# PA-DSS Implementation Guide


**mPower v4.0.1.x**

**PA-DSS Implementation Guide**
**Document Version 3.0**
**April 15, 2015**

# Table of Contents

# 1 SCOPE AND APPLICABILITY

## *1.1 Intent of the PA-DSS*

The intent of the PA-DSS is to develop secure payment procedures within mPower Beverage Software that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure payment applications support compliance with the PCI-DSS.

## *1.2 Scope of this Guide*

This guide will explain the features included within mPower Beverage software, and the best practices which will help users maintain PCI-DSS compliance.

# 2 NETWORK AND SOFTWARE COMPONENTS

While mPower Beverage strives to provide its customers and partners with software that protects against security weaknesses, the security of the platforms and networks on which mPower Beverage reside are essential to the overall security of the organization and its information. As such, consider the security and layout of the systems and networks before installing mPower Beverage.

## *2.1 A Word about PCI DSS Scope*

The rule for considering scope for a merchant's PCI DSS compliance is this: scope includes any system that *stores*, *processes*, or *transmits* cardholder data AND any system logically connected to the systems that store, process or transmit that are not separated by a firewall. Thus, if a merchant's network contains a payment application and a back-office PC on the same local network, both systems are in scope. If the payment application resides on its own network segment and is separated with firewall rules that preclude access in either direction to the back-office PC, only then is this second PC removed from scope.

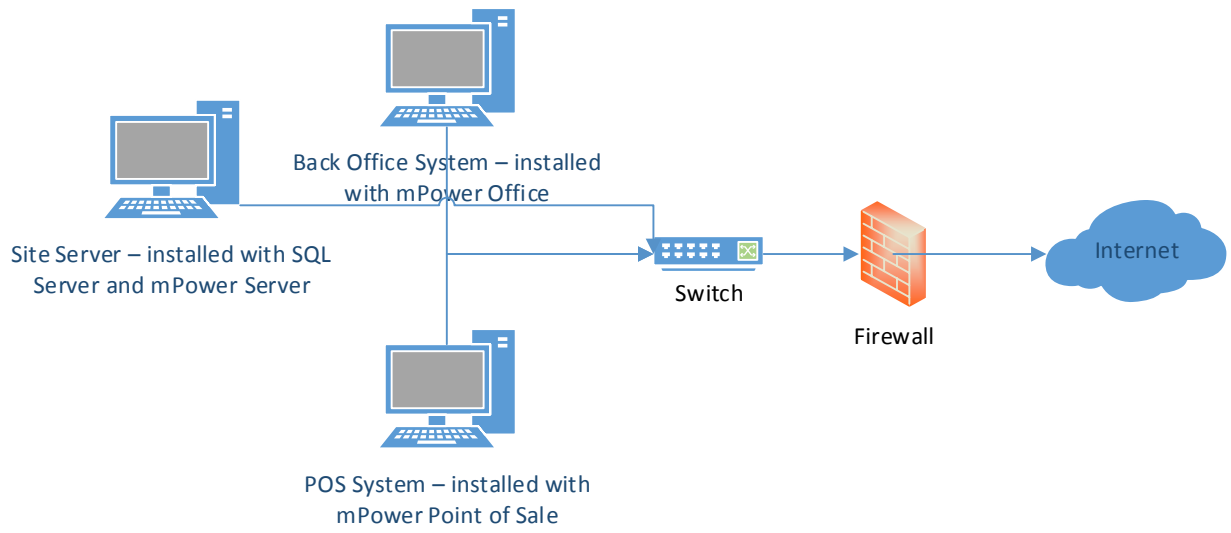
The purpose of the PA-DSS is to:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

## *2.2 Network Security*

First and foremost, placing the components of mPower Beverage into an appropriately protected network will both reduce the risk of exposure or misuse and meet several essential compliance requirements. A typical proper network implementation will have the mPower Beverage system reside behind a firewall in an internal network segment that allows only the necessary network traffic both in and out. While network configurations may vary depending on need and circumstance, below is an example diagram of a network that demonstrates proper network architecture:

## Network Diagram – Recommended Configuration




The traffic necessary for the normal function of mPower Beverage is listed in the table below:

| Protocol | Source IP(s) | Destination IP(s) | Port(s) | Inbound / Outbound | Description |
|---|---|---|---|---|---|
| HTTPS | Element | Address of payment processor: https://transaction.elementexpress.com | 443 | Outbound | Communication for transaction processing |
| HTTPS | Global | Address of payment processor: https://m0.globalpay.com:50000 | 443 | Outbound | Communication for transaction processing |
| HTTPS | T-SYS | Address of payment processor: https://gateway.transit-pass.com/servlets/TransNox_API_Serve | 443 | Outbound | Communication for transaction processing |
| XML | mPower Server | mPower Office | 11000 | Inbound/ Outbound | Communication to and from mPower Server |
| SQL | SQL Server | mPower Office, mPower Point of Sale | 1433 | Inbound/ Outbound | Communication to and from SQL database |

The only system service required by the Point of Sale application is SQL Server.

Other hardware and software requirements include:

**Supported Operating Systems**
Windows 7 Professional or Windows 8.1 Professional*

- 32-bit systems
  - Computer with Intel or compatible 1GHz or faster processor (2 GHz or faster is recommended.)
- 64-bit systems
  - 1.4 GHz or faster processor
- Minimum of 512 MB of RAM (2 GB or more is recommended.)
- 2.2 GB of available hard disk space

**Microsoft .NET is installed by default with Windows 7 and Windows 8.1 Professional; however, the Point of Sale requires .NET 4.0 or higher in order to run.*

**Supported Data Platforms/Databases**

- SQL Server 2008 R2 Express
- SQL Server 2012 Express

**Application Software Modules**

- mPower Server 1.2.1 282
- mPower Back Office 2.5.0.1056
- mPower Point of Sale 3.6.0.68

**Processing Hardware**

- Magnetic card reader, such as the MagTek 21073062 Dynamag Magnesafe Triple Track Magnetic Stripe Swipe Reader

## *2.3 Wireless Networks*

mPower does not broadcast anything over a wireless network or regular network without encryption. If mPower is installed onto a wireless network, the customer must address PCI-DSS requirements, such as:

A. Use of approved encryption technologies such as Wi-Fi Protected Access (WPA).
B. If using wireless networks, you should install perimeter firewalls between any wireless network and systems that store, process and/or transmit cardholder data. Perimeter firewalls must deny or control all traffic from the wireless environment coming into the cardholder data environment. Perimeter firewalls are designed to serve those users outside the internal network such as employees, remote users, etc. The following rules should be implemented when setting up perimeter firewalls, per Microsoft (http://technet.microsoft.com/en-us/library/cc700828.aspx#XSLTsection137121120120):
    a. Deny all traffic unless explicitly allowed.
    b. Block incoming packets that claim to have an internal or perimeter network source IP address.
    c. Block outgoing packets that claim to have an external source IP address (traffic should only originate from bastion hosts).
    d. Allow for UDP-based DNS queries and answers from the DNS resolver to DNS servers on the Internet.
    e. Allow for UDP-based DNS queries and answers from the Internet DNS servers to the DNS advertiser.
    f. Allow external UDP-based clients to query the DNS advertiser and provide an answer.
    g. Allow TCP-based DNS queries and answers from Internet DNS servers to the DNS advertiser.
    h. Allow outgoing mail from the outbound SMTP bastion host to the Internet.
    i. Allow incoming mail from the Internet to the inbound SMTP bastion host.
    j. Allow proxy-originated traffic from the proxy servers to reach the Internet.
    k. Allow proxy-responses from the Internet to be directed to the proxy servers on the perimeter.
C. WPA2 – Wi-Fi Protected Access 2 – This mode of wireless network provides stronger data protection and network access control. It provides a higher level of security allowing only authorized users access to the wireless network.
D. Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.
E. Removal of any default keys from affected wireless equipment
F. Transmission of cardholder data over a wireless network is not approved by MSI. Wireless networks transmitting cardholder data, per PCI DSS, require encryption of transmissions by using Wi-Fi protected access technology. Merchants should never rely exclusively on WPA2 to protect confidentiality and access to a wireless LAN. If WPA2 (Wi-Fi Protected Access 2 ) is used, PCI-DSS dictates the following:
    a. Use with a minimum 104-bit encryption key and 24 bit-initialization value
    b. Enable strong encryption by ensuring one of the following encryption methodologies is in place for any wireless transmissions:

        - Virtual Private Network (VPN)
        - Secure Sockets Layer (TLS) at 128 bit, or
        - WPA2 (Wi-Fi Protected Access 2 ) at 128 bits
    c. Change any other default values as applicable
    d. Rotate shared WPA2 keys quarterly (or automatically if the technology permits)
    e. Rotate shared WPA2 keys whenever there are changes in personnel with access to keys
    f. Restrict access based on media access code (MAC) address
    g. Update any firmware to help in supporting encryption for authentication and data transmission
    h. Update virus protection programs to include wireless virus signatures
G. Change wireless vendor defaults, including but not limited to:
    a. WPA2 encryption keys
    b. Default service set identifier (SSID)
    c. Disable SSID broadcasts
    d. Default passwords
    e. SNMP community strings
    f. Verify logging/auditing is enabled

Refer to PCI-DSS for more information on protecting wireless transmissions.

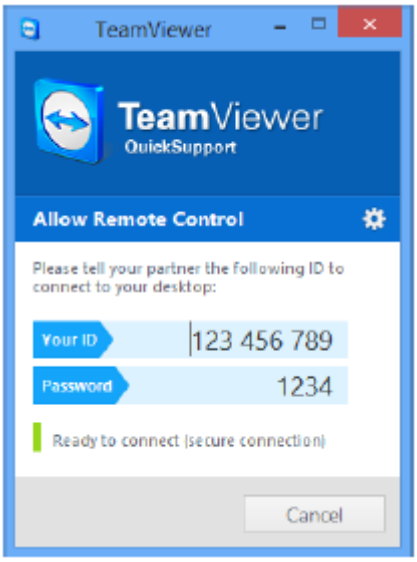
## *2.4 Remote Access*

**TeamViewer – Two-Factor Authentication**

mPower installs TeamViewer on mPower Server and SQL database systems in order to provide remote support for system-critical issues. TeamViewer offers two-factor authentication on a per-user basis, requiring a username and password at login, as well as a token supplied by Google Authenticator. All remote access must use two-factor authentication in order to meet PCI DSS requirements.

On any systems that do not have TeamViewer installed, a customer may also initiate a support request by following the steps below:

1. Go to http://www.mpowerbeverage.com.
2. At the top of the page, click on **Quick Support**.
3. Download TeamViewer.
4. Choose **Run**.
5. Your screen will say, “Loading TeamViewer now...” This may take a few moments. (You may also need to check the Downloads section of your browser to find the file to run.) If no window appears after several minutes, click on “Try Again” and repeat steps 3-5.
6. When the install is complete, a TeamViewer window like the one below will appear with your ID and password.




7. Provide mPower Support with your ID and password so they can establish a remote connection.

When used by vendors and business partners, TeamViewer should be activated only when needed and immediately deactivated after use.

The *PA-DSS Implementation Guide* advises customers and resellers/integrators to use all available remote access security features. Examples of security features that may be supported by remote access software are as follows:

- All users are assigned a unique ID for access to system components or cardholder data
- Two-factor authentication was observed to be implemented for remote network access
- Generic user IDs and accounts were observed to be disabled or removed
- Shared user IDs for system administration activities and other critical functions were not observed to exist
- Shared and generic user IDs were not observed to be in use to administer any system components
- Vendor ID has password policies/procedures that group and shared passwords are explicitly prohibited
- System administrators were interviewed to verify that group and shared passwords are not distributed, even if requested
- Passwords are changed every 45 days
- A minimum password length of at least seven characters is required
- Passwords containing both numeric and alphabetic characters are required
- New passwords that are the same as any of the last four are not allowed
- Repeated access attempts are blocked by locking out the user ID after not more than six attempts
- The lockout duration is set to a minimum of 30 minutes or until administrator enables the user ID
- If a session has been idle for more than 15 minutes, the user must re-enter the password to reactivate the terminal
- 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 and complex passwords for logins according to PCI-DSS Requirements 8.1, 8.3, and 8.5.8–8.5.15

It is strongly recommended that the end user use a securely configured firewall or personal firewall product. (See Section 8: **Antivirus Software**.)

## *2.5 Non-Console Administrative Access*

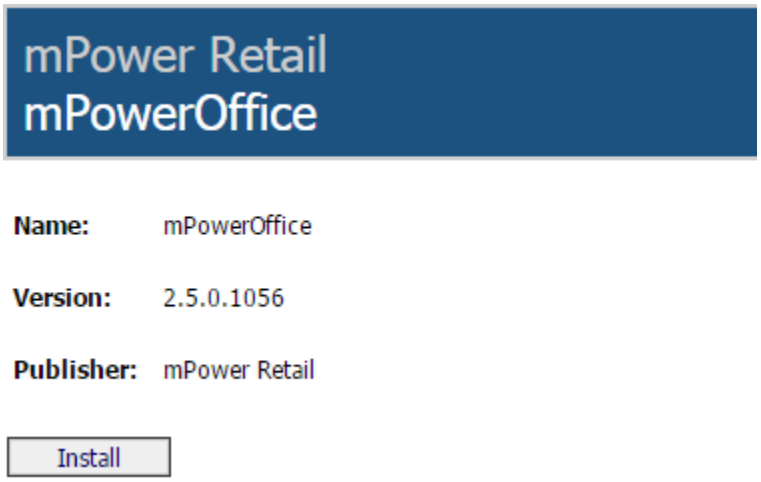
The use of a VPN is required for encrypted off-site access to mPower payment application or servers in the cardholder data environment. mPower does not permit or facilitate the sending of primary account numbers by end-user messaging technologies. mPower recommends the use of strong cryptography such as SSH, VPN or TLS for non-console administrative access.

# 3 INITIAL INSTALLATION

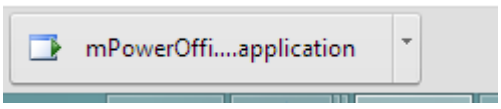
The implementation team at mPower performs the initial installation of the product on the system that will function as the mPower Server and all Office and Point of Sale machines. Customers are allowed unlimited licenses for the mPower Office product and will be issued a web link to the install site for that product. mPower Office must be installed on a Windows system (supported operating systems are listed above) with .NET 3.5 SP1 or higher.

Installation is user-specific, so each user that plans to run the software must install it under his or her Windows profile. mPower strongly recommends limiting user access in Windows such that only designated administrators can download and install software. For users that do not have administrative access in Windows, the installation will have to be run as an administrator by someone with access credentials. See section 6.4 – **Access Control** – for information on limiting administrative access for user accounts.

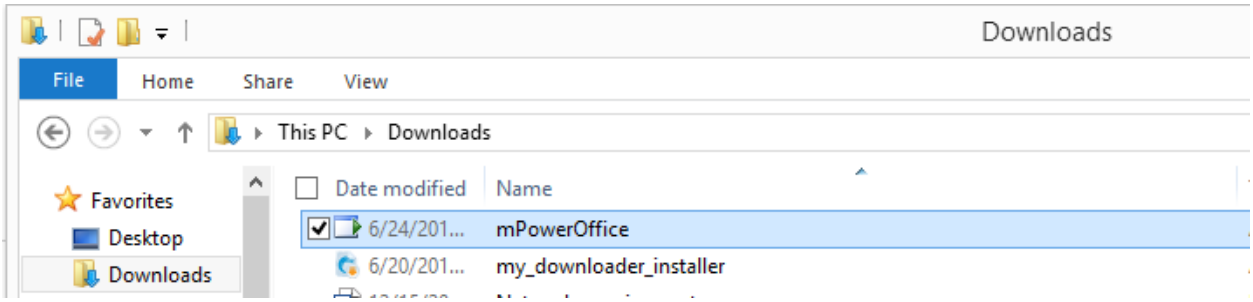
mPower software products are delivered securely through ClickOnce with TLS encryption and are signed via a GoDaddy code-signing certificate. The code-signing certificate checks the integrity of the deliverable to validate that none of the install files have been modified. To install mPower Office, log in as the intended user, go to the web link provided by the implementation team, and click on **Install**.



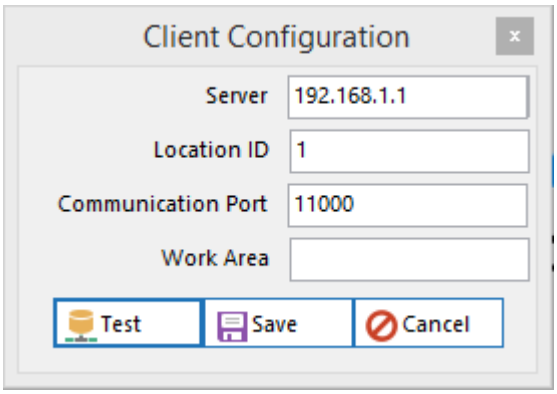

The application will download to your PC. To run the installation, either click on the download at the bottom left of your browser page:




or go to the Downloads folder on your PC and double-click the downloaded file:




A progress bar will appear, tracking the status of the installation. When the product is fully installed, the product will ask if you would like to set up the configuration file. Click **Yes** to see the configuration screen:




- **Server:** Enter the internal IP address of the machine that is running mPower Server
- **Location ID:** Enter the Location ID of the store (1, unless there is more than 1 location)
- **Communication Port:** 11000
- **Work Area:** [leave blank]

When all of the connection information has been entered, click **Test** to test the connection. If all settings are correct, the software will reply with, "Test Succeeded!" Click **OK**, then click **Save**. This will bring up the login prompt for mPower Office. For information on secure logins, see section 6: **User Management**.

For information on updates and application versioning, see section 8: **Software Updates**.

# 4 PREVIOUS SOFTWARE VERSIONS AND HISTORICAL DATA

## *4.1 Historical Data Removal*

Data will not need to be removed from any previous version of mPower as the application automatically masks previous information stored. No magnetic strip data, card validation codes, PIN's or PIN blocks were stored by previous versions of the software. (See Section 4.1, **Data Retention Settings**.)

The mPower product accepts transactions containing magnetic stripe data. This information is transmitted directly to credit card processors and is never stored. mPower integrates with credit card processing companies. The processing is all done through the processor, authorization and batch settlement functions. mPower acts as a secure interface to an outside credit card processor.

Merchants should avoid recording credit card numbers in any software application that has not been subject to PA-DSS. If such information is stored by another method or in another application, consistent, diligent removal of information that has reached the customer-defined retention period is absolutely necessary for PCI-DSS compliance. If the end user chooses to store cardholder data, they should store it on a system that is not public-facing.

# 5 DATA PROTECTION AND ENCRYPTION

## *5.1 Data Retention Settings*

mPower has a default retention period for cardholder data of forty-five (45) days, at which time the data is automatically purged. The retention period can be increased or decreased depending upon the requirements for the implementation. It can be changed in the System Configuration screen using the entry called *Credit Card Retention (in days)*.

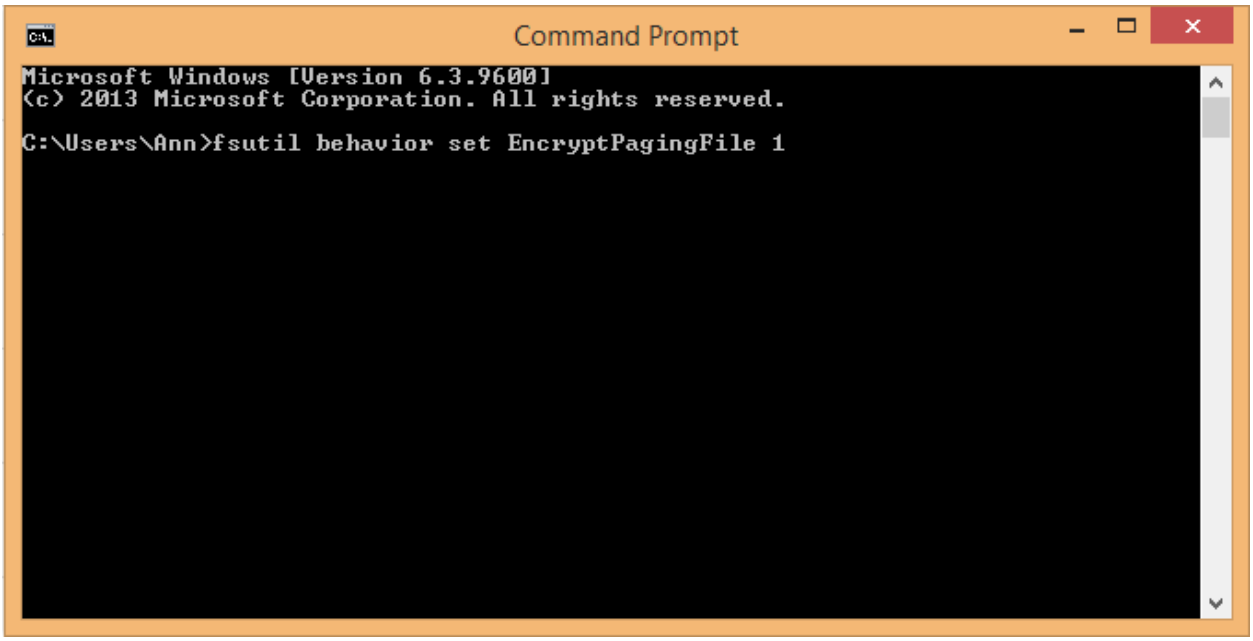

No cardholder data will be retained beyond the customer-defined retention period. Cardholder data is stored in the Customer_Preference table in the mPower database and can be manually purged from customer records, if necessary. Upon decommissioning of the mPower system, all cardholder information will be purged from the database. Cardholder data should not be stored on public-facing systems such as web servers.

### Preventing Inadvertent Cardholder Data Capture

Below is a step-by-step process showing the end user how to configure the underlying software or systems to prevent inadvertent capture or retention of cardholder data.

The following steps provide instructions for encrypting the page file in Windows 7:

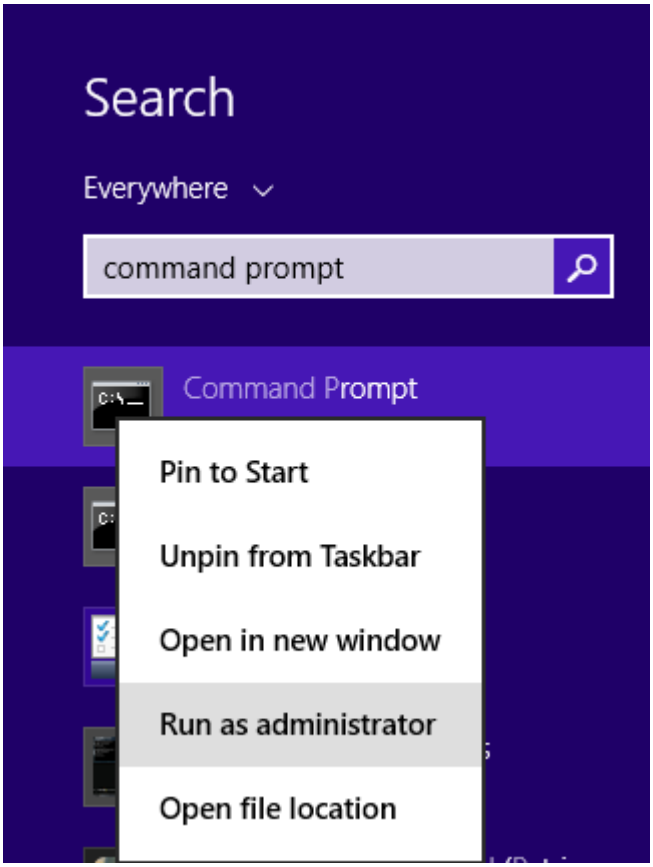
1. Go to **Start -> All Programs -> Accessories**.
2. Right-click on **Command Prompt**.
3. Click on 'Run as administrator.' (NOTE: Authentication credentials may be required. If a User Account Control window pops up, click **Yes** or enter valid administrator credentials.)
4. Enter the following text and press the ENTER key: **fsutil behavior set EncryptPagingFile 1**




5. Reboot the computer for the settings to take effect.
6. Verify that the system is encrypting by returning to Command Prompt, entering the following text, and pressing the ENTER key: **fsutil behavior query EncryptPagingFile**
   If encryption is properly enabled, the response should read: **EncryptPageFile = 1**

The following steps provide instructions for encrypting the page file in Windows 8.1:

1. Point to the lower-right corner of the screen, move the mouse pointer up, and then click **Search**.
2. In the search box, type: **Command Prompt**
3. Right-click on the program and choose 'Run as administrator.' (NOTE: Authentication credentials may be required. If a User Account Control window pops up, click **Yes** or enter valid administrator credentials.)




4. Enter the following text and press the ENTER key: **fsutil behavior set EncryptPagingFile 1**
5. Reboot the computer for the settings to take effect.
6. Verify that the system is encrypting by returning to Command Prompt, entering the following text, and pressing the ENTER key: **fsutil behavior query EncryptPagingFile**
   If encryption is properly enabled, the response should read: **EncryptPageFile = 1**

To further secure cardholder data, set the PC to clear the page file on reboot by setting/creating the following:

1. Start Registry Editor (Regedt32.exe) from Command Prompt.
2. Change the data value of the **ClearPageFileAtShutdown** value in the following registry key to a value of **1**: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management**
3. If the value does not exist, add the following value:
   Value Name: ClearPageFileAtShutdown
   Value Type: REG_DWORD
   Value: 1
4. Reboot the computer for the settings to take effect.

For the encrypted page file to be deleted nightly, each Point of Sale PC should be rebooted before or after use.

mPower Software does encourage all of its customers to create Windows restore points before installing any new software or hardware, and to back up the database to a non-premise computer or disk drive on a regular basis. Doing so does not expose the merchant or its customers to risk, since a) the restore point is not capturing data files, and b) any cardholder data contained in the backup is encrypted.

## *5.2 Data Encryption in Storage*

The management of encryption keys is largely handled automatically by mPower and requires limited action by mPower customers. Encryption keys are standalone keys, not bundles, and are encrypted by Chilkat using an AES 256 Bit Encryption algorithm. Encrypted keys are stored either in the registry or in the mPower database, depending on the application. There are no configurable options in the application that enable, disable, or change encryption; secure protocols are enabled by default and cannot be changed or undone.

The mPower suite of applications does not support the export of cardholder data. mPower strongly advises all customers not to export card data.

There are four types of encrypted keys generated by the mPower software; these are:

- **Application key**. This is the same for all instances of mPower, regardless of product or version.
- **Server key**. Unique to mPower Server (each instance) and stored in the registry on the customer's server computer.
- **Customer key**. Unique to each customer with a credit card on file – auto-generated when a credit card number is entered in the customer record. Customer key is stored, encrypted, in the mPower database.
- **Employee key**. Unique to each employee – auto-generated when a password is created for an employee. Employee key is stored, encrypted, in the mPower database.

The **Server key** can be changed from the mPower Server client. Customers should update this key at least once a year by clicking on **File -> Set Key**. The key that is stored in the registry will be replaced by a new encrypted key, and the old key will no longer exist on the system or in any databases. Irretrievability of old keys is a requirement for PCI DSS compliance.

**Customer keys** are rekeyed by an auto-rotator in mPower every thirty (30) days. Once the process is triggered within the software, all old keys are replaced with new keys. No historical cryptographic data is stored; expired keys are replaced with new keys, regardless of the software version, and are no longer stored anywhere in the database. This process happens independently of any software updates or upgrades, so reverting to an old version of the software does nothing to change the accessibility or usability of previously-used keys. To manually re-key customers, administrators can log into mPower Back Office and click on **System Utilities -> Re-Key Customers** to generate new keys and delete the old ones. Irretrievability of old keys is a requirement for PCI DSS compliance.

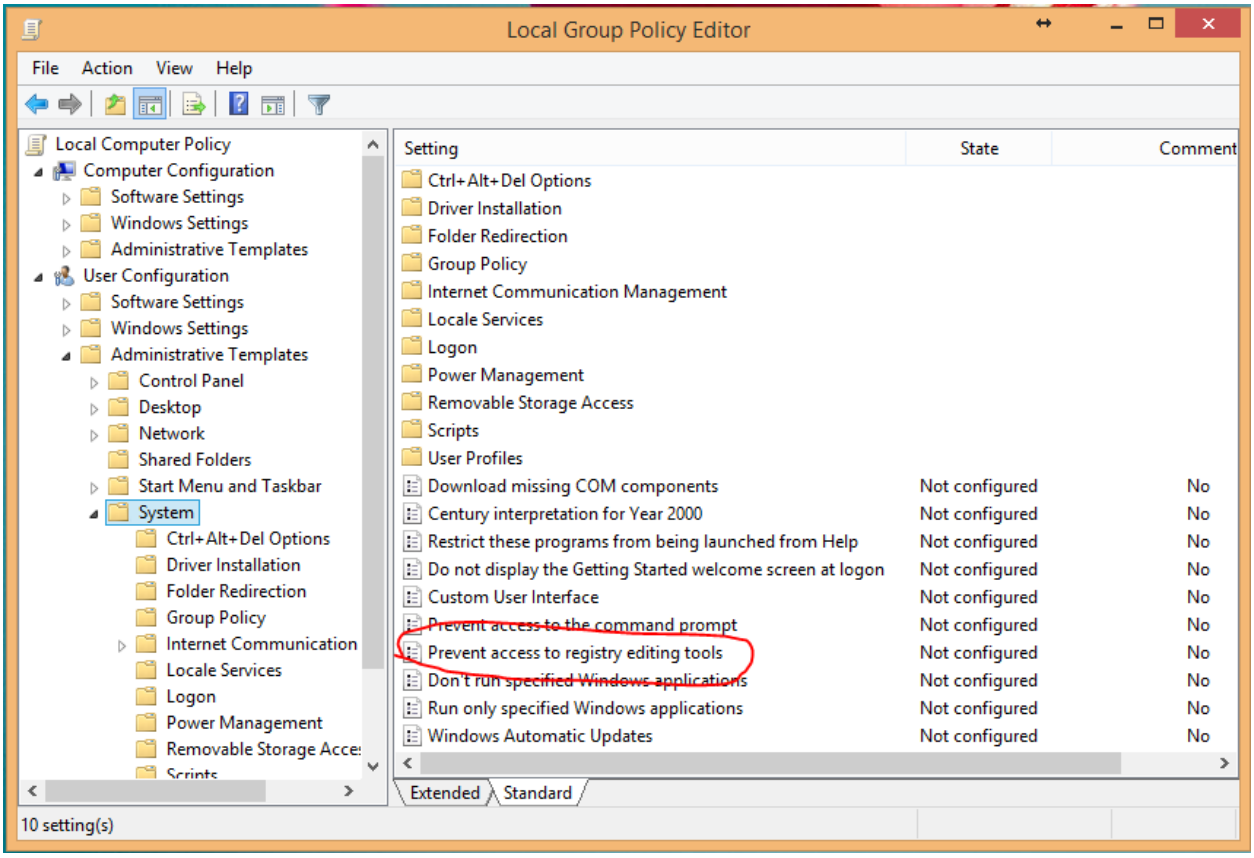
**Employee keys** are regenerated every ninety (90) days, when passwords expire. Once a password has expired and a new password has been entered, the new employee key is automatically generated within the database and replaces the old key. No historical cryptographic data is stored; expired keys are replaced with new keys, regardless of the software version, and are no longer stored anywhere in the database. This process happens independently of any software updates or upgrades, so reverting to an old version of the software does nothing to change the accessibility or usability of previously-used keys. To manually re-key employees, administrators can log into mPower Back Office and click on **System Utilities -> Re-Key Employees** to generate new keys and delete the old ones. Irretrievability of old keys is a requirement for PCI DSS compliance.

The customer is required to rotate server, customer and employee keys at a minimum of once a year and should always re-key when a major update is installed, when an employee leaves, or if some sort of compromise is suspected. **It is important to restrict access to keys to the fewest number of custodians necessary.**

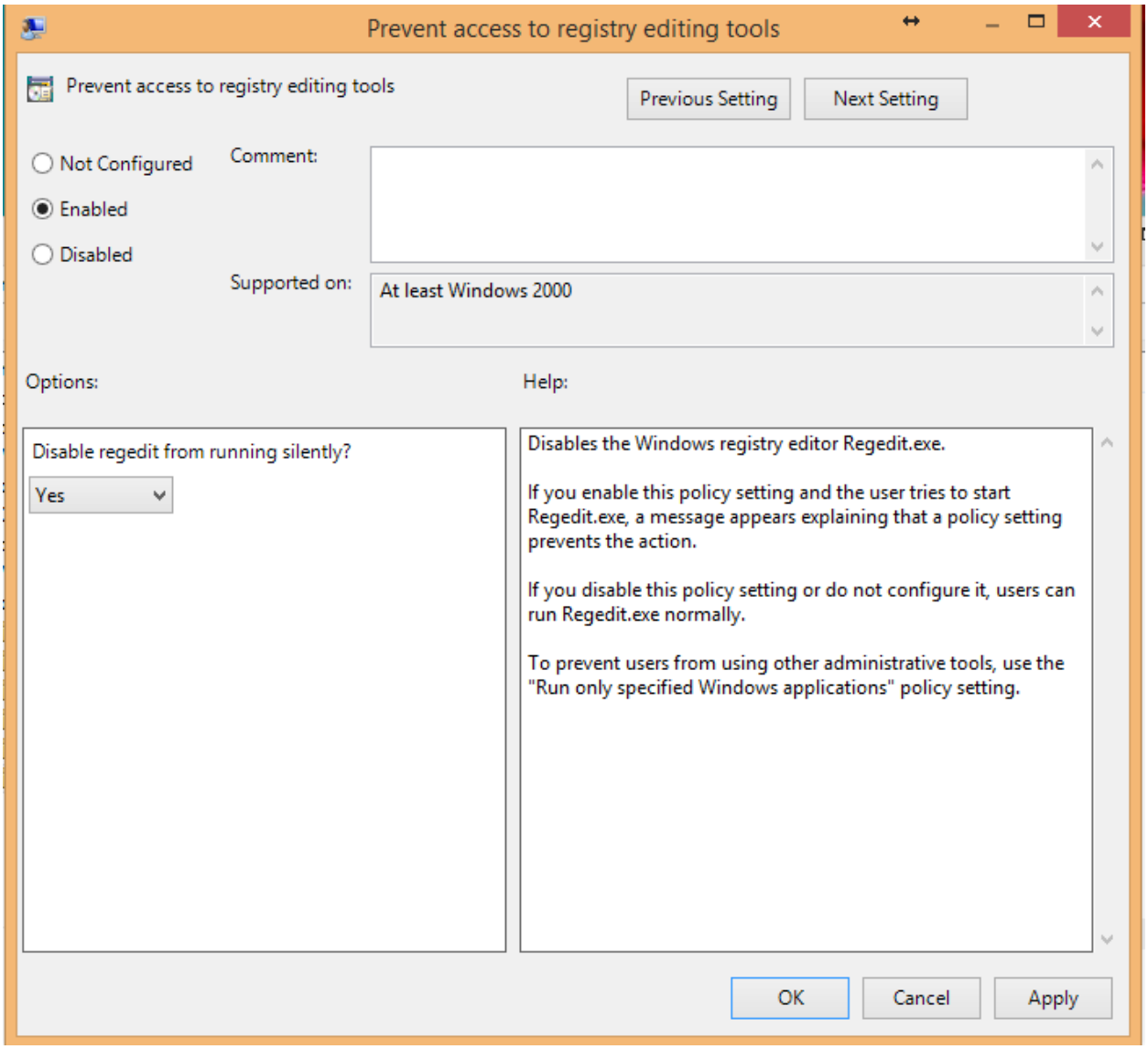
Key rotation encrypts historic data with new keys. The re-keying process unencrypts the data with the old key, generates a new key, and re-encrypts the data with the new key, replacing the old key with the new key in the database. The retired/replaced keys are deleted and are not stored anywhere in the database or on the host machine.

Restricting access to the computer on which encrypted keys are stored is another necessary step in ensuring the security of those keys. mPower recommends installing the SQL database on a dedicated server computer and placing the computer in a secure location in the office. Administrators should also restrict access to the registry on the server by following the steps below:

1. Hold down the Windows key on the keyboard and press R. This will open the 'Run' dialog box.
2. Type *gpedit.msc* and click **OK** to launch **Local Group Policy Editor**.
3. Go to **User Configuration -> Administrative Templates -> System**.
4. In the right panel, double-click on "Prevent access to registry editing tools."



5. In the next window, choose “Enabled.”




This will restrict access to the registry for all users.

mPower also strongly suggests that no one outside of mPower employees be given a SQL login or password. Windows Authentication for SQL Server should also be limited to the least number of accounts possible. To restrict access for a particular user:

1. Log into SQL Server.
2. In the left-hand pane, click on the plus sign next to **Security**.
3. Click on the plus sign next to **Logins**.
4. For each account that should NOT have SQL access:
   a. Right-click on the username and choose **Properties**.
   b. In the left-hand pane, select **Status**.
   c. Under “Login,” choose **Disabled** and click OK.

***Key Custodian Form:***

All Company staff that hold responsible authorized positions where they manage or handle encryption keys must sign the following document.

As a condition of continued employment with Company, and as an employee that has access to key management tools and equipment, you are obligated to sign the following to indicate acceptance of your responsibility.

The signatory of this document is in full employment with Company on the date shown below and has been afforded access to key management devices, software and equipment, and hereby agrees that, he or she

• Has read and understood the policies and procedures associated with key management and agrees to comply with them to the best of his/her ability, and has been trained in security awareness and has had the ability to raise questions and has had those questions answered satisfactorily.

• Understands that non-compliance with the key management procedures can lead to disciplinary action including termination and prosecution. Exceptions to compliance only occur where such compliance would violate local, state, or federal law, or where a senior officer of the company or law enforcement officer has given prior authorization.

• Agrees to never divulge to any third party any key management or related security systems, passwords, processes, security hardware or secrets associated with the Company systems, unless authorized by an officer of the Company or required to do so by law enforcement officers.

• Agrees to report promptly and in full to the correct personnel, any suspicious activity including but not limited to key compromise or suspected key compromise. Suspicious activity can include: signs of unauthorized equipment usage during evenings and weekends, phone requests from unidentifiable callers for access to secure information, unidentifiable files found on file servers, and unusual activity recorded in log files.

I agree to the above and understand that this original copy will be held on my personnel record and kept by the company indefinitely.

Signed: [_____] Witnessed: [_____]

Print Name: [_____] [_____]

Date: [_____]

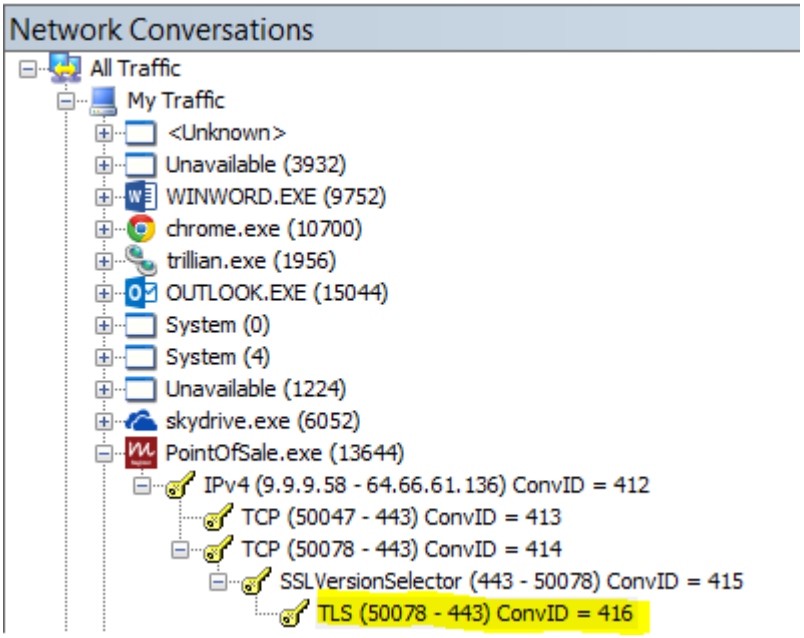
## *5.3 Data Encryption in Transmission*

mPower is intended and designed for deployment on a local merchant's private network. Exposure to a public network is not in the scope of product design; as such, sensitive cardholder data is not transmitted over a public network.

mPower utilizes strong cryptography whenever data is transmitted over public networks.

When cardholder data is sent out over the internet for processing, it is sent via TLS 1.2 with 128-bit encryption over an https connection (see the Protocol table under section 2.2 – **Network Security**). To verify that cardholder data is being encrypted in transit:

1. Run Microsoft Network Monitor 3.4.
2. Select 'Ethernet' as the network to monitor.
3. Click on **New Capture**.
4. Click **Start** to start the capture.
5. Process a card transaction using the Point of Sale and/or the Sales Order module in Back Office.
6. Click **Stop** to stop the capture.
7. Under 'Network Conversations,' expand **PointOfSale.exe**.
8. Continue to expand the selections until items have been expanded.
9. Under 'SSLVersionSelector,' look for the TLS encryption protocol that is being used:




# 6 USER MANAGEMENT

## *6.1 Unique User Accounts*

None of the mPower applications make use of built-in accounts that cannot be deleted. The only user account that is created as part of the software installation is the admin account, and it is created with a password that meets PA-DSS requirements. To delete this account, see instructions in section 5.4 of this document.

mPower utilizes the following login procedures:

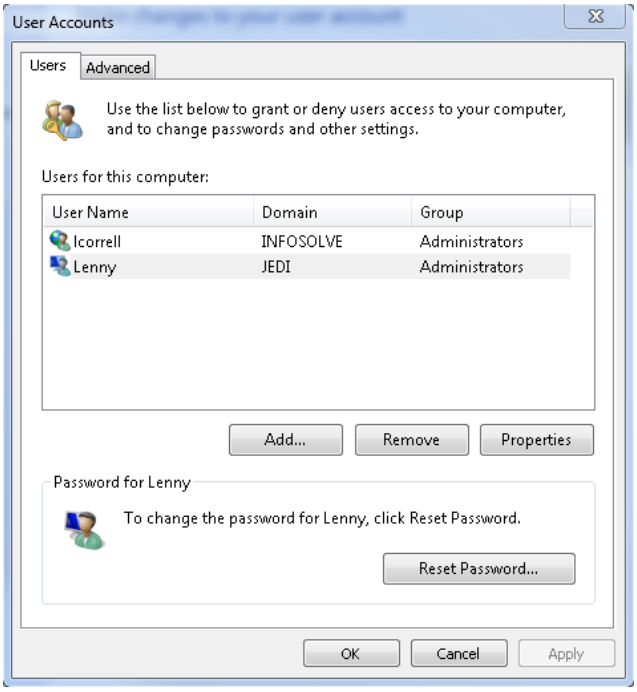
a. After an employee or user attempts to login to mPower and fails six (6) consecutive times, the account is locked and the mPower application is closed. Although mPower closes due to failed login attempts, the user retains his normal security rights on the Operating System and within other software products. Once an mPower account has been locked, the user cannot login for 30 minutes or until an administrator of mPower enables the user's account.
b. mPower strongly suggests that each user log into the OS under their own user account with a "strong" password. Since, after three login attempts, mPower closes the application and sends the user to the OS Desktop, it is advised that limited users be logged into the OS under their limited user account name. Administrators should be logged into the OS under their administrator login account.
c. All the password controls listed above should be used on the Operating System user accounts. These controls should especially be used on administrator accounts on the operating system.
d. Limit who has administrator rights for the Operating System.
e. Every user should be set up on the OS with their own username and strong password. They should be set up using a standard account, not an administrator account, as this helps prevent users from making changes to the operating system that would affect all users. If someone is an administrator, they should also have a standard account set up for them for day-to-day use.
f. The OS usernames and passwords should be unique and should not be the same as the usernames and passwords used for the mPower payment applications.
g. For more information on Operating System User Accounts and Control, go to: http://technet.microsoft.com/en-us/library/ee623984(WS.10).aspx for instructions on setting up limited user accounts.
h. Once a user is logged in and the mPower system has not been used for 15 minutes, mPower secures the application, and the user must re-enter their username and password. This process should be the same for the Operating System. If the computer has not been used for a specified amount of time (15 minutes), the OS should log out and require a username and password to log back into the Operating System desktop.
**i. You must require unique usernames and secure passwords within mPower. If you don't require these, the result will be non-compliance with PCI DSS.**

## *6.2 Strong Passwords*

*Administrative System Accounts*
In order to maintain PCI Compliance, "strong" passwords must be used in setting up administrator accounts for Windows, for the database in SQL Server and in the mPower Software solution. A strong password should appear to be a random string of characters to an attacker. Such a password should be a minimum of eight characters and include a combination of uppercase and lowercase letters, numbers, and symbols.

To set up strong passwords for Administrators, go to **Control Panel -> Users**. On this screen, you can set the appropriate rights for Administrators as well as change settings and passwords. To add new users, click **Add**, then follow the steps to set up new users. Once you get to the password screen, set strong passwords using the above guidelines. Each Cashier and Administrator must have his/her own username and password for the operating system.

See screen shot below:




mPower utilizes the following password guidelines:

a. Do not use administrative accounts for payment application logins.
b. Make sure passwords are unique for your operating system login, database login, and the mPower application.
c. Make sure that all default accounts, even if not used, are assigned with secure authentication.
d. If an account is not used, disable the account so it can no longer be used.
e. Each user must have a unique username within mPower and must only have access to his/her user account. When logging into the mPower payment application, you must always use your secure username and password. There should not be any group, shared or generic passwords.
f. Passwords must be at least 8 characters long.
g. Passwords must contain both numeric and alpha characters, upper and lower case.
h. Password cannot be re-used within the last four (4) password changes.
i. Password expires in 90 days.

mPower suggests that merchants not utilize administrative or other system accounts. Administrative system accounts should not be used for application logins.

## *6.3 Cashier Users*

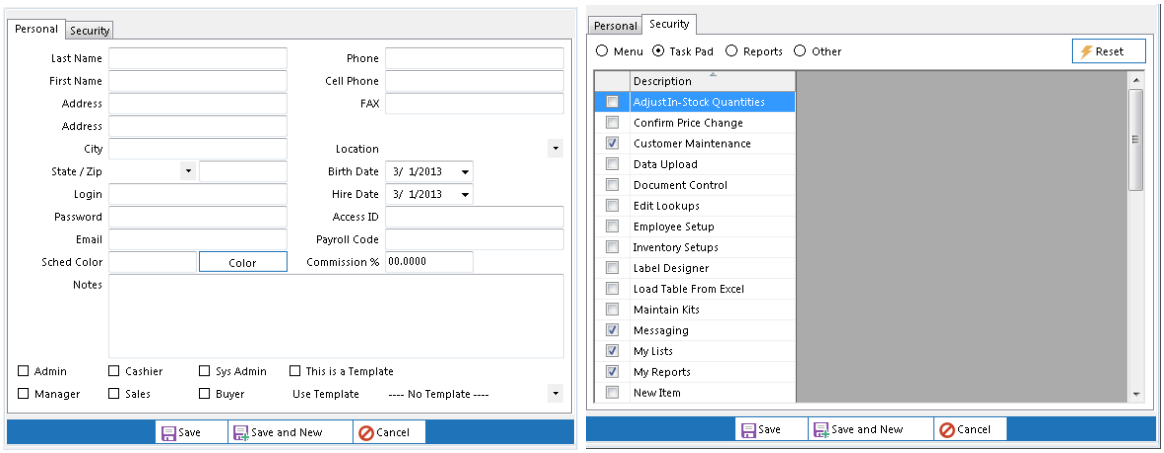
Cashier Users have direct access to all types of tender, including credit cards. While the Point of Sale does not store credit card information, it does allow for clear-text manual entry of PAN, in the event that a card does not swipe. That is why it is very important to make sure that each cashier, as well as every other user, logs into the register when the register is in use, and then logs out when it is no longer in use. Each Cashier will be given their own unique username and strong password. All transactions logged in mPower are associated with the cashier that is logged in during the time of the transaction.

## *6.4 Access Control*

The PCI-DSS requires that access to all systems with payment applications and/or cardholder data be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by more than one user or process. Additionally, any default accounts provided with operating systems, databases and/or devices should be removed/disabled/renamed, or at least should have PCI-DSS compliant complex passwords assigned and should not be used. Examples of default administrator accounts include “administrator” (Windows systems) and “sa” (SQL/MSDE).

As an administrator of mPower, you will have all the tools available to manage accessibility to the various functions within mPower. You can set unique usernames and passwords for each employee along with security rights governing access to the various functions within the software.

In order to set up access control for employees, you must login as an administrator, then go to our Employee screen. (See screen shot below.) From here, you can create employees and grant access to the various controls within mPower on an individual level.



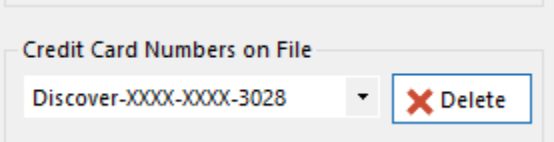

In mPower, the admin user account can be changed by editing the record. Or, after a new administrative clerk has been created, it can be removed in the database manager. Select the user account, then Record and Delete the account. In mPower, the password parameters are built within the code of the software and are required for all current and new employees. At the very least, the password for the admin account should be changed and all guidelines for strong passwords adopted, in accordance with PCI standards.

The only situations and locations in which the primary account number (PAN) on a credit card is readable in clear-text in the mPower software are:

1) Sales Order module in mPower Office - Manual entry of PAN in the Payment screen
2) Customer module in mPower Office – Initial (manual) entry of PAN for card to be kept on file
3) Point of Sale tender screen – Manual entry of PAN if a card will not swipe

This information will appear on the display only, so that the user can verify that he or she has entered the card number correctly. PAN is masked by default on all other displays, and even when manually entered, will not be printed on the receipt or stored in the database in clear-text, so no logging or reporting can capture this information for output, either. In fact, cardholder data should not be stored at all unless the customer requests that their card information be kept on file, and it should be securely deleted when no longer required for business purposes. Cards stored on file are encrypted as described in section 5.2 – **Data Encryption in Storage** – and can only be used as payment for Sales Orders. These card numbers are not accessible by the Point of Sale, so a

customer cannot use a card on file to purchase items at the register. To delete a stored card, a user with access to the customer screen needs only to choose the masked card from the drop-down list and click **Delete**. Doing so will purge the card information securely and completely from the database and the system.




Because of the sensitive nature of the data that is being handled, **access to the Point of Sale application and the Sales Order module must be limited to those individuals who have a legitimate business need to view full PAN.** The Point of Sale installs under specific user accounts in Windows and is limited to a certain number of registers (however many the customer purchases). Any mPower profile can log into the Point of Sale, since the application is the lifeblood of a retail store. To properly secure the application, then, it will be necessary to a) install the Point of Sale for just those users that will be functioning as cashiers, b) set Windows to lock the screen after 15 minutes, and c) enable logging (see section 7.1 – **Logging Configuration**).

To verify that a user is not a member of the Administrators group:

- Go to **Computer Management**.
- Click on the arrow next to 'Local Users and Groups.'
- Click on the **Groups** folder.
- Double-click on 'Administrators.' The members of the Administrators group are listed here.
- To remove a member, highlight that member's name and click **Remove**.
- If the user is currently logged in, changes will not take effect until he/she logs out and back in.

To lock your computer after 15 minutes of inactivity on Windows 7:

- Go to **Appearance and Personalizations**
- Go to **Screen Save Settings**
- Adjust wait time to **15 minutes**
- Choose a screen saver and check the box next to 'On resume, display logon screen'

To lock your computer after 15 minutes of inactivity on Windows 8.1:

- Go to **Control Panel -> Hardware and Sound -> Power Options**
- Click on **Change when the computer sleeps**
- Set both 'Turn off the display' and 'Put the computer to sleep' for **15 minutes**
- Click on the **Save changes** button

  To require a password:
- Go to **Control Panel -> Hardware and Sound -> Power Options**
- Click on **Require a password on wakeup**
- Under 'Password protection on wakeup,' select **Require a password**

To limit user access to the Sales Order module:

- Go to **Database -> Employee**
- From the Maintain – Employee window, select a specific user account and click the **Edit** button
- Click on the Security tab
- Select **Task Pad**
- Verify that both 'New Sales Order' and 'Sales Order Maintenance' are unchecked. If they are checked, uncheck and click on **Save**.

*NOTE: The Sales Order module is not enabled by default, so these options may not be visible. If they are not enabled, the Sales Order screen with the Payment option cannot be launched.*

## *6.5 User Accounts for Additional Components*

Please use caution when setting up user accounts on any additional components that are running or have access to systems running mPower. All passwords for additional components should comply with the standard for PCI compliance and each user for those components should have a unique account. This includes logins for routers, servers, and any other system using mPower.

# 7 EVENT LOGS AND AUDITING

## *7.1 Logging Configuration*

"Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs." (Payment Card Industry (PCI) Data Security Standard doc, p. 55, v 2.0, October, 2010)

### mPower Beverage Logging

mPower Beverage includes a logging system that logs changes to the following:

- **Transactions**
  - Employee running the transaction
  - The amount of the transaction
  - The Credit Card processing approval code
  - Tender type used for the transaction
  - If items were deleted from the transaction
  - If the cashier voided the transaction

For every credit and debit transaction, mPower logs:

- Type of event
- Origination of event
- Affected data, system component, or resource
- Date and time
- Card type used
- Success or failure indication
- Username
- Approval code

- **Customer Accounts -** mPower logs any change to customer account records.

- **Documents -** Within mPower office, logs are created via documents that show who created each document, what they did and what action was taken. These documents include but are not limited to: purchase orders, receiving, sales orders, transfers, item movement history, adjustments, purchase requests, and price changes.

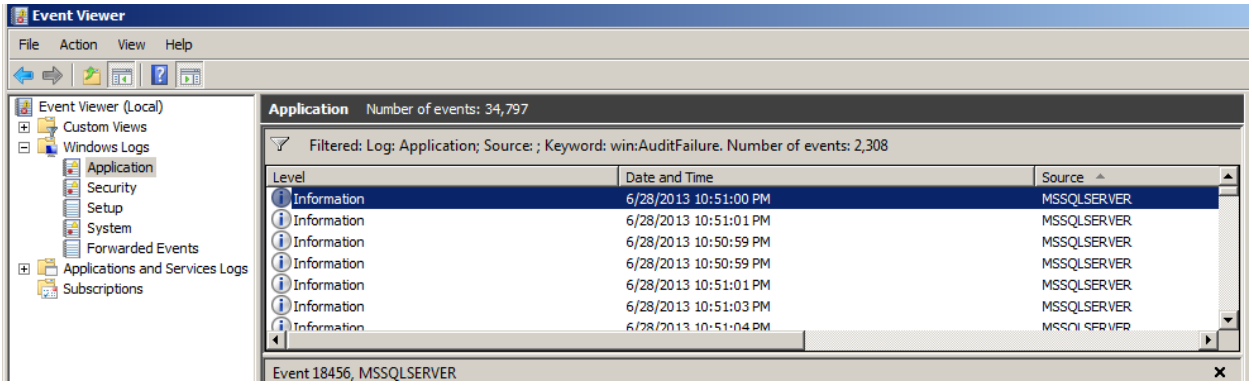
System logging is enabled by default in mPower and cannot be disabled or turned off. The log file, *mpower.ldf*, records all activity associated with the database. This log file should only be able to be accessed by a system administrator; other users should be excluded from access via Windows security settings. The log file is found under the C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA folder.

Trained mPower programmers use Red Gate software to open, view, and evaluate this log file, when necessary. The following information is included in the information captured:

- Individual access to cardholder data
- Actions taken by any individual with administrative privileges
- Access to application audit trails managed by or within the application
- Invalid logical access attempts
- Use of payment application's identification and authentication mechanisms, and all changes, additions, deletions to application accounts with root or administrative privileges
- Initialization, stopping or pausing of application audit logs
- Creation and deletion of system level objects within or by the application

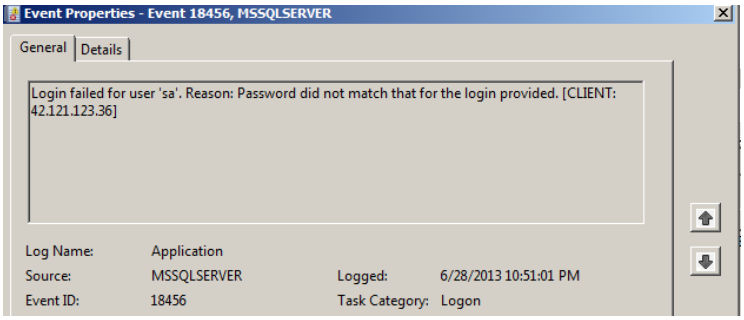
## Windows Event Log

Windows logs should be activated on every computer and must be monitored on every computer in the mPower Beverage system. Logging should not be disabled; doing so will result in non-compliance with PCI DSS. To monitor the logs, view logon and logoff attempts and other management movement, go to the Windows Event Viewer (shown below). If you are using Event Viewer properly, only system administrators should have access to this feature. Go to **Control Panel -> Administrative Tools -> Event Viewer**




- Highlight **Application**
- Right-click on **Application** and click on **Find**, type in *MSSQLSERVER*, and press ENTER

Each row in the list represents an event. To view detail on the event, highlight it, right-click on it and choose **Event Properties** to bring up the window below.




**Event Properties** provides additional detail on the event, including:

- User identification
- Type of event

- Date and time stamp
- Success or failure indication
- Origination of event
- Affected data, system component, or resource

To filter event data for specific records (failed login attempts, for instance):

- Right-click on **Application** and click on **Filter Current Log**
- Click on the drop-down box next to "Keywords" and, for this example, select **Audit Failure**

The list of results will include only those items that have to do with audit failures. This list can then be exported; simply right-click on **Application** and click on **Save Filtered Log File As…** Choose a folder in which to save the file and enter a filename. Leave "Save as type" set to **Event Files (*.evtx)** and click on **Save**. This file can then be sent to a processor or other party for further examination, if needed.

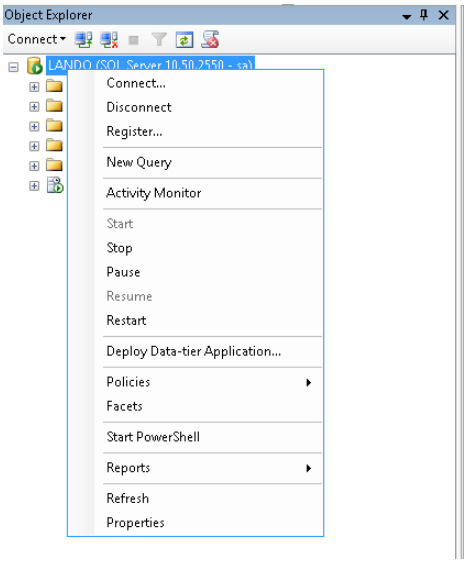
## SQL Logging

SQL Server logs all activity, including queries, in the transaction log by default.

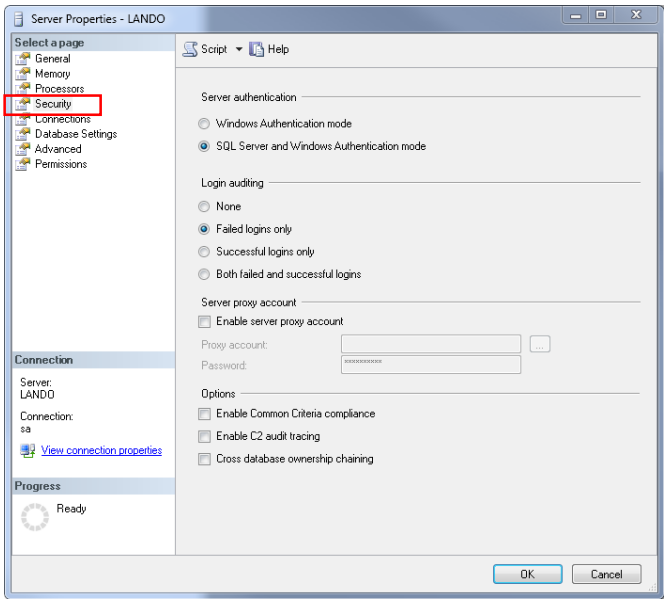
To audit security-specific records within Microsoft SQL Server, follow the steps below to enable C2 Audit Tracing or refer to the following link from the Microsoft Developer network website, http://msdn.microsoft.com/en-us/library/ms187634(v=SQL.100).aspx. Logging should not be disabled; doing so will result in non-compliance with PCI DSS.

### Enabling C2 Audit Tracing

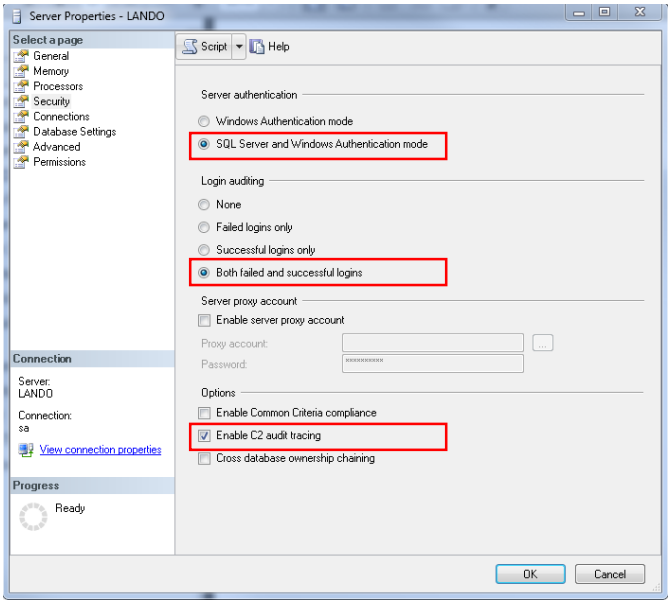
1. Within Microsoft SQL Server Management Studio, select the appropriate Server. Right-click the Server and select **Properties**.




2. Click on **Security** in the left pane.




3. Follow these steps:



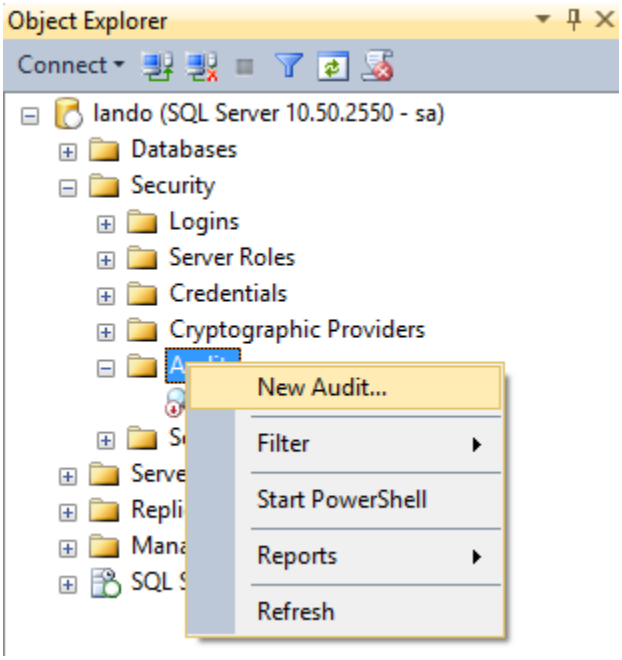

- Within the “Server authentication” section, select the “SQL Server and Windows Authentication mode” option, as shown above.
- Within the “Login auditing” section, select the “Both failed and successful logins” option.
- Within the “Options” section, select the “Enable C2 audit tracing” option.

The C2 audit log file is stored at C:\Program Files\Microsoft SQL Server\Data as AuditTrace_yyyymmddhhmmss.trc, indicating when the log file was created. A new file is automatically created in the same folder every 200MB as long as there is disk space. To review the data, double-click on the appropriate trace file, which will open in SQL Profiler.

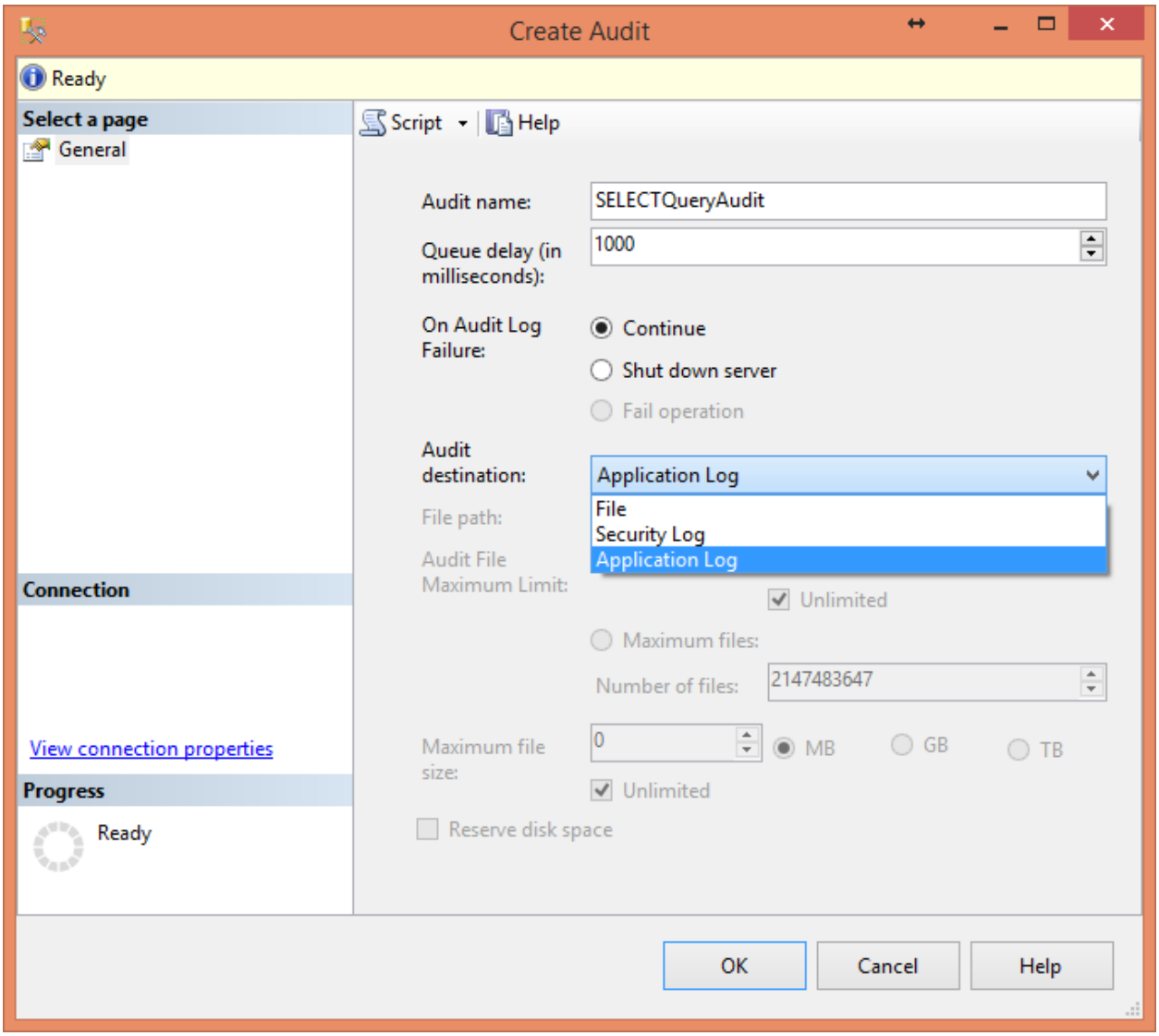
## Enabling SQL Logging to Windows Event Viewer

To incorporate the payment application logs into a centralized logging environment per PA-DSS requirements, SQL Server audits can be created and configured to log to the Windows Security Log or Applications Event Log. Below are the steps for enabling a Database Audit Specification for a SELECT query.

1. Create a new audit object within SQL Server Management Studio. Go to **Security -> Audits**, right-click on **Audits**, and choose **New Audit**.



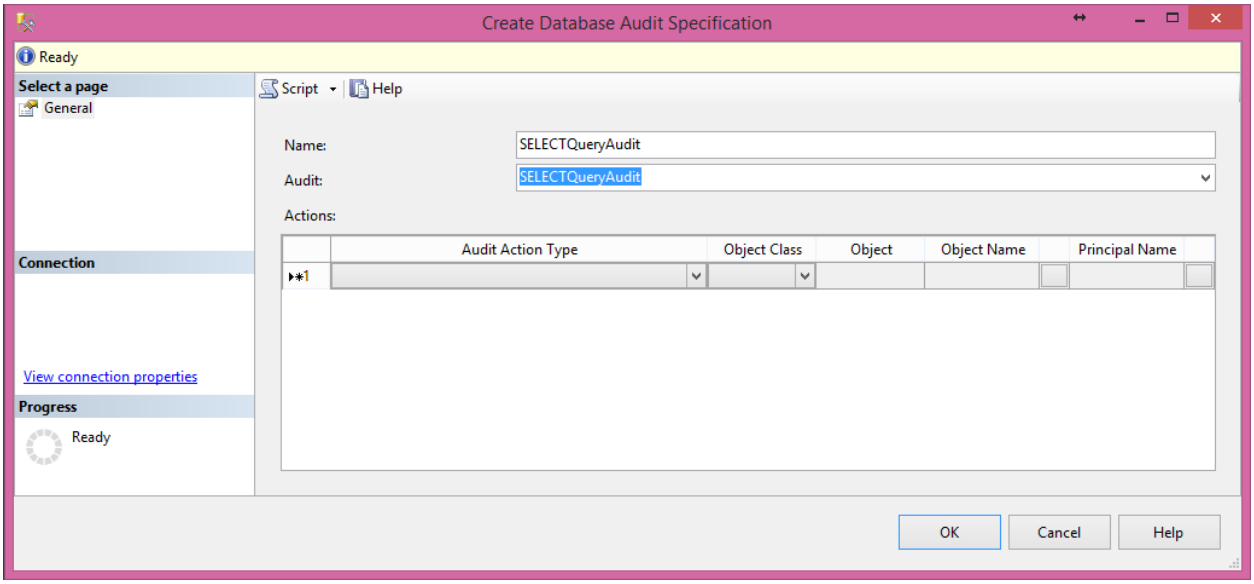

2. Create the Audit



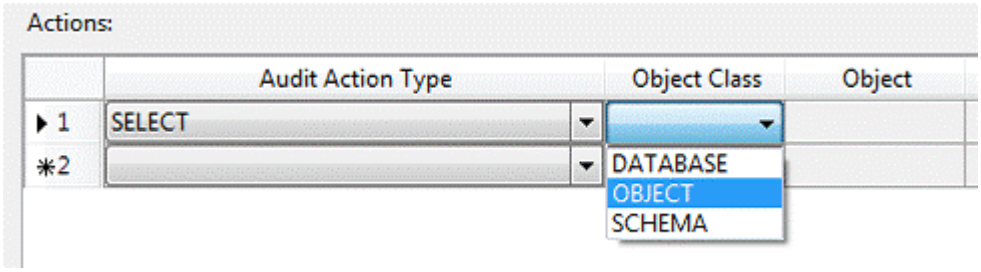

- Enter a name for the Audit that describes the type of records that will be logged.
- Leave the "Queue delay" set to 1000.
- For "On Audit Log Failure," choose **Continue**. *Not doing so could result in a failure to restart SQL and subsequent failure of the dependent mPower software modules*.
- For 'Audit destination,' choose **Application Log** from the drop-down box.
- Click **OK**. You should now see the audit you just created under **Security -> Audit**.

3. Create a Database Audit Specification

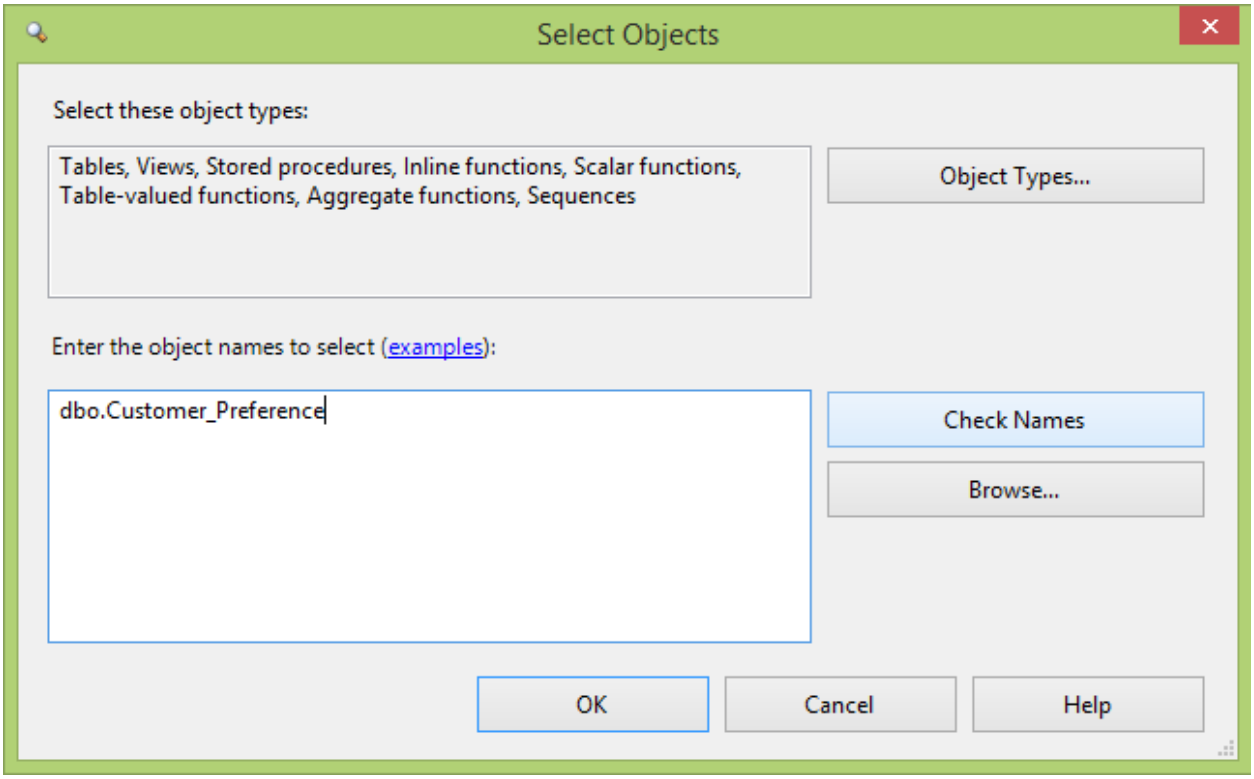
- Under **Databases**, go to the mPower database and click on the plus sign to the left to expand the selection.
- Go to **Security**, expand the selection, and right-click on **Database Audit Specification**. Click on **New Database Audit Specification**.



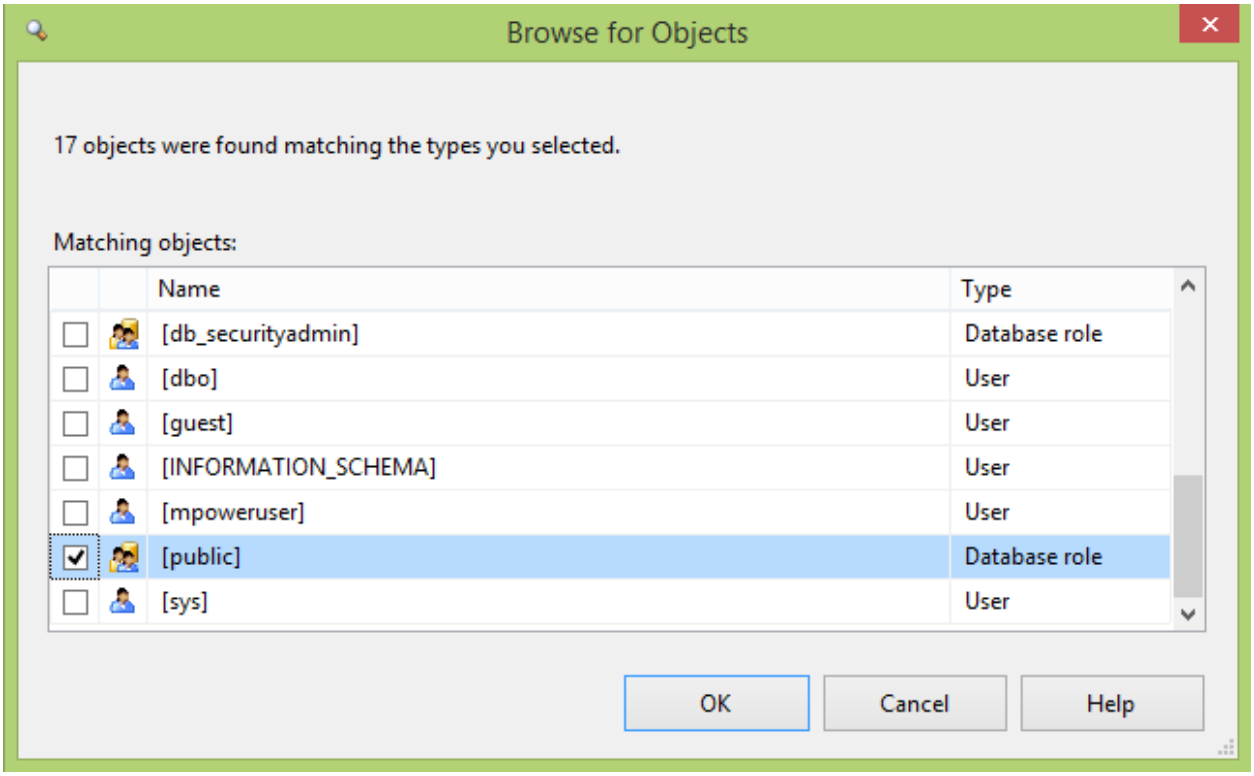

- Enter the name of the audit specification (it can be the same as the name of the Audit you just created).
- Select the Audit you created from the drop-down box.




- Click on the drop-down arrow under “Audit Action Type” and choose **SELECT**.
- Click on the drop-down arrow under “Object Class” and choose **OBJECT**.
- Click on the **…** button under “Object Name.” The following window will appear:




- To limit the amount of data that is exported to the event log, enter the name of the table or tables whose data you would like to review. (We have listed one of the customer databases above.) Click **Check Names** to validate the table name. Then click **OK**.
- Click on the **…** button under "Principal." A 'Select Objects' window similar to the one above will pop up. Click on **Browse**.




- To retrieve records for all users, select **[public]** from the list of users by checking the box to the left.
- Click **OK**.

4. Enable Audit

- Audits are not started by default. To start logging data to the Windows application log, first go to the audit object created in steps 1 and 2. Right-click on the audit object and choose **Enable Audit**.
- Next, go to the Database Audit Specification (created in step 3), right-click, and choose **Enable Audit**.

Data can now be viewed through Event Viewer (see *Windows Logs* section above).

Note that many other types of logs can be recorded, including login/logout activity and other types of queries. See http://msdn.microsoft.com/en-us/library/cc280386.aspx for additional detail.

# 8 SOFTWARE UPDATES

## *8.1 Application Updates*

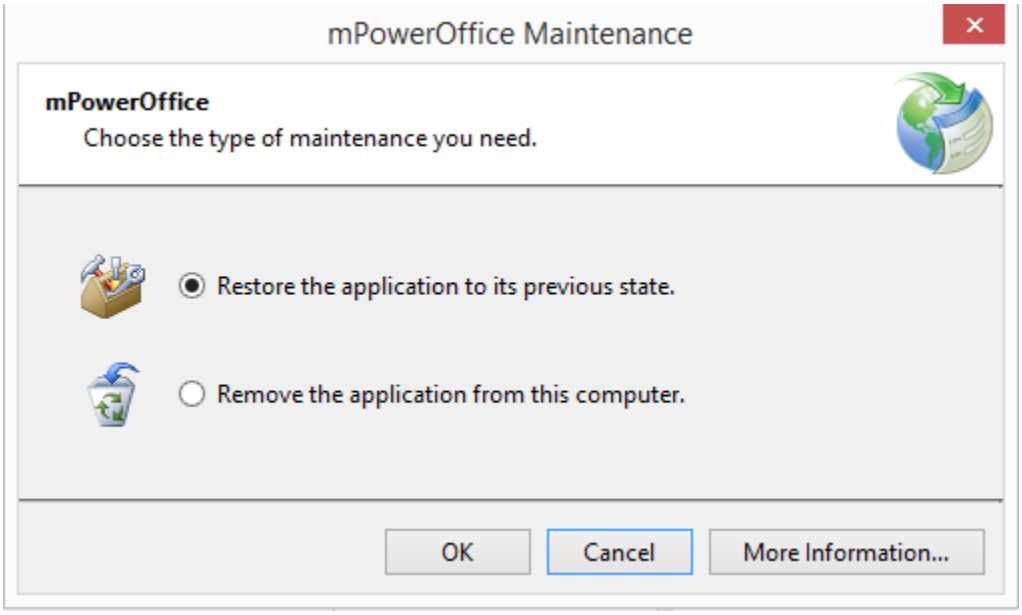
mPower programs check for updates upon application startup (when a user launches the program). Upgrades or updates to the mPower software are delivered securely through ClickOnce with TLS encryption and are signed via a GoDaddy code-signing certificate. The code-signing certificate checks the integrity of the deliverable to validate that none of the install files have been modified. mPower recommends that customers establish an internal policy and/or standard operating procedure with employees pertaining to software updates and upgrades.

When a user launches an mPower application, the program checks for updates. If no update is available, the user will be prompted to log in normally. If an update is available, a dialog box will pop up saying, “A new version of

[mPower Office] is available. Do you want to download it now?" If the user clicks **OK**, the new update will be downloaded and installed. If the user chooses to **Skip** the update, no more prompts will pop up until the next release is issued.

Any update can be rolled back to the previous version through the following process:

1. Go to **Start -> Control Panel -> Programs and Features**.
2. Highlight the mPower program to be rolled back by clicking on it.
3. Click **Uninstall/Change** from the menu bar.
4. A window will pop up with two options:




5. Choose "Restore the application to its previous state" to roll back to the previous version.

If the release is a major version update, **all cryptographic keys in the system must be re-keyed**. See Section 4.2 of this document for instructions on re-keying. mPower defines major and minor version updates (as pertains to PA-DSS) as follows:

- A **major update** (or **High Impact Change**) is defined as a change that has a high impact on PA-DSS requirements. This would include changes to code involving the following:
  - Sensitive Authentication Data
  - Remote Access
  - Default Passwords
  - Protection of Stored PAN

Updates such as these would be signified by a change in the second number in the version set. For example, if the original version were 1.2.1.290, the new version would be 1.**3**.1.290.

- A **minor update** (or **Low Impact Change**) is defined as a change that has a low impact on PA-DSS requirements. This would include changes to code involving the following:
  - Inclusion of minor updates or patches to supported OS versions upon which the Payment Application was previously validated
  - Inclusion of minor updates or patches to supported third-party databases with which the Payment Application was previously validated

- Additions or deletions of supported payment processors
- Inclusion of minor updates or patches to supported middleware with which the Payment Application was previously validated
- Recompilation of unchanged code base with either the same compiler using different flags or with a completely different compiler

Updates such as these would be signified by a change in the third number in the version set. For example, if the original version were 1.2.1.290, the new version would be 1.2.**2**.290.

- A **No Impact** or **Wildcard Change** is defined as having no impact on PA-DSS requirements. Examples are:
  - Administrative, such as an application name change
  - A revision to any previously listed mPower application that has no impact on PA-DSS

Updates such as these would be signified by a change in the fourth number in the version set. For example, if the original version were 1.2.1.290, the new version would be 1.2.1.**291**.

"Wildcards" are never used for any change that has an impact on security or PA-DSS requirements. If the last number in the set increments, the change has no impact on security and represents a non-security-impacting change. No other elements of the version number will be added to indicate a wildcard change (to the right, for example). Any security-impacting changes will increment either the second or third version sets, to the left of the wildcard designation, in accordance with the **High Impact** and **Low Impact** descriptions listed above.

Within the policy the customer creates for upgrading and updating software applications, the following criteria should be considered.

a. Management approval is needed for all software upgrades and updates.
b. If remote software is needed to update, authentication for use of technology should be validated.
c. You should list all the devices that need updates and the personal with access to those devices.
d. All devices should be labeled with the owner, contact information and purpose of upgrade and update.
e. Make a list of acceptable uses of the technologies.
f. Make a list of acceptable network locations for the technologies to reside.
g. Make a list of company approved products.
h. Once the software has been updated and/or upgraded, the upgrade session should be disconnected after a specified period of time or a specified period of inactivity at the location.
i. Vendors should only have access when needed and authorized by the customer and should be immediately disconnected and deactivated after use.

Release Notes for Back Office and Point of Sale application updates are published to mPower's web site at:
http://www.mpowerbeverage.com/officereleasenotes
http://www.mpowerbeverage.com/registerreleasenotes

Please review the Release Notes for any software release(s) before downloading to your systems.

# 9 ANTIVIRUS SOFTWARE

*Malicious software, commonly referred to as "malware" – including viruses, worms, and Trojans – enters a network via many business-approved activities, including employee e-mail and use of the internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Antivirus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.*

In accordance with the PCI Data Security Standard, mPower Beverage mandates regular use and regular updates of antivirus software.

Antivirus software must be deployed on all systems commonly affected by viruses, particularly personal computers and servers.

To ensure your antivirus software is set up in compliance with requirement 5 of the PCI Data Security Standard, "Use and regularly update anti-virus software," please consult the PCI Security Standards Council website, https://www.pcisecuritystandards.org.

# 10 TROUBLESHOOTING AND SERVICE

When troubleshooting issues, mPower will not collect any magnetic stripe data, card validation codes, PINs or PIN blocks at any time. mPower users should not collect or distribute any magnetic stripe data, card validation codes, PINs or PIN blocks during the process of troubleshooting any issues they might encounter.

If you must collect cardholder data for any reason during troubleshooting, make sure to:

- Collect data only when needed to solve a specific problem
- Store data only in a specific, known location with limited access
- Collect as little data as necessary to solve the specific problem
- Encrypt data when stored
- Securely delete data immediately after use

**About This Guide**

mPower Retail will distribute this PA-DSS implementation guide to all customers. The PA-DSS Implementation guide will be utilized in the training of all mPower customers regarding the use of the credit processing through mPower. mPower's Training and Install team will use the guide to construct training plans consistent with the recommendations contained with the PA-DSS Implementation Guide.

**Contact Information**

**mPower Software**
8330 LBJ Freeway, Suite B520
Dallas, TX 75243
Phone – 972-234-5884
Fax – 972-234-5856
www.mpowerbeverage.com