Versions.....	12	Section	2
Print Bar Code	33	Running.....	12
Enable	33	EBMS	12
Proactively	9	S	
Process button.....	28	Sale Station Id.....	22
Processing	31, 43	Point	22
Credits.....	31	Sales	1, 2, 3, 22, 25, 43, 60
Payment Cards	43	Point	22
Processor.....	57		
causing.....	57		
Processor ID	43		

selecting	43
Scanning	37
Bar Codes	37
Seamlessly	39
Search button	28
Section	2, 11
Refer	11
Review	2
Secure Authentication Features	12
Secure Remote Access	12
Payment Application	12
Secure Remote Access Requirements	12
Secure Remote Software Updates	12
Secure Socket Layer	12
Securely Delete Cryptographic Material	12
Security management	9
See screenshot	12
Verifone PAYware PC Administration Center	12
See Verifone PAYware PC	12
Select	3, 22, 25, 43
Connect	3
Inventory Item	25
Properties	22
Sales	43
Sensitive Authentication Data	12
Sensitive credit	12
Serial	3
Service Rep	43
Settlement URL	43
Shielding	57
POS	57
Shipping	39
Signature Pad	3
Signature Size	3
MX830	3
Since EBMS	12
Smartcard	12
SNMP	12
SO Window	2
Software design	9
SSL	12
Step	57
Suite	1
Support@EagleBusinessSoftware.com	1
Sync	21
Sync tool	21
using	21
System Services menu	60
Expand	60
Systems Connected	12
Internet	12
T	
TACACS	12
Technical Support	1

Termina Processor Type	43
Terms	12
PCI DSS Glossary	12
The Payment Application	12
The PCI Data Security Standard	9
TLS	12
Touch Screen	3, 21
Touch Screen POS	21, 31
Touch Screen POS System	2, 21
Troubleshooting	12, 57
Credit Card Processing	57
Two-Factor Authentication	12

U

Undo	25
Unique ID	12
Assign	12
Unit	33
UOM dialog	33
UPC	33, 39
UPC Association	39
Include	39
UPC Code	33
URL	43
USB	3
User	60
User Management	60
Uses	2, 9, 12, 37
POS	9, 37
Verifone Payware PC	2
Using	21, 28
POS station	28
Sync tool	21

V

Verifone	3
Verifone MX Payment	57
Verifone MX830	3
Verifone MX830 Payment	3
Verifone Payware PC	2, 12
implementing	12
number	12
part	12
refer	12
require	12
uses	2
Verifone PAYware PC Administration Center	12
See screenshot	12
Verifone PAYware PC application	12
Verifone PAYware PC PA	12
Refer	12
Verifone PAYware PC's	12
Verifone PAYware PC's Users Manual	12
Verifone PAYware SIM SSL	12
Verifone's Payware PC's	60

View	22
POS Profile list	22
View Configuration	60
Visa	9
VPN	12

W

Warehouse.....	22, 37, 39
Weigh Scale.....	3
WEP	12
Wireless Technology Included.....	12
Www.EagleBusinessSoftware.com	1
