
PCI IMPLEMENTATION GUIDE
FOR EXTREMEPOS® PAYMENT

CONTENTS

Chapter 1: Introduction	4
1a: What is this guide for?.....	4
1b: What are PCI-DSS and PA-DSS?.....	4
1c: Updates to this guide.....	4
1d: Versions	4
Chapter 2: Deletion of Sensitive Data.....	5
2a: Data from previous versions of the software	5
2b: Purging Cardholder Data after Expiration.....	5
Chapter 3: User IDs and Passwords.....	6
3a: Where are usernames and passwords needed?	6
3b: Password usage guidelines:	6
3c: PCI requirements for strong passwords	6
3d: Using Windows Settings to meet password requirements.....	6
Chapter 4: Logging and Auditing	7
4a: Merchant Responsibility	7
4b: Viewing the Logs	8
4c: Logging within Windows.....	8
Chapter 5: Networking.....	9
5a: Merchant Responsibility	9
5b: Web Servers and the DMZ.....	9
5c: Required Wireless Settings	10
5d: Updates to ExtremePOS® Payment.....	10
Chapter 6: Remote Access.....	11
6a: ExtremePOS® Payment.....	11
6b: Remote Access from Vendors (Including Extreme POS)	11
Chapter 7: Encryption and Key Management	12
7a: Encryption.....	12
7b: Key Storage.....	12
7C: Changing Keys	12
Chapter 8: Handling Sensitive Authentication Data.....	13
8a: Within ExtremePOS Payment.....	13
8b: Outside of ExtremePOS Payment	13
Appendix A: Configuring Windows for PCI-DSS Compliance	14

A.1: Password policies	14
A.2: Account lockout policy	15
A.3: Windows logging	16
A.4 Windows restore points.....	17
A.5: Windows screensaver.....	17
Appendix B: Sample Key Custodian Form.....	19

CHAPTER 1: INTRODUCTION

1A: WHAT IS THIS GUIDE FOR?

This guide is intended to assist merchants and others in implementing ExtremePOS® Payment in a store in a PCI-DSS compliant manner. This is not intended to be a full installation or instruction manual, but rather a guide on configuring ExtremePOS® Payment in such a way as to ensure compliance with regards to the payment system for PCI-DSS and PA-DSS.

1B: WHAT ARE PCI-DSS AND PA-DSS?

PCI-DSS is the set of security standards that all merchants dealing with credit card transactions from the PCI member brands (Currently, Visa, Mastercard, American Express, and Discover) must meet. PA-DSS is a related set of requirements and practices regarding payment applications.

1C: UPDATES TO THIS GUIDE

This guide will be updated with future versions of the software, or as standards change. Updates to this guide may be found at the website <http://www.extremepos.com>.

1D: VERSIONS

This guide is written for PA-DSS version 1.2.1 (English) and PCI-DSS version 1.2.1 (English). These may currently be found at <http://www.pcisecuritystandards.org>.

CHAPTER 2: DELETION OF SENSITIVE DATA

2A: DATA FROM PREVIOUS VERSIONS OF THE SOFTWARE

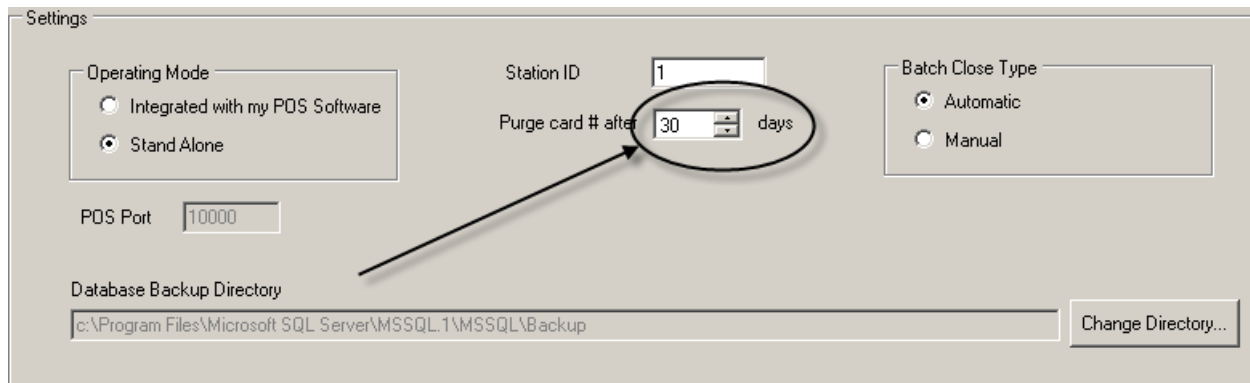
There is no data from previous versions of ExtremePOS® Payment, as it is a new application.

If you are using an integrated Point of Sale system with the payment module that had previous data, consult the guide for that software for removal of that data. That data's removal is absolutely required for PCI compliance.

2B: PURGING CARDHOLDER DATA AFTER EXPIRATION

The administrative user may set a number of days to retain PAN data in the settings screen. PAN, or Primary Account Number, data is the key to PCI-DSS. This data will automatically be purged after the set time has passed with no need for further action on the part of the merchant.

This setting should be set as low as possible for business purposes; the less data that is stored, the less is at risk in the event of a breach.



CHAPTER 3: USER IDS AND PASSWORDS

3A: WHERE ARE USERNAMES AND PASSWORDS NEEDED?

Merchants and resellers should set unique usernames and PCI-DSS compliant passwords for all computers, servers, databases, and networking support equipment supporting the payment application.

3B: PASSWORD USAGE GUIDELINES:

- Default usernames and passwords should NOT be used on any equipment or programs, including the payment application.
- Default accounts must be assigned secure credentials, and then either disabled or not used.
- Use strong passwords and security wherever possible
- Do not use the same username or password for multiple logins

3C: PCI REQUIREMENTS FOR STRONG PASSWORDS

The following, drawn from PCI-DSS 8.5.8 through 8.5.15, are the requirements for passwords:

- Do not use shared, group, or generic accounts and passwords
- Change passwords at least every 90 days
- Passwords must be at least seven characters
- Passwords must contain at least both letters and numbers
- Users must not reuse any of the last four passwords used
- Limit repeat attempts by locking the user out for at least half an hour after at most six incorrect attempts.
- If a terminal has been idle for more than fifteen minutes, require the user to reenter a password to re-enter the terminal

3D: USING WINDOWS SETTINGS TO MEET PASSWORD REQUIREMENTS

Many of the PCI requirements for passwords can be met through proper configuration of Windows; for details, consult Appendix A, "Proper Settings for PCI-DSS Compliant Windows."

CHAPTER 4: LOGGING AND AUDITING

4A: MERCHANT RESPONSIBILITY

Within ExtremePOS® Payment, the merchant will not need to configure logging. The settings are hard coded to be compliant with PCI DSS requirements 10.2.1-10.2.7 and 10.3.1-10.3.6. There is no way for the user to view full cardholder data within the system after transactions or storage of the number; if the KEK is loaded, however, the void functionality, tip functionality, and process manually for a specific customer with a stored card functionality will access the data. However, these do not display the information to the user aside from the last four digits of the card number.

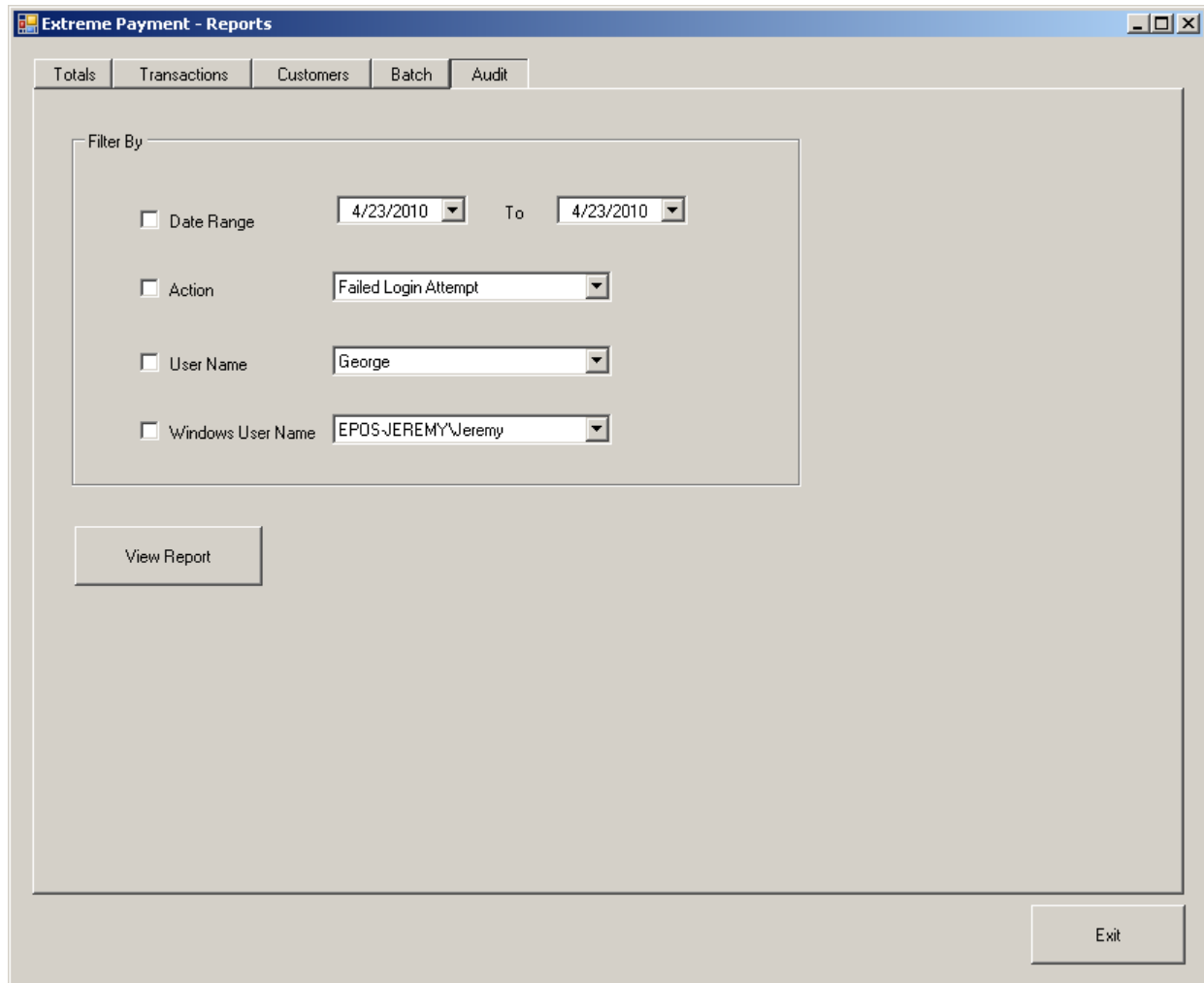
The following information is logged in the audit table about each event that is logged: The action (including the success or failure of it and the affected data), the date and time, the user name within Payment, the workstation the action was taken from, and the windows user name of the account making the action.

The following events cause log entries: Initializing the logs; administrative actions taken including changing settings, login changes, viewing audit logs, and creating new encryption keys; logins and failed logins; accessing of individual cardholder data (such as storing or deleting a card on file for a customer),

Logging cannot be disabled within ExtremePOS Payment.

4B: VIEWING THE LOGS

The audit logs may be viewed from within ExtremePOS® Payment by an administrative level user. This is found within the reports section of the program, under 'audit'.



The screenshot shows a window titled "Extreme Payment - Reports" with a menu bar containing "Totals", "Transactions", "Customers", "Batch", and "Audit". The "Audit" tab is selected. Below the menu bar is a "Filter By" section with four filter options, each with a checkbox and a dropdown menu:

- Date Range: 4/23/2010 To 4/23/2010
- Action: Failed Login Attempt
- User Name: George
- Windows User Name: EPOS-JEREMY\Jeremy

Below the filter section is a "View Report" button. In the bottom right corner of the window is an "Exit" button.

4C: LOGGING WITHIN WINDOWS

The merchant or reseller must make certain that logging within Windows is configured in a PCI-DSS compliant manner. Details on this may be found in Appendix A.

CHAPTER 5: NETWORKING

5A: MERCHANT RESPONSIBILITY

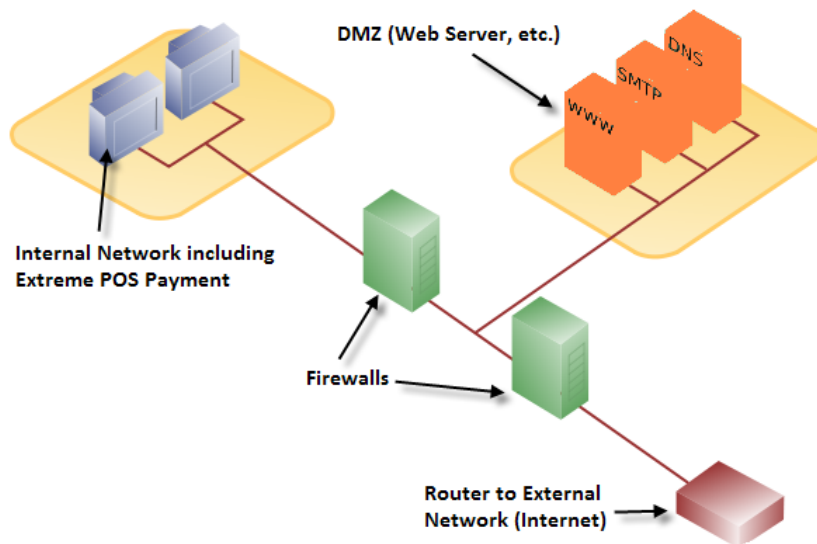
If wireless networking is used, the Merchant is responsible for ensuring that their configuration meets the requirements of PCI-DSS 2.1.1 and 4.1.1. **We strongly recommend that wireless networking not be used on the network ExtremePOS® Payment is used on.** If wireless is used, merchant is responsible for installing a firewall as per PCI-DSS requirement 1.3.8. If a wireless network is going to be connected to the payment processing network, then a firewall must be in place to control or deny all traffic between the networks. All firewall rules allowing traffic between the networks must be documented with business justification. Wireless access points must not use default SNMP community strings. Wireless keys must be changed from the defaults, and must be changed at any time than an employee who knows them leaves the company. Strong encryption such as WPA2 must be used, and if necessary firmware of the router must be updated to support it. Passwords and other security settings must also be changed from the default.

In the event that PAN information is sent over an open or wireless network, or via an end-user communication tool such as email or instant message, it **MUST** be encrypted. We recommend against ever using these tools for communicating card holder information, and no features of ExtremePOS® Payment inherently do so. ExtremePOS® Payment does not have an ecommerce or web server module, and at no time should cardholder information need to be communicated in this way.

All PAN data transmitted via network to the database server or to the payment processor is encrypted in accordance with PCI-DSS Requirement 4.1

5B: WEB SERVERS AND THE DMZ

ExtremePOS® Payment is designed to work on an internal network, and has no need to be in a DMZ for any component of it. Should there be a web server on the network, it must be in a DMZ as per PCI-DSS 1.3.4. If the merchant is keeping card holder data outside of the system, it also should not be kept on a system with incoming internet connectivity.



5C: REQUIRED WIRELESS SETTINGS

In the event that a wireless network is configured, PCI-DSS requires that modern, secure standards are used. WEP Encryption is no longer allowed for PCI Compliance, and a more modern alternative such as WPA should be used instead.

5D: UPDATES TO EXTREMEPOS® PAYMENT

Updates to ExtremePOS® Payment are downloaded and installed only by manually agreeing to them as an administrative user. In order to utilize this, the connection must be secured with a firewall. These updates will take the form of a complete new installation of the program, and will require an administrator both in windows and in ExtremePOS Payment to uninstall the old version and install the new one. You will be notified of the availability of any updates you are entitled to. Updates may also be shipped on disc via fedex or USPS for a shipping and handling fee.

However you choose to receive the setup, the files may be verified as being genuinely from Extreme Point of Sale, Inc via MD5 hash numbers that will be provided through the updates screen for each version. These may be checked using any tool that generates these; Microsoft offers a free command-line utility at <http://support.microsoft.com/kb/841290>. Additionally, the MD5 hash will be displayed after the file is downloaded, and users should compare it before installing.

CHAPTER 6: REMOTE ACCESS

6A: EXTREMEPOS® PAYMENT

There is no built in remote access for ExtremePOS® Payment. In the event that merchants want to use a remote access tool, they are required to use security features that include two-factor authentication, such as requiring both a username and password and a token, per PCI-DSS requirement 8.3. Additionally, if they are going to have administrative level access, the tool MUST use SSH, VPN, or SSL/TLS type encryption.

6B: REMOTE ACCESS FROM VENDORS (INCLUDING EXTREME POS)

In the event that remote access must be granted to a vendor, the account should be temporary or the password should be changed immediately after the granted access is complete.

Note that currently, Extreme POS support staff use a tool called LogMeIn Rescue for remote access to customer computers; this tool only allows access for so long as the customer grants it, and does not generally require that a Windows account be set up for the support staff. It meets the two-factor requirement by having a username and password required from the support staff, and a pin code entry required from the customer at the physical machine. This pin code is unique for each session, and must be obtained from the support staff at time of access. The customer must initiate each session, and it is securely encrypted. In the case of a tool like this, a temporary windows account or password change as mentioned above is not required. LogMeIn Rescue sessions time out if left idle for 15 minutes, and will need to be reinitialized.

All file transfers and connections are logged by LogMeIn, and accounts are assigned to individual support technicians, with usernames and passwords being assigned to each individual by the logmein administrative user. All accesses and data are logged permanently to the logmein account, and will be made available upon request in writing. Sensitive data will not be collected unless absolutely required, and there is no troubleshooting mode that will expose PAN data beyond the extent of normal program operations. Any sensitive data that is collected will be secured in known, secure, encrypted locations and permanently deleted once it is no longer required. LogMeIn uses end-to-end 256 bit SSL for encryption.

CHAPTER 7: ENCRYPTION AND KEY MANAGEMENT

7A: ENCRYPTION

PAN data is encrypted using AES with a 256 bit key; the key itself is then again encrypted using another key. These are referred to respectively as the data encrypting key (DEK) and the key encrypting key (KEK). DSI Client, which is the component that ExtremePOS Payment uses for communication, uses RSA key negotiation followed by RC4 symmetric encryption.

7B: KEY STORAGE

The encrypted DEK is stored on the server computer. The KEK is stored elsewhere, such as on a removable drive that is locked away when it is not needed for loading the program. (The exact location is selected by the administrator during key setup.)

7C: CHANGING KEYS

The keys must be changed at least annually, and additionally may be changed at any time, for instance if there is concern that there is a breach. This may be done from the administrative screen. Access to both old keys is required for this change; otherwise, old data will be rendered inaccessible.

CHAPTER 8: HANDLING SENSITIVE AUTHENTICATION DATA

8A: WITHIN EXTREMEPOS PAYMENT

There is no way to view sensitive cardholder data within ExtremePOS Payment.

8B: OUTSIDE OF EXTREMEPOS PAYMENT

Avoid storing any type of PAN data outside of ExtremePOS Payment. In the event that you must test something outside of ExtremePOS, sensitive data can only be stored with the following restrictions:

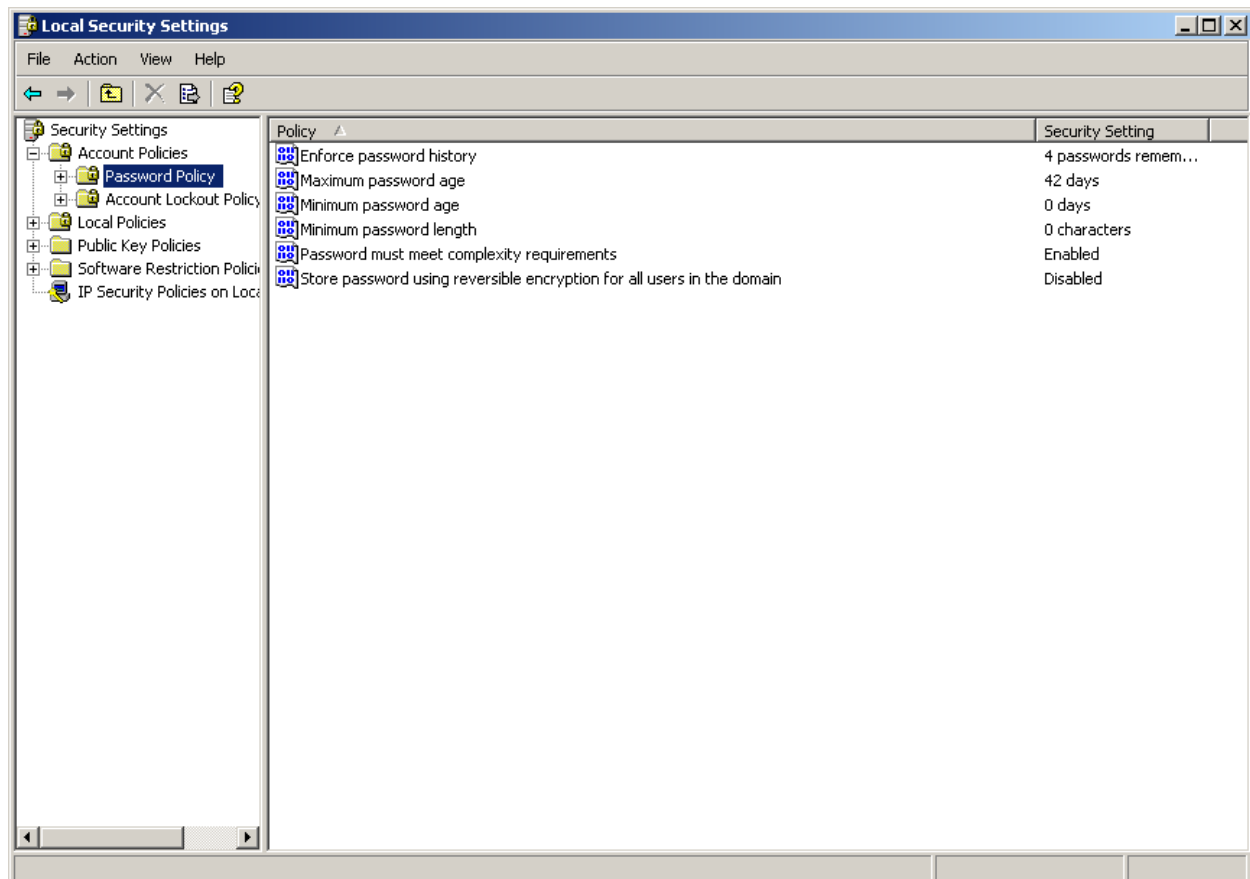
- Data may only be collected to solve a specific problem
- Such data can only be stored in specific, known locations with restricted access.
- Only collect the amount of data needed to solve the problem
- PAN data **MUST** be encrypted while stored.
- Data must be securely deleted after use.

APPENDIX A: CONFIGURING WINDOWS FOR PCI-DSS COMPLIANCE

Correct configuration of Windows is vital to PCI-DSS Compliance, and to protecting PAN data. Merchants, resellers, and integrators must make certain they are configured correctly as listed in this chapter.

A.1: PASSWORD POLICIES

Windows allows the administrator to set up required password policies. To reach this screen, go to Start -> Control Panel -> Administrative Tools -> Local Security Policy. From the menu on the left, click the plus sign next to Account Policy and then open Password Policy.



THE PASSWORD POLICY SCREEN IN WINDOWS XP PROFESSIONAL WITH DEFAULT SETTINGS

The following settings are required for PCI Compliance:

Enforce password history: 4 or more

Maximum password age: 90 or less

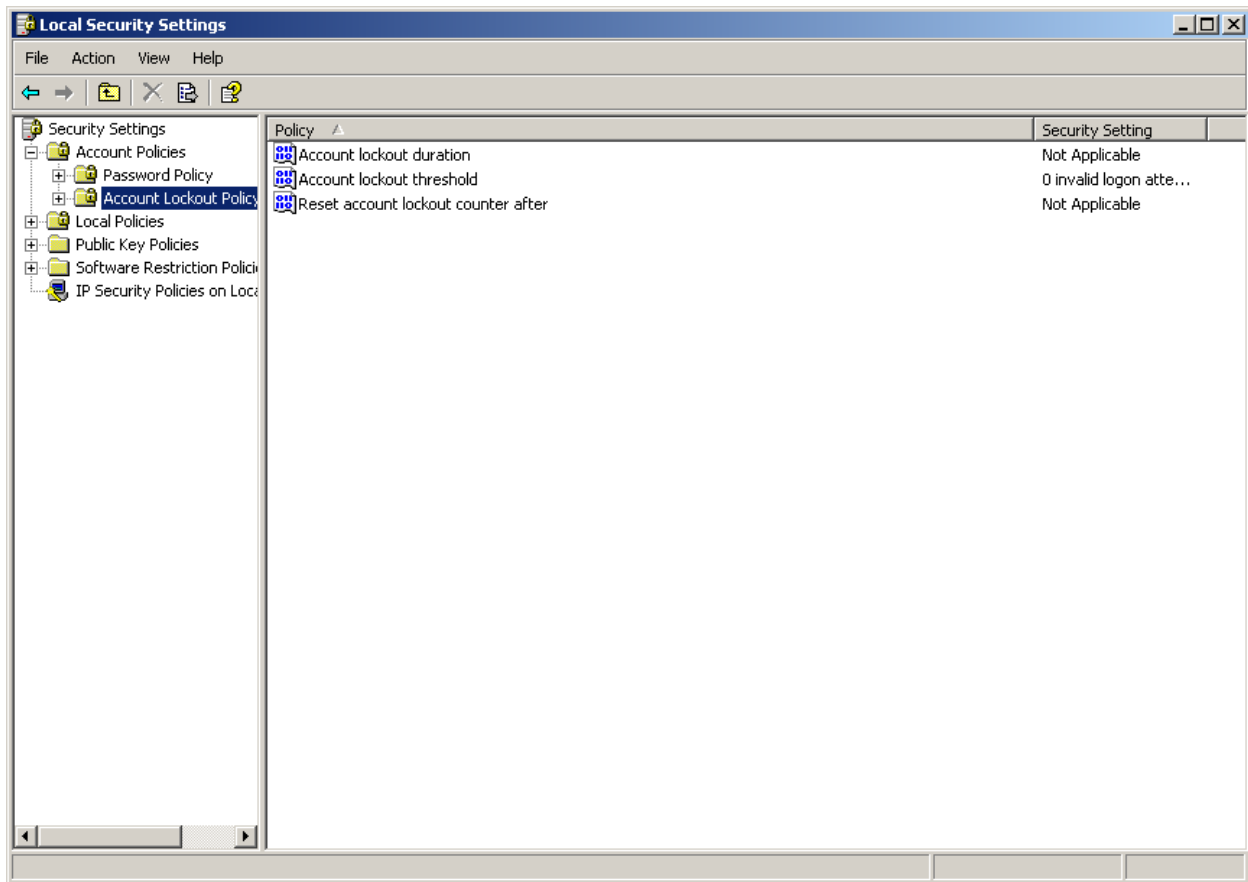
Minimum password length: 7 characters

Password must meet complexity requirements: Enabled

Store Password using reversible encryption: Disabled.

A.2: ACCOUNT LOCKOUT POLICY

This option prevents further attempts on the account should the password be repeatedly attempted incorrectly. To reach this screen, go to Start -> Control Panel -> Administrative Tools -> Local Security Policy. From the menu on the left, click the plus sign next to Account Policy and then open Account Lockout Policy.



ACCOUNT LOCKOUT SCREEN WITH DEFAULT WINDOWS XP PRO SETTINGS

The following settings are required:

Account lockout duration: 30 minutes or more.

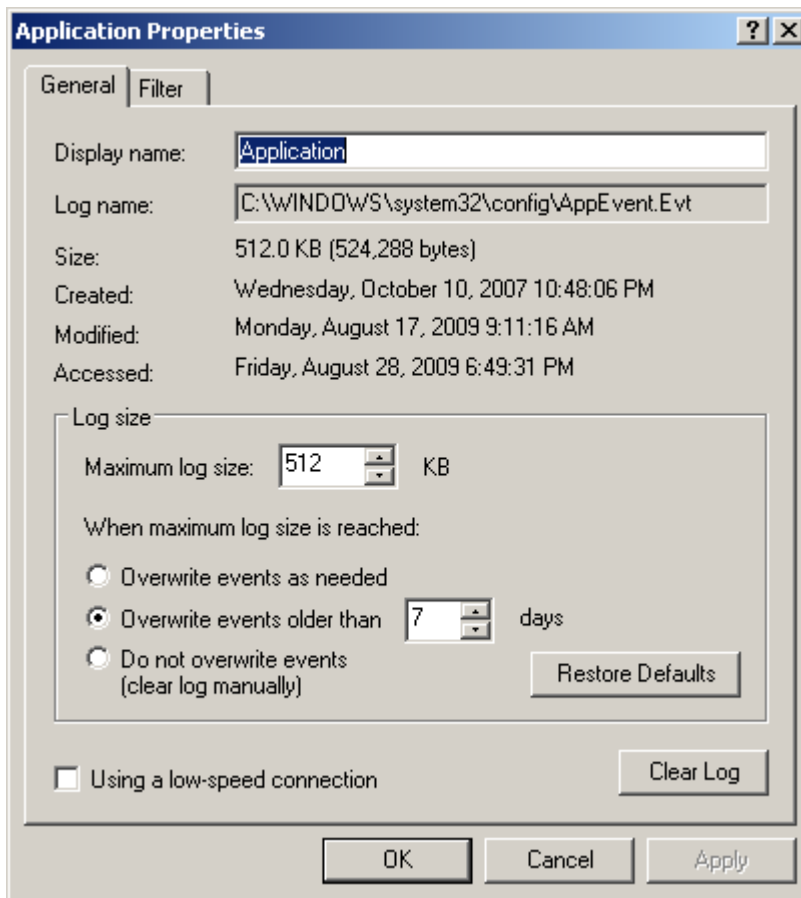
Account lockout threshold: 6 invalid logon attempts or less

Reset account lockout counter after: 30 minutes or more.

A.3: WINDOWS LOGGING

The Event Viewer is the Windows-provided auditing solution. Some configuration of this is required to meet the PCI-DSS. To access this tool, go to start -> control panel -> administrative tools and open the event viewer.

You may access properties of each log by right clicking it in the menu on the right and hitting properties.



Use the following settings:

Under the general tab, set maximum Log Size: 4096 KB and “When maximum log size is reached:” to “overwrite events older than 365 days.”

Under the filter tab, check all boxes under event type, make certain that event source and category are set to all, and that From is set to first event and To is set to last event.

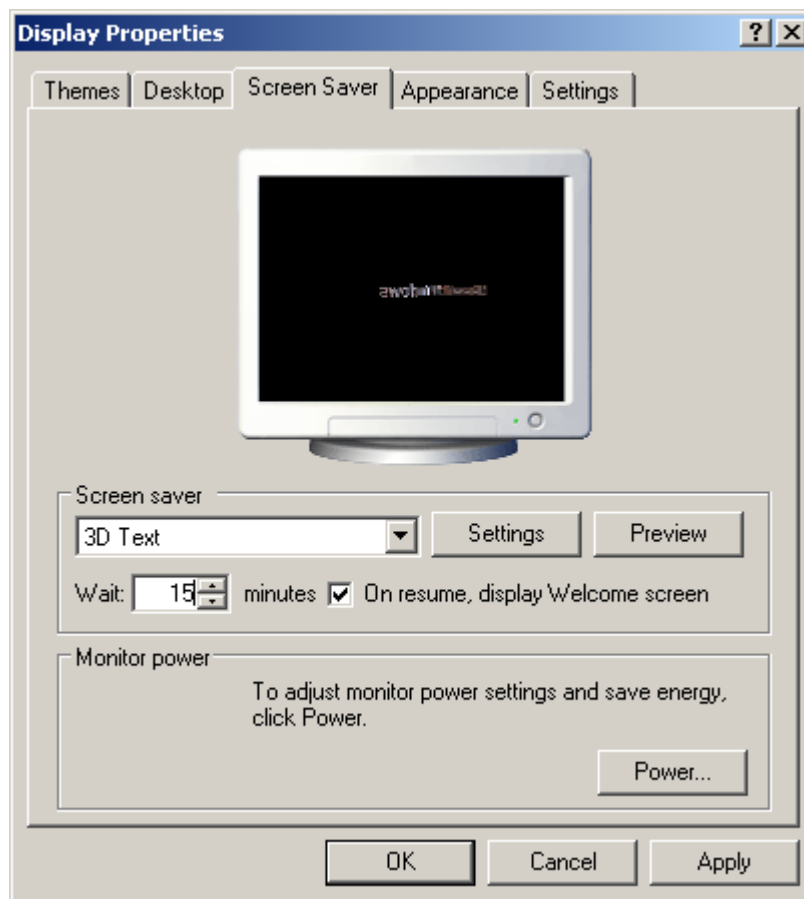
A.4 WINDOWS RESTORE POINTS

Windows Restore Points are a helpful backup system for the average home user. However, due to the manner in which they are stored, **Windows Restore Points must be disabled for PCI-DSS Compliance on any system where ExtremePOS® Payment is running.**

To do this, go to start -> control panel -> system, and under the “System Restore” tab check the turn off system restore box. Agree if it asks you about losing restore points.

A.5: WINDOWS SCREENSAVER

Windows screensaver should be configured to require reentry of the password to access the system. This can be configured in display properties, which may be reached either by right clicking the desktop and going to properties or by going to start -> control panel -> display. In either case, the relevant settings are found under the Screen Saver tab.



You may use whatever screensaver is appropriate for your business; the settings required are the following:

Wait: should be set to fifteen minutes or less.

On resume, display welcome screen: Enabled. Alternatively, in some versions of windows this may be called "On resume, require password"

APPENDIX B: SAMPLE KEY CUSTODIAN FORM

The below is a sample of a form your key custodians should sign, customized for your company. This is available in an editable .doc format upon request. All staff with authorization to access the encryption keys (whether physical access to the Key Encrypting Key or administrator access to ExtremePOS Payment) should be required to sign this.

As a condition of continued employment with _____ and as an employee with responsibilities regarding the cryptographic security of confidential data, you are required to sign the following document to acknowledge those responsibilities.

The signer of this document is an employee with _____ on the date shown below, with access to key management devices, software, and/or equipment, and hereby agrees that he/she:

- Has read and understood the policies and procedures associated with key management and agrees to comply with them to the best of their ability. He/she has had the opportunity to ask questions regarding this policy, and has had those questions answered to their satisfaction.
- Understands that non-compliance with these policies can lead to termination of employment and possible prosecution.
- Agrees to never divulge to any unauthorized party the key management practices or any related security systems, passwords, processes, or other secrets associated with the company's systems.
- Agrees to promptly report to management any suspicious activity, including but not limited to system or key compromise or theft.

I agree to the above in full and understand my responsibilities as indicated above.

Signed: _____

Printed Name: _____

Date: _____

Witnessed: _____

Printed Name: _____