PA DSS Implementation Guide

Megan De Freitas - 2025-06-12 - Miscellaneous

Important Notice

After October 29, 2019, SalesPad will no longer be supporting CardControl. Additionally, the application will cease to be a PA-DSS validated solution as of this date, and therefore CardControl customers would no longer be PCI compliant.

Instead, SalesPad Desktop now offers built-in credit card processing via Nodus PayFabric. If you have questions or want more information on our credit card processing services, please contact your sales rep.

About this Document

This document describes the steps that must be followed in order for your CardControl installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application Data Security Standards program (version 3.0 dated November, 2013).

Sales Pad, LLC instructs and advises its customers to deploy SalesPad Solutions applications in a manner that adheres to the PCI Data Security Standard (v3.0). Subsequent to this, best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various “Benchmarks,” should be followed in order to enhance system logging, reduce the chance of intrusion and increase the ability to detect intrusion, as well as other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, the disabling of infrequently-used or frequently vulnerable networking protocols and the implementation of certificate-based protocols for access to servers by users and vendors.

You must follow the steps outlined in this *Implementation Guide* in order for your CardControl installation to support your PCI DSS compliance efforts.

Revision Information

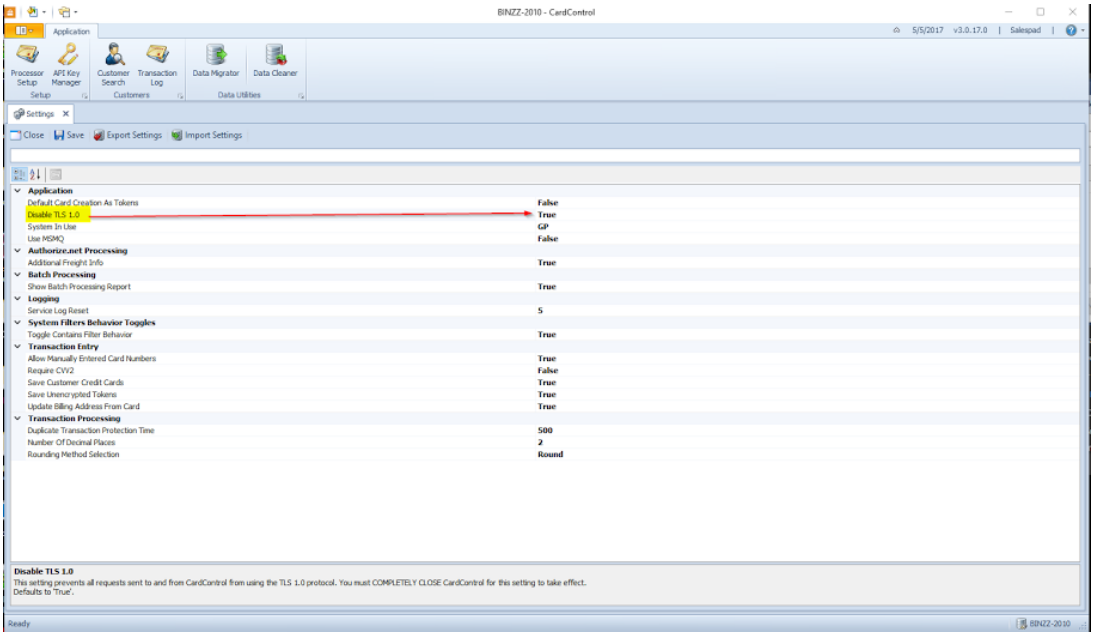
Name	Title	Date of Update	Summary of Changes
Blake Meinke	Developer	2/26/12	Document Creation

Dustin Chilson	Developer	10/19/13	2.0 Updates
Brock Flewelling & Donovan Moore	Developer	4/7/15	3.0 Updates
Avery Martin	Developer	9/1/15	3.0 Revisions
Jarrett Weber	Technical Writer	10/12/15	Format Update
Sarah Schaefer	Technical Writer	10/12/15	Minor edit
Christian Hartford	Technical Writer	5/8/20	Updated PCI/PA DSS links

Note: This PA-DSS Implementation Guide (IG) must be reviewed on a yearly basis, whenever the underlying application changes or whenever the PA-DSS requirements change. Updates should be tracked and reasonable accommodations should be made to distribute or make the updated guide available to users. Sales Pad, LLC will distribute the IG to new customers via URL links distributed to the end-user at the time of purchase and upon request.

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document then provides specific installation, configuration, and ongoing management best practices for using CardControl as a PA-DSS validated Application operating in a PCI Compliant environment.

Note: As of version 3.0.12.0, the 'Disable TLS 1.0' setting must be set to True in order to fulfill PCI requirements. Earlier versions will need to upgrade in order to remain compliant.



PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related

security programs (PA-DSS, PCI DSS, etc):

- PCI Security Standards Council Document Library (PA DSS)
- PCI Security Standards Council Document Library (PCI DSS)
- Open Web Application Security Project (OWASP) http://www.owasp.org

Application Summary

Payment Application Name:	CardControl
Payment Application Version:	3.0.x.x
Application Description:	CardControl allows users to securely process credit card payments through multiple transactional gateways. CardControl can be out-of-the-box integrated an ERP system such as Microsoft Dynamics GP with/without SalesPad GP or QuickBooks with/without SalesPad ERP.
Application Target Clientele:	Users of Microsoft Dynamics GP 2010, Microsoft Dynamics GP 2013, and users of SalesPad GP. Users of QuickBooks and SalesPad ERP.
Clientele Description:	CardControl is designed to be used by small to large merchants, ranging from local, national, or global. CardControl contains multi-language support for multi-regional usage. CardControl supports out-of-the-box integration with multiple ERP systems, including, but not limited to, Dynamics GP and SalesPad ERP. Therefore, CardControl is designed industry unspecific and can be applied in any type of customer channel (E-commerce, brick-and-mortar, etc). Merchants using CardControl typically operate on a mixed-usage basis, that is, a combination of mail order, telephone order, and web orders. CardControl supports both card-present and card-not-present transactions.
Components of Application Suite (i.e. POS, Back Office, etc.)	**End User Computer Deployed Applications** **CardControl.exe**: Credit card processing application, with a windows Graphical User Interface (GUI). **Additions.exe**: Plugin applications that give users the ability to launch the primary CardControl application from within Dynamics GP/QuickBooks and SalesPad GP/ERP. Handles no sensitive data. **Server Deployed Applications** **CardControlWebRest**: Rest interface to the CardControl Application Programming Interface (API) hosted within Microsoft Internet Information Services (IIS). Communicates with the CardControlWebSoap application. **CardControlWebSoap**: Soap interface using Microsoft Windows Communication Foundation (WCF) hosted in IIS. Contains all processing utilities of the CardControl.exe application without the GUI.

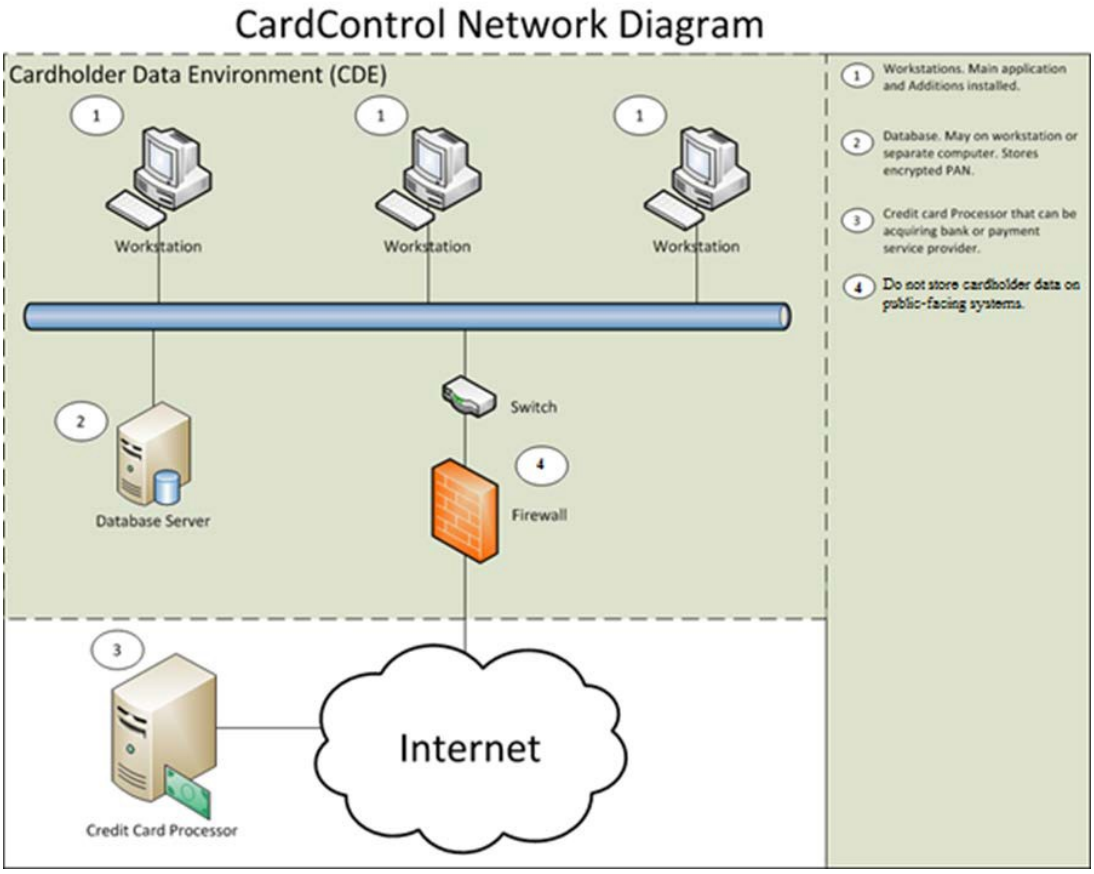
Required Third-Party Payment Application Software:	Authorize.NET Payment Gateway (version 3.1) - https://www.authorize.net AssureBuy Payment Gateway (version 4.6) - http://www.bluepay.com EBizCharge Payment Gateway (version 2) - http://ebizcharge.com PayFlowPro Payment Gateway (version 4.3.1.0) - https://www.paypal.com LitleOnline Payment Gateway (version 8.14) - http://www.litle.com FirstData E4 Payment Gateway (version 11) - https://www.firstdata.com 3Delta Payment Gateway (version 1) - http://www.3dsi.com Moneris Payment Gateway (version 2.5) - https://www.moneris.com

POS Suite	**POS Admin**	**Shopping Cart & Store Front**
POS Face-To-Face	**Payment Middleware**	**Others (Please Specify):**
POS Kiosk	**Payment Back Office**	
POS Specialized	**Payment Gateway/Switch**	

Database Software Supported:	Microsoft SQL Server 2012
Other Required Third Party Software:	Microsoft Dynamics GP 2010 or Microsoft Dynamics GP 2013 or QuickBooks Microsoft .Net Framework version 4.5.
Operating System(s) Supported:	The latest supported versions of: Windows 8
Application Functionality Supported	Select one or more from the following list: ☒ ☒ ☒ ☒
Payment Processing Connections:	CardControl, utilizing a payment processor gateway account setup by the user, transmits credit card transaction data using a secure connection to the payment processing gateway. Any response from the payment processor is then presented to the user.

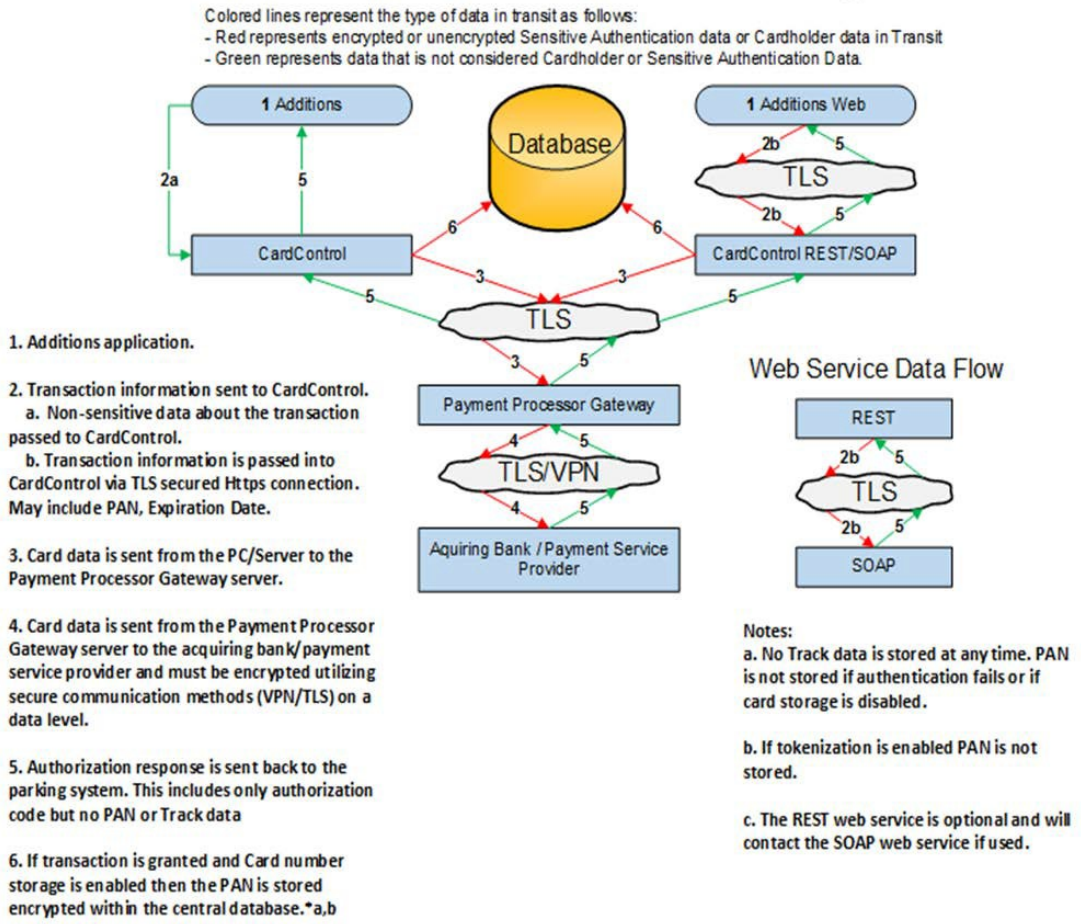
Application Authentication	CardControl user names and passwords are stored in a Microsoft SQL Server 2012 database. Access to the SQL Server database should be secured with industry best practices. Passwords are one-way hashed using industry standard 256 bit SHA2 hashes; a unique input variable is concatenated with each password before the cryptographic algorithm is applied and passwords are unreadable at all times during transmission. CardControlWeb uses unique API Keys generated with information related to the application environment for authentication. Theses keys can be disabled by CardControl administrators or via Application updates. API Keys are two-way hashed using industry standard 256 bit SHA2 hashes.
Description of Versioning Methodology:	CardControl versioning has four levels, Major PA-DSS version, Major, Minor, and Wildcard: X.X.X.X. 'X' is a numeric value only. Major PA-DSS Version: Indicates the major version of PA-DSS the application is validated for. Major: Changes including significant changes to the application and would have an impact on PA-DSS requirements. Minor: Changes including small changes such as minor enhancements and may or may not have an impact on PA-DSS requirements. Wildcard: Build changes including bug fixes and would have no negative impact on PA-DSS requirements.
List of Resellers/Integrators (If Applicable):	CardControl requires that SalesPad staff install and configure every installation.

Typical Network Implementation



Data Flow Diagram

CardControl Data Flow Diagram



Difference between PCI Compliance and PA-DSS Validation

As a software vendor, our responsibility is to be “PA-DSS Validated.”

We have performed an assessment and certification compliance review with our independent assessment firm to ensure that our platform does conform to industry best practices when handling, managing, and storing payment related information.

PA-DSS is the standard against which CardControl has been tested, assessed, and validated.

PCI Compliance is then later obtained by the merchant, and is an assessment of your actual server (or hosting) environment.

Obtaining “PCI Compliance” is the responsibility of the merchant and your hosting provider, working together, using PCI compliant server architecture with proper hardware & software configurations and access control procedures.

The PA-DSS Validation is intended to ensure that CardControl will help you achieve and maintain PCI Compliance with respect to how CardControl handles user accounts, passwords, encryption, and other payment data related information.

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The

security requirements defined in the DSS apply to all members, merchants, and service providers that store, process, or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment, which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed, or transmitted.

THE 12 REQUIREMENTS OF THE PCI DSS:

Build and Maintain a Secure Network and Systems

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

1. Protect stored cardholder data.
2. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

1. Protect all systems against malware and regularly update anti-virus software
2. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

1. Restrict access to data by business need-to-know
2. Identify and authenticate access to system components
3. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

1. Track and monitor all access to network resources and cardholder data
2. Regularly test security systems and processes

Maintain an Information Security Policy

1. Maintain a policy that addresses information security

Considerations for the Implementation of CardControl in a PCI-Compliant Environment

The following areas must be considered for proper implementation in a PCI-Compliant environment.

- Sensitive Authentication Data requires special handling.
- Remove Historical Cardholder Data.
- Set up Good Access Controls.
- Properly Train and Monitor Admin Personnel.
- Key Management Roles & Responsibilities.

- PCI-Compliant Remote Access.
- Use SSH, VPN, or TLS for encryption of administrative access.
- Log settings must be compliant.
- PCI-Compliant Wireless settings.
- Data Transport Encryption.
- PCI-Compliant Use of Email.
- Network Segmentation.
- Never store cardholder data on public facing or internet-accessible systems.
- Configure the application to use a DMZ to separate the internet from systems storing cardholder data.
- Use TLS for Secure Data Transmission.
- Delivery of Updates in a PCI Compliant Fashion.

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4)

No previous versions of CardControl stored sensitive authentication data. Therefore, there is no need for secure removal of this historical data by the application as required by PA-DSS v3.0.

Sensitive Authentication Data Requires Special Handling (PA-DSS 1.1.5)

Sales Pad, LLC does not store Sensitive Authentication Data for any reason, and we strongly recommend that you do not do this either. However, if for any reason you should do so, the following guidelines must be followed when dealing with sensitive authentication data (swipe data, validation values or codes, PIN or PIN block data):

- Collect sensitive authentication data only when needed to solve a specific problem
- Store such data only in specific, known locations with limited access
- Collect only the limited amount of data needed to solve a specific problem
- Encrypt sensitive authentication data while stored
- Securely delete such data immediately after use - If you do not currently have or use a secure delete tool, you can use one of the following for the Windows operating system:
    - Heidi Eraser can be obtained from http://www.heidi.ie/eraser/
    - Microsoft SDelete can be obtained from https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete

Securely Deleting Cardholder Data (PA-DSS 2.1)

The following guidelines must be followed when dealing with cardholder data (PAN alone or with any of the following: expiration date, cardholder name, or service code):

- A customer defined retention period must be defined with a business justification
- Cardholder data exceeding the customer-defined retention period must be securely deleted.
- Any cardholder data that is no longer required for legal, regulatory, or business purposes must be securely deleted.

- The locations of the cardholder data that must be securely deleted are as follows:
    - Credit Card Data – Located in the CustomerCreditCard table under the ‘spcc’ schema in the database
    - Credit Card Processor Log – Located in the CreditCardProcessorLog table under the ‘spcc’ schema in the database
    - Transaction History – Located in the CreditCardTransaction table under the ‘spcc’ schema in the database

To securely delete the cardholder data, you must do the following:

1. In the application, you must use the Data Cleaner utility to securely delete historical data. The Data Cleaner utility contains the functionality to securely delete Credit Card Data, Credit Card Logs, and Transaction History. To delete, a user with permission to use the Data Cleaner must navigate to the Data Cleaner form, specify the parameters regarding the information to be deleted, and click the **Clear Data** button. Example:

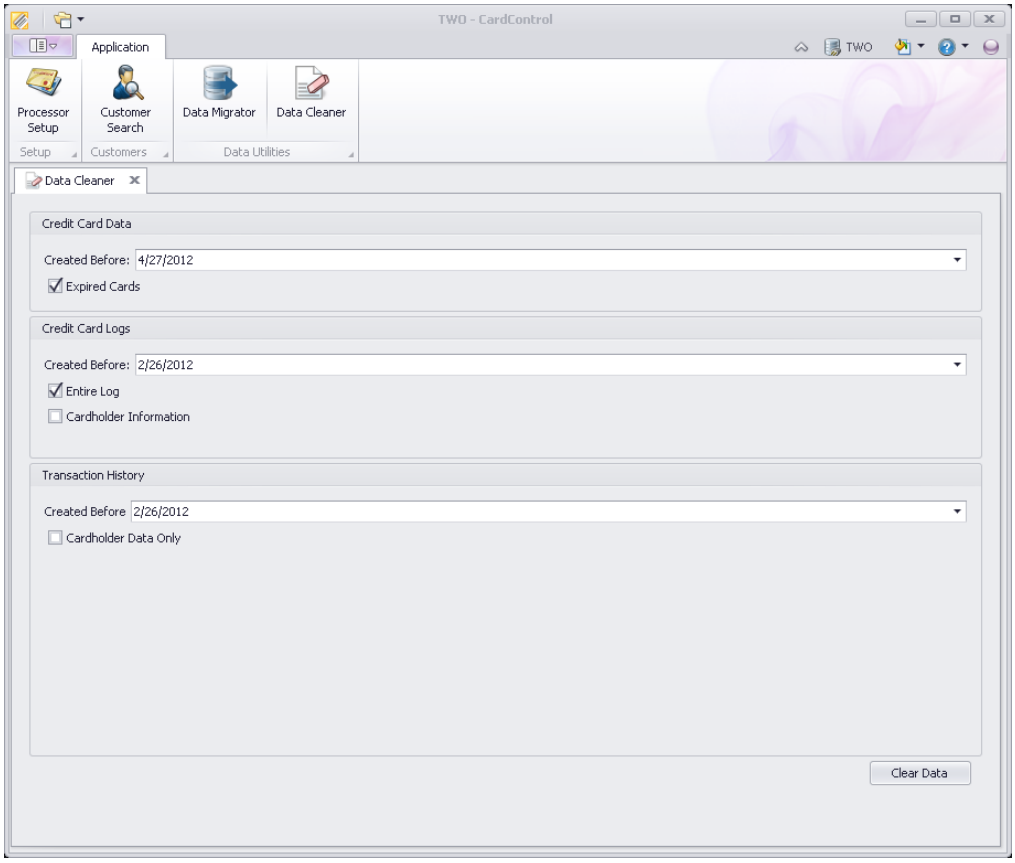


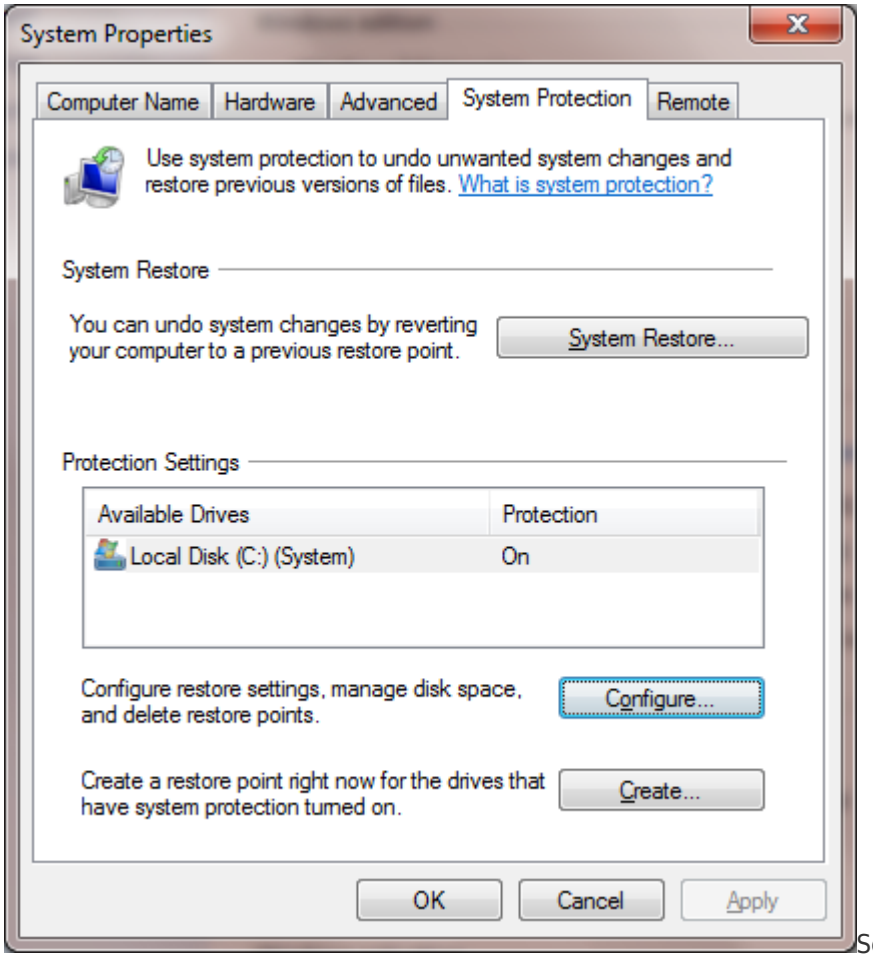
Figure 1. Data Cleaning Example 1

2. Use the following section of instructions, titled Addressing Inadvertent Capture of PAN, to configure your Windows 8 operating system to prevent inadvertent retention of cardholder data.

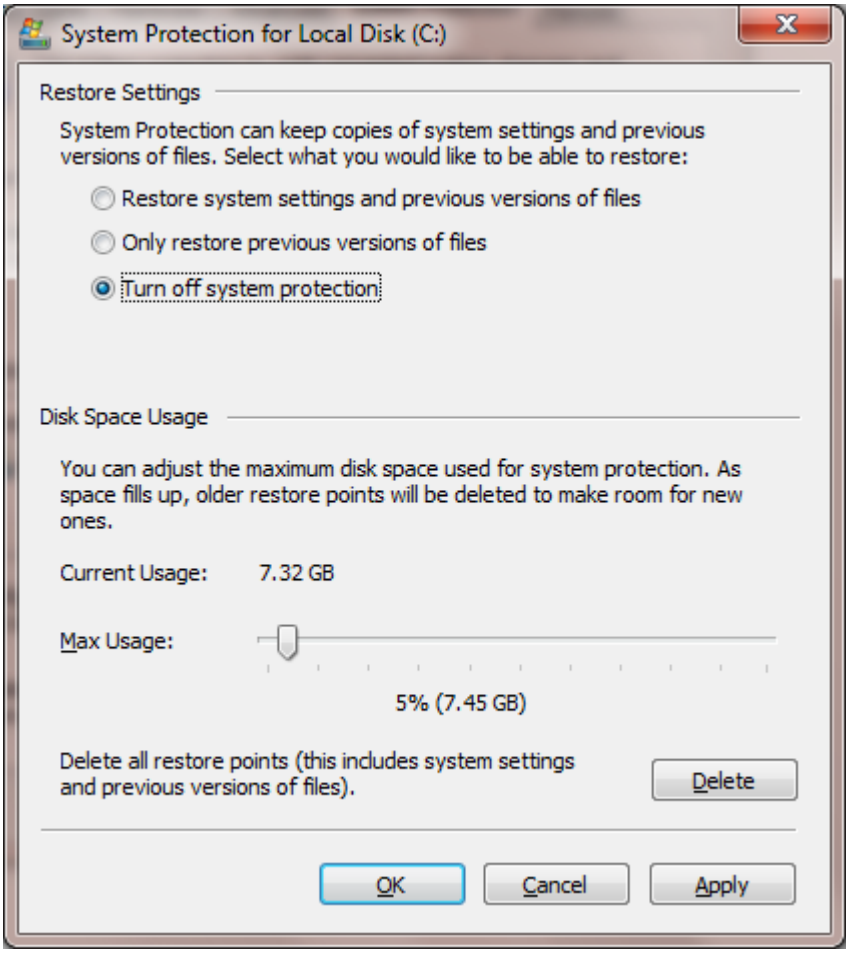
Addressing Inadvertent Capture of PAN

DISABLE SYSTEM RESTORE SETTINGS

Disable System Restore

1. Right-click on Computer and select Properties (In Windows 8, this can be done through the start menu and right clicking ‘This PC’)
2. 

Select System Protection from the top left list. The following screen will appear:
3. Select **Configure**. The following screen will appear:

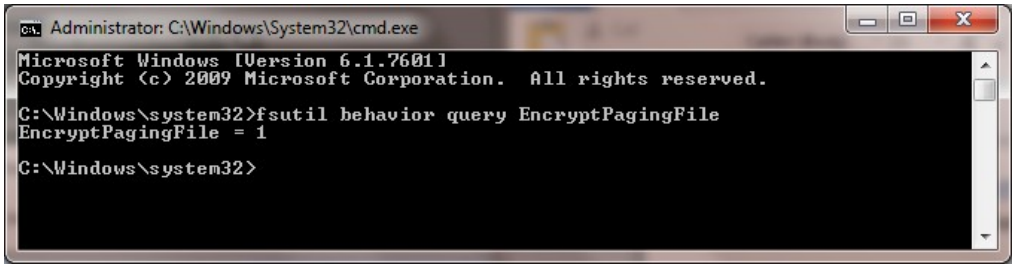


1. Select **Turn off system protection** (In Windows 8, this says 'Disable system protection')
2. Click **Apply**, and click **OK** to close the System Protection window
3. Click **OK** again to close the System Properties window
4. Reboot the computer

Encrypt the System PageFile.sys

Encrypting PageFile.sys

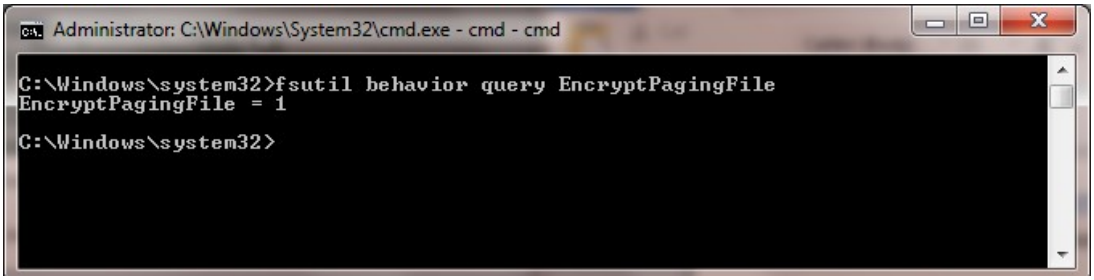
In order to perform this operation, the hard disk must be formatted using NTFS.

1. Open Command Prompt - On the Windows task bar, click on the Windows "Orb" and in the search box type in "**cmd**" – for Windows 8, this can be done through the start menu.
2. Right-click on **cmd.exe** and select **Run as Administrator**
3. 

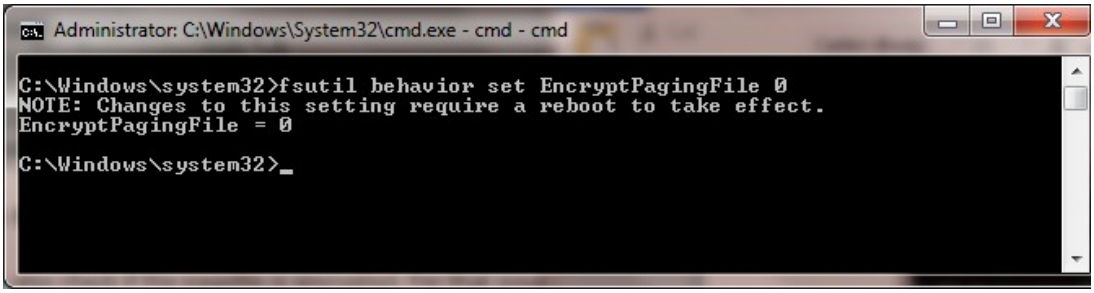
   To Encrypt the PageFile, type the following command: "**fsutil behavior set**

EncryptPagingFile 1”

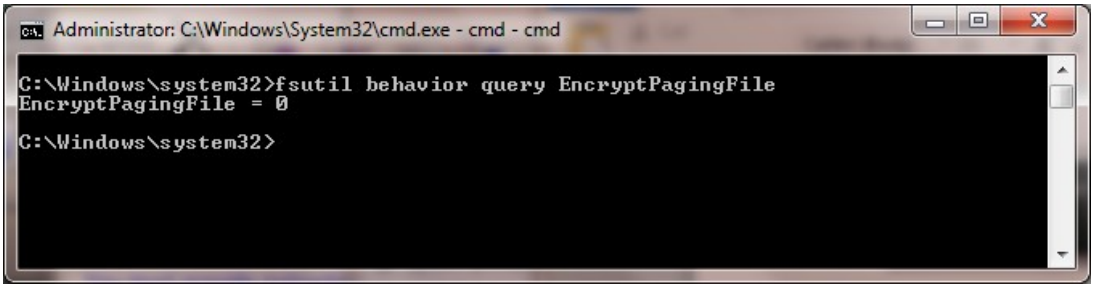
4. To verify configuration, type the following command: “**fsutil behavior query EncryptPagingFile**”



1. If encryption is enabled, **EncryptPagingFile = 1** should appear
2. In the event you need to disable PageFile encryption, type the following command: “**fsutil behavior set EncryptPagingFile 0**”



1. To verify configuration, type the following command: “**fsutil behavior query EncryptPagingFile**”



1. If encryption is disabled, **EncryptPagingFile = 0** should appear

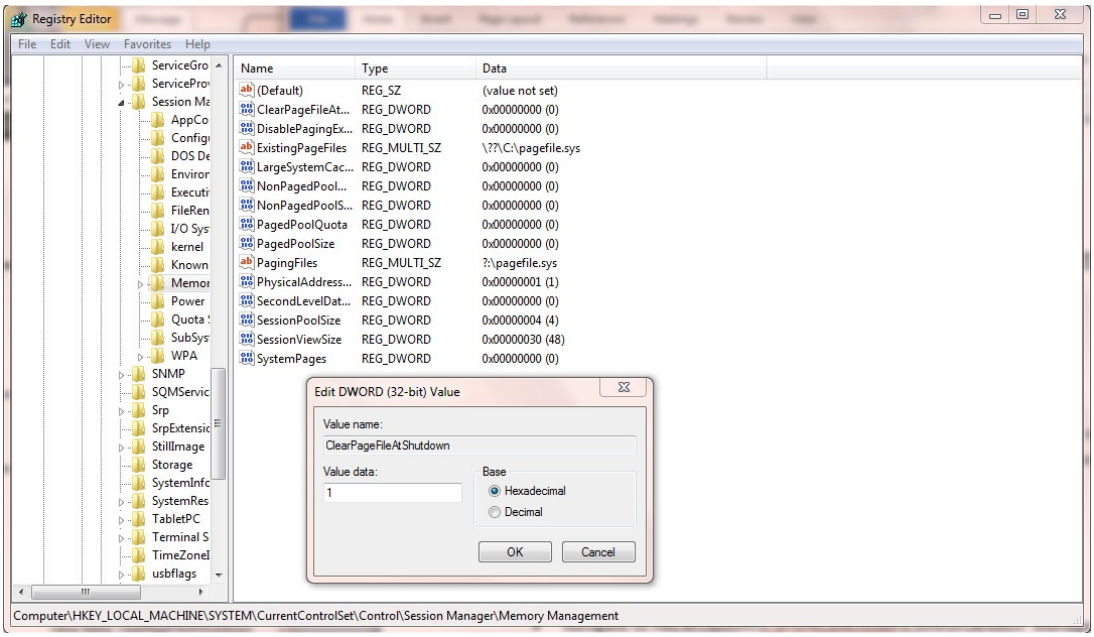
Clear the System PageFile.sys upon Shutdown

Windows has the ability to clear the PageFile.sys upon system shutdown. This will delete all temporary data from the PageFile.sys (temporary data may include system and application passwords, cardholder data (PAN/Track), etc.).

Note: Enabling this feature may increase windows shutdown time.

1. Click on the Windows “Orb” and in the search box type in “**regedit**”
2. Right-click on **regedit.exe** and select **Run as Administrator**
3. Navigate to HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
4. Change the value from **0 to 1**

5. Click **OK** and close Regedit



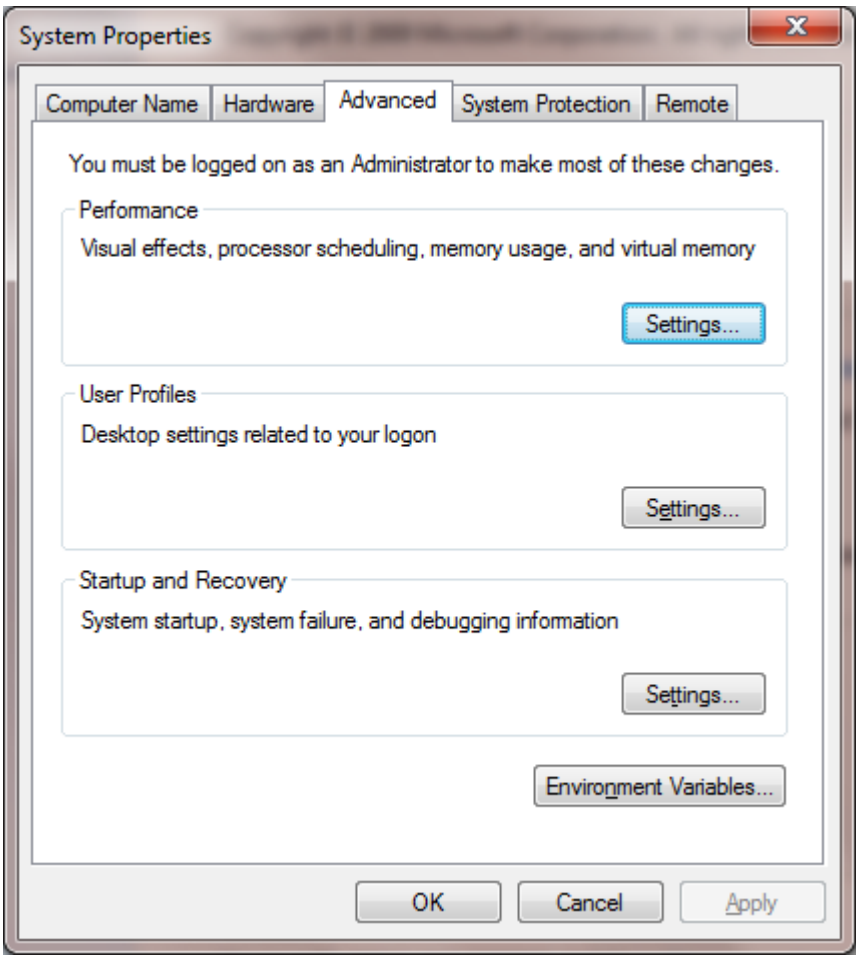
1. If the value does not exist, add the following:

- Value Name: ClearPageFileAtShutdown
- Value Type: REG_DWORD
- Value: 1

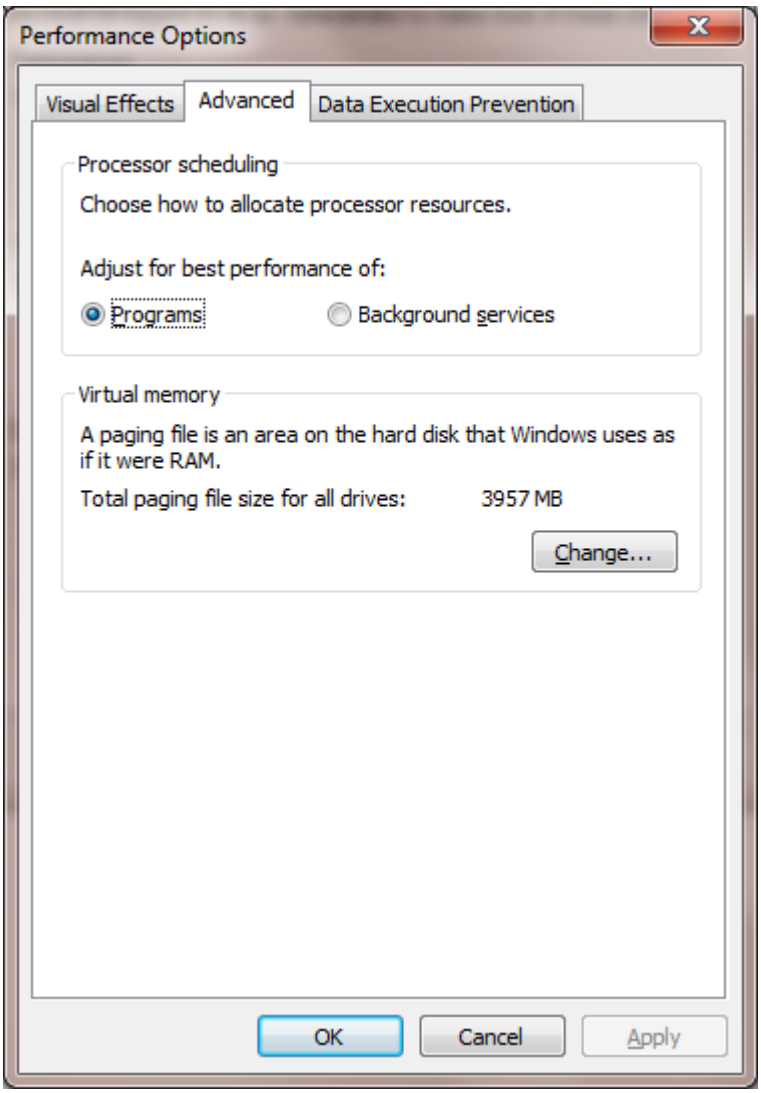
Disable System Management of PageFile.sys

Disabling System Management of PageFile.sys

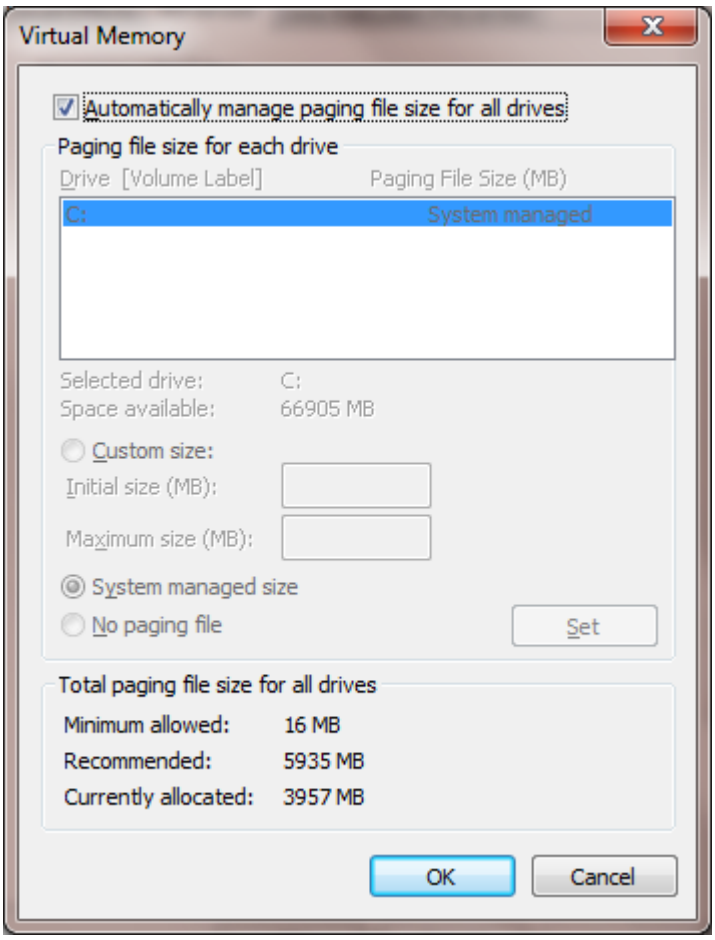
1. Right-click on **Computer** and select **Properties –** on Windows 8, this can be done through right clicking ‘This PC’ from the start menu.
2. Select **Advanced System Settings** from the top left list. The following screen will appear:



1. Under Performance, select **Settings** and click on the **Advanced** tab. The following screen will appear:



1. Select **Change** under Virtual Memory. The following screen will appear:

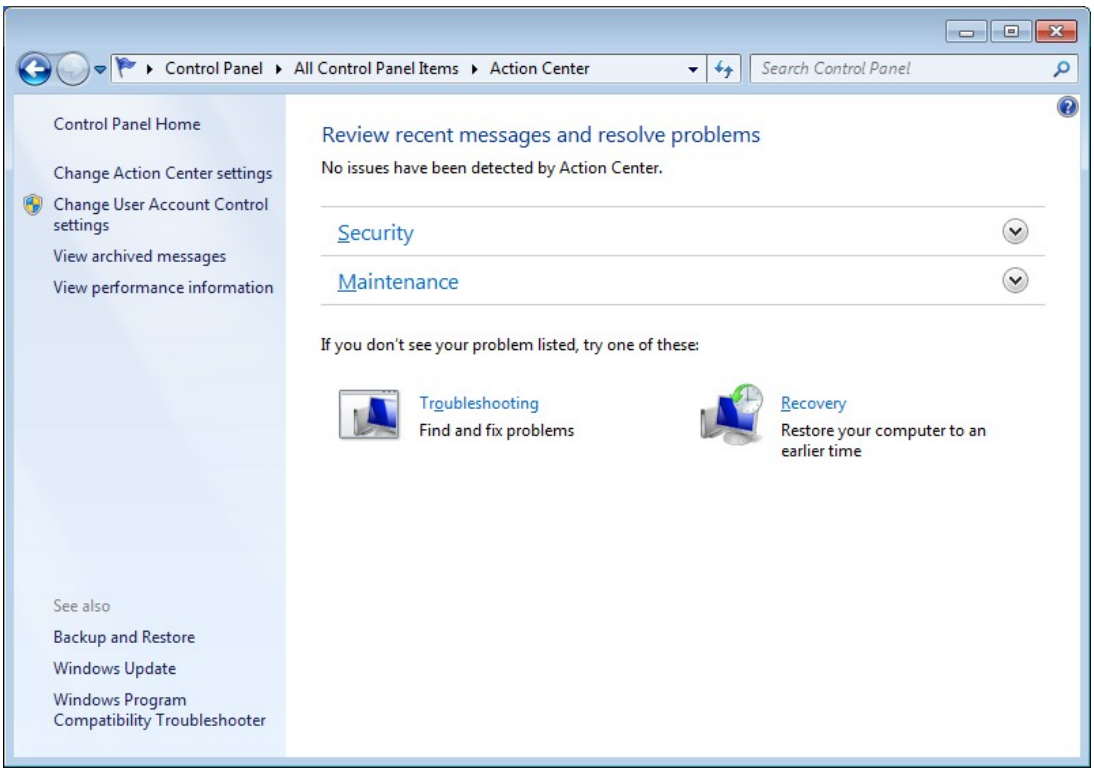


1. Uncheck **Automatically manage page file size for all drives**
2. Select **Custom Size**
3. Enter the following for the size selections:
    - Initial Size – as a good rule of thumb, the size should be equivalent to the amount of memory in the system.
    - Maximum Size – as a good rule of thumb, the size should be equivalent to 2x the amount of memory in the system.
4. Click **OK** three times. You will be prompted to reboot your computer

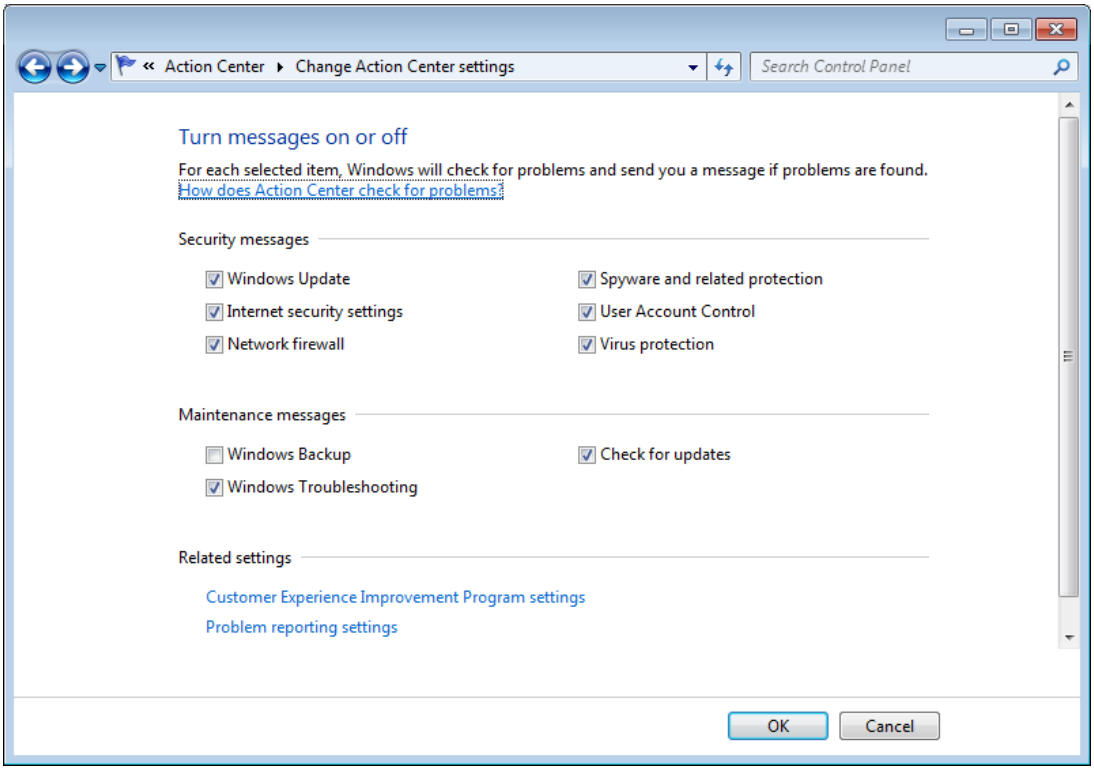
DISABLE WINDOWS ERROR REPORTING

Disabling Windows Error Reporting

1. Open the **Control Panel**
2. Open the **Action Center** (In windows 8, this can be selected from the start menu search)
3. Select **Change Action Center Settings**



1. Select **Problem Reporting Settings**



1. Select **Never Check for Solutions**

Mask PAN when displayed (PA-DSS 2.2)

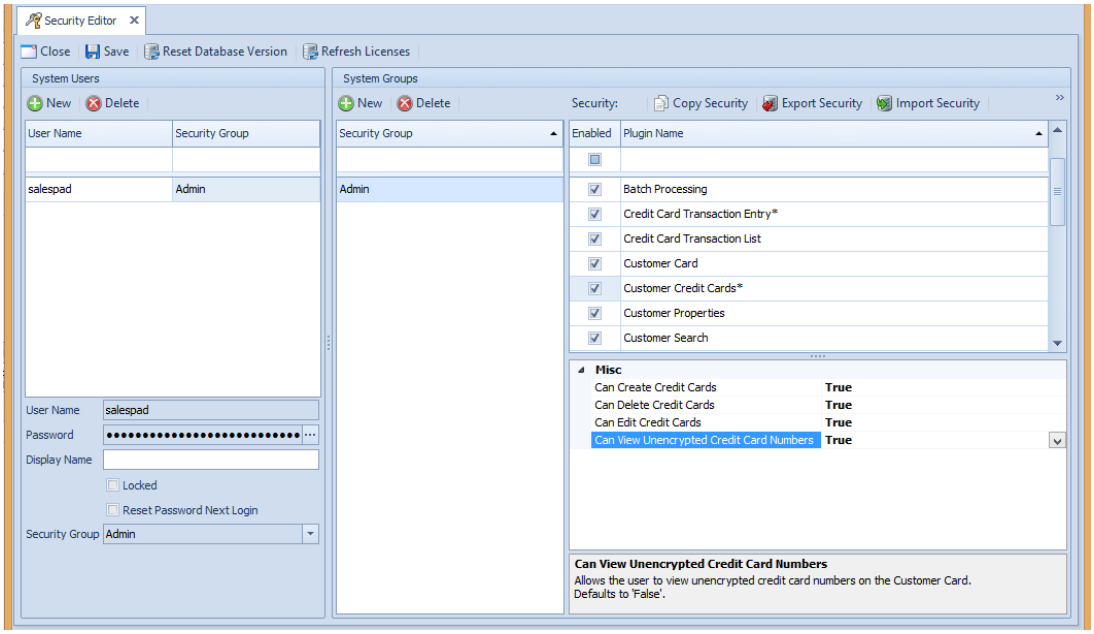
There are only three instances when a full PAN is displayed to the user:

- When a new credit card is created on the Customer Credit Card creation screen. The

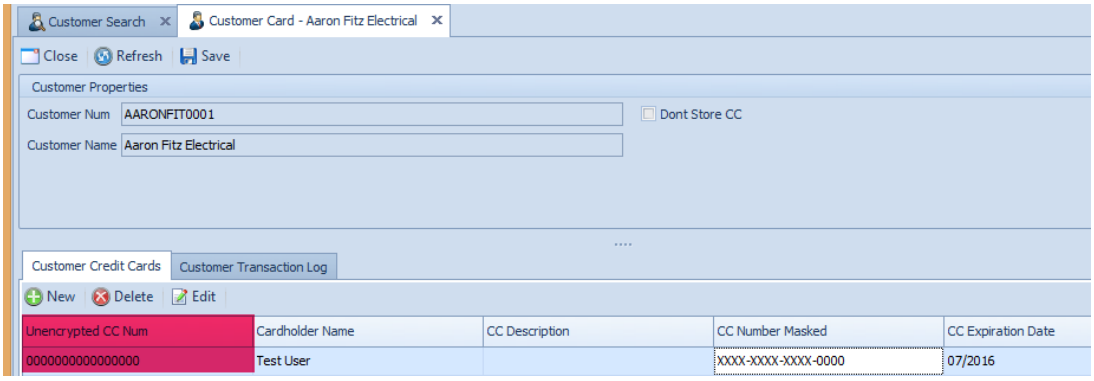
PAN is displayed to the user as it is entered. Once the card is saved, the PAN is masked.

- The POS screen, “CC Transaction Entry”, displays the PAN to the user as it is entered. Once the transaction is processed, the PAN is masked. Saved credit cards and tokens are always masked on this screen.
- The two previously mentioned situations are the only times when the PAN is viewable by the user by default. The following are instructions to configure CardControl in a way that allows personnel with a legitimate business need to see the full PAN.

1. A user with CardControl **Security** access must open the CardControl **Security** menu.
2. Select the authorized security group from the **System Groups**. Under the security setting **Customer Credit Cards**, you can enable the security setting **Can View Unencrypted Credit Card Numbers**. Only personnel with a legitimate business need to view the full PAN should be included in this security group. Whenever this security is enabled, it is logged in the **SystemLog** table - schema **spcc** - which user enabled the setting and for what group.



1. Once the security is enabled, the authorized users will need to log out of CardControl to apply the security setting.
2. Upon logging back in, the members of the authorized security group will be able to view full PANs of stored credit cards on the **Customer Card**. It is also logged in the **SystemLog** each time a user views a **Customer Card** to view a full PAN.



In addition to the above-mentioned locations where either a masked, truncated, or full PAN is displayed, there are the following locations where truncated PANs are visible:

- Within the Customer Card form, a “CC Number Masked” column displays the truncated PAN (only the last four digits are available).
- Within the Customer Transaction Log form, a “CC Number Masked” column displays the truncated PAN (only the last four digits are available).
- Within the Transaction Log form, a “CC Number Masked” column displays the truncated PAN (only the last four digits are available).

The above list contains every location where any form of PAN is visible within the application.

Render Stored PAN Unreadable (PA-DSS 2.3)

PAN information is always encrypted and masked before any storage occurs. CardControl truncates or masks all PANs before writing them to transaction history, processor logs, response messages, all screens, and all tables in the database. PAN information is always unreadable when stored unless authorized personnel are given explicit permission to view full PAN information as detailed above.

Protect Secure Data Keys (PA-DSS 2.4)

CardControl does not require storing keys used to secure cardholder data as they are dynamically created. Thus, users are not responsible to

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

Cardholder Data Encryption Key Management (PA-DSS 2.5)

The following key management functions must be performed per PCI DSS:

- Generation of strong cryptographic keys
- Secure cryptographic key distribution
- Secure cryptographic key storage