QS/1 PaySentry®
Card Transaction Tool

Payment Application Data Security Standard (PA-DSS)

PaySentry Implementation Guide

Version 19.4.x
## History of Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision History</th>
<th>Revision Class</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 17, 2008</td>
<td>19.1.0</td>
<td>Major</td>
<td>Initial Publication</td>
</tr>
<tr>
<td>January 20, 2009</td>
<td>19.1.1</td>
<td>No Change</td>
<td>No changes to the meaning or language of technical content</td>
</tr>
<tr>
<td>January 22, 2009</td>
<td>19.1.1</td>
<td>No Change</td>
<td>No changes to the meaning or language of technical content</td>
</tr>
<tr>
<td>May 27, 2010</td>
<td>19.1.1</td>
<td>Minor</td>
<td>Initial Setup Revision</td>
</tr>
<tr>
<td>April 25, 2013</td>
<td>19.2.0</td>
<td>Major</td>
<td>Incorporated v2.0 Updates</td>
</tr>
<tr>
<td>July 12, 2013</td>
<td>19.2.0</td>
<td>Minor</td>
<td>Diagram Update</td>
</tr>
<tr>
<td>July 23, 2013</td>
<td>19.2.0</td>
<td>No Change</td>
<td>No changes to the meaning or language of technical content</td>
</tr>
<tr>
<td>August 14, 2013</td>
<td>19.2.0</td>
<td>Minor</td>
<td>Diagram Update</td>
</tr>
<tr>
<td>September 24, 2013</td>
<td>19.2.0</td>
<td>No Change</td>
<td>No changes to the meaning or language of technical content</td>
</tr>
<tr>
<td>February 24, 2014</td>
<td>19.2.0</td>
<td>No Change</td>
<td>No changes to the meaning or language of technical content</td>
</tr>
<tr>
<td>June 23, 2014</td>
<td>19.2.0</td>
<td>No Change</td>
<td>No changes to the meaning or language of technical content</td>
</tr>
<tr>
<td>September 26, 2014</td>
<td>19.2.0</td>
<td>Minor</td>
<td>Diagram Update</td>
</tr>
<tr>
<td>April 22, 2015</td>
<td>19.2.0</td>
<td>No Change</td>
<td>No changes to the meaning or language of technical content</td>
</tr>
<tr>
<td>May 20, 2015</td>
<td>19.3.x</td>
<td>Major</td>
<td>Update to include PA-DSS v3.0</td>
</tr>
<tr>
<td>December 2, 2015</td>
<td>19.3.x</td>
<td>Minor</td>
<td>Update to include PA-DSS v3.1</td>
</tr>
<tr>
<td>November 4, 2016</td>
<td>19.3.x</td>
<td>No Change</td>
<td>No changes to the meaning or language of technical content</td>
</tr>
<tr>
<td>September 14, 2017</td>
<td>19.4.x</td>
<td>Minor</td>
<td>Updated to include PTS Device Dependencies</td>
</tr>
</tbody>
</table>
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction to Security</td>
<td>5</td>
</tr>
<tr>
<td>1.1 Payment Card Industry Data Security Standard (PCI-DSS)</td>
<td>5</td>
</tr>
<tr>
<td>1.2 Payment Application Data Security Standard (PA-DSS)</td>
<td>5</td>
</tr>
<tr>
<td>2. Glossary of Terms</td>
<td>6</td>
</tr>
<tr>
<td>3. Compliance</td>
<td>10</td>
</tr>
<tr>
<td>4. PaySentry Setup</td>
<td>11</td>
</tr>
<tr>
<td>5. Security Validation</td>
<td>13</td>
</tr>
<tr>
<td>5.1 Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2) or PIN block data</td>
<td>13</td>
</tr>
<tr>
<td>5.2 Protect stored cardholder data</td>
<td>13</td>
</tr>
<tr>
<td>5.3 Provide secure authentication features</td>
<td>14</td>
</tr>
<tr>
<td>5.4 Log payment application activity</td>
<td>14</td>
</tr>
<tr>
<td>5.5 Payment application must facilitate centralized logging</td>
<td>15</td>
</tr>
<tr>
<td>5.6 Versioning methodology</td>
<td>15</td>
</tr>
<tr>
<td>5.7 Protect wireless transmission</td>
<td>16</td>
</tr>
<tr>
<td>5.8 Facilitate secure network implementation</td>
<td>16</td>
</tr>
<tr>
<td>5.9 Facilitate secure remote access to payment application</td>
<td>16</td>
</tr>
<tr>
<td>5.10 Facilitate secure remote software updates</td>
<td>17</td>
</tr>
<tr>
<td>5.11 Encrypt sensitive traffic over public networks</td>
<td>17</td>
</tr>
<tr>
<td>5.12 Encrypt all non-console administrative access</td>
<td>17</td>
</tr>
<tr>
<td>6. Appendices</td>
<td>18</td>
</tr>
<tr>
<td>7. Release Notes</td>
<td>34</td>
</tr>
</tbody>
</table>
1 Introduction to Security

1.1 Payment Card Industry Data Security Standard (PCI-DSS)

The PCI-DSS program is a mandated set of security standards that were created by the major credit card companies to offer a complete, unified approach to safeguarding credit cardholder information for all credit card brands.

A group of five leading payment brands including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International jointly announced formation of the PCI Security Standards Council, an independent counsel established to manage ongoing evolution of the PCI standard. Concurrent with the announcement, the council released version 3.1 of the PCI standard.

The PCI Data Security Standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data. The requirements apply to all methods of credit card processing, from manual to computerized; the most comprehensive and demanding of which apply to e-commerce websites, and retail point-of-sale systems that process credit cards over the internet.

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

1.2 Payment Application Data Security Standard (PA-DSS)

The PA-DSS applies to software vendors and others who develop payment applications that store, process or transmit cardholder data as part of authorization or settlement, where these payments applications are sold, distributed or licensed to third parties.

Traditional PCI-DSS compliance may not apply directly to payment application vendors since most vendors do not store, process or transmit cardholder data. However, vendor’s payment applications are used by customers to store, process and transmit cardholder data. Therefore, the requirements for the PA-DSS are derived from the PCI-DSS and detail the mandates for payment applications to facilitate customer’s PCI-DSS compliance.
## Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Includes all purchased and custom software programs or groups of programs designed for end users, including both internal and external (web) applications</td>
</tr>
<tr>
<td>ASP</td>
<td>Application service provider. Subscription service in which companies can rent some or all of their resources in lieu of purchasing software, servers, computers and hiring IT staff</td>
</tr>
<tr>
<td>Authentication</td>
<td>Process of verifying identity of a subject or process</td>
</tr>
<tr>
<td>Cardholder</td>
<td>Customer to whom a card is issued or individual authorized to use the card</td>
</tr>
</tbody>
</table>
| Cardholder data    | Full Magnetic stripe or the PAN plus any of the following:  
  - Cardholder name  
  - Expiration date  
  - Service Code                                                                                                                                 |
| Card Validation    | Data element on a card’s magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV or CSC depending on payment card brand. The following list provides the terms for each brand:  
  - CAV – Card Authentication Value (JCB payment cards)  
  - CVC – Card Validation Code (MasterCard payment cards)  
  - CVV – Card Verification Value (Visa and Discover payment cards)  
  - CSC – Card Security Code (American Express)  
  Note: The second type of card validation value or code is the three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit unembossed number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic. The following provides an overview:  
  - CID – Card Identification Number (American Express and Discover payment cards)  
  - CAV2 – Card Authentication Value 2 (JCB payment cards)  
  - CVC2 – Card Validation Code 2 (MasterCard payment cards)  
  - CVV2 – Card Verification Value 2 (Visa payment cards) |
<p>| CCC                | Central Credit Card processing                                                                                                           |
| Console            | Screen and keyboard which permits access and control of the server or mainframe computer in a networked environment                            |
| Default accounts   | System login account pre-defined in a manufactured system to permit initial access when system is first put into service                      |
| Default password   | Password on system administration or service accounts when system is shipped from the manufacturer; usually associated with default account. Default accounts and passwords are published and well known |
| DSS                | Data Security Standard                                                                                                                     |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure</td>
</tr>
<tr>
<td>Enterprise</td>
<td>Software system configuration which allows multiple retail pharmacy, HME or closed-shop pharmacy locations to reside on a single server for more efficient and cost-effective central management within a shared environment (allowing drug and physician information or transfer of prescriptions between stores) or non-shared environment (no data is shared between stores)</td>
</tr>
<tr>
<td>EULA</td>
<td>End-user license agreement</td>
</tr>
<tr>
<td>Firewall</td>
<td>Hardware, software or both that protect resources of one network from intruders from other networks. Typically, enterprises with an intranet that permits workers access to the wider internet must have a firewall to prevent outsiders from accessing internal private data resources</td>
</tr>
<tr>
<td>FTP</td>
<td>File transfer protocol</td>
</tr>
<tr>
<td>Host</td>
<td>Main computer hardware on which computer software is resident</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext transfer protocol. Open-internet protocol to transfer or convey information on the World Wide Web</td>
</tr>
<tr>
<td>ID</td>
<td>Identity</td>
</tr>
<tr>
<td>Information Security</td>
<td>Protection of information to ensure confidentiality, integrity and availability</td>
</tr>
<tr>
<td>IP</td>
<td>Internet protocol. Network-layer protocol containing address information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the internet protocol suite</td>
</tr>
<tr>
<td>IP address</td>
<td>Numeric code that uniquely identifies a particular computer on the internet</td>
</tr>
<tr>
<td>IPSEC</td>
<td>Internet Protocol Security. Standard for securing IP communications by encrypting and/or authenticating all IP packets. IPSEC provides security at the network layer</td>
</tr>
<tr>
<td>Key</td>
<td>In cryptography, a key is an algorithmic value applied to unencrypted text to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message</td>
</tr>
<tr>
<td>LAN</td>
<td>Local area network. Computer network covering a small area, often a building or group of buildings</td>
</tr>
<tr>
<td>MAC</td>
<td>Message authentication code</td>
</tr>
<tr>
<td>Magnetic Stripe Data (Track Data)</td>
<td>Data encoded in the magnetic stripe used for authorization during transactions when the card is presented. Entities must not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/Card Validation Codes/Values and proprietary reserved values must be purged; however, account number, expiration date, name and service code may be extracted and retained, if needed for business</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Use of system that constantly oversees a computer network including for slow or failing systems and that notifies the user in case of outages or other alarms</td>
</tr>
</tbody>
</table>
Network
Two or more computers connected together to share resources

Offline
Refers to processing credit card transactions either when the server is down, the internet is down or when standalone credit card processing is not switching through QS/1

PAN
Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Account Number

PA
Payment Application

PABP
Payment Applications Best Practices

Password
A string of characters that serve as an authenticator of the user

PCI
Payment Card Industry

PIN
Personal identification number

Policy
Organization-wide rules governing acceptable use of computing resources, security practices and guiding development of operational procedures

POS
Point-of-sale

Public Network
Network established and operated by a telecommunications provider or recognized private company, for the specific purpose of providing data transmission services for the public. Data must be encrypted during transmission over public networks as hackers easily and commonly intercept, modify and/or divert data while in transit. Examples of public networks in scope of PCI DSS include the Internet, GPRS and GSM

Recurring Billing
Process of running credit card transactions without needing the customer’s credit card present. Customer’s card numbers are stored the first time they swipe their card. For subsequent transactions, neither the customer nor the card need be present

Router
Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways

SAD
Sensitive authentication data. Security-related information (card validation codes/values, complete track data, PINs and PIN Blocks) used to authenticate cardholders, appearing in plain text or otherwise unprotected form. Disclosure, modification or destruction of this information could compromise the security of a cryptographic device, information system or cardholder information or could be used in a fraudulent transaction

Security Policy
Set of laws, rules and practices that regulate how an organization manages, protects and distributes sensitive information

Service Code
Three- or four-digit number on the magnetic-stripe that specifies acceptance requirements and limitations for a magnetic-stripe read transaction

SQL
Structured (English) Query Language. Computer language used to create, modify and retrieve data from relational database management systems

SSH
Secure shell. Protocol suite providing encryption for network services like remote login or remote file transfer
| **SSL** | Secure sockets layer. Established industry standard that encrypts the channel between a web browser and web server to ensure the privacy and reliability of data transmitted over this channel |
| **Token** | A token is the result of a technology process that converts a card number to a totally random number suitable for risk-free storage |
| **Transaction data** | Data related to electronic payment |
| **TLS** | Transport Layer Security. Protocol that ensures privacy between communicating applications and their users on the internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message |
| **Two-factor authentication** | Authentication that requires users to produce two credentials to access a system. Credentials consist of something the user has in their possession (for example, smart cards or hardware tokens) and something they know (for example, a password). To access a system, the user must produce both factors |
| **User ID** | A character string used to uniquely identify each user of a system |
| **VPN** | Virtual private network. Private network established over a public network |
| **WPA** | Wi-Fi Protected Access (WPA and WPA2). Security protocol for wireless (Wi-Fi) networks |
3 Compliance

PaySentry is a software utility designed for integration into existing QS/1 Point-of-Sale systems. PaySentry is the actual program that handles credit card transactions. PaySentry was developed with all the necessary tools to allow customers to be PCI DSS compliant. This does not mean that merely owning the system ensures compliance.

This guide is intended for customers who wish to create and maintain an environment within the PaySentry card transaction tool that adheres to the guidelines mandated by the Payment Card Industry (PCI) within the Payment Card Industry Data Security Standard (PCI DSS) and the Payment Application Data Security Standard (PA-DSS).

The PaySentry Implementation Guide is available on the QS/1 Customer Support Web page under Product Documents. It is also available in Point-of-Sale Web Help>Getting Started>QS/1 PaySentry.
4 PaySentry Setup

PaySentry must be installed on a computer that is not connected to the internet and must be installed on SQL Server 2012 Express SP 2. Refer to Appendix A – SQL Server 2012 Express SP 2 for system requirements.

To install PaySentry, follow the steps below:

1. Install PaySentry on a SQL station. **Important:** If downloading the PaySentry self-extractable, you must be authorized to receive the PaySentry Quick Service Update (QSU). Contact QS/1 Customer Support at 800.845.7558 to request this update or a copy of the PaySentry CD.
   a. Download the PaySentry self-extractable from the QS/1 website. Make a note as to where the file downloads.
      **Note:** It may be possible that you received the PaySentry self-extractable on CD from QS/1. If this is the case, insert the medium into the appropriate drive on the station where SQL is to be installed, open the contents of the medium and start this process at e.
   b. Transfer the file to the SQL station. Refer to Appendix B – Transferring Files for more information.
      **Note:** If transferring files from a CD, the files MUST be copied to the SQL station before the installation is attempted.
   c. Right click on the PaySentry full install executable. Then left click on Run as Administrator. A list of files are extracted and copied into the current file path.
   d. Double click the setup batch file (.bat). New files and folders display and temporary ones are deleted. **DO NOT RUN AS ADMINISTRATOR.**
   e. Right click the client install executable then left click on Run as Administrator to install the Windows Client program (if using the QS/1 CD, this file is located in the WindowsClient folder).
   f. Right click the system dependency executable and then left click on Run as Administrator to install the systems dependency program (if using the QS/1 CD, this file is located in the SysDepends folder).
      **Note:** In order for the Winclient to run properly, a local, generic/text only printer must be installed. Refer to Appendix C – Generic/Text Only Printer Setup for more information.
   g. Right click on the QIA Install executable and then left click on Run as Administrator. Follow the system prompts.
   h. Double click Windows Client icon and connect to the QS/1 Server. System prompts to run updates; click OK. Then close the Windows Client.
   i. Right click the setup executable and then left click on Run as Administrator to install the PaySentry program (if using the QS/1 CD, this file is located in the PaySentry folder). Click Install.
      - Accept EULA license for .NET framework 4.0 if prompted
      - Accept EULA license for SQL Server 2012 Express SP 2 if prompted
      **Note:** .NET framework 4.0 and SQL Server 2012 Express SP 2 run an unattended installation. It will take several minutes to complete.
      - The PaySentry Welcome screen displays. Click Next.
      - Adjust the installation path so that the QS1 folder is the root of the PaySentry folder (for example: C:\QS1\PaySentry\). Click Next.
      - The confirmation screen displays. Click Next.
      - The Update Settings screen displays. Enter the Hostname and Port number of your system for downloading updates from the QS/1 Server. Click Save.
      **Note:** Hostname and Port number can be entered at a later time by opening PaySentry Manager, clicking on the Settings tab and entering the information.
      - Click Finish.
   j. Verify the installation.
      - Right click My Computer icon on the desktop and select Manage.
      - Click + beside Services and Applications to expand the selections.
      - Click Services.
      - Scroll through the list and verify that Services, Name, QS/1 PaySentry Gateway and SQL Server (PAYSENTRY) exist and have Status of Started.
   k. Set PSUser2 password and configure PaySentry Manager to run under that account.
      - Right click My Computer icon on the desktop and select Manage.
      - Click + beside Local Users and Groups to expand the selections.
      - Click Users.
      - Right click PSUser2 and click Set Password.
      - Click Proceed.
      - Enter a strong password that, at the least, consists of numeric and alpha-characters, is a minimum length of twelve (12) characters and includes at least one capital letter, one lower case letter, one number and one special character (@ # $ % ^ & * + =).
Click **OK**. If the password meets system requirements, click **OK**. If not, enter a new password.

- Navigate to the **PaySentry, PaySentryMgr** folder on your system (this may be different for each system).
- Right click PaySentryMgr.exe and click **Run as…**.
- Click **The following user:** check box.
- If on a domain, type **XXX\PSUser2** where **XXX** is the name of the computer. If not on a domain, type **PSUser2** only.
- Enter the strong password you created in the previous step.
- Click **OK**. An instance of PaySentry Manager opens, but may take several minutes before it displays.

### Backup Service Master Key and Database Master Key using PaySentry Manager.

1. **Backup Service Master Key and Database Master Key using PaySentry Manager.**
   - After the PaySentry Manger displays from the previous step, select **Backup**.
   - Click **SMK and DMK Backup**. A default path for the backup file is pre-populated. Change this path as desired.
   - For the Service Master Key Backup, enter a password and confirm the password. Click **Backup SMK**.
   - For the Database Master Key Backup, enter a password and confirm the password. Click **Backup DMK**.
   - Click **Close**.
   - Move SMK/DMK backup files to a secure off-site location.

2. **Manually go into Central Credit Card config (CCC) and check the SQL box to enable communication with the PaySentry SQL database.** Also, check the Log All Transactions box depending on your preference to log all transactions (highly recommended) and type in the IP address of the SQL server in the Gateway Host field.

   **Note:** Unless otherwise moved, CCC is installed on the QS/1 server. Refer to **Appendix F – Install CCC on a Separate Server** to move the CCC service.

   **Note:** This procedure should be performed after regular business hours as it may interfere with credit card processing.

   a. Click the Windows **Start** icon.
   b. Select **All Programs, QS1, Utilities, CCC Config**.
   c. Click **Action**.
   d. Click **Configure**.
   e. A prompt displays asking if you want to review/change the CentralCreditCard.ini. Click **Yes**.
   f. Check the SQL and Log All Transactions (highly recommended) fields.
   g. Type the IP address of the SQL server in the Gateway Host field. Click **OK**.
   h. A prompt displays asking if all changes have been made. Click **Yes**.
   i. A prompt displays asking if the service started without errors. Click **Yes**.
   j. A prompt displays asking if you want to terminate the CCC configuration program. Click **Yes**.
   k. A prompt displays asking if you wish to perform activation. Click **Yes**.
   l. A prompt displays asking if you want to keep the CentralCreditCardCfg.log. Click **Yes**.

3. **Verify that the IP Address of the Windows Client options of all workstations and registers is set to the IP Address of the server on which Central Credit Card is installed (typically the QS/1 Server).**

   a. Click the Windows **Start** icon located on the QS/1 Server or server on which Central Credit Card is installed
   b. Click **Run….**
   c. Type **cmd** and click **OK**. The Command Prompt displays.
   d. Type **ipconfig** and press **Enter**.
   e. Make note of the IP Address.
   f. On all workstations and registers, double click **QS1 Windows Client**.
   g. On the Connect screen, click **Options….**
   h. Click the Central Credit Card tab.
   i. Enter the IP Address from step e. Click **OK**.

4. **Disable hibernation on the SQL station.**

   a. Click the Windows **Start** icon located on the SQL station.
   b. Click **Control Panel**.
   c. Double click **Power Options**.
   d. Select the **Hibernate** tab.
   e. If the Enable hibernation field is checked, uncheck it.
   f. Click **OK**.
5 Security Validation

5.1 Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2) or PIN block data*

* Includes EMV Track Equivalent Data
PA-DSS - 1.1.4a
PCI-DSS - 3.2

PaySentry has been developed to limit the data retained to the credit card number, expiration date and name on the card. Full magnetic stripe, card validation code or value, PIN block data and EMV track equivalent data are not stored.

PA-DSS - 1.1.5c
PCI-DSS - 3.2

To ensure PCI compliancy, PaySentry will never store sensitive authentication data (SAD). QS/1 provides troubleshooting via log files. There is no debug mode for PaySentry. No sensitive authentication data is collected or stored.

5.2 Protect stored cardholder data
PA-DSS - 2.1, 2.2a
PCI-DSS - 3.1

There are no configuration options for masking (first 6 and last 4) PAN. The process is automated and cannot be turned off.

PaySentry does not store PAN post authorization. Instead, a token is sent back from QS/1’s PCI DSS certified Data Center to replace PAN for storage in the PaySentry database. The token is generated using HP’s Voltage Secure Stateless Tokenization technology, and will contain at least 1 alpha character while preserving the first 6 and last 4 numbers. The token is then encrypted using a Data Encryption Key (DEK) generated by a SQL Server Certificate using a 1024-bit RSA cipher for storage in the PaySentry database. Refer to Appendix G – Tokenization for more information on how tokens are generated.

There are no configuration options for masking (first 6 and last 4) PAN. The process is automated and cannot be turned off. Since PaySentry does not store PAN, customers will not have access to see the full PAN.

The masked PAN (first 6 and last 4) is displayed for view in the following areas of the system:

- Scan Credit Card File
- Transaction Journal
- Customer Record.

The truncated PAN (last 4 only) is displayed for print out on the signature pad when electronically signing for the credit card payment.

The truncated PAN (last 4 only) is stored for print out on the following areas:

- Payment Detail Audit Report
- Credit Card Analysis Report
- IIAS Audit Report
- Cardholder and Merchant Receipts

Customers should establish a retention period for cardholder data. Cardholder data exceeding the retention period must be purged from all locations where the data is stored.

This data may be purged by doing the following:

1. Double click PaySentry Manager icon located on your desktop.
2. Click SQL tab.
3. In the Purge section, you have three options for deletion: Transaction, Customers and Audit Log. Click the down arrow next to the Purge Records Older Than field for the type of records you wish to purge and choose a date from which to begin the purge. QS/1 recommends that you check with your credit card processor for the recommended period of time to retain records.
4. Click the button of the type of records you wish to purge.
5. A confirmation message displays. Click OK.
6. The status section displays the system activity. If necessary, choose another record type and repeat the process.

To prevent the inadvertent capture or retention of cardholder data, Refer to Appendix J - Microsoft Disable System Restore. This feature prevents the system from being rolled back, or restored, to a point before certain events took place.

**5.3 Provide secure authentication features**

**PA-DSS - 3.1.1-3.1.11**  
**PCI-DSS - 8.1, 8.2, and 8.5.8-8.5.15**

PaySentry provides unique IDs and secure authentication for administrative access and access to cardholder data.

Do not use default administrative accounts for payment application logins (e.g., do not use the “sa” account for payment application access to the database).

- You must assign secure authentication to default accounts (even if they won’t be used), and then disable or do not use the accounts.
- You must assign secure authentication for payment applications and systems whenever possible.
- Do not use group, shared or generic accounts/passwords.
- Change user passwords at least every 90 days.
- Require a minimum password length of at least seven characters.
- Use passwords containing both numeric and alphabetic characters.
- Do not allow individuals to submit a new password that is the same as any of the last four passwords they have used.
- Limit repeated access attempts by locking out user ID after not more than six attempts.
- Set the lockout duration to 30 minutes or until administrator enables the user ID.
- If a session has been idle for more than 15 minutes, require the user to re-enter password to re-activate terminal.

Refer to Appendix I–PaySentry PCI Security Settings.

**WARNING:** Security Settings for passwords default with PCI-compliant settings. While these settings may be changed by an administrator with proper access clearance, it is recommended to keep them at the default settings. If for any reason these settings must be changed, consult PCI DSS requirements 8.5.8-8.5.15. Customers are advised that changing “out of the box” installation settings may result in non-compliance with PCI DSS.

**PA-DSS - 3.2**  
**PCI-DSS - 8.1 and 8.2**

Customers are strongly advised to require a unique username and complex password to access any computer, server or database with payment applications installed or that store cardholder data.

**5.4 Log payment application activity**

**PA-DSS - 4.1, 4.2, 4.3,**  
**PCI-DSS - 10.1, 10.2, 10.3**

PaySentry has been designed to provide extensive event logging for security audits. The types of events logged by PaySentry are as follows:

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

In these circumstances, the following data is recorded:
Type of event (from the aforementioned list)
User identification
Date and time
Success or failure indication
Origination of event
Identity or name of affected data, system component or resource

Note: Log settings are not configurable by the user. They are automatically enabled and it is not possible to disable these logs.

5.5 Payment application must facilitate centralized logging
PA-DSS - 4.4b
PCI-DSS - 10.5.3

To incorporate the payment application logs into a centralized logging environment, Syslog functionality has been added to the implementation of PaySentry. To utilize this functionality, the Syslog feature should be enabled and Syslog Configuration Settings should be modified according to the environment using PaySentry Manager. Refer to Appendix E – Set Up Syslog Server for instructions on configuring this server.

5.6 Versioning methodology
PA-DSS – 5.4.4

The version format for the QS/1 PaySentry application is the following: MM.mm.ww, where MM is the major attribute, mm is the minor attribute and ww is the wildcard attribute. Attributes are designated as numbers. Preceding zeros will not display. For example: 19.4.x reflects the Major.Minor.Wildcard. 19.4.0 and 19.4.1 would be covered under the wildcard version.

The major attribute is an indicator that substantial changes (changes to 50% or more of the code base) were made to the overall architecture and/or design of the system. Changes of this magnitude could reflect major rewrites to the user interface in PaySentry and/or to the PaySentry architecture of the system. Therefore, these types of changes will impact the PA-DSS requirements and require a PA-DSS assessment. Since PaySentry is a middleware application, the major release changes would be infrequent. The only exception to changing the major attribute without significant changes would be if the major attribute changed in the QS/1 integrated software applications and PaySentry’s major attribute is changed to reflect the release of those QS/1 integrated software applications. Currently all our integrated application versions begin with 19.

The minor attribute is an indicator of significant changes made for new PaySentry functionality and/or for PaySentry security updates, but affect less than 50% of the PaySentry code base. Minor changes can be rolled into a major if an upcoming major release is already scheduled. Minor changes include enhancements that provide additional features such as EMV and tokenization. It can also include security updates to provide a greater level of encryption. These changes can affect the PA-DSS requirements and therefore may require a new PA-DSS assessment.

The wildcard attribute reflects small changes made to PaySentry that do not compromise the integrity of the system. These changes could include updates to reporting and to other user interface features, updates to add/remove payment processors, and non security patches. These changes do not impact the security of the PaySentry system nor do they affect the PA-DSS requirements.
5.7 Protect wireless transmissions
PA-DSS - 6.1
PCI-DSS - 1.2.3 and 2.1.1

Customers using a wireless configuration must install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny any traffic from the wireless environment or from controlling any traffic. Refer to Appendix D – Security Specifications.

PA-DSS - 6.2, 6.3
PCI-DSS - 4.1.1

For customers with wireless environments, certain guidelines and settings are appropriate, such as:
- System defaults (encryption keys, passwords and SNMP community strings, etc.) must be changed upon installation so that the known defaults are not used and must also be changed when anyone with knowledge of the settings changes positions or leaves the company.
- Wireless networks should be segregated by a firewall that denies (or if necessary, controls access to) the cardholder data environment. Industry best practices should be used to provide strong encryption for authentication and transmission for any data on that network (e.g., IEEE802.11i).
- Enable Wi-Fi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable
- Encrypt wireless transmissions by using Wi-Fi Protected Access (WPA or WPA2) technology, Internet Protocol Security (IPSEC) VPN or Transport Layer Security version 1.1 or higher ‘Live’ (TLS).

5.8 Facilitate secure network implementation
PA-DSS – 8.2.c
PCI-DSS - 1.2.3 and 2.1.1

PaySentry must be installed on a computer with SQL Server 2012 Express SP 2 that is not connected to the internet. Refer to Appendix D – Security Specifications for a review of hardware and software firewalls, the payment card processing configuration and the components comprising the configuration.

5.9 Facilitate secure remote access to payment application
PA-DSS - 10.1, 10.2 and 10.3
PCI-DSS - 8.3

PaySentry may be accessed remotely if systems are equipped with the web-based tool, ScreenConnect. ScreenConnect allows ad-hoc communications between servers or computers for the purpose of training, diagnosing and fixing an issue or installing software. Customers have the option of not installing ScreenConnect or not connecting to the ScreenConnect switchboard. If ScreenConnect is not installed, systems may not be accessed remotely.

When accessing a system remotely, QS/1 support personnel cannot initiate a connection to the user’s system. All ScreenConnect sessions are initiated by the customer. ScreenConnect uses an AES-256 bit data encryption algorithm to secure all data travelling across the communication path. ScreenConnect supports role-based security, where users only have access once explicitly provided by the software administrator.

If customers plan on using third-party software for remote access, two-factor authentication (username and password and an additional authentication item such as a token or certificate) is required for PCI compliance. It is strongly recommended that customers use other remote access security features, such as:
- Change the default settings in the remote access software
- Allow connections only from specific (known) IP/MAC addresses via IPSEC
- Use strong authentication and complex passwords for logins (refer to PCI DSS requirements 8.1, 8.3 and 8.5.8-8.5.15)
- Enable encrypted data transmission (refer to PCI DSS requirement 4.1). Enable account lockout after a certain number of failed login attempts
**Note:** Credit card data is not viewable to QS/1 support personnel who are asked to remote access customers’ systems.

### 5.10 Facilitate secure remote software updates

**PA-DSS - 10.2.1**  
**PCI-DSS - 1 and 12.3.9**

PaySentry utilizes an update feature in which customers download new releases/service packs from a secure server through the internet. These updates never require QS/1 to access a customer’s system. Once the release/service pack is downloaded, an installer program completes the process.

If customers utilize VPN, or other high-speed connection such as cable modem, the use of a firewall product is necessary. Secure modem use requirements are listed in PCI DSS requirement 12.3. Refer to 5.6 and *Appendix D - Security Specifications* for firewall details.

### 5.11 Encrypt sensitive traffic over public networks

**PA-DSS - 11.1**  
**PCI-DSS - 4.1**

PaySentry implements TLS 1.1 or above by default with only trusted TLS keys/certificates. This protects cardholder data by encrypting with a strong key strength of at least 256 bit using AES. There are no user configurations to make changes.

**Enable Encryption on Console and Non-Console Ports:**

1. Close the QS/1 Server.
2. Click **Start**, Select **All Programs**, **QS1**, **Utilities**, **Setports**, **Set Logical Ports**.
3. Select the system.
4. Double click the line item for the console port.
5. The Edit Port Entry window displays. Check the Encryption box.
6. Click **OK**.
7. Repeat these steps for the non-console port.

**PA-DSS - 11.2**  
**PCI-DSS - 4.2**

PANs are never sent unencrypted by PaySentry via email. PANs will never be requested explicitly by QS/1 by email.

### 5.12 Encrypt all non-console administrative access

**PA-DSS - 12.1**  
**PCI-DSS - 2.3**

PaySentry does not support non-console administrative access; however, if you plan on accessing the servers where our payment application is stored via non-console administrative access, you must implement strong cryptography, using technologies such as SSH, VPN or TLS for encryption of all non-console administrative access.
6 Appendices

Appendix A – SQL Server 2012 Express SP 2

You must have SQL Server 2012 Express SP 2 installed on a station/computer that is not connected to the internet and that is separate from the server where the QS/1 application is currently stored.

- SQL Server 2012 Express allows a maximum of 10GB of data to be stored.
- Minimum system requirements for credit card storage on a SQL server include:
  - Windows 7 Pro or higher
  - Windows 8 Pro or higher
  - Windows Server 2008 R2
  - Windows Server 2012
  - 1 GHz CPU Pentium III-compatible or better
  - 512 MB RAM or more (recommended)
  - 4.2 GB available hard disk space
  - CD-ROM or DVD-ROM drive
  - Microsoft Mouse or compatible pointing device
  - Super VGA (1,024x768) or higher-resolution video adapter and monitor
  - Microsoft Internet Explorer 7.0 or later

If you are unsure of your current system’s technical specifications, contact QS/1 Customer Support at 800.845.7558 to assess your system.

The SQL station does not need to be purchased through QS/1, although, it is highly recommended. If using an existing station, it is necessary to reformat the current hard drive and re-install the operating system.

Disable Hibernation on the SQL Station

1. Click the Windows Start icon located on the SQL station.
2. Click Control Panel.
3. Double click Power Options.
4. Click the Hibernate tab.
5. If the Enable hibernation box is checked, uncheck it.
6. Click OK.
Appendix B – Transferring Files

CD ROM
In order to do this procedure, your system must have a CD burner and data burning software installed. If not, use one of the other forms of transfer mentioned. If you are unsure, ask your IT department or call QS/1 Customer Support at 800.845.7558.

Flash Drives
1. Insert your flash drive into a USB port on the server where the .txt files are stored.
2. Locate the path where the .txt files are stored.
3. Copy the .txt files by highlighting them, then press CTRL+C (after highlighting, you may also right click on one of the files and click Copy).
4. Navigate to My Computer and locate the flash drive you inserted.
5. Double click the flash drive, and paste the copied files by pressing CTRL+V (you may also right click inside the flash drive folder and click Paste).
6. Once the files have been copied to the flash drive, remove the drive from the server and insert it into a USB port located on the SQL server.
7. Navigate to My Computer and locate the flash drive you inserted.
8. Double click the flash drive, and copy the .txt files by highlighting them, then press CTRL+C or right click and click Copy.
9. Navigate to a location on your SQL server, preferably the C drive, and paste the files by pressing CTRL+V or right click and click Paste.
Appendix C – Generic/Text Only Printer Setup

1. Click the Windows Start icon and choose Control Panel.
2. Double click Printers and Faxes.
3. Under Printer Tasks, select Add a printer.
4. Click Next.
5. Select the Local printer attached to this computer option. Be sure the Automatically detect and install my Plug and Play printer option is unchecked. Click Next.
6. Click Next.
7. Choose the Generic manufacturer and Generic/Text Only printer. Click Next.
8. Name the printer QS1LPT1 and set as the default printer. Click Next.
9. Be sure the Do not share this printer option is checked. Click Next.
10. On the Print Test Page screen, choose No. Click Next.
11. Click Finish.
Appendix D – Security Specifications

When setting up an internal software firewall or external hardware firewall, certain security specifications must be designated. Follow the tables below.

The PaySentry payment card processing configuration includes the follow components:

**Qcci0103.dll:** QCCI0103.DLL provides the client with support for communicating with CentralCreditCard for the purpose of interacting with the PaySentry SQL DB.

**CentralCreditCard.exe:** CentralCreditCard.exe is a multi-threaded application that runs as a Windows service. Its purpose is to process incoming PaySentry database queries and payment requests from multiple clients. It routes PaySentry Queries to PaySentry.exe and Payment requests to the QS/1 Data Center.

**PaySentry.exe:** PaySentry.exe is a Windows service running on the server where the PaySentry SQL database resides. PaySentry.exe processes requests relayed by CentralCreditCard.exe using stored procedures to read from and write to the PaySentry database tables. The service also manages the automatic database backup process on a daily basis.

**Qccinet.dll:** QCCINET.DLL provides the support for communicating with CentralCreditCard for the purpose of adding and deleting credit card information from the PaySentry SQL DB. QCCINET.DLL provides our web applications with a very small subset of the support that QCCI0103.DLL provides for our client application.

### QS/1 Server

<table>
<thead>
<tr>
<th>Program</th>
<th>Direction</th>
<th>Protocol</th>
<th>Remote Address</th>
<th>Local Port</th>
<th>Remote Port</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>CENTRALCREDITCARD.EXE</td>
<td>Outbound</td>
<td>TCP</td>
<td>PaySentry Server</td>
<td>Any</td>
<td>1173</td>
<td>PaySentry</td>
</tr>
</tbody>
</table>

### PaySentry Server

<table>
<thead>
<tr>
<th>Program</th>
<th>Direction</th>
<th>Protocol</th>
<th>Remote Address</th>
<th>Local Port</th>
<th>Remote Port</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAYSENTRY.EXE</td>
<td>Inbound</td>
<td>TCP</td>
<td>Central Credit Card Server</td>
<td>1173</td>
<td>Any</td>
<td>Connection from Central Credit Card</td>
</tr>
<tr>
<td>QS1COM.EXE</td>
<td>Outbound</td>
<td>TCP</td>
<td>QS/2 Server</td>
<td>Any</td>
<td>1150</td>
<td>Connection for getting updates</td>
</tr>
<tr>
<td>PAYSENTRY.EXE</td>
<td>Outbound</td>
<td>TCP</td>
<td>webservices.cornerdrugstore.com</td>
<td>Any</td>
<td>80</td>
<td>Log uploads</td>
</tr>
<tr>
<td>PAYSENTRY.EXE</td>
<td>Outbound</td>
<td>UDP</td>
<td>Any</td>
<td>Any</td>
<td>514</td>
<td>Syslog Server Messages</td>
</tr>
</tbody>
</table>

Notes:
- Installed programs and their ports may vary depending on system configuration.
- The PaySentry Server is considered a specialized QS/1 Workstation. Also refer to the Firewall settings for a QS/1 Workstation.

### Central Credit Card Server

<table>
<thead>
<tr>
<th>Program</th>
<th>Direction</th>
<th>Protocol</th>
<th>Remote Address</th>
<th>Local Port</th>
<th>Remote Port</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>CENTRALCREDITCARD.EXE</td>
<td>Inbound</td>
<td>TCP</td>
<td>Any</td>
<td>1171</td>
<td>Any</td>
<td>Connection from QS/1 Windows Client</td>
</tr>
<tr>
<td>CENTRALCREDITCARD.EXE</td>
<td>Outbound</td>
<td>TCP</td>
<td>pwlcssl.qs1.com and/or pwlcssl2.qs1.com</td>
<td>Any</td>
<td>443 and/or 5843</td>
<td>QS/1 Payment Gateway</td>
</tr>
<tr>
<td>CENTRALCREDITCARD.EXE</td>
<td>Outbound</td>
<td>TCP</td>
<td>PaySentry Server</td>
<td>Any</td>
<td>1173</td>
<td>PaySentry</td>
</tr>
<tr>
<td>CENTRALCREDITCARD.EXE</td>
<td>Outbound</td>
<td>TCP</td>
<td>downloads.qs1.com and errors.qs1.com</td>
<td>Any</td>
<td>80 or 12345</td>
<td>Central Credit Card Updates and MSM Error Uploads</td>
</tr>
</tbody>
</table>
Appendix E – Set Up Syslog Server

To incorporate the payment application logs into a centralized logging environment, Syslog functionality has been added to the implementation of PaySentry. To utilize this functionality, the Syslog feature should be enabled and Syslog Configuration Settings should be modified according to the customer environment using PaySentry Manager.

**Note:** This feature is off by default; the customer should enable this feature in order to collect and capture application log messages from PaySentry software.

The configuration settings that correspond to the application log shipment are located under Syslog Settings in the Settings tab of PaySentry Manager.

### Syslog Settings fields:

**Priority:** Defines the severity/priority of the message. The acceptable values are integers in the range from 0 to 7 as follows:

- 0 = Emergency
- 1 = Alert
- 2 = Critical
- 3 = Error
- 4 = Warning
- 5 = Notice
- 6 = Informational
• 7 = Debug

The default = 6 Notice. Therefore, if the Syslog feature is enabled, it sends all messages generated by PaySentry with a priority of 6 or higher (5, 4, 3, 2, 1, 0) to the Syslog server. The higher the priority value, the more messages are captured and sent to the Syslog server.

**Facility Code:** Corresponds to the type of program that is logging the message. Values range from 0 – 23 as follows:

• Kernel = 0 – Kernel messages
• User = 1 – User-level messages
• Mail = 2 – Mail system
• System = 3 – System daemons
• Security = 4 – Security/authorization messages
• Syslog = 5 – Messages generated internally by Syslog
• Printer = 6 – Line printer subsystem
• Network = 7 – Network news subsystem
• UUCP = 8 – UUCP subsystem
• Clock = 9 – Clock daemon
• AuthMsg = 10 – Security/Authorization messages
• FTPDaemon = 11 – FTP daemon
• NTP = 12 – NTP subsystem
• LogAudit = 13 – Log audit
• LogAlert = 14 – Log alert
• ClockDaemon = 15 – Clock daemon
• Local0 = 16 – Local use 0
• Local1 = 17 – Local use 1
• Local2 = 18 – Local use 2
• Local3 = 19 – Local use 3
• Local4 = 20 – Local use 4
• Local5 = 21 – Local use 5
• Local6 = 22 – Local use 6
• Local7 = 23 – Local use 7

**Host:** IP or host of the machine where Syslog listener is located.

**Port:** UDP port of the machine where Syslog listener is located.

Click **Save** when fields are populated.
Appendix F – Install CCC on a Separate Server

The initial setup for PaySentry installs CCC on the QS/1 Server. To install CCC on a server other than the QS/1 Server, follow the instructions noted here.

The first step is to contact QS/1 Customer Support and request to download the latest CCC installation wizard. After downloading the CCC installation wizard, follow the screen prompts as follows:

![Image of InstallShield Wizard]

Welcome to the InstallShield Wizard for the QS/1 CentralCreditCard.

The InstallShield Wizard will install QS/1 CentralCreditCard on your computer. To continue, click Next.
Choose Destination Location
Select folder where setup will install files.

Setup will install QS/1 CentralCreditCard in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder
C:\QS1\CentralCreditCard

Start Copying Files
Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:
Destination folder: C:\QS1\CentralCreditCard
The InstallShield Wizard is installing QS/1 CentralCreditCard

Installing the Microsoft Visual C++ 2008 Redistributable...
When setting up an internal software firewall or external hardware firewall, certain specifications must be designated. Follow the table below.

<table>
<thead>
<tr>
<th>Program</th>
<th>Direction</th>
<th>Protocol</th>
<th>Remote Address</th>
<th>Local Port</th>
<th>Remote Port</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>CENTRALCREDITCARD.EXE</td>
<td>Inbound</td>
<td>TCP</td>
<td>Any</td>
<td>1171</td>
<td>Any</td>
<td>Connection from QS/1 Windows Client.</td>
</tr>
<tr>
<td>CENTRALCREDITCARD.EXE</td>
<td>Outbound</td>
<td>TCP</td>
<td>pwlccsid.qs1.com and/or pwlccsid2.qs1.com</td>
<td>Any</td>
<td>443 and/or 5945</td>
<td>QS/1 Payment Gateway</td>
</tr>
<tr>
<td>CENTRALCREDITCARD.EXE</td>
<td>Outbound</td>
<td>TCP</td>
<td>Paysentry-Server</td>
<td>Any</td>
<td>1173</td>
<td>Paysentry</td>
</tr>
<tr>
<td>CENTRALCREDITCARD.EXE</td>
<td>Outbound</td>
<td>TCP, HTTP, Microsoft BITS service</td>
<td>downloads.qs1.com and errors.qs1.com</td>
<td>Any</td>
<td>80 or 12345</td>
<td>Central Credit Card Updates and MSM Error Uploads</td>
</tr>
</tbody>
</table>

Notes:
- Installed programs and their ports may vary depending on system configuration.
- Typically QS/1 Central Credit Card will be installed on a QS/1 Server or QS/1 Enterprise Server machine.

Populate the Central Credit Card address with the IP address of the Central Credit Card Server.
If credit card transactions should be submitted to the "Central Credit Card" service, provide the host address and port number that should be used when making the connection.

Address: 10.1.20.18
Port #: 1171

Timeout values:
- Connect: 5 seconds
- Send/Recv: 90 seconds
Appendix G – Tokenization

Tokenization is a technology process that converts a card number to a totally random number (i.e., token) suitable for risk-free storage. PaySentry does not store PAN post authorization. Instead a token is generated by QS/1’s PCI DSS certified Data Center and then sent to PaySentry for storage. Tokenization is required so that PAN is never stored in PaySentry.

QS/1’s PCI DSS certified Data Center generates tokens using HP’s Voltage Secure Stateless Tokenization technology which generates a token containing at least 1 alpha character, while preserving the first 6 and last 4 numbers. The token is then sent to PaySentry for storage where it is encrypted using a Data Encryption Key (DEK) generated by a SQL Server Certificate using a 1024-bit RSA cipher.

Refer to HP’s documents concerning HP’s Voltage Secure Stateless Tokenization technology:
https://www.voltage.com/technology/tokenization-and-key-management/hp-secure-stateless-tokenization/
Appendix H – PaySentry PCI Security Settings

Security settings are accessed by an administrator going to Store Control, Security Access, PCI Security Options.

![Security Settings](image)

**Default settings per PCI-DSS Requirements:**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Min</th>
<th>Max</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Expiration Days</td>
<td>1</td>
<td>90</td>
<td>90</td>
<td>The max is 90 days per PCI DSS requirement 8.5.9.</td>
</tr>
<tr>
<td>Password Expiration Notice</td>
<td>0</td>
<td>99</td>
<td>5</td>
<td>The max is 5 per PCI DSS requirement 8.5.13.</td>
</tr>
<tr>
<td>Maximum Login Attempts</td>
<td>1</td>
<td>6</td>
<td>6</td>
<td>The max is 6 per PCI DSS requirement 8.5.13.</td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td>7</td>
<td>64</td>
<td>7</td>
<td>The min is 7 per PCI DSS requirement 8.5.10.</td>
</tr>
<tr>
<td>Automatic Logoff Time</td>
<td>1</td>
<td>15</td>
<td>15</td>
<td>The max is 15 minutes per PCI DSS requirement 8.5.13.</td>
</tr>
<tr>
<td>Inactive Employee Days</td>
<td>1</td>
<td>90</td>
<td>90</td>
<td>The max is 90 days per PCI DSS requirement 8.5.5.</td>
</tr>
<tr>
<td>Purge Audit Log Days</td>
<td>365</td>
<td>999</td>
<td>365</td>
<td>The min is 365 days of history that must be kept per PCI DSS requirement 10.7.</td>
</tr>
<tr>
<td>Purge Transaction Records Days</td>
<td>0</td>
<td>999</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>Purge Customer Records Days</td>
<td>0</td>
<td>999</td>
<td>365</td>
<td></td>
</tr>
<tr>
<td>Require Special Characters</td>
<td>N</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Require Mixed Case</td>
<td>N</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**WARNING:** Security Settings for passwords default with PCI-compliant settings. While these settings may be changed by an administrator with proper access clearance, it is recommended to keep them at the default settings. If for any reason these settings must be changed, consult PCI DSS requirements 8.5.8-8.5.15. Customers are advised that changing “out of the box” installation settings may result in non-compliance with PCI DSS.
Appendix I – Disable System Restore

The System Restore feature is enabled by default. To disable System Restore:

1. Right-click My Computer and then click Properties.
2. On the Performance tab, click File System, or press ALT+F.
3. On the Troubleshooting tab, click to select the Disable System Restore check box.
4. Click OK twice, and then click Yes when you are prompted to restart the computer.
5. To re-enable System Restore, follow steps 1-3, but in step 3, click to clear the Disable System Restore check box.
Appendix J – PaySentry Password Overview

QS/1 follows the procedures below for the transmission, encryption and storage of passwords used in conjunction with PaySentry, the QS/1 credit card transaction tool.

Password Storage

Each password created is stored as a 64 byte one-way hashed value based on a combined random salt value and a SHA256 hash of the salt and password. The random salt value and the SHA256 hash values are computed in PaySentry.exe using Microsoft cryptographic API functions specifically for these purposes.

This hashed and salted password is then stored in the userdata.employees table in the CCCTransactions database in the PaySentry SQL Server instance.

Password Transmission

The password is sent from the Point-of-Sale register to the CentralCreditCard server over a 256 bit AES encrypted transmission. From the CentralCreditCard server, the password is forwarded over a secure TLS 1.1 transmission to PaySentry.exe, where it is salted, hashed and saved in the database.
Appendix K – PTS Device Dependencies

- Ingenico, ISC Touch 480 (4-30125)
- Ingenico, ISC350 (4-20133)
- Ingenio, ISMP (4-20175)
- Ingenico, iSMP (4-20183)
7 Release Notes

The following application/system updates were added to PaySentry Version 19.4.x:

- Made changes to support tokenization
- Made changes to support end-to-end encryption
- Made changes to support processing Europay, MasterCard and Visa (EMV) chip cards
- Made changes to support Transport Layer Security (TLS) 1.1 or higher versions of TLS
- Made changes to support Windows 8.1 OS
- Made changes to meet PA-DSS requirement 3.3.2
- Made changes to prevent users from making security settings non-PCI compliant
- Made changes to support near field communication (NFC) contactless for payment
- Renamed MOTO and Verification fields to Mail or Phone Order and Voice Auth Number respectively, on the Credit/Debit Payment Details window
- Updated to include PTS Device Dependencies Appendix