Sensible Cinema Software®

Box Office for Windows 2009

Cardholder Information Security Program (CISP)
Payment Card Industry Data Security Standard (PCI-DSS)
Field Implementation Guide

Revision 8
July 14, 2009

Installation Questions?
Call **Rusty Gordon (615) 799-6366** · Office Hours: M-F 9am-5pm CST
E-Mail: **rusty@sensiblecinema.com**

Introduction

Systems which process payment transactions necessarily handle sensitive cardholder account 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. This implementation guide is designed to help you identify weaknesses and install and use the software in a manner consistent with Payment Application Best Practices (PABP).

The following high level 12 Requirements comprise the core of the PCI DSS:

Build and Maintain a Secure Network
1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data
3. Protect Stored Data
4. Encrypt transmission of cardholder data and sensitive information across 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 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

The remainder of this document describes the essential guidance for implementing Sensible Cinema Box Office for Windows in a PCI compliant environment. In order to satisfy these requirements you may find it necessary to hire professionals to assess your network and hardware and perform some of the tasks called for in this implementation guide.

Please schedule a conference call with us and your installer so that we can explain the basics of this requirement.

Access Control

The PCI DSS requires that access to all systems in the payment processing environment be protected through use of complex passwords. Additionally any default accounts provided with operating systems, programs and/or devices should be removed/disabled/renamed as possible, or at least should have PCI DSS compliant complex passwords. Default administrator accounts include those named “administrator” or “admin”. Be certain the hidden Administration account in Windows XP has been given a password. Start Windows in Safe Mode for access to the account and set a password. You should use a different password for administrator account and standard user accounts. Standard accounts should be used at all times except when software installation or system configuration is necessary. As a rule, use the least privilege needed.

The PCI standard requires the following password complexity for compliance:

- Passwords must be at least 7 characters
- Passwords must be changed at least every 90 days
- New passwords cannot be the same as the last 4 passwords
- Passwords must include both numeric and alphabetic characters

PCI user account requirements beyond uniqueness and password complexity are listed below:

- If an incorrect password is provided 6 times the account should be locked out
- Account lock out duration should be at least 30 min. (or until an administrator resets it)
- Sessions idle for more than 15 minutes should require re-entry of username and password

These same account and password criteria must also be applied to any applications or databases included in payment processing to be PCI compliant.

Remote Access

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism such as a user name and password and the enabling of the remote host by an individual at the physical location on a need-to-use basis rather than running the host mode perpetually. While the extra effort may be less convenient, it ensures a hacker does not obtain access to your network after hours.

Non-Console Administration

Users and hosts within the payment application environment may need to use third-party Software such as Symantec PCAnywhere. 128 Bit encryption must be used in addition to

satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). For RDP/Terminal Services this means using the high encryption setting on the server, and for pcAnywhere it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements will apply to these access methods as well.

Wireless Access Control

Sensible Cinema Software strongly recommends against using wireless networks because the Jet database is known to behave erratically with unstable connections. The PCI standard requires the encryption of cardholder data transmitted over wireless connections. The following items identify the PCI standard requirements for wireless connectivity to the payment environment:

- Firewall/port filtering services should be placed between wireless access points and the payment application environment with rules restricting access
- Use of appropriate encryption mechanisms such as VPN, SSL/TPS at 128 bit, or WPA (WEP encryption at 64 or 128 bit will no longer be acceptable in new PCI-DSS guidelines.)
- Vendor supplied defaults (administrator username/password, SSID, and SNMP community values) should be changed
- Access point should restrict access to known authorized devices (using MAC address filtering)

Transport Encryption

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with SSL or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard sensitive cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments). The Sensible Cinema Software program meets these requirements when paired with a computer running Microsoft Internet Explorer version 6.0 or later with all appropriate software patches. There are no user configurable settings within the application.

Additionally, PCI requires that cardholder information is never sent via email without strong encryption of the data. Regular e-mail messages are not encrypted and easily readable.

Network Segmentation

The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access.

Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

Information Security Policy/Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.

- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.

- Create an action plan for on-going compliance and assessment

- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self Assessment Questionnaire.

- Call in outside experts as needed. Visa has published a Qualified Security Assessor List of companies that can conduct on-site CISP compliance audits for Level 1 Merchants, and Level 1 and 2 Service Providers. MasterCard has published a Compliant Security Vendor List of SDP-approved scanning vendors as well.

Operating System Requirements

- Microsoft Windows XP Pro SP3 (Recommended), WEPOS with SP3, Windows 2000 SP4, Windows Server 2003 SP2, Windows Vista Business SP1 or Windows Server 2008, POSReady Embedded

This document specifically addresses Windows XP and Vista. For best performance, Windows Embedded for Point of Service (WEPOS or POSReady) is recommended for selling terminals. It is a special embedded version of Windows XP designed to run on minimal hardware.

Operating System Configuration

Windows XP Security

1. Setting up Windows XP User Accounts on the host system

Each individual with access to the computer should have their own login. There should be two Permanent Windows User Accounts configured with Administrator access, and as many Standard User accounts as necessary for the management staff.

Notes on User Settings:

a. Administrative accounts should not be used for routine application logins.
b. Strong passwords must be assigned to these admin accounts, and any that are not required should be disabled or removed from the system
c. Always assign strong application and system passwords whenever possible. See Section 2 - **Local Security Settings** for more information on strong passwords.

2. Local Security Settings

In order to maintain the required level of password security on the system, the following settings must be configured in the Windows XP Local Security Settings module:

Password Policy:

Enforce password history – Set to remember last 4 passwords
Maximum Password Age - 90 Days
Minimum Password Age - 0 Days
Minimum Password Length - 7 Characters

Account Lockout Policy:

Account Lockout Threshold - 6 Attempts
Account Lockout Duration - 30 Minutes
Reset Account Lockout Counter After - 30 Minutes

3. Disabling Unnecessary Services

All unnecessary and insecure services and protocols (e.g., NetBIOS, file-sharing, Telnet, FTP server, HTTP server, etc.) should be disabled on the PC running the Sensible Cinema Box Office for Windows software. The POS PC should never be used to host a public FTP or HTTP (Web) server.

Protocols and Ports can be disabled from the Windows Firewall and the Hardware Firewall. Services can be disabled from Control Panel => Administrative Tools => Services.

Anti-Virus

Anti-virus software must be installed on the Manager's PC and every PC accepting payments, and must be configured to automatically receive and install updates. It is the owner's responsibility to make sure the anti-virus database is kept up to date and the software license is renewed as needed. Failure to do so compromises all other efforts to limit exposure to the possibility of data theft. Software should automatically update its virus definition database. Free open source anti-virus software may be obtained from **http://www.clamwin.com**.

Credit Card Server

The Mercury Pay credit card server address has been hard-coded in the Sensible Cinema Software application to prevent unauthorized changes. The merchant account and terminal ID number are the only information that may be changed by the end user.

Firewall

The firewall should be configured to allow incoming network connections for only those services required for operations. Examples are a Digital Video System, and VPN. Outbound connections should also be restricted to only those services required for proper POS operation. Examples are HTTP client, FTP client, POP3 client, SMTP client, Credit Card processing, and Gift Card processing.

Internet Applications

In order to meet the requirements of PCI DSS, sensitive cardholder data cannot be stored on a server connected to the internet. The Sensible Cinema Box Office for Windows application does not provide internet services, and does not require that any internet applications reside on the computer containing cardholder data. Software that provides internet services (such as a web server or FTP server) must never be run on the same computer as the Sensible Cinema application.

Best Practices for Support and Troubleshooting

The following guidelines must be followed by Resellers, Integrators, Support Technicians, and End-Users when dealing with sensitive information in order to meet the requirements of PCI compliance:

1. The Sensible Cinema Software program does not collect or store sensitive data.
2. Personnel must collect only the limited amount of data needed to solve a problem.
3. Personnel must encrypt sensitive authentication data while stored.
4. Personnel must securely delete such data immediately after use.

Sensible Cinema Management Software Installation Procedure

The following steps should be followed when installing this software on the server and/or management computer system:

1. ***Prepare Operating System***
   Ensure the Microsoft Windows version on the target system is **Windows 2000 (SP4)**, **Windows XP (SP3), Windows Vista (SP1), Windows Server 2003 (SP2) or Windows Server 2008 (Currently no SP), Windows POSReady or WEPOS (SP3).**

2. ***Antivirus and Firewall***
   Verify that the computer is protected using anti-virus software and that the virus definitions are current. Further, ensure the subscription is active and that the software is configured to automatically update the virus definitions as they become available. Verify that the Windows Firewall or firewall included with the anti-virus suite is enabled. Note: Windows File and Printer Sharing must be enabled in the firewall in order for the workstation computers to "see" this server PC. Free open-source antivirus software is available from **http://www.clamwin.com**.

3. ***Removal of Old Version***
   Use **Add/Remove Programs** (**Programs and Features** in Vista and Windows 7) to remove prior Sensible Cinema versions and updates. Delete all Sensible Cinema Software desktop shortcuts which remain or drag them into your recycle bin. All configuration and playdate files created with prior versions will remain under C:\Program Files\Sensible Cinema Software\Box Office for Windows.

4. ***Run Installation Installshield® Wizard***
   Install the software on your target system using the installation defaults unless otherwise instructed.

5. ***Share Database Folder***
   Share the new database folder **C:\Sensible Database**. Be sure to check the check box to "Allow Other Users to Change My Files." Not doing so will prevent database writes from your selling terminals resulting in Error #75, File/Path Access Error.

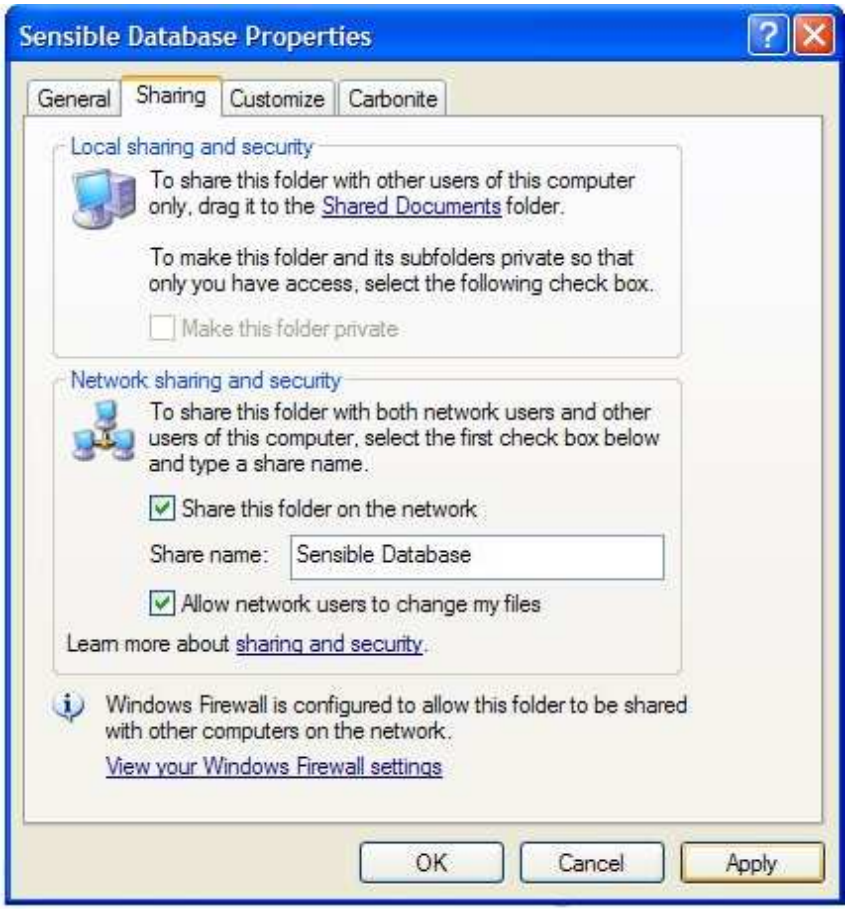
   a.) Press "START" button on your Windows desktop. Then select **My Computer Local Drive C:**

   b.) Browse to **C:\Sensible Database**

   c.) Once you locate the **Sensible Database** folder, right-click on it and choose **Sharing and Security** (You understand the risks if it prompts you to confirm this.)

Sensible Cinema Management Software Installation Procedure (continued)

d.) Next, find **Network Sharing and Security** about at the middle of the sharing dialog box. Check the checkbox that says **Share this folder on the Network**. The default share name will be **Sensible Database**. Leave it as it is. Then check the checkbox that says **Allow network users to change my files**.



Press the **Apply** button. A warning window will appear when you do so telling you that the share name is too long to be accessed on computers running older operating systems. This is okay since you won't be. Click "Yes."

Sensible Cinema Management Software Installation Procedure (continued)

6. ***Copy Configuration Data from Previous Version***

   By copying the configuration files from your previous installation you save the need to re-configure program settings, ticket and concession prices and save yourself considerable time.

   Using **"My Computer"** browse to the previous version's configuration data folder **C:\Program Files\Sensible Cinema Software\Box Office for Windows\Config**

   Once inside the folder you will typically find the files shown below:
   bp_settings.mdb ***bp_film.mdb*** ***bp_appt.mdb***

   a.) **Select** all files by pressing and holding **Ctrl + A** (they should highlight)

   b.) **Copy** all files by pressing and holding **Ctrl + C** (nothing will appear to happen)

   c.) **Navigate** back to **C:\Sensible Database\Config**

   d.) **Paste** files into the Config folder by clicking in the window area and pressing and holding **Ctrl + V.** You will be prompted to allow overwrite if you have done this correctly. Answer **Yes**. The "overwrite" prompt confirms that you have copied to the right place.

7. ***Copy Playdate Data Files from Previous Version***

   Using **"My Computer"** browse to the previous version's configuration data folder **C:\Program Files\Sensible Cinema Software\Box Office for Windows\Playdates**

   a.) **Select Files to Copy** Once inside the folder you will likely find hundreds of playdate files. You do not want to copy them all because they are not needed and having a folder with fewer files will improve overall performance. Select the **Details** View from the View Menu. Sort the playdate files by clicking the sort heading **Date Modified** until the files are sorted with the most recent playdates at the top. Left click the top file with your mouse then hold **Shift** and the **down arrow** keys, highlighting the files you intend to copy. You should probably select files created within the past 30 days.

   b.) **Copy** all selected files by pressing and holding **Ctrl + C** (nothing will appear to happen)

   c.) **Navigate** back to **C:\Sensible Database\Playdates**

Sensible Cinema Management Software Installation Procedure (continued)

d.) **Paste** files into the new Playdates folder by clicking inside the window area then pressing and holding **Ctrl + V**. Files will copy into the playdates folder along with the existing sample playdate file. This confirms your success.

8. ***Create License Key***
Using the Sensible Local Settings desktop shortcut, start the terminal setup utility. Enter your license information exactly as shown on your license code sheet.

9. ***Remove Share from Previous Software Version***
Remove the share from the folder previously used as the database folder on the server computer. This was probably **C:\Program Files\Sensible Cinema Software\Box Office for Windows**. This is done by navigating to the folder above using **My Computer**. Once you find the **Box Office for Windows** Folder, Right-Click the folder icon, select Sharing and Security and uncheck the "Share this Folder" checkbox. The "Sharing Hand" will disappear from the folder icon.

Sensible Cinema Terminal Client Software Installation Procedure

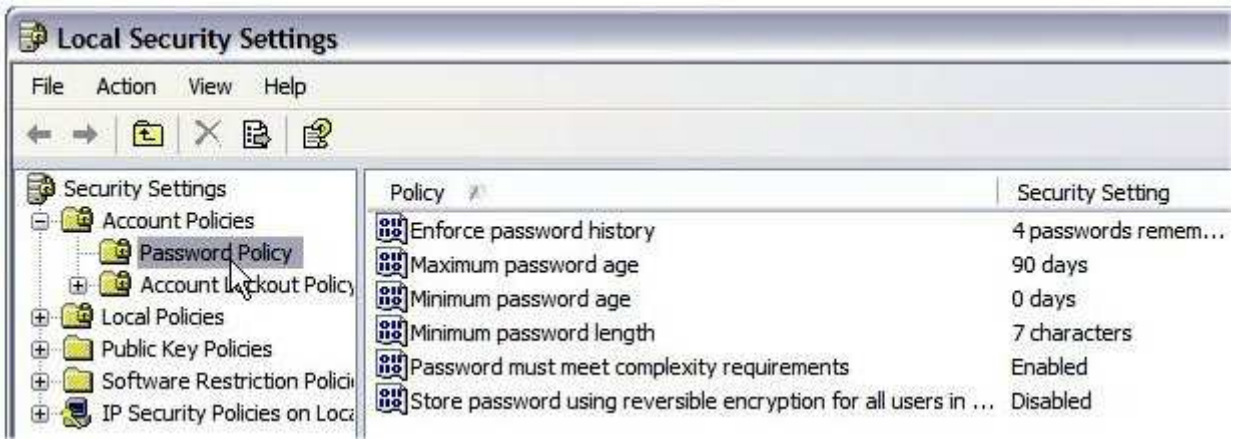
The following steps should be followed when installing this software on the terminal client computer system:

1. ***Prepare Operating System***
   Ensure the Windows version on the target system is **Windows XP Professional**, **WEPOS** or **Windows Embedded**, all running Service Pack 3, **Windows Vista Business** or **Windows Vista Ultimate**, either running Service Pack 1 or **POSReady**.

2. ***Antivirus and Firewall***
   Verify that the computer is protected using anti-virus software and that the virus definitions are current. Further, ensure the subscription is active and that the software is configured to automatically update the virus definitions as they become available. Verify that the Windows Firewall or firewall included with the anti-virus suite is enabled. Free open-source antivirus software is available from **http://www.clamwin.com**.

3. ***User Accounts and Privileges***
   Create a new **Administrator** user account in the Windows Control Panel under User Accounts**.** *Later* you will change the privileges of this new account to **Limited User**. Keep your existing Administrator account as is. Do not use the name "Administrator." **Important:** Use a different password for Administrator and Limited user accounts.

4. ***Local Security Policy***
   Change the **Local Security Policy** found in Windows **Control Panel** as shown in the graphic below. (see page 16 for the procedure in Windows Vista). Note: PCI Compliance cannot be achieved with home versions of Windows XP or Vista because they lack the local security policy configuration applet.



Sensible Cinema Terminal Client Software Installation Procedure (continued)

5. ***Printer Drivers***
   Install Printer Drivers for your system and configure them appropriately. If installing on a system you have previously used you likely will not need to make any changes here. Take note that certain drivers require the paper type to be changed in order to render the print job correctly. Ticket Printers require a **Generic Text Only** printer with the paper type changed from "Automatically Select" to "Cut Sheet." Receipt printers often require changing the printer preferences for paper type to one which adds a receipt cut.

6. ***Software Setup***
   Install the **Sensible Cinema Terminal Client Software**. You should use the default settings unless stated otherwise.

7. ***User Accounts***
   Log out of this user account and log into your original **Administrator** account. Open the Windows **Control Panel** and **User Accounts** and change the new Administrator account to the **Limited User** account type. Log out of the **Administrator** account. Log back into the new account which is now a **Limited User**. *This* account will always be used whenever the Sensible Cinema Terminal Client Software is active on the computer. The Administrator account should only be accessed when software updates and other administrative tasks are necessary.

8. ***Path Configuration***
   If the management software was installed on the server PC using the default setup parameters, a folder called **Sensible Database** was created on drive C:. This folder should be shared on the server and the checkbox "Allow other users to change my files" should be checked. This permits the client computer to write data to the database files. On the client computer you can either enter the true path (required in Windows Server versions) or map a network drive pointing to the **Sensible Database**.

   In the **Sensible Local Settings** utility, select **Configure Path to Database**. Enter the mapped drive letter in the path window (e.g. ***Z:***) or enter the true path, (e.g. ***\\SERVERNAME\Sensible Database)***

   If this system is a standalone PC and the management software is installed on the same computer with the client, simply choose the "Local" path option to use ***C:\Sensible Database***.

9. ***Log File***
   For your information, a **systemlog.txt** file (stored in the database directory by

Sensible Cinema Terminal Client Software Installation Procedure (continued)

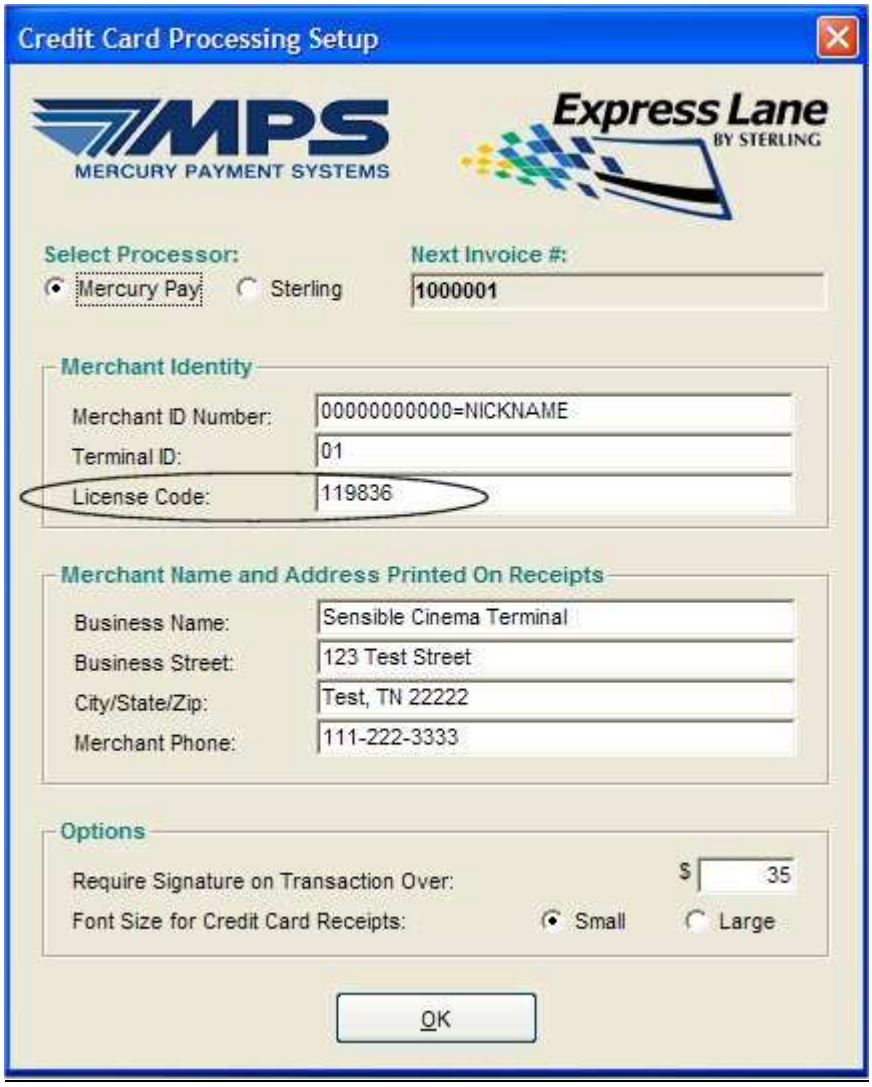
default) keeps a record of file operations and other user invoked changes made in the course of using the software, for example deletion of playdate files and any values contained in those files when deleted. If necessary, you can configure the system log for storage in another location. Call support for information on how to do this.

10. ***Create License Key***
    Using the **Sensible Local Settings** desktop shortcut, start the terminal setup utility. Enter your license information exactly as shown on your license code sheet. You will also have to enter the license code for the credit card processing module if you are accepting credit cards. This is entered in the credit card merchant setup. (See 11)

Sensible Cinema Terminal Client Software Installation Procedure (continued)

11. ***Credit Card Merchant Setup***

    Using the Sensible Terminal Setup, select Credit Card Merchant Setup. If upgrading from a previous version you will find the address and merchant number intact. You must enter your new credit card processing module license code on line #3. The terminal ID field is optional for Mercury Payment Systems merchants and may be left blank. If processing using Sterling Payment Systems, enter your SPS Terminal ID on line #2. This is not the same terminal ID as the Sensible Cinema Terminal ID entered in the registration screen.



Windows Vista/Windows 7 Password Policy Variation:

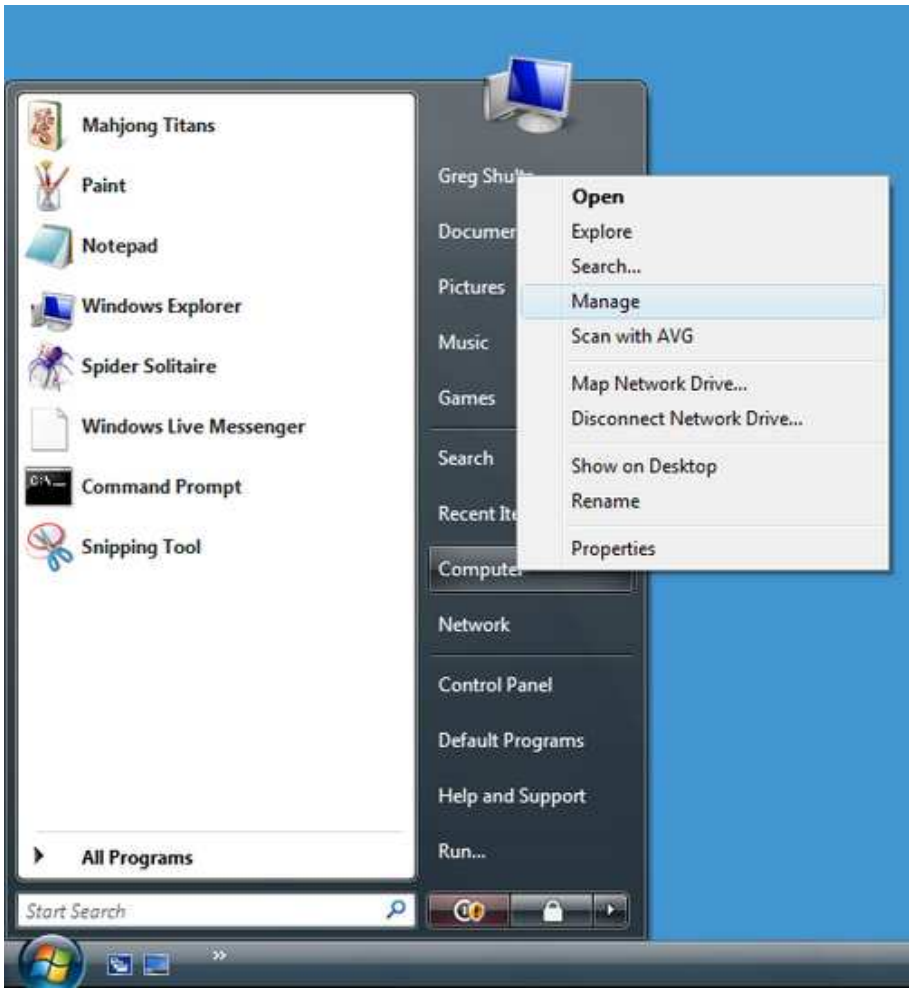
Version caveats

This technique will only work in the Ultimate and Business editions of Vista. Home and Home Premium users will have to rely on a manual change password operation.

Local User and Groups

By default, Vista allows your original password never to expire. As such, the first thing that you have to do is configure your password such that it expires; you'll make that change in the Local Users and Groups tool. To access this tool, click the Start button, right-click on Computer and select Manage from the context menu (**Figure A**). You'll then encounter a UAC dialog box and will need to respond accordingly.

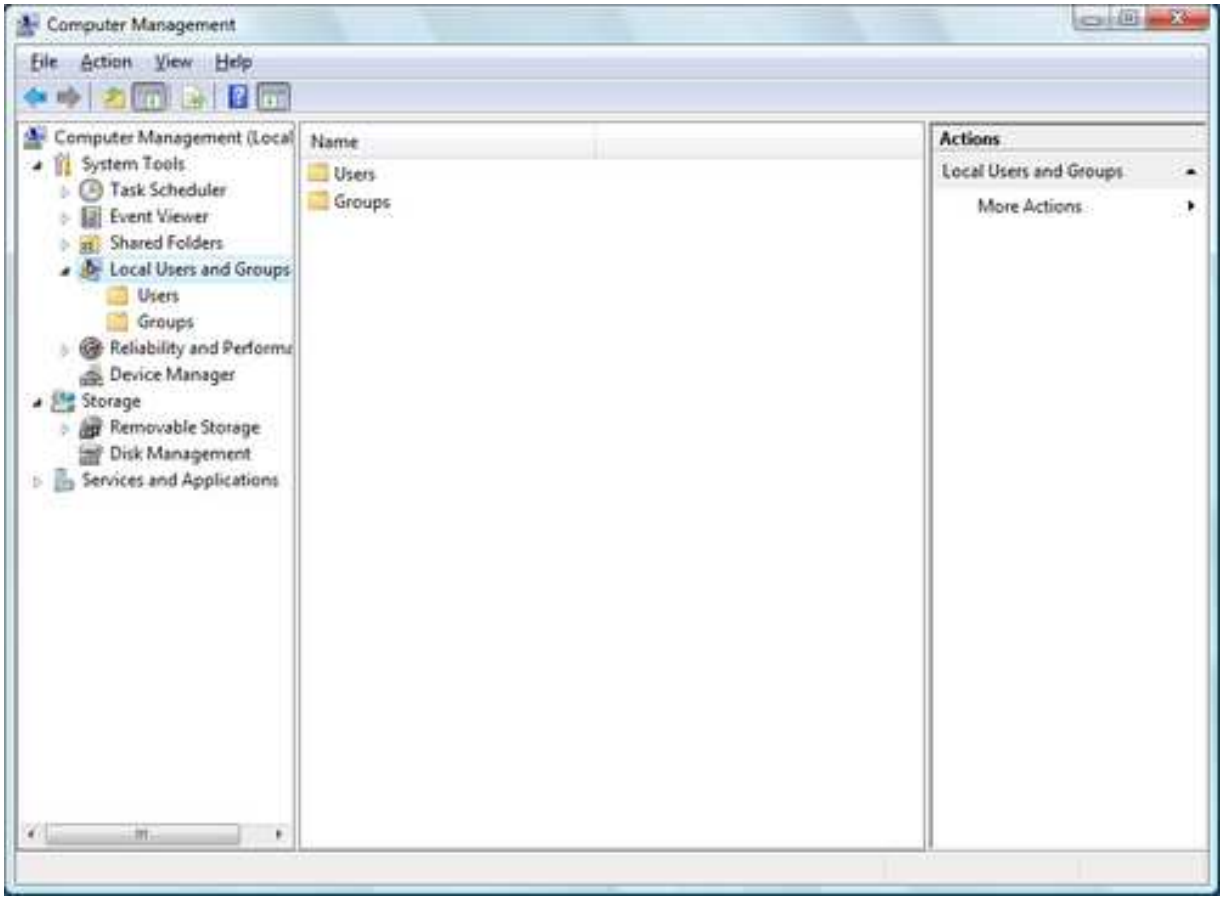
Figure A



To get to the Local Users and Groups tool, begin by selecting Manage from the Computer context menu.

At this point, you will see the Computer Management console and will need to select Local Users And Groups in the tree so that the branch opens (**Figure B**).

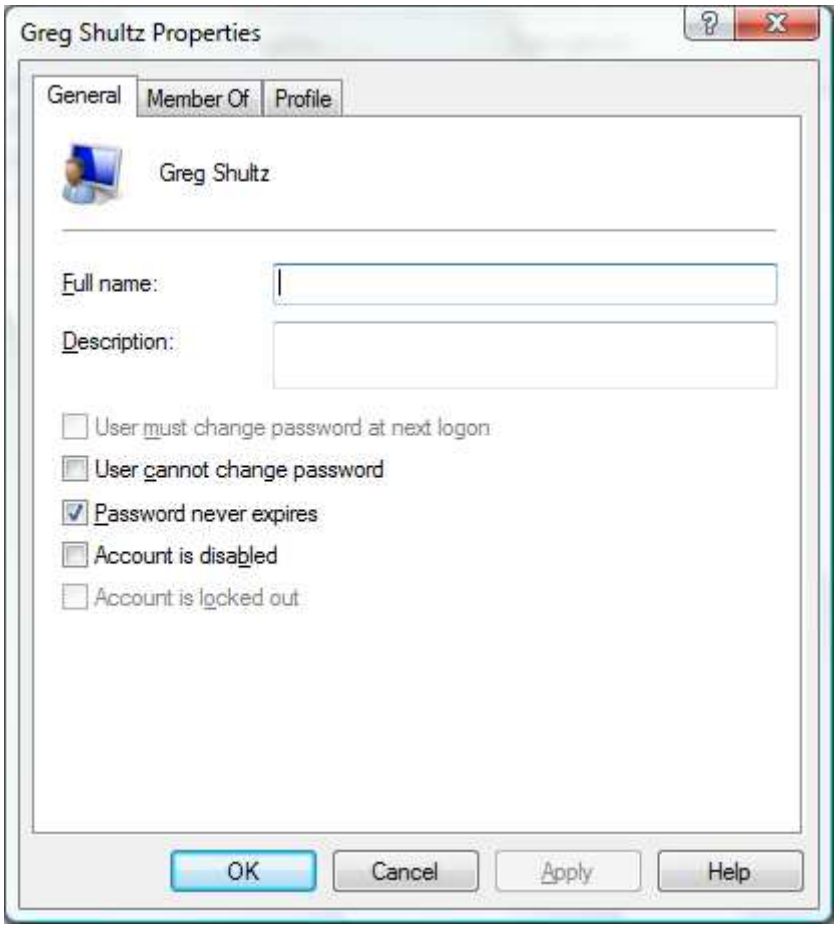
Figure B



When the Computer Management console appears, open the Local Users And Groups branch.

Now, select the Users branch and double-click your username to access your user account Properties dialog box (**Figure C**).

Figure C



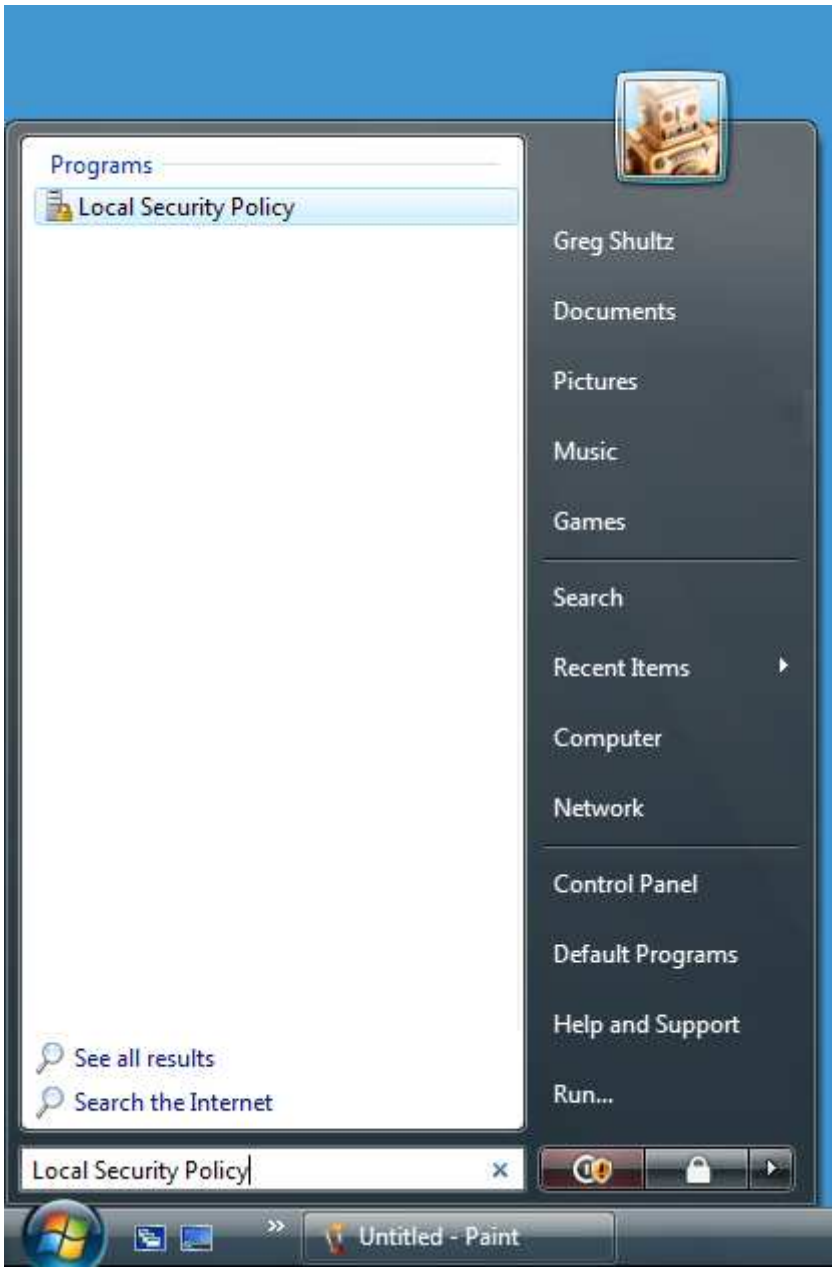
You'll need to clear the Password Never Expires check box to allow your password to expire.

The default setting for Password Never Expires is checked. Clear the Password Never Expires check box by selecting it, then click OK and close the Computer Management console.

The local security policy

The second thing you'll need to do is alter the local security policy. To make these types of alterations, you'll need to launch and work from the Security Settings Extension snap-in. To do so, click the Start button, type *local security policy* in the Start Search box (**Figure D**), and press [Enter]. When you do, you'll encounter a UAC dialog box and will need to respond accordingly.

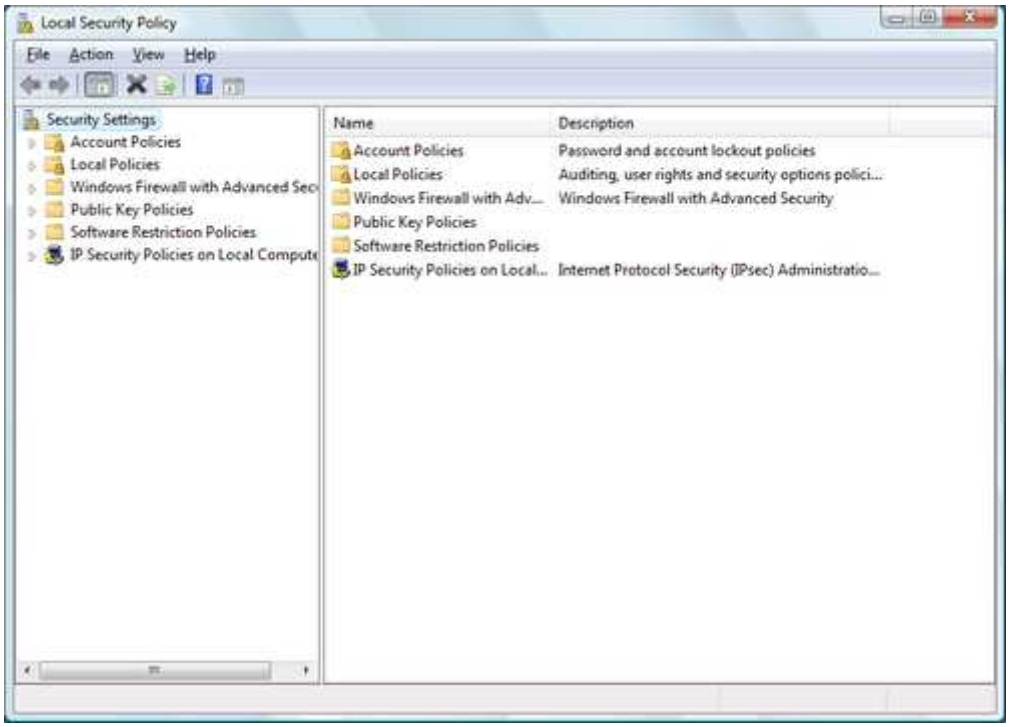
Figure D



To access the Security Settings Extension snap-in, enter local security policy *in the Start Search box.*

In a moment, you'll see the Security Settings Extension snap-in in a console window titled Local Security Policy (**Figure E**).

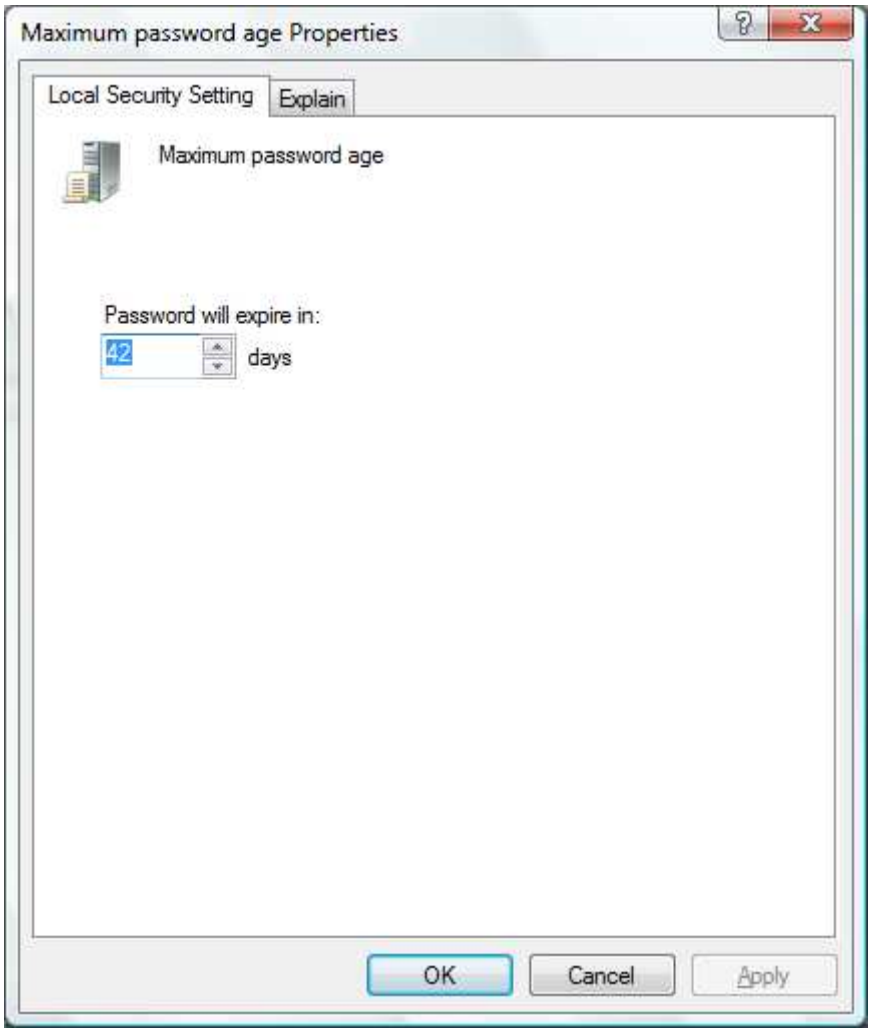
Figure E



The Security Settings Extension snap-in appears in the Local Security Policy window.

Now, select Account Policies in the tree pane to open the branches. Select the Password Policy branch and double-click Maximum Password Age Policy. When you see the Maximum Password Age Properties dialog box (**Figure F**), use the spin buttons to select a length of time that you wish to use a password before a prompt appears to change it. To complete the operation, click OK, close the Local Security Policy console, and restart your system.

Figure F



Type a value in the Password Will Expire In box or use the spin buttons to select a value for the length of time.

Once the specified time has lapsed, go to log on to your system as you normally would and type your current password. When you do, you'll see an error message on your logon screen, similar to the one shown in **Figure G**, which tells you that your password has expired and you must change it.

Figure G

Vista will inform you that you must change your password once it has expired.

When you click OK, you'll see a screen similar to the one shown in **Figure H**, which prompts you to enter and confirm a new password and create a password reset disk. (For more information on creating a password reset disk, see the article Create A Vista Password Reset Disk Using A USB Flash Drive.)

Figure H

When you change your password on a regular basis, it is a good idea to create a new a password reset disk each time.

Once you change your password, you'll see a confirmation message. When you click OK, Vista will log you on.

Changing your password

Changing your password on a regular basis is a good way to enhance the security of your Vista system and using the maximum password age policy to enforce the change is a good solution. How often do you or your users change passwords?

Sensible Cinema Software
Activity Logs

Beginning with Build 8 of the management software and Build 6 of the Terminal Client Software user activity is logged and stored for future reference..

The most current logging information is stored in the file called **systemlog.txt** found in the sub folder called **Activity Logs** under **Sensible Database** on your server machine. Once this file grows to 1Mb in size, the file is archived with the last date of the log in the new filename and is stored until deleted (e.g. **archived_systemlog_050409.txt**) and a new systemlog.txt file is created to replace it. These files are plain text and readable by Windows Notepad, Microsoft Word, Open Office and many other text editors.

It is recommended that all logs be retained in case a forensic examination of the POS operation is ever necessary. No action on the part of the user is required to perpetually keep these records.

The **systemlog.txt** file contains the following information:

a) User account creation inside the Sensible Cinema program
b) Password changes
c) Changes of user level
d) Deletion of Sales Data
e) Log in/Log out of the management software
f) Accessing ticket price setup
g) Use of the NO SALE button by a cashier
h) Display of playdate/date discrepancy message
i) Normal program termination
j) Abnormal program occurrences

Sample file contents:

```
04/22/2009  16:28:05  admin    99   Logged into Sensible Cinema Terminal #1
04/22/2009  16:28:13  admin    99   Used NO SALE function to open cash drawer on Sensible Cinema Terminal #1
04/22/2009  16:28:18  admin    99   Normal termination of Sensible Cinema Terminal #1
04/22/2009  16:28:37  rustang  99   Box Office Manager Software Invoked
04/22/2009  16:28:54  rustang  99   User: rustang (User: Rusty Gordon) user level was changed from 99 to 80
04/22/2009  16:28:54  rustang  99   User: rustang (User: Rusty Gordon) Level = 80, was added or edited
04/22/2009  16:29:01  rustang  99   User: admin (User: Administrator User) user level was changed from 99 to 81
04/22/2009  16:29:01  rustang  99   User: admin (User: Administrator User) Level = 81, was added or edited
04/22/2009  16:29:14  rustang  99   Ticket pricing setup was accessed
04/24/2009  11:26:52  admin    81   Box Office Manager Software Invoked
04/24/2009  11:27:00  admin    81   Normal Termination of Box Office Manager Software
04/24/2009  12:40:19  admin    81   Box Office Manager Software Invoked
04/24/2009  12:41:26  admin    81   Normal termination of Box Office Manager Software
04/24/2009  12:46:58  admin    81   Box Office Manager Software Invoked
04/24/2009  12:49:14  admin    81   Normal termination of Box Office Manager Software
04/24/2009  14:29:44  rustang  81   Box Office Manager Software Invoked
04/24/2009  14:30:52  admin    99   Logged into Sensible Cinema Terminal #1
```

Sensible Cinema Software
Installing Updates: The Latest Cumulative Patch

On the Sensible Cinema Software web site (http://www.sensiblecinema.com) you will find the latest software updates for your software major version. All patches are cumulative and include any and all prior updates. You will find the updates under the "Support" heading of the web site menu. A history file will detail the changes that have occurred with each revision.

In order to install updates on your computer you must have **full administrative privileges** as well as be authorized to make changes to files in the Program Files folder. Make sure the update is installed for use by all users of the computer or at least installed on the same account used for the original software installation. On Windows Vista and Windows 7 systems it will be necessary to disable the User Account Control until the software has been updated and run successfully for the first time. See below.

Turning Off Windows Vista / Windows 7 User Account Control
In addition to installing the update on an account with full administrative privileges it will also be necessary to disable the User Account Control (UAC) on Windows Vista and Windows 7 systems because modifications to DLL and database template files stored in the program folder must be made when the software is used for the first time. The UAC can be turned back on after the software has been run once after installing the patch. On systems properly secured using anti-virus, anti-spyware and firewall software, leaving UAC turned off may simplify future updates and cause no harm to your systems. Effectively you would be leaving it in a state similar to Windows XP.

To turn off the UAC, go to the Windows Control Panel and select:
Windows 7 -> System and Security -> Action Center -> User Account Control
Windows Vista -> User Accounts -> Turn User Account Control On or Off