PA-DSS Implementation Guide

for

Sage MAS 90 and 200 ERP

Versions 4.30.0.18 and 4.40.0.1

and

Sage MAS 90 and 200 Extended Enterprise Suite

Versions 1.3 with Sage MAS 90 and 200 ERP 4.30.0.18
and 1.4 with Sage MAS 90 and 200 ERP 4.40.0.1

March 17, 2010

©2010 Sage, Inc. All rights reserved. Sage, the Sage logos and the Sage product and service names mentioned herein are registered trademarks or trademarks of Sage Software, Inc., or its affiliated entities. All other trademarks are the property of their respective owners.

©2010 Sage, Inc. All rights reserved.

Table of Contents

©2010 Sage, Inc. All rights reserved.

©2010 Sage, Inc. All rights reserved.

1 INTRODUCTION AND SCOPE

1.1 Introduction

The purpose of this PA-DSS Implementation Guide is to instruct merchants, resellers and integrators on how to implement Sage MAS 90 and 200 ERP and Sage MAS 90 and 200 Extended Enterprise Suite into their environment in a PA-DSS compliant manner. It is not intended to be a complete installation guide. The software, if installed according to the guidelines documented here, should facilitate and support a merchant's PCI compliance. This guide applies to Sage MAS 90 and 200 ERP and Sage MAS 90 and 200 Extended Enterprise Suite as released by Sage. Any modifications to the application, for example Customizer, Web Services, Extended Solutions and other Master Developer enhancements, must be reviewed to determine their impact to the PA-DSS requirements.

1.2 What is Payment Application Data Security Standard (PA-DSS)?

The Payment Application Data Security Standard (PA-DSS) is a set of security standards that were created by the PCI SSC to guide payment application vendors to implement secure payment applications.

1.3 Distribution and Updates

This PA-DSS Implementation Guide should be disseminated to all relevant application users including merchants, resellers, and integrators. It should be updated at least annually and after changes in the software. The annual review and update should include new software changes as well as changes in the PA-DSS standard.

Updates to the PA-DSS Implementation Guide can be obtained by going to the Sage Online Customer Support Web site at: www.sagesoftwareonline.com. In addition, Sage will publish updates and send update notifications as needed.

1.4 Versions

This PA-DSS Implementation Guide references both the PA-DSS and PCI requirements. The following versions are referenced in this guide.

- PA-DSS version 1.2
- PCI DSS version 1.2

©2010 Sage, Inc. All rights reserved.

1.5 Legal Terms and Conditions

The following legal terms and conditions must be provided to the owner of the software being implemented.

Acceptance of a given payment application by the PCI Security Standards Council, LLC (PCI SSC) only applies to the specific version of that payment application that was reviewed by a PA-QSA and subsequently accepted by PCI SSC (the "Accepted Version"). If any aspect of a payment application or version thereof is different from that which was reviewed by the PA-QSA and accepted by PCI SSC – even if the different payment application or version (the "Alternate Version") conforms to the basic product description of the Accepted Version – then the Alternate Version should not be considered accepted by PCI SSC, nor promoted as accepted by PCI SSC.

No vendor or other third party may refer to a payment application as "PCI Approved" or "PCI SSC Approved", and no vendor or other third party may otherwise state or imply that PCI SSC has, in whole or part, accepted or approved any aspect of a vendor or its services or payment applications, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with PCI SSC, or in a PA-DSS letter of acceptance provided by PCI SSC. All other references to PCI SSC's approval or acceptance of a payment application or version thereof are strictly and actively prohibited by PCI SSC.

When granted, PCI SSC acceptance is provided to ensure certain security and operational characteristics important to the achievement of PCI SSC's goals, but such acceptance does not under any circumstances include or imply any endorsement or warranty regarding the payment application vendor or the functionality, quality, or performance of the payment application or any other product or service. PCI SSC does not warrant any products or services provided by third parties. PCI SSC acceptance does not, under any circumstances, include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose or noninfringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services that have received acceptance from PCI SSC, shall be provided by the party providing such products or services, and not by PCI SSC or any payment brands."

©2010 Sage, Inc. All rights reserved.

2 SECURE DELETION OF SENSITIVE DATA AND PROTECTION OF STORED CARDHOLDER DATA

2.1 Merchant and Reseller/Integrator Applicability

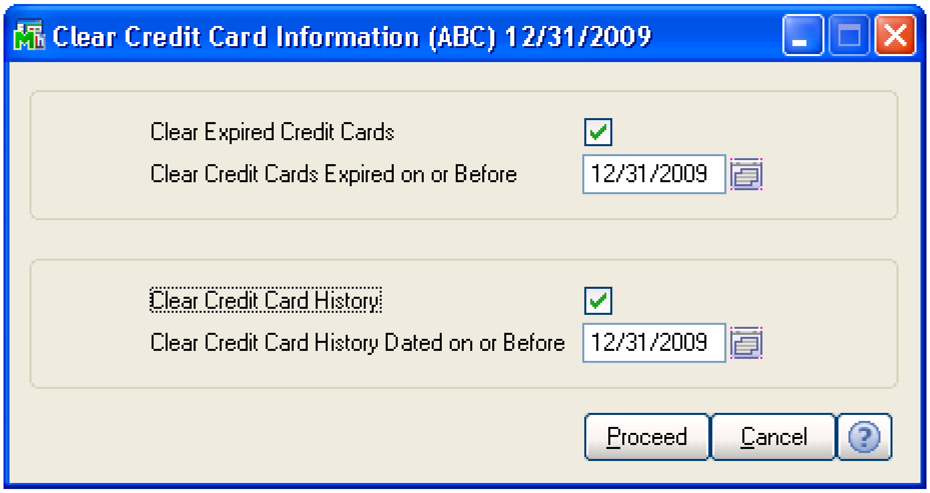
Magnetic stripe data, card validation values or codes, PINs or PIN block data, cryptographic key material, or cryptograms should not be stored in the data. The software does not store any of this in the data. The software does provide batch processing of credit card transactions to optimize the merchant's fee. The card validation number will be temporarily stored encrypted until that request is attempted. After the request is attempted the card validation number is removed whether the transaction request was successful or unsuccessful.

2.2 Secure Deletion Instructions

The following instructions can be used to securely delete prohibited historical data and to purge cardholder data after expiration:

- Cardholder data should be purged on a regular basis depending on a balance between the needs of the business and PCI compliance. The software provides a purge task that will remove cardholder data and can be run when needed. This process will only purge credit card related data. Customer and sales related information will be retained.

- Cardholder data can be deleted using the Clear Credit Card Information utility. Based on criteria specified for the utility, cardholder data will be purged. Data will be purged if it is determined that it is not part of any open transaction and matches criteria specified on the form. The Activity Log indicates each time the Clear Credit Card Information utility is run. In the event of a power failure or some other unplanned event while producing reports containing unencrypted credit card numbers, run the Clear Credit Card Information utility to ensure deletion of sensitive data.



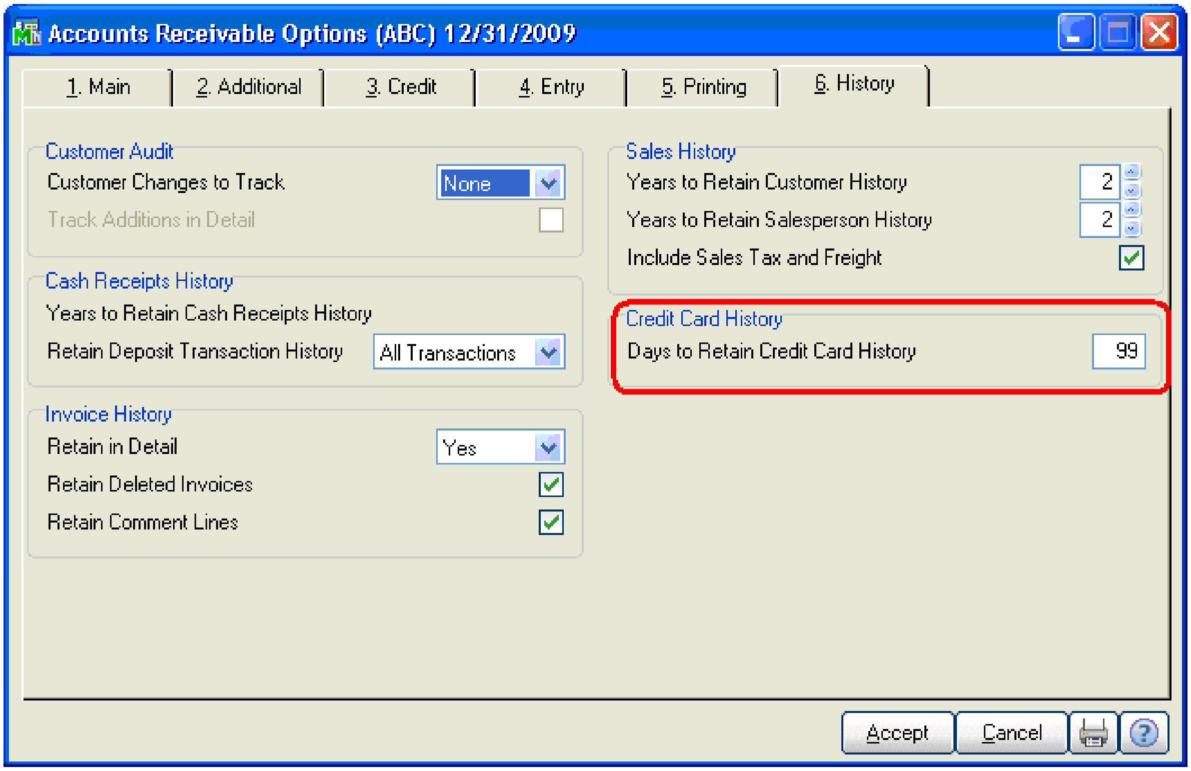
Clear Credit Card Information (ABC) 12/31/2009

Clear Expired Credit Cards ☑
Clear Credit Cards Expired on or Before 12/31/2009

Clear Credit Card History ☑
Clear Credit Card History Dated on or Before 12/31/2009

©2010 Sage, Inc. All rights reserved.

- Expired credit cards will also be purged during period end prior to the number of days entered at the Days to Retain Credit Card History field in Accounts Receivable Options.



Customer Audit

Customer Changes to Track: None

Track Additions in Detail □

Cash Receipts History

Years to Retain Cash Receipts History

Retain Deposit Transaction History: All Transactions

Invoice History

Retain in Detail: Yes

Retain Deleted Invoices ☑

Retain Comment Lines ☑

Sales History

Years to Retain Customer History: 2

Years to Retain Salesperson History: 2

Include Sales Tax and Freight ☑

Credit Card History

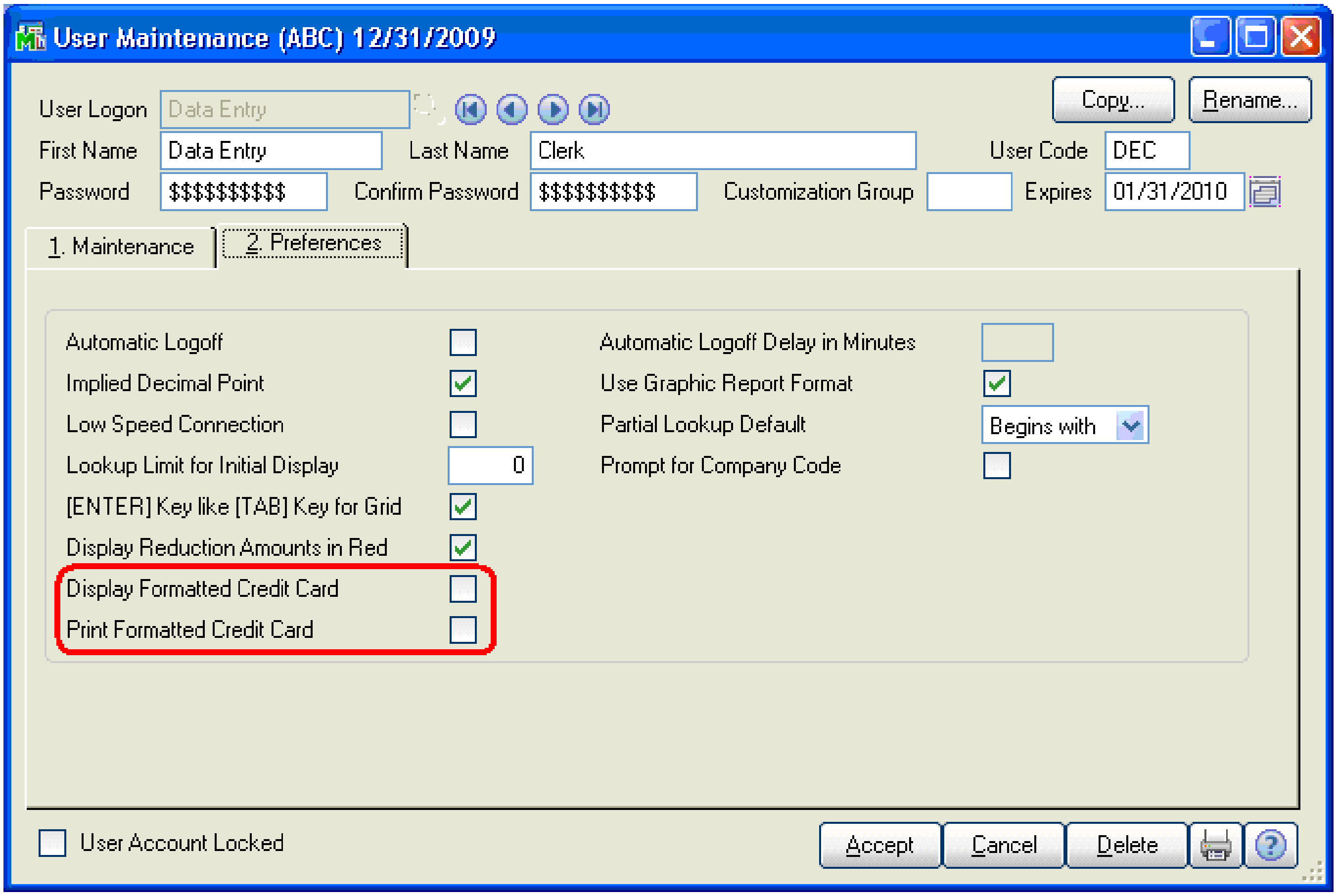
Days to Retain Credit Card History: 99

©2010 Sage, Inc. All rights reserved.

2.3 Display Formatted Credit Card and Print Formatted Credit Card Options

The Customer Listing, Customer Credit Card Listing, Deposit Transaction Report, and the Visual Integrator Exports for tables that include credit card number provide a means where cardholder data can be retrieved and viewed in a usable format. Because of the sensitivity of these reports, access to the reports and protection of the reports after they have been produced is critical to PA-DSS compliance. Similarly, the formatted credit card can be viewed in credit card related maintenance, inquiry and data entry windows. By default, cardholder data is in masked format. The following instructions describe steps that can be taken to secure the displaying and printing of formatted credit card data.

Access to the formatted credit card is controlled through User Maintenance, and should be limited to only those with a business need to obtain the formatted credit card. Limit access to as few people as possible by leaving the Display Formatted Credit Card and Print Formatted Credit Card checkboxes unchecked as shown below:



User Maintenance (ABC) 12/31/2009

User Logon	Data Entry				
First Name	Data Entry	Last Name	Clerk	User Code	DEC
Password	$$$$$$$$$$	Confirm Password	$$$$$$$$$$	Customization Group	
				Expires	01/31/2010

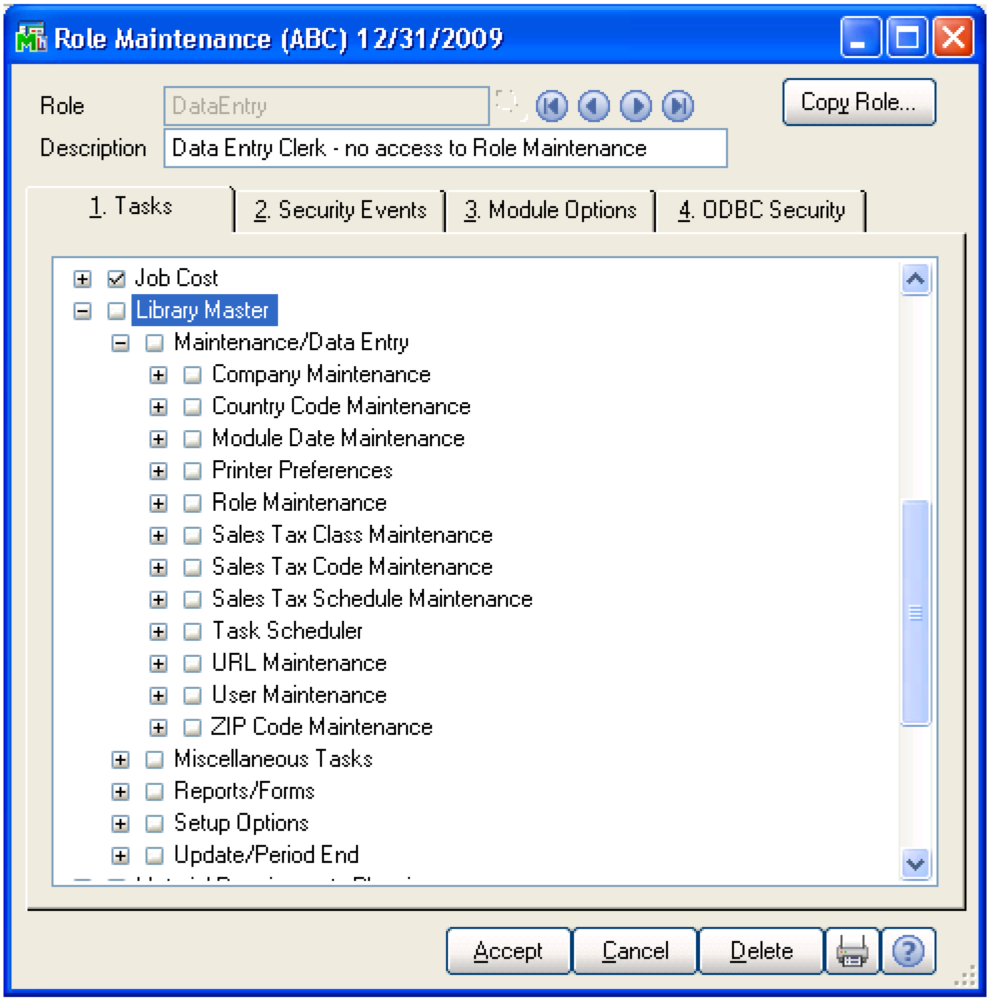
Automatic Logoff	☐	Automatic Logoff Delay in Minutes	
Implied Decimal Point	☑	Use Graphic Report Format	☑
Low Speed Connection	☐	Partial Lookup Default	Begins with
Lookup Limit for Initial Display	0	Prompt for Company Code	☐
[ENTER] Key like [TAB] Key for Grid	☑		
Display Reduction Amounts in Red	☑		
Display Formatted Credit Card	☐		
Print Formatted Credit Card	☐		

☐ User Account Locked

The ability to print and display the formatted credit card is set in User Maintenance; therefore, it is crucial that User Maintenance be secured to only those with authority to change the values.

©2010 Sage, Inc. All rights reserved.

Securing User Maintenance is accomplished in Role Maintenance as shown below:



Role: DataEntry

Description: Data Entry Clerk - no access to Role Maintenance

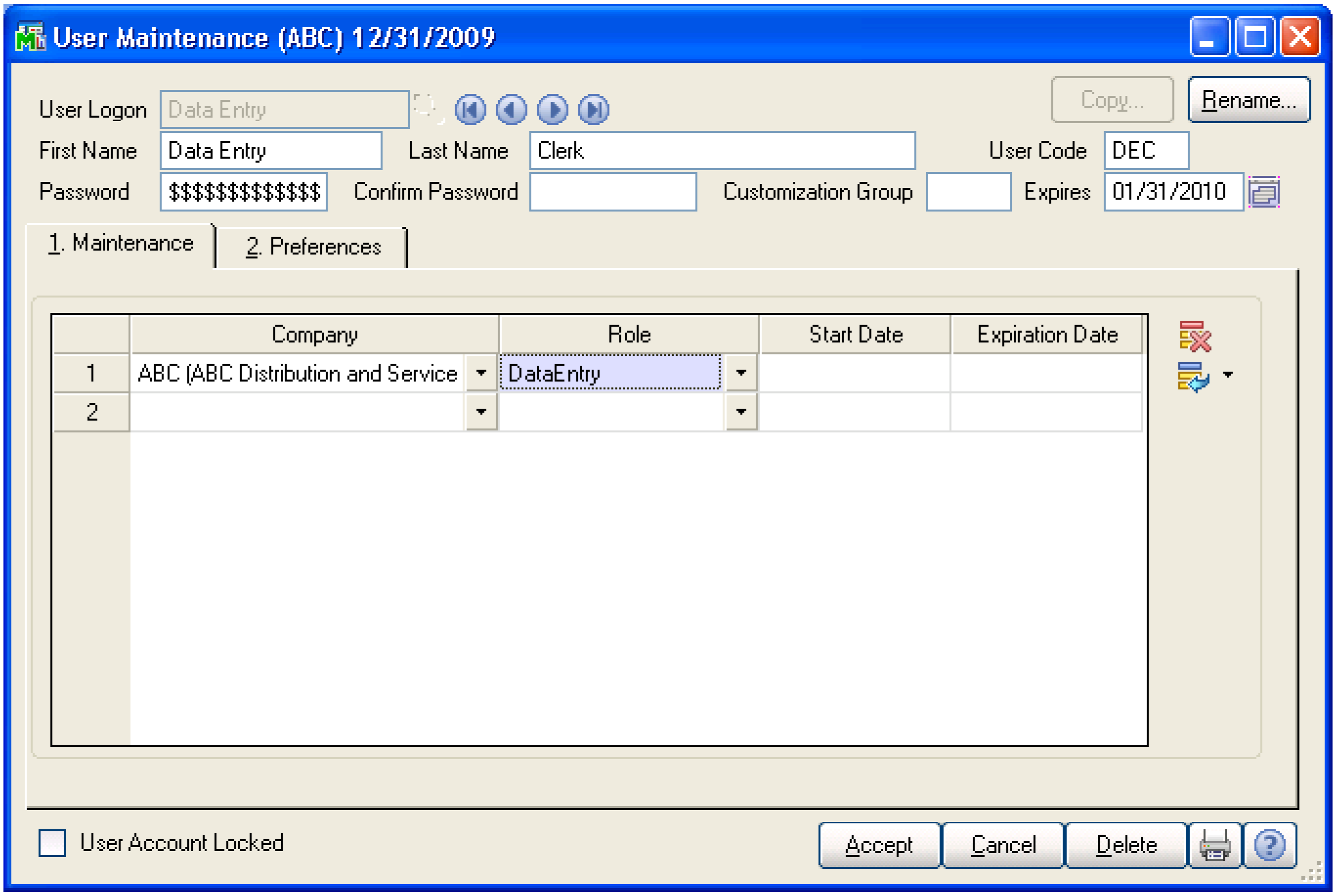
- ☑ Job Cost
- □ Library Master
  - □ Maintenance/Data Entry
    - □ Company Maintenance
    - □ Country Code Maintenance
    - □ Module Date Maintenance
    - □ Printer Preferences
    - □ Role Maintenance
    - □ Sales Tax Class Maintenance
    - □ Sales Tax Code Maintenance
    - □ Sales Tax Schedule Maintenance
    - □ Task Scheduler
    - □ URL Maintenance
    - □ User Maintenance
    - □ ZIP Code Maintenance
  - □ Miscellaneous Tasks
  - □ Reports/Forms
  - □ Setup Options
  - □ Update/Period End

Role Maintenance and User Maintenance are unchecked for this role.

Note: Access to all Library Master tasks should be limited to only those with a need to modify system setup.

©2010 Sage, Inc. All rights reserved.

The user can then be assigned this role in User Maintenance.


User Maintenance (ABC) 12/31/2009

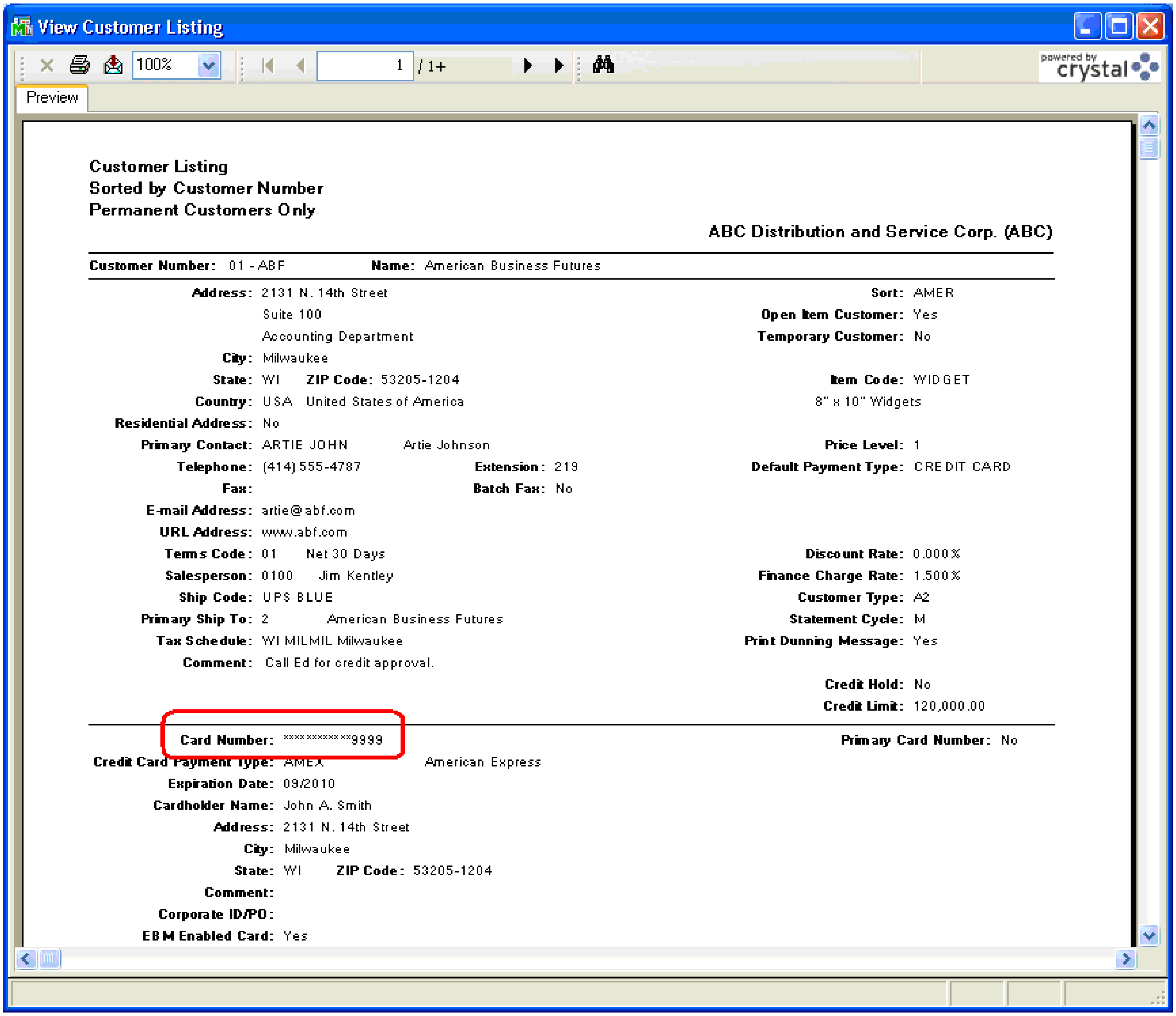
User Logon: Data Entry
First Name: Data Entry
Last Name: Clerk
User Code: DEC
Password: $$$$$$$$$$$$$$
Confirm Password:
Customization Group:
Expires: 01/31/2010

	Company	Role	Start Date	Expiration Date
1	ABC (ABC Distribution and Service	DataEntry		
2				

□ User Account Locked

©2010 Sage, Inc. All rights reserved.

The Print Formatted Credit Card setting in User Maintenance defaults to unchecked and sensitive cardholder data will be masked as shown below:



Customer Listing
Sorted by Customer Number
Permanent Customers Only

ABC Distribution and Service Corp. (ABC)

Customer Number: 01 - ABF **Name:** American Business Futures

Address: 2131 N. 14th Street
Suite 100
Accounting Department
City: Milwaukee
State: WI **ZIP Code:** 53205-1204
Country: USA United States of America
Residential Address: No
Primary Contact: ARTIE JOHN Artie Johnson
Telephone: (414) 555-4787 **Extension:** 219
Fax: **Batch Fax:** No
E-mail Address: artie@abf.com
URL Address: www.abf.com
Terms Code: 01 Net 30 Days
Salesperson: 0100 Jim Kentley
Ship Code: UPS BLUE
Primary Ship To: 2 American Business Futures
Tax Schedule: WI MILMIL Milwaukee
Comment: Call Ed for credit approval.

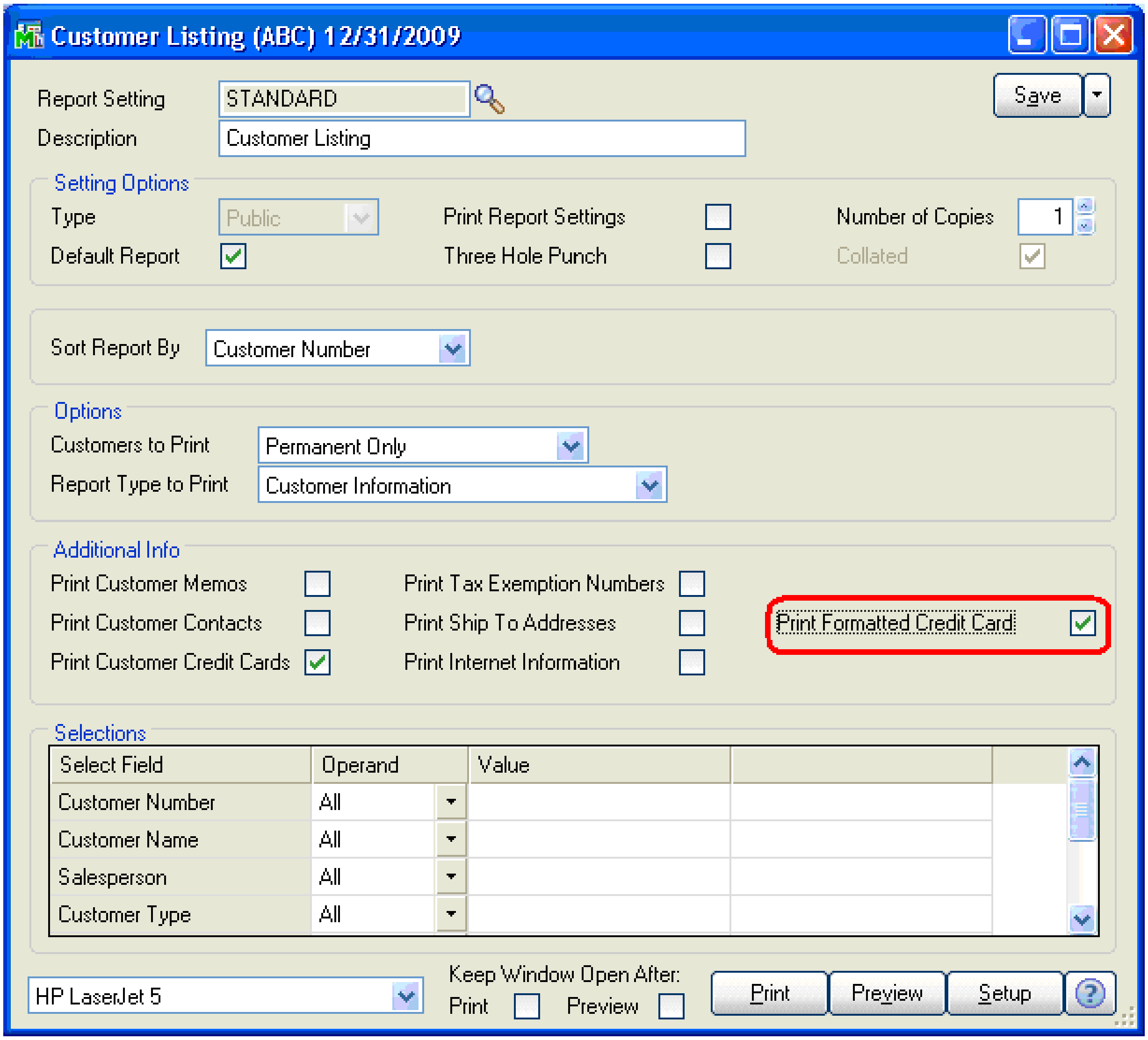
Sort: AMER
Open Item Customer: Yes
Temporary Customer: No
Item Code: WIDGET
8" x 10" Widgets
Price Level: 1
Default Payment Type: CREDIT CARD
Discount Rate: 0.000%
Finance Charge Rate: 1.500%
Customer Type: A2
Statement Cycle: M
Print Dunning Message: Yes
Credit Hold: No
Credit Limit: 120,000.00

Card Number: xxxxxxxxxxxx9999 **Primary Card Number:** No
Credit Card Payment Type: AMEX American Express
Expiration Date: 09/2010
Cardholder Name: John A. Smith
Address: 2131 N. 14th Street
City: Milwaukee
State: WI **ZIP Code:** 53205-1204
Comment:
Corporate ID/PO:
EBM Enabled Card: Yes

©2010 Sage, Inc. All rights reserved.

Selecting the Display Formatted Credit Card and/or Print Formatted Credit Card check box in User Maintenance gives permission to display the cardholder data in its unmasked form. This permission should be limited to only those with a business need to have access to sensitive cardholder data. If this access is not necessary, then no user needs to have the Display Formatted Credit Card or Print Formatted Credit Card check box selected.

When printing the report, by default, even when the user has rights to print the formatted credit card a Print Formatted Credit Card check box is still disabled on the report dialog. For example, on the Customer Listing the Print Customer Credit Cards check box would enable the Print Formatted Credit Card check box. Only when both check boxes are selected is the formatted credit card printed on the report.



Customer Listing (ABC) 12/31/2009

Report Setting: STANDARD
Description: Customer Listing

Setting Options
Type: Public
Print Report Settings □
Number of Copies: 1
Default Report ☑
Three Hole Punch □
Collated ☑

Sort Report By: Customer Number

Options
Customers to Print: Permanent Only
Report Type to Print: Customer Information

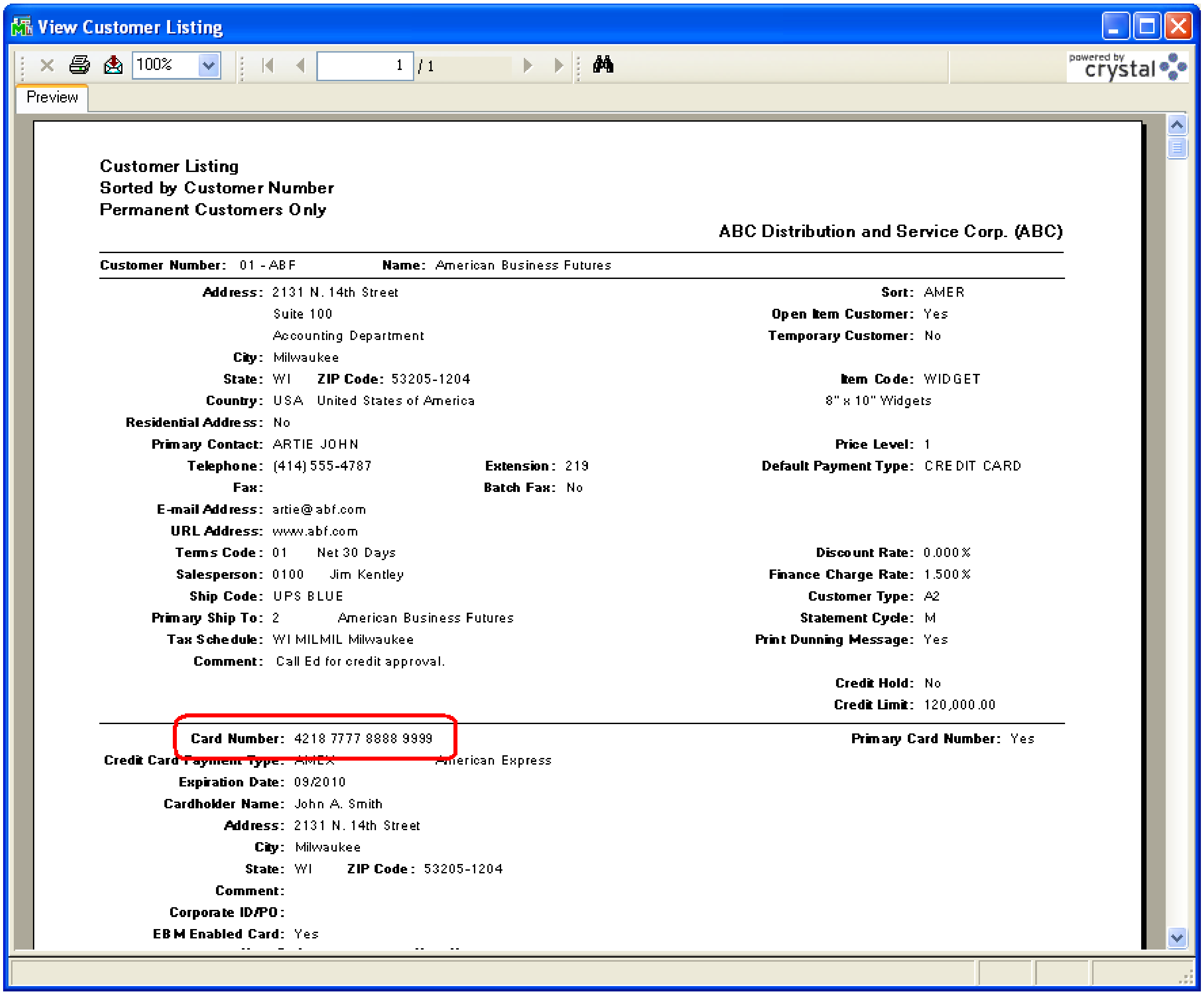
Additional Info
Print Customer Memos □
Print Tax Exemption Numbers □
Print Customer Contacts □
Print Ship To Addresses □
Print Formatted Credit Card ☑
Print Customer Credit Cards ☑
Print Internet Information □

Selections

Select Field	Operand	Value	
Customer Number	All		
Customer Name	All		
Salesperson	All		
Customer Type	All		

HP LaserJet 5
Keep Window Open After: Print □ Preview □

©2010 Sage, Inc. All rights reserved.



Customer Listing
Sorted by Customer Number
Permanent Customers Only

ABC Distribution and Service Corp. (ABC)

Customer Number: 01 - ABF **Name:** American Business Futures

Address:	2131 N. 14th Street	**Sort:**	AMER
	Suite 100	**Open Item Customer:**	Yes
	Accounting Department	**Temporary Customer:**	No
City:	Milwaukee		
State:	WI **ZIP Code:** 53205-1204	**Item Code:**	WIDGET
Country:	USA United States of America		8" x 10" Widgets
Residential Address:	No		
Primary Contact:	ARTIE JOHN	**Price Level:**	1
Telephone:	(414) 555-4787 **Extension:** 219	**Default Payment Type:**	CREDIT CARD
Fax:	**Batch Fax:** No		
E-mail Address:	artie@abf.com		
URL Address:	www.abf.com		
Terms Code:	01 Net 30 Days	**Discount Rate:**	0.000%
Salesperson:	0100 Jim Kentley	**Finance Charge Rate:**	1.500%
Ship Code:	UPS BLUE	**Customer Type:**	A2
Primary Ship To:	2 American Business Futures	**Statement Cycle:**	M
Tax Schedule:	WI MILMIL Milwaukee	**Print Dunning Message:**	Yes
Comment:	Call Ed for credit approval.		
		Credit Hold:	No
		Credit Limit:	120,000.00

Card Number:	4218 7777 8888 9999	**Primary Card Number:**	Yes
Credit Card Payment Type:	AMEX American Express		
Expiration Date:	09/2010		
Cardholder Name:	John A. Smith		
Address:	2131 N. 14th Street		
City:	Milwaukee		
State:	WI **ZIP Code:** 53205-1204		
Comment:			
Corporate ID/PO:			
EBM Enabled Card:	Yes		

After the report has been printed, control physical access to the report by unauthorized users; limiting access to those with a need to know. After the report is no longer needed, ensure secure destruction of the report using a crosscut shredder or incineration.

2.4 Secure Deletion of Sensitive Data

Per PCI DSS requirement 3.2, securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files, and other data sources received from customers, to ensure that magnetic stripe data, card validation codes or values, and PINs or PIN block data are not stored on the software vendor systems. These data sources must be collected in limited amounts and only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use.

Pursuant to this requirement, the system stores a debugging log in the HOME directory when the Debugging Log check box is selected in Company Maintenance. It is automatically deleted when this check box is cleared.

©2010 Sage, Inc. All rights reserved.

3 PASSWORD AND ACCOUNT SETTINGS

3.1 Access Control

Merchants, resellers, and integrators are advised to control access, using unique username and PCI DSS compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

3.2 Passwords

The following guidelines should be followed.

- Customers and resellers/integrators are advised against using administrative accounts for application logins. (PA-DSS 3.1c)
- Customers and resellers/integrators are advised to assign strong passwords to these default accounts (even if they will not be used), and then disable or do not use the accounts. (PA-DSS 3.1c)
- Customers and resellers/integrators are advised to assign strong application and system passwords whenever possible. (PA-DSS 3.1c)
- Customers and resellers/integrators are advised how to create PCI DSS-compliant complex passwords to access the payment application, per PCI Data Security Standard 8.5.8 through 8.5.15. (PA-DSS 3.1c)
- Customers and resellers/integrators are advised to control access, using unique username and PCI DSS-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data. (PA-DSS 3.2)

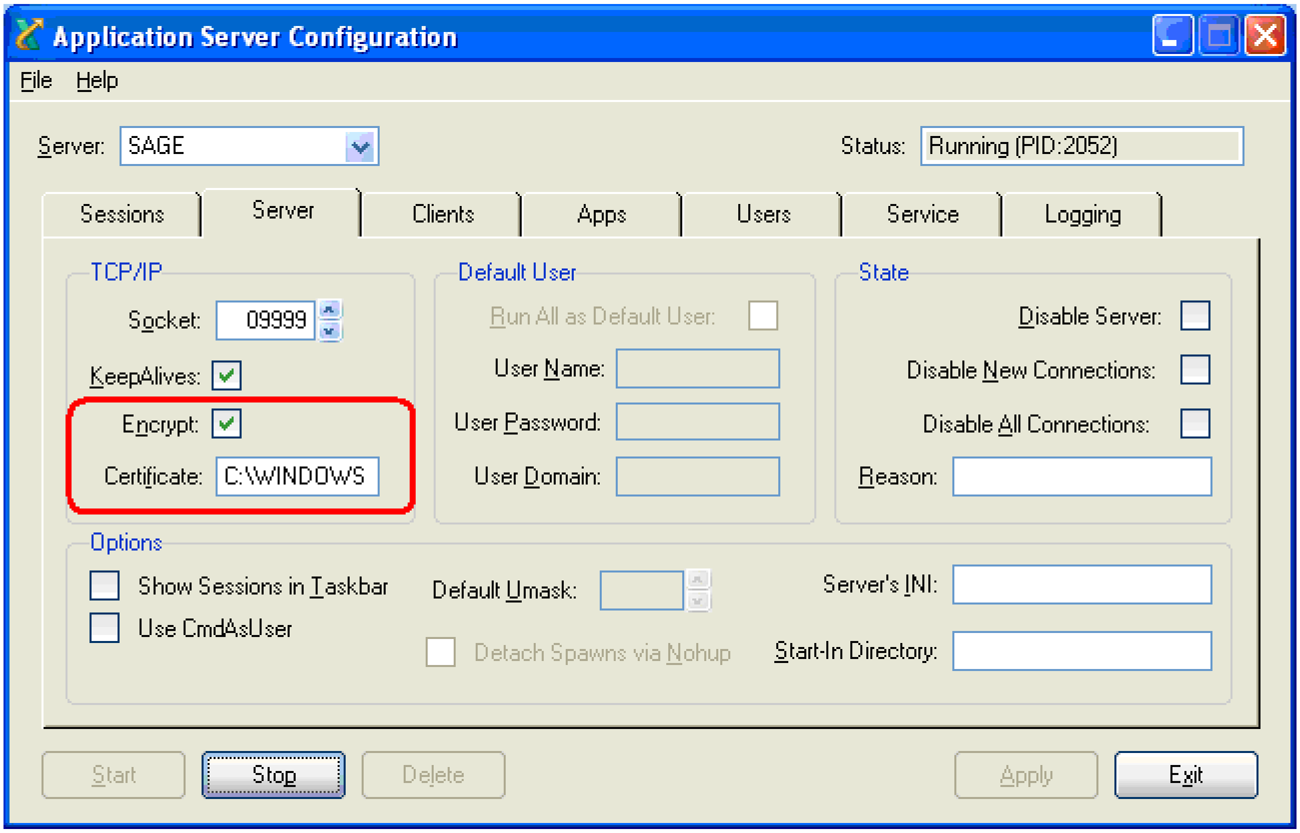
Passwords should meet the requirements set in PCI DSS section 8.5.8 through 8.5.15, as listed here.

- Do not use group, shared, or generic accounts and passwords
- Change user passwords at least every 90 days
- Require a minimum password length of at least 7 characters
- Use passwords containing both numeric and alphabetic characters
- Do not allow an individual to submit a new password that is the same as any of the last 4 passwords he or she has used
- Limit repeated access attempts by locking out the user ID after not more than 6 attempts
- Set the lockout duration to 30 minutes or until administrator enables the user ID
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal

Pursuant to this requirement, define the above password settings in System Configuration.

©2010 Sage, Inc. All rights reserved.

Pursuant to PCI DSS requirements 8.4, the MAS 200 Application Server must be configured to require encryption. See the *Sage MAS 200 ERP Installation and System Administrator's Guide* or the *Sage MAS 200 Extended Enterprise Suite Installation and System Administrator's Guide* for instructions on configuring to use SSL to encrypt data being sent to and from the Application Server.



Server: SAGE

Status: Running (PID:2052)

Socket: 09999

KeepAlives: ☑

Encrypt: ☑

Certificate: C:\WINDOWS

Run All as Default User: □

User Name:

User Password:

User Domain:

Disable Server: □

Disable New Connections: □

Disable All Connections: □

Reason:

□ Show Sessions in Taskbar

□ Use CmdAsUser

Default Umask:

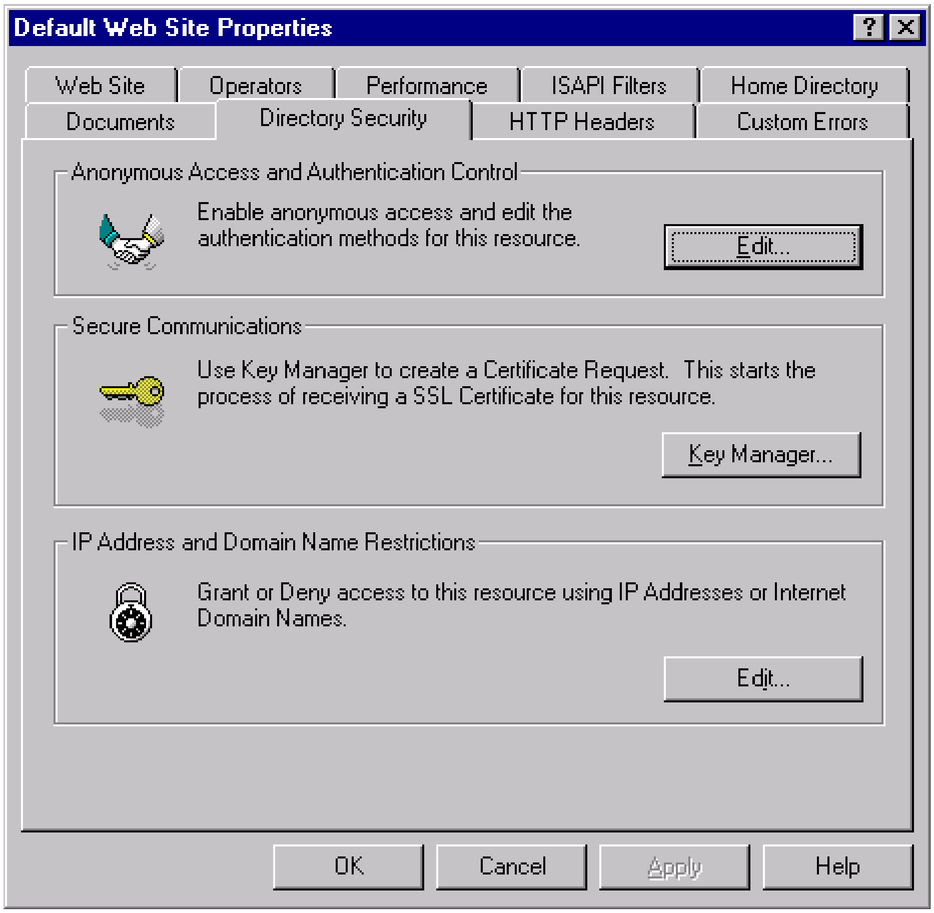
□ Detach Spawns via Nohup

Server's INI:

Start-In Directory:

©2010 Sage, Inc. All rights reserved.

When configuring Sage CRM in Sage MAS 90 or Sage MAS 200 Extended Enterprise Suite, an SSL certificate can be imported into IIS to create a secure connection between Sage CRM and its users. When a client logs onto CRM, the SSL certificate is downloaded and the data sent to and from the client is encrypted. Using this method, anybody can log on and download the SSL certificate. To be more secure, IIS should be configured to only allow clients with a SSL certificate installed on their machine and deny anybody without the appropriate certificate. Also, IIS should use Windows NT Challenge/Response, which basically requests a user to log on using a valid username and password for that domain, before giving them access to any data.



Enable anonymous access and edit the authentication methods for this resource.

Use Key Manager to create a Certificate Request. This starts the process of receiving a SSL Certificate for this resource.

Grant or Deny access to this resource using IP Addresses or Internet Domain Names.

3.3 Key Management

Customers must implement key management procedures to support periodic key changes and replacements of known or suspected compromised encryption keys (PA-DSS 2.6). The software provides a procedure for securely changing the key for a company used to protect cardholder data in Company Maintenance.

3.4 Backups

It is recommended to have a backup procedure in place. For enhanced system credit card security, store the application data separate from the system data.

©2010 Sage, Inc. All rights reserved.

4 LOGGING

4.1 Merchant Applicability

Currently, there is no end-user, configurable, logging settings. All logging conforms to PCI DSS version 1.2 requirements 10.2.1-10.2.7 and 10.3.1-10.3.6. Logs are enabled automatically when selecting a credit card server payment selection in Company Maintenance and cannot be disabled.

4.2 PCI Guidelines for Logging

Implement automated audit trails for all system components to reconstruct the following events:

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

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

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

4.3 Configuring Log Settings

The following instructions can be used to set up auditing that is required to satisfy PCI-DSS compliance. Disabling or failing to implement the following audits could cause your installation to be no longer PCI-DSS compliant.

4.3.1 Capturing Access to Cardholder Data Outside the Software

ODBC allows access to encrypted credit card numbers, but not decrypted credit card numbers; however, security can be set up to disable access to the encrypted credit card number by using System Configuration and Role Maintenance.

4.3.2 Capturing Read Access to Cardholder Data

The software logs any time a credit card is decrypted for any reason. We store the last four credit card numbers unencrypted and display credit card numbers masked. If a user is only requiring read access, there is no need to decrypt or log the credit card number because the user would have had no access to the full credit card number.

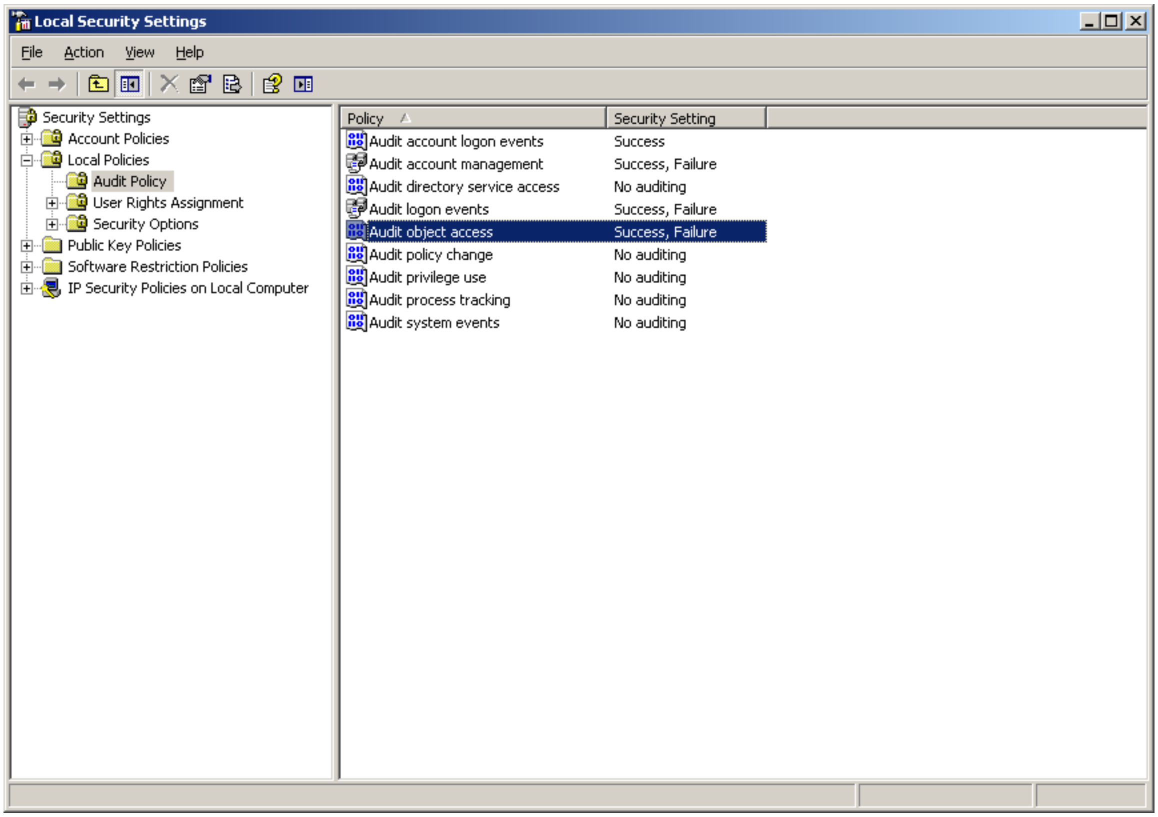
©2010 Sage, Inc. All rights reserved.

4.3.3 Access to Audit Trails

Pursuant to PCI DSS 10.2.6 which requires the ability to reconstruct the initialization of audit logs, Sage recommends enabling Auditing in Advanced Security Settings on the ..\MAS90\MAS_SYSTEM folder where your software has been installed to monitor access to the system Activity Log and the Credit Card Audit Log files.

For example, on an MAS 90 system running on Windows Server 2003 the following steps should be performed:

1. Select the Administrator Tools menu > Local Security Policy.
2. On the Local Security Settings window that appears, enable Audit Object Access.

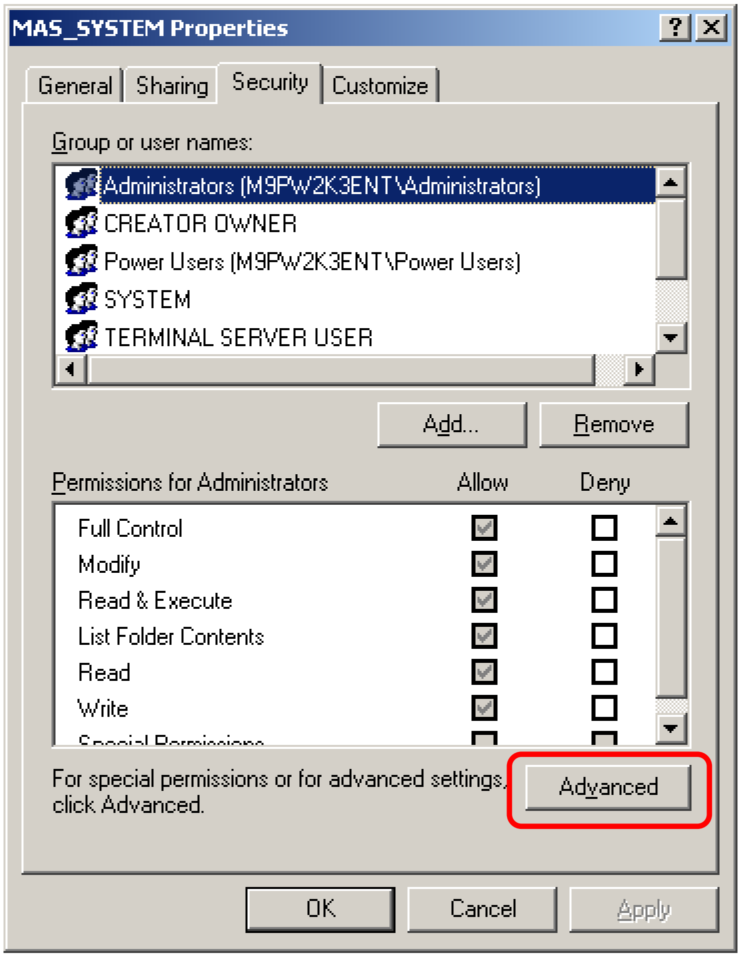


Policy	Security Setting
Audit account logon events	Success
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

3. Using Windows Explorer, navigate to the ..\MAS90\MAS_SYSTEM folder and right-click the MAS_SYSTEM folder, and then click Properties.

©2010 Sage, Inc. All rights reserved.

4. In the MAS_SYSTEM Properties window, click the Security tab, and then click Advanced.



Group or user names:

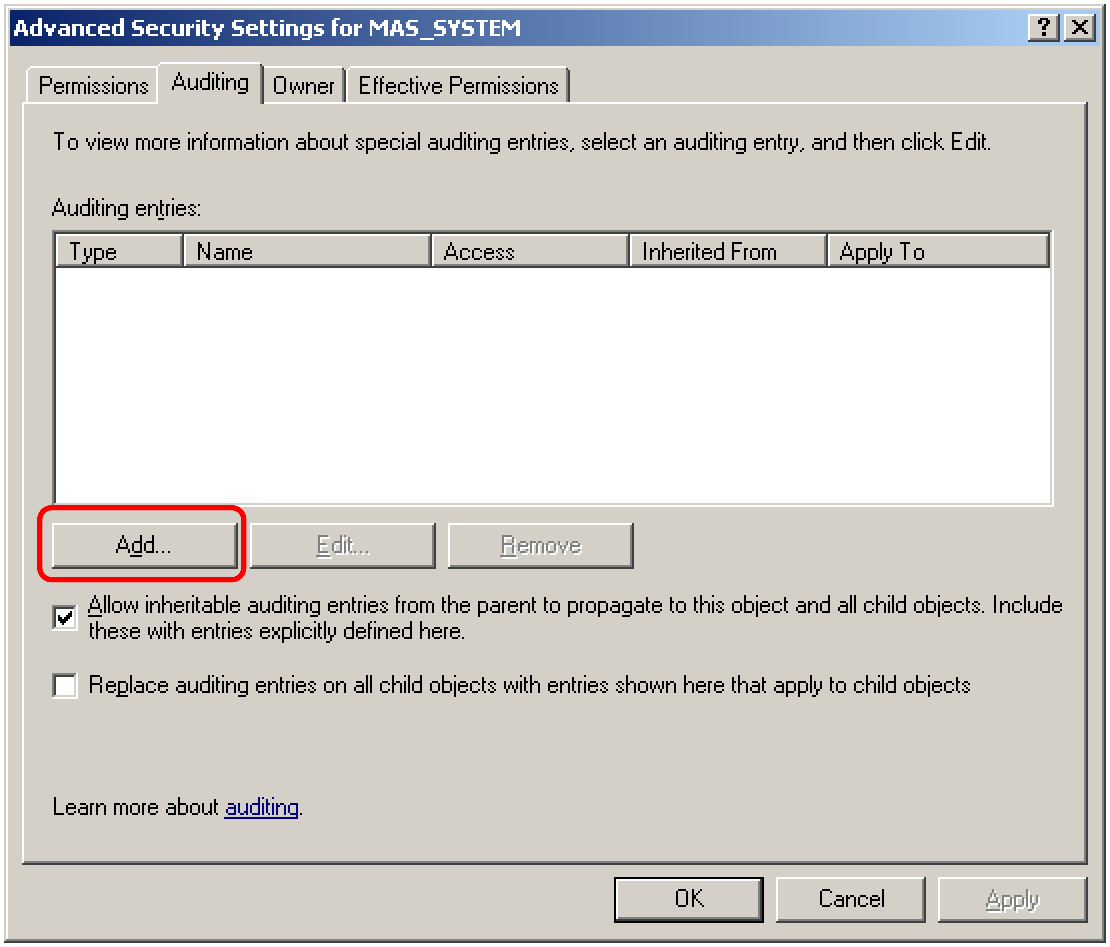
- Administrators (M9PW2K3ENT\Administrators)
- CREATOR OWNER
- Power Users (M9PW2K3ENT\Power Users)
- SYSTEM
- TERMINAL SERVER USER

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

©2010 Sage, Inc. All rights reserved.

5. In the Advanced Security Settings for MAS_SYSTEM window, click the Auditing tab, and then click Add.



Advanced Security Settings for MAS_SYSTEM

To view more information about special auditing entries, select an auditing entry, and then click Edit.

Auditing entries:

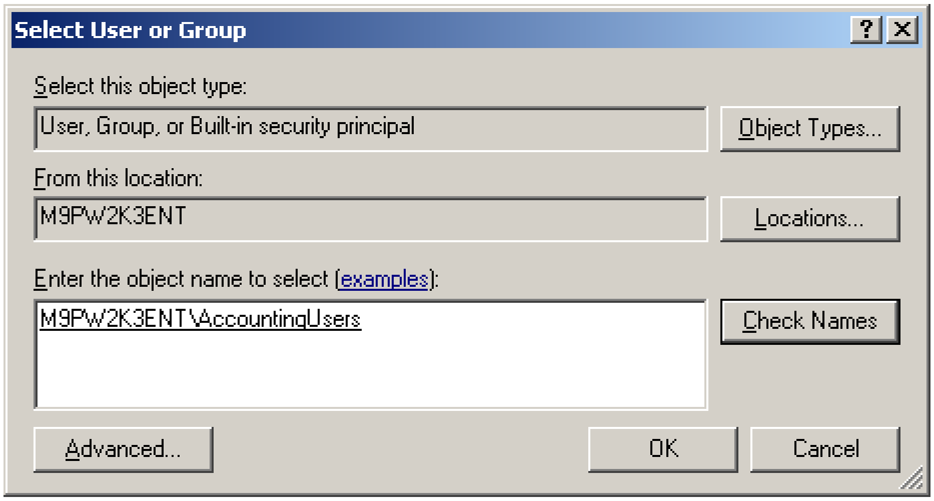
Type	Name	Access	Inherited From	Apply To

☑ Allow inheritable auditing entries from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.

□ Replace auditing entries on all child objects with entries shown here that apply to child objects

Learn more about auditing.

6. In the Select Users and Groups window, enter the User or Group (object name) to select for auditing.



Select User or Group

Select this object type: User, Group, or Built-in security principal

From this location: M9PW2K3ENT

Enter the object name to select (examples): M9PW2K3ENT\AccountingUsers

7. Click OK.

©2010 Sage, Inc. All rights reserved.

8. In the Auditing Entry for MAS_SYSTEM window, select the Successful/Failed check box for the actions to be audited. Check with your system administrator to determine which actions to select.
9. Select the Apply these auditing entries to objects and/or containers within this container only check box.
10. Click OK to close the Auditing Entry for MAS_SYSTEM window.
11. In the Advanced Security Settings for MAS_SYSTEM window, click Apply, and then click OK.
12. In the MAS_SYSTEM Properties window, click OK.

Auditing will be recorded in the Event Viewer’s Security log.

©2010 Sage, Inc. All rights reserved.

5 WIRELESS NETWORKS

5.1 Merchant Applicability

If wireless is used or implemented in the payment environment or application, the wireless environment must be configured per PCI DSS version 1.2 requirements 1.2.3, 2.1.1, and 4.1.1. Wireless technology must be securely implemented and transmissions of cardholder data over wireless networks must be secure.

5.2 PCI Requirements

Install and configure perimeter firewalls between wireless networks and systems that store credit card data, per PCI DSS version 1.2 and 1.2.3.

Modify default wireless settings, as follows, per PCI DSS 2.1.1:

- Change wireless equivalent privacy (WEP) keys
- Change default service set identifier (SSID)
- Disable SSID broadcasts
- Change default passwords
- Change SNMP community strings
- Enable Wi-Fi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable

For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. (PA-DSS 6.2 and PCI DSS 4.1.1)

If WEP is used, do the following, per PCI DSS 4.1.1:

- Use with a minimum 104-bit encryption key and 24 bit-initialization value
- Use ONLY in conjunction with Wi-Fi protected access (WPA or WPA2) technology, VPN, or SSL/TLS
- Rotate shared WEP keys quarterly (or automatically if the technology permits)
- Rotate shared WEP keys whenever there are changes in personnel with access to keys
- Restrict access based on media access code (MAC) address

Handheld devices that communicate wirelessly with the software, such as the Intermec 730 handset from ScanCo, must use strong encryption algorithms such as WPA to secure wireless communications.

©2010 Sage, Inc. All rights reserved.

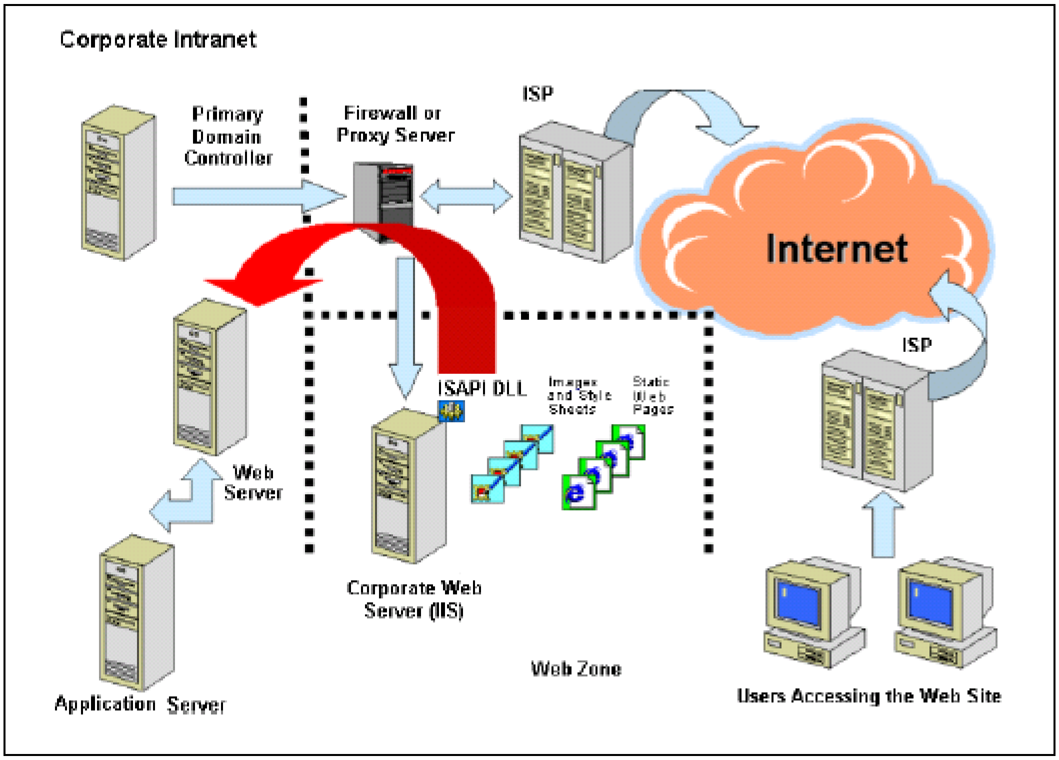
6 NETWORK SEGMENTATION

6.1 Merchant Applicability

Credit card data cannot be stored on systems directly connected to the Internet. For example, web servers and database servers should not be installed on the same server. A network DMZ (Demilitarized Zone, also known as Demarcation Zone) must be set up to segment the network so that only machines on the DMZ are Internet accessible.

e-Business Manager must be configured to submit .order and .store shopping card pages using SSL encryption. Disabling the use of SSL protocol will adversely affect PCI DSS compliance. The web engine should be installed on a separate server than the application server. This will ensure that the credit card initially submitted by the customer is encrypted when it is sent to the application server. After it is received by the application server, e-Business Manager always communicates using the encrypted credit card number plus the last four unencrypted credit card numbers.

Having the web engine on a separate server ensures that should the network become compromised, the application server would not be directly exposed.



In the WebServer Details Configuration, the Port Style Directory Browsing check box defaults to off and should not be turned on to avoid network exposure should the web engine be exposed. Additionally, the user logon that is connecting to the sharepoint should have restricted access to the rest of the system that the software is installed on. Create a new user logon for the Web Server that only has access to the software data.

For information on eBusiness Web Services, refer to the *eBusiness Web Services Installation and Reference Guide*. Use and deployment of applications using eBusiness Web Services requires independent PA-DSS certification and is not covered by this guide.

©2010 Sage, Inc. All rights reserved.

7 SECURE REMOTE SOFTWARE UPDATES

7.1 Merchant Applicability

The software securely delivers remote payment applications by high-speed connections. Merchants should develop an acceptable use policy for critical employee-facing technologies, per the guidelines below.

For VPN, or other high-speed connections, updates are received through a firewall or personal firewall, per PCI DSS 1 and 1.3.9.

7.2 Acceptable Use Policy

The merchant should develop usage policies for critical employee-facing technologies, like modems and wireless devices, as per PCI DSS requirement 12.3. These usage policies should include:

- Explicit management approval for use
- Authentication for use
- A list of all devices and personnel with access
- Labeling the devices with owner
- Contact information and purpose
- Acceptable uses of the technology
- Acceptable network locations for the technologies
- A list of company approved products
- Allowing use of modems for vendors only when needed and deactivation after use
- Prohibition of storage of cardholder data onto local media when remotely connected

7.3 Personal Firewall

Any "always-on" connections from a computer to a VPN or other high-speed connection should be secured by using a personal firewall product, per PCI DSS 1.3.9. The firewall is configured by the organization to meet specific standards and not alterable by the employee.

7.4 Remote Update Procedures

The software does not provide for the remote update of the application.

©2010 Sage, Inc. All rights reserved.

8 REMOTE ACCESS

8.1 Merchant Applicability

If the software can be accessed remotely, all network connectivity should be performed using two-factor authentication per PCI DSS requirement 8.3. Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates. For example, you can use GoToAssist™ or similar compliant technologies.

8.2 Remote Access Software Security Configuration

Implement the following applicable security features for all remote access software used by the merchant, reseller, or integrator.

- Change default settings in the remote access software (for example, change default Passwords and use unique Passwords for each customer)
- Allow connections only from specific (known) IP/MAC addresses
- Use strong authentication or complex passwords for logins
- Enable encrypted data transmission
- Enable account lockout after a certain number of failed login attempts
- Configure the system so a remote user must establish a Virtual Private Network (VPN) connection using a firewall before access is allowed
- Enable the logging function
- Restrict access to customer Passwords to authorized reseller/integrator personnel
- Establish customer Passwords according to PCI DSS requirements 8.1, 8.2, 8.4, and 8.5

©2010 Sage, Inc. All rights reserved.

9 ENCRYPTING NETWORK TRAFFIC

9.1 Transmission of Cardholder Data

The software uses encryption, such as SSL/TLS or IPSEC, for transmission of cardholder data over public networks, per PCI DSS 4.1.

9.2 E-mail and Cardholder Data

The software does natively support the sending of e-mail. As per PCI DSS requirement 4.2, cardholder data should never be sent unencrypted by e-mail. To meet this requirement, the e-mail must be sent with the Use 128-bit Encryption for Password Protection Documents check box selected in Company Maintenance and with a password.

©2010 Sage, Inc. All rights reserved.