acPMS'
Payment Card Industry (PCI)
Payment Application Data Security Standard (PA-DSS 3.2)
Implementation Guide
For acPMS Version 9
October 2021

Table of Contents

Copyright Information

AutoClerk, Inc.

Address: 1990 N California Blvd, Suite 20 PMB1139, Walnut Creek, CA 94596

Phone: 925.284.1005

URL: www.autoclerk.com

Version	Date	Reviewed by	Changes made
3.0	8/22/16	Holly McGlothlin	First pass at document for PA-DSS ver. 3.2
3.1	9/16/2016	David Ferris, Holly McGlothlin	Updated for grammar and clarification.
3.2	9/20/2016	David Ferris	Updated after review.
3.3	12/8/2016	Holly McGlothlin	Corrections to match PCI Council changes
4.0	11/18/2019	Holly McGlothlin	Update for accuracy
4.1	9/29/2020	Holly McGlothlin	Update Server version
5.0	10/19/2021	Holly McGlothlin	Update wording, Windows versions, and clarity for 2021 Attestation of Validation

Introduction

AutoClerk, Inc. is a software application developer and vendor. As a vendor that integrates and implements credit card processing for deposits, authorizations, and payments, we are required to comply with the *Payment Card Industry's (PCI) Payment Application Data Security Standard (PA-DSS)*.

As a business entity that processes credit cards, by getting authorizations and processing sales, you (a hotel) are required to be compliant with *the Payment Card Industry Data Security Standard (PCI DSS)*. There are several levels of PCI DSS compliance. One criterion is the number of credit card transactions processed in a year. You must review the compliance documentation at http://www.pcisecuritystandards.org and take the necessary steps to obtain and maintain your appropriate PCI DSS compliant status.

AutoClerk's and acPMS' PA-DSS compliance serves to support your PCI DSS compliance. Our being PA-DSS compliant does *not* make you PCI DSS compliant.

The PCI DSS consists of 12 Requirements, which cover the handling, processing, and storage of credit card data. The following table lists the requirements.

Objective	**12 PCI-DSS Compliant Requirements**
Build and Maintain a Secure Network and Systems	Requirement 1: Install and maintain a firewall configuration to protect cardholder data Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	Requirement 3: Protect stored cardholder data Requirement 4: Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs Requirement 6: Develop and maintain secure systems and applications
Implement Strong Access Control Measures	Requirement 7: Restrict access to cardholder data by business need to know Requirement 8: Identify and authenticate access to system components Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks	Requirement 10: Track and monitor all access to network resources and cardholder data Requirement 11: Regularly test security systems and processes
Maintain an Information Security Policy	Requirement 12: Maintain a policy that addresses information security for personnel

This PA-DSS Implementation Guide explains acPMS' role in the security of your guests' credit card data. It instructs you and your network administrator how to enable security settings in your network and hardware. It instructs you on secure acPMS product implementation; and defines some of your responsibilities for meeting your PCI DSS requirements.

Following these guidelines does *not* make you PCI DSS compliant, nor does it guarantee your network's security. It is your responsibility, along with your network administrator, to ensure that your hardware and network systems are secure from internal as well as external intrusions.

acPMS makes neither claim on the security of your network, nor on the level of your PCI DSS compliance.

acPMS Version 9 can only be updated from acPMS Version 8, which does not allow the storing of legacy data even from previous versions of acPMS. (PA-DSS 1.1.4)

Anytime acPMS was installed at your property, you were required to follow its System Specifications (Specs). You must review the current Specs and have your network administrator verify that your acPMS system meets or exceeds them. Changes may need to be made to bring your system to acPMS' current specs. Following the Specs does *not* make you PCI DSS compliant; however, it contributes to your PCI DSS compliance. acPMS' Complete System Specifications can be found at http://myautoclerk.com. Once you have logged in, there is a link on the home page. The Specs are also attached as "Appendix A" to this document.

This document is organized by the PA-DSS requirements, which acPMS must meet to be PA-DSS certified. Many of the measures you need to take are detailed in the acPMS System Specifications. This Guide also references the PCI DSS (Version 3.2.1 May 2018) and the attached Appendixes.

1. Do Not Retain Full Magnetic Stripe, Card Verification Code or Value (CAV2, CID, CVC2, CVV2) or PIN Block Data

The magnetic stripe on the back of a credit card contains sensitive data including the cardholder's name, Primary Account Number (PAN), expiration date, and other information necessary to process the card for an authorization and/or sale. The Card Validation Code or Value, or Card Security Code refers to either 1) the data element on a card's magnetic stripe or 2) the 3-digit number next to the signature field on the back of a Discover, JCB, MasterCard, and Visa payment card; or the 4-digit number on the face of an American Express card. These are also referred to as the CVC, CVV and/or CSC. A PIN (Personal Identification Number) is used when a debit card is processed as a debit transaction rather than a credit card transaction.

AutoClerk's credit card interface (Data capture) is certified with Shift4, Heartland Payment Systems (Heartland), and Elavon Payment Processing Solutions (Elavon) EMV (Europay, MasterCard and Visa) technology. Shift4 and its "Lighthouse Transaction Manger" (formerly "Dollars on the Net™") is "a real-time payment gateway between merchants' point-of-sale systems and their bank/processor". By processing guests' credit cards through Shift4, Heartland or Elavon, the credit card number is kept by acPMS on your hardware as a masked number with a token. A token is a unique code, which represents and points to the actual card number, which resides at Shift4, Heartland or Elavon.

"Masked" is when a cardholder's PAN has been substantially replaced by X's. For example, XXXXXXXXXXXX4957 is a masked format used when viewing and/or printing a guest folio receipt in acPMS; 5474XXXXXXXX4957 is a masked format used by Shift4, Heartland, Elavon, and/or acPMS for a hotel's internal reporting purposes, such as a Transaction report.

acPMS requires *all* properties which have the acPMS data capture interface use Shift4, Heartland or Elavon as the property's payment gateway.

When a credit card is used within the acPMS client for an authorization or sale it can be entered as a tap, swipe, manually or chip in the EMV pin pad; or the card data is manually entered in the acPMS program. The data is then sent by the acPMS client to Shift4's Universal Transaction Gateway (UTG) or to Heartland or Elavon. Shift4, Heartland or Elavon process the card authorization and/or sale and return the number in encrypted format to acPMS as a truncated number and a token. The full magnetic stripe data is not kept on your hardware and the tokens that are returned by Shift4, Heartland or Elavon are of no value to a thief.

When a credit card number is manually entered into the PMS for an authorization and/or sale, the staff can include the name on the card, the card's validation code or value as well as the billing address's zip code. If the card's code and/or value is entered, neither are retained anywhere within the PMS. They are passed to the processor who uses them only to further validate the card and are not returned to the PMS once an authorization or sale is obtained.

A debit card's PIN and/or PIN block data is one of the most dangerous numbers to retain. acPMS does not support pin-based debit transactions. acPMS' credit card interface processes debit cards only as a credit card; therefore, transmitting the PIN is not possible.

When a reservation is entered in the PMS, a valid credit card number and expiration date is usually required as a guarantee. Once the credit card number is entered in acPMS, it is sent in an encrypted format to the Shift4 UTG or to Heartland or Elavon. The processor then returns a token with a partial credit card number. This token is used for all future authorizations, sales and refunds made to the card through the PMS. Any user looking at the reservation's credit card data only sees a masked credit card number and expiration date.

If a reservation was taken prior to acPMS' tokenization being enabled, when the credit card number and expiration date was entered, acPMS encrypted the card information. Anyone looking at the reservation sees a masked credit card number and expiration date. Only a user with specific 'view rights' can see the unmasked card number. All credit card 'views' are logged by acPMS and reference the reservation's confirmation number.

acPMS' reservation forms do not have a field to enter the Card Validation Code/Value and/or the PIN block data, so any card validation codes/values and PIN block data cannot be kept within the PMS.

acPMS masks PANs and expiration dates on reports and encrypts them on backups. The PMS' backups are compressed using zip methodology and are kept on the acPMS server computer on other removable media, and/or sent off site.

There may be instances when you need to retrieve a guest's full credit card number and expiration date. Depending on the situation, you will get the card number and expiration date from your processor, or in limited circumstances, from within the PMS.

The PMS can show an unencrypted credit card number only on an existing reservation and only to specific staff. View ability is based on user permissions which are set by property management through the ACAdmin module. All views of unencrypted credit cards numbers held in the PMS are logged by acPMS. You must limit the number of staff who has access to this data. When setting up your users in acPMS, only those employees on a "need to know" basis should have access to read full card numbers, process refunds, etc. (PCI DSS Reqs. 7.1).

acPMS retains active reservations that do not have an advance deposit posted to them for a default of 60 days past the arrival date. The retention date is configurable by the hotel in the ACConfig module. These reservations have a status of guaranteed, hold, share-with, wait list, checked in/out, no show, or canceled. During that time, an authorized staff member has the ability to go back and retrieve a guest's unmasked credit card information if they have 'view rights' and if the reservation was created prior to tokenization. If a reservation has an advance deposit posted to it and it is not checked in, it will remain in the reservation file until the Deposit balance is $0.00, and then will be purged based on its arrival date. The ability to see an unmasked credit card in a past reservation also depends on your property's retention period as discussed in Section 2 of this document.

Per PA-DSS 1.1.5.c, acPMS support staff, customers and integrators will: collect sensitive authentication only when needed to solve a specific problem; store such data only in specific, known locations with limited access; collect only the limited amount of data needed to solve a specific problem; encrypt sensitive authentication data while stored; and securely delete such data immediately after use.

A customer's dataset is only downloaded when necessary to troubleshoot a problem.

An AutoClerk technician downloads the dataset to a virtual computer (VM Island) via Bomgar. The dataset is 1) restored using the backupkeys provided by the property;2) cleaned by running a utility which replaces credit card numbers and expiration date information with bogus information; 3) the Users file is replaced; and 4) the backupkeys are changed. A new backup is then done. The cleaned and backed up dataset is placed in the client's folder on the AutoClerk Date SharePoint site. The dataset on the virtual computer is then securely deleted.

The dataset on the SharePoint site can then be used to troubleshoot the problem. Once the issue has been resolved that hotel's data is securely removed from any support/development/QA computer it was restored on and deleted from the client folder on the SharePoint.

2. Protect Stored Cardholder Data

Protecting cardholder data includes the following: 1) Securely deleting cardholder data after a customer-defined retention period as well as when it is no longer required for business, legal, or regulatory purposes; 2) Masking and truncating card numbers when displayed; 3) Rendering the card's PAN unreadable; and 4) Protecting and managing cryptographic keys.

Cardholder data exceeding the customer-defined retention period must be securely deleted per PCI DSS. Cardholder data must also be securely deleted when it is no longer required for legal, business and/or regulatory purposes. Listed below are all the locations where acPMS stores cardholder data so you know the locations of data that will be deleted.

acPMS is configured so a property can define 1) How often acPMS checks; and 2) A retention period, after which, acPMS securely deletes cardholder data. Both parameters are expressed in days. The default settings are to check every 7 days and to retain 90 days.

acPMS stores credit card data in four files: Reservations, Group masters, Inhouse folios, and Folio history. When acPMS checks these files at the defined interval, cardholder data is selected for purging according to the following criteria:

1. All Reservations except Permanent Reservations: Departure date is older than today - <retentionperiod>.
2. Permanent Reservations: Reservation creation date is older than today - <retentionperiod>.

3. Group Masters: The later of (group departure date, last room block) is older than today - <retentionperiod>.
4. Inhouse folios: (1) Folio is checked out, and departure is older than today -2, or (2) Folio is checked in, and arrival is older than today - <retentionperiod>.
5. Folio History: Departure date is older than today - <retentionperiod>.

The credit card data is cleared by encrypting the truncated credit card number over the encrypted full card number and rewriting the record. A manager can also run the utility at any time to delete cardholder data past a defined number of days. Call acPMS support for the option codes and steps.

What does this mean to the hotelier? For example, let's assume a hotel manager defines a check interval of 14 days and retention period of 120 days. acPMS will, automatically, every 14 days, on the Night Audit, examine the cardholder data locations and clear sensitive cardholder data per the rules stated above.

The nalog.txt, which is produced at each Night Audit, logs the secure deletion which took place during that audit.

Prior to deleting, a user with view rights can see a full credit card number on a reservation created prior to tokenization being enabled. Post deletion, even with view rights, all the user will see is a truncated and masked credit card number on a reservation. Credit card data which is part of an advance deposit folio, inhouse folio credit card data, and historical folio history already is truncated and contains a token from Shift4, Heartland or Elavon.

acPMS' responsibility is to make sure that any PAN is masked when displayed but can be displayed "to those employees and other parties with a specific need to see full PAN". The PAN is unreadable anywhere it is stored. The PMS stores credit card PANs using encryption or tokenization. The full credit card data is securely stored at the processor. The reports and historical data produced and maintained by the PMS contain only the truncated credit card numbers and expiration dates.

Displays of masked PANs include guest folios, daily sales transmittal batch, reservations, inhouse folios, receipts for non-guest charges and payments, credit card logs and advance deposit receipts. With tokenization enabled, the only place an unmasked PAN can be viewed is in a prior created reservation; and even then, the user must have 'view rights'.

When acPMS is installed at a property, the manager is instructed to set up all acPMS users with a unique login using the ACAdmin module. Part of the user set-up includes assigning users the 'right' to view unmasked credit cards. The manager is instructed to assign that right to as few employees as necessary. With the introduction of tokenization from the card processors, the only unmasked PANs a user would be able to see would be on a reservation created prior to tokenization being enabled. Instructions and details on acPMS user setup are in the acPMS training document: ACAdmin Module.

Everywhere that acPMS stores a PAN, it is unreadable. There are no options the user can configure to make them unreadable as it is part of the program.

Every backup of the acPMS data is encrypted by two (2) user defined and changeable keys. Regardless of where these backups may be stored: on the server, on portable devices, off-site, the PAN is unreadable. These backup keys are different than the keys used to encrypt the credit card data.

There are no logs in acPMS which have readable PANs. They are all masked and encrypted.

acPMS uses two (2) cryptographic key elements: a Key-Encryption-Key (KEK) and a Data-Encryption-Key (DEK) which are used to encrypt credit card data. The KEK is composed of a 72-byte random key. The KEK is used to encrypt/decrypt the DEK; the DEK is used to encrypt/decrypt the data. Both keys are stored in the server registry in binary format. They are protected by the Windows registry protection mechanism which, when properly set up by the property's network administrator, prevents access by any network user or any user of the same computer without the correct credentials. The KEK is also protected by being obfuscated using an internal encryption routine. You must restrict access to these keys to the fewest number of people necessary and store them securely in the fewest possible locations and forms. (PA-DSS Req. 2.4)

The backup and cryptographic encryption keys expire every 365 days. The Encryption Key Expiration report is produced every day by the Night Audit function. If a key's expiration is in the next 14 days, it will be listed so the property knows it needs to be changed. The report will continue to be produced until the key(s) has been changed. The report can be produced at will through the Utilities menu.

When the credit card encryption keys have expired, or on demand, an acPMS administrative user can invoke a program through the ACAdmin module that generates two (2) new keys, re-encrypts every cc number in the data set, including historical data, using the new DEK, and stores the new keys. The user does not have the ability to enter their own keys; the program automatically generates them.

Properties can change the backup encryption keys at any time. They must change them when they expire, anytime they suspect their data has been compromised, or when the integrity of the keys has been weakened or possibly compromised. (PA-DSS 2.5)

acPMS does not retain the retired or replaced cryptographic keys, which make them irretrievable. (PA-DSS Reqs. 2.5.5, 2.6) Irretrievability is absolutely necessary for PCI DSS compliance.

acPMS' backups are also encrypted using two (2) separate keys. The backup encryption keys must be entered and kept by two separate employees. When the backupkeys are changed, each key custodian enters their key manually, and stores it per the property's security policy. When the keys are entered, they are not clear text.

"Appendix B" is a sample Key Custodian form (PA-DSS Req. 2.5 and PCI DSS Req. 3.6.8) which all key custodians should complete and keep in a secure place.

The only cryptographic key material in earlier versions of the acPMS client was a built-in credit card encryption key in executables such as ac2g.exe. Part of the acPMS conversion/upgrade process to Version 9 included securely deleting all instances of the acPMS client executables within the active data. This process securely deleted any cryptographic key material and/or cryptogram from previous versions in the active data and made them irretrievable.

3. Provide Secure Authentication Features

Per acPMS' System Specifications ("Appendix A"), and as a requirement for your PCI DSS compliance, every employee who has computer access must have a unique username and password on every computer they use. Your network administrator must assist you in setting up these computer users. The users must be standard users and NOT administrator users. It is your responsibility, as staff members change, to ensure that the users are disabled/removed and added; as necessary.

acPMS' ACAdmin User Guide details the requirements and procedures for setting up acPMS users, for both admin and general user purposes.

Every employee using acPMS must have a unique user name and password they use when they log into an acPMS session. Duplicate user names or initials are not allowed. acPMS passwords must be at least 7 characters and contain at least one number and one letter. In addition, they can contain upper and lower case letters, and/or special characters (e.g., punctuation). Setting up a user's login name and password must be done immediately upon their hire. Do *not* set up or use any default acPMS user accounts or passwords. A manager must have two user accounts in acPMS: one for everyday use and another to administer user names and passwords within the ACAdmin module. A user's name and password to log into acPMS will not allow them to log into ACAdmin.

acPMS enforces secure changes to authentication credentials by the completion of installation by providing the GM a user name with a one-time use password. This allows the manager to access ACAdmin to then set up all the acPMS users.

Properties and any third-party integrators must assign secure authentication to any default accounts (even if they won't be used), and then disable or not use the accounts. (PA-DSS 3.1)

acPMS users' passwords expire after 90 days and then must be reset. The new password cannot be any of the past four passwords. If an acPMS user fails to log into a terminal 6 times, they will be locked out of that terminal for 30 minutes. Rebooting the terminal does not shorten the timeout of this feature. Your network vendor must set up all computers to require Windows logon if the station has been idle for more than 15 minutes. All acPMS user passwords are encrypted and are never seen in clear text. In addition, all login attempts are logged by the PMS server and are viewable through the ACAdmin module.

When an employee leaves your employment, you must immediately delete *all* their users' logins including Windows and acPMS. Take any other steps necessary depending upon the duties and/or access the ex-employee had, such as changing locks on storage areas for credit card data or being a key custodian.

acPMS strongly advises its customers to control access, via unique user ID and PCI DSS compliant secure authentication, to *all* systems, PCs, servers, and databases that contain payment applications and/or cardholder data. (PA-DSS 3.2)

Your property's written security policy must include your rules regarding users, passwords, and access to ALL credit card data whether it is on the active dataset, within Shift4, Heartland or Elavon, on removable backup media, and/or on paper.

4. Log Payment Application Activity

acPMS automatically creates a variety of logs, such as credit card logs and user access logs. (PA-DSS 4.1) Credit card logs include the logged in user identification (clerk ID), type of event (I.e., Authorization), date and time, success, or failure indication (I.e., Approved), origination of event (Shift and Station Number), Identify or name of affected data, system component, or resource (Room/Folio Code).

The server application logs those events that affect security including each time a staff member logs into acPMS, successful or not, when an employee views an unmasked credit card PAN and expiration date; as well as actions taken by an acPMS administrator. These logs are accessible to an acPMS administrator logged into the ACAdmin module.

Logs are automatically created; they cannot be configured or disabled by the user. (PA-DSS 4.1) Logs are automatically exported into a CSV or text file. The log files are located on the property's server computer in:
\app\autoclerk\060.002\[hotelid]\logs
\autoclerk\[hotelid]\data\credit

These logs can be imported into any standard centralized logging system. To access the logs, you must log onto the acPMS server computer as an administrator. From the centralized logging system, you can import the data. The file type should be CSV or text. (PA-DSS 4.4)

5. Develop Secure Payment Applications

This section of the *PA-DSS Requirements* applies to acPMS and how we write, develop, test, and implement our software application. It is important you are made aware of how the PMS is developed, tested, released, and implemented to aide you in complying with PCI DSS.

Prior to release from Development to UAT, all code is run through an analyzer to test for vulnerability and is reviewed by the Best Western Security Team. If any 'fails' are found, the code is fixed and re-submitted to the Security Team for review before being passed to UAT. In addition, the developers go through yearly training on secure coding.

Prior to being released to our clients as either a beta or a production version, all new builds of the PMS and interface applications are tested in-house under the direction of our UAT department per their test plans. "Test only" credit cards are issued by the processors to be used for testing. No active or "live" credit card numbers are used.

Development, UAT, and Production are separate departments. Any new code comes from Development goes through Security and is passed to UAT. UAT oversees the testing of the new code. Once successfully tested, UAT passes the build to Production for implementation in the field. The code passed from UAT to Production to be implemented in the field is an executable file. No test data is included.

When a new version is implemented at a property, the General Manager is advised they can go to http://www.myautoclerk.com for the current version of the 'What's New' and any other additional release documentation.

acPMS releases follow a 'Versioning Methodology'. Release versions are numbered as follows:

Version 9 is the major version number; this is also referred to as 060

002 is the minor version number;

005 is the release number;

xxxx is the build.

The versioning methodology is:

A change in major version number indicates a change in application architecture, data structure, or both.

A change in minor version indicates a smaller change in data structure such as the addition of fields to a record.

A change in release number indicates a noticeable improvement to one executable. Programs with different release numbers are interoperable. Moving from one release to another involves changing only the executable concerned.

The build edition changes every time a bug or non-noticeable (behind the scenes) change is made. It is used to identify the exact version of each executable independently of the above versioning system. Build numbers change through the alpha and beta test cycle and stop when the program is released in its final form.

6. Protect Wireless Transmissions

Wireless connections to the acPMS network segment are not recommended or supported. acPMS has not been developed to be used in a wireless environment.

If *any* workstations are wirelessly connecting to your network, they *must* be configured to use industry best practices such as IEEE 802.11i to implement strong encryption for authentication and transmission. It is prohibited to implement WEP.

In addition, if wireless is used, customers, integrators and/or your network administrator must:

1) Verify all encryption keys are changed from default at the time of installation and are changed if anyone with knowledge of the keys leaves the company or changes positions

2) Change the SNMP community strings

3) Change all default passwords/passphrases on access points

4) Update firmware is updated to support strong encryption for authentication and transmission over wireless networks

5) Verify other security-related wireless vendor defaults are changed

6) Install a firewall between any wireless networks and systems that store cardholder data

7) Configure firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

Your network administrator must verify that the wireless technology is protected with personal firewall software. The firewall software secure configuration must not be alterable by an employee. All vendor defaults, including keys, are changed at installation and whenever the person knowing the key leaves or changes positions; SSID broadcast is disabled; default Simple Network Management Protocol (SNMP) community strings are changed; all access point passwords are changed; WPA or WPA2 are enabled, if possible. At all times, industry best practices to implement strong encryption for authentication and transmission of cardholder data must be implemented.

7. Test Payment Applications to Address Vulnerabilities and Maintain Payment Application Updates

This section of the PA-DSS refers to acPMS' internal processes, which keep acPMS up to date on potential security risks to the acPMS program and credit card data.

If any possible threats are found to the acPMS application, they are investigated, fixed, tested, and deployed to our customers in a timely manner.

It is your responsibility to do the same for your network, including having your network administrator run regular network scans to check for any intrusions and/or unauthorized access attempts. Internal and external network vulnerability scans must be run at least quarterly by a PCI approved scanning vendor, as well as after any significant change in your network. In addition, intrusion-detection systems must be installed to monitor all traffic in the cardholder data environment and to alert personnel to any suspected compromises.

All acPMS updates are delivered securely via two-factor authentication and through our internal "chain-of-trust."

When UAT has completed testing of a new build, it advises Production via email that the build is ready for beta deployment. Production and UAT select a beta property. Production advises the property that a build is available and schedules the update.

To install the update, an AutoClerk Technician 1) initiates an acPMS Bomgar session with the property; 2) renames the old executable; 3) transfers over the new executable; 4) verifies the build with the property; 5) deletes the old executable; and 6) the Bomgar session is ended. Lastly, the manager is advised that the updated What's New documentation is available on www.myautoclerk.com

8. Facilitate Secure Network Implementation

You must have certain security tools in place. These tools include, but are not limited to, an external hardware firewall, anti-virus software, and traffic filtering devices.

Updates to these entities such as your Windows Operating System, anti-virus program, etc., need to be managed, monitored, and installed. Your network administrator must install these tools and train management and staff on their use, management, and maintenance.

Having these security tools implemented on your network computers does *not* interfere with acPMS when they are properly configured. They also do not interfere with acPMS' staff's ability to remotely connect to your system via Bomgar.

The only third-party service, protocol, component, etc. that acPMS requires is Actian's Pervasive PSQL 13 and above. acPMS technicians install Pervasive as part of your initial acPMS installation.

9. Cardholder Data Must Never be Stored on a Server Connected to the Internet

acPMS does not use a web server or database server.

10. Facilitate Secure Remote Access to Payment Application

Multi-factor authentication must be used whenever *anyone* remotely accesses your network. Multi-factor authentication requires users to produce at least two (2) credentials to access a system. Credentials consist of something the user has in their possession e.g., smartcards or tokens; something they know e.g., a password; and/or something they are e.g., a biometric such as a fingerprint or retina pattern. To access a system, the user must produce at least two (2) of the factors. (PA-DSS 10.1)

acPMS does not interfere with outside entities using multi-factor authentication to access your network. acPMS support staff use two-factor authentication whenever we need to gain access to a hotel's network. All remote access by acPMS support is facilitated by known secure solutions: Bomgar and secure tokens.

Bomgar is a security cloud application. acPMS has its own dedicated and protected segment on the application. Each acPMS Support employee has their own hardware (or software) token which generates a unique number every 60 seconds and is used to initiate a Bomgar session and then connect with a property. Only authorized acPMS employees with a valid token generated number can access our segment.

Support and/or tech sessions with our customers can be conducted in the following ways:

1. Customers initiate an acPMS support session by visiting esupport.autoclerk.com from a browser and enter the pin code the support agent gives them over the phone. The pin is only good for that support session.
2. An acPMS support agent may email a link to the customer.
3. The link may be accessible via other locations.

The Bomgar connection does not interfere with RADIUS, TACACS, or corporate VPNs. All remote access is logged by Bomgar.

For all remote access, you *must* use and implement remote access software security features such as requiring a unique user name, authenticating all users, changing all default settings, enabling lockouts, enabling data encryption, enabling logging, allowing connections only from specific (known) IP/MAC addresses, and establishing customer passwords according to the PCI DSS requirements. PCI compliant use of all remote stations must be part of your property's security policy.

acPMS requires that the computer running the AutoServe program have high-speed Internet access. It must be persistent and static and must be accessible via public (not private) address. Examples of such broadband services would be DSL, T1, or Cable Modem. acPMS does not access properties via a dial-up modem.

Because the server has a static and persistent IP, it must be secured behind your hardware firewall. Proper configuration of the firewall will allow access only to those approved vendors/persons/entities. Any Regional stations must also have at minimum, a personal software firewall installed and properly configured in a secure manner.

Properties must insist that all remote-access technologies used by their vendors and business partners be activated only when needed and immediately deactivated after use. This includes any updates delivered by a payment application.

acPMS recommends its customers use a securely configured firewall or a personal firewall product if a computer is connected via VPN or other high-speed connection and to secure these “always-on” connections, per PCI DSS Requirements 1 and 12.3.9. (PA-DSS 10.2.1)

The access should be logged and be disabled when not in use, multiple incorrect log ins must lock out the account.

11. Encrypt Sensitive Traffic over Public Networks

Customers and integrators are to use strong cryptography and security protocols if they send any cardholder data over a public network. (PA-DSS 11.1)

acPMS can send guests a reservation, cancellation and/or thank you letter via email. However, even if the letters are formatted to send the guest's credit card number used to guarantee the reservation, it sends the masked PAN and only the last four digits of the number. The full PAN is never sent . A property must specifically request to have the masked credit card number appear in the emails and the default letters updated. (PA-DSS 11.2.b) Full PANs are, in the limited areas they are viewable, viewable only. acPMS does not facilitate the sending of full PANs over public networks or any end-to-end messaging such as instant messaging. Any credit card information sent to the payment processor is encrypted and tokenized. In addition, communication to/from Shift4 goes through their UTG.

12. Secure All Non-Console Administrative Access

acPMS program does not facilitate non-console administrative access.

13. Maintain a PA-DSS Implementation Guide for Customers, Resellers, and Integrators

acPMS' website for our customers is http://www.myautoclerk.com. It contains: the System Specifications, a link to our interactive training videos, training documentation, user documentation and the 'What's New' documents. The What's New is updated with each release. These are available under the "Documentation" tab. Customers can also select Help at the top of the PMS' Main menu to access the documentation.

Prior to AutoClerk's installation, a link to this document is provided to the property. The *acPMS PA-DSS Implementation Guide* can also be found at http://www.myautoclerk.com.

It is reviewed and updated at minimum on a yearly basis and is updated as needed to document all major and minor changes to acPMS.

14. Assign PA-DSS Responsibilities for Personnel, and Maintain Training Programs for Personnel, Customers, Resellers, and Integrators.

acPMS' Dir. of IT is responsible for assigning PA-DSS responsibilities; providing annual security training for personnel; as well as developing and implementing training and communication programs.

Appendix A: System Specifications

AutoClerk's goal is for your hotel to have a reliable and secure acPMS installation. To ensure all acPMS functions and capabilities perform as specified, please follow these steps.

Your network set up and installation *must* comply with the *Payment Card Industry Data Security Standard (PCI DSS) version 3.2.1 of May 2018*. The PCI DSS requirements include but are not limited to the firewall, antivirus programs, user accounts and their permissions, and physical and network access to the server. This document references the PCI DSS Requirements for your reference. It is your responsibility to ensure that your computers and network comply.

You must make sure your computer/hardware/network administrator follows best practices with regards to network security. Your network administrator should hold current Microsoft Certifications, for example: Microsoft Certified IT Professional (MCITP). Having this credential does not give assurance of Information Technology (IT) competency, but it shows your vendor is keeping up-to-date with industry standards.

We require the purchase of business-grade computers. This is important because the property operates 24/7 and many of the computers, especially the acPMS server, will also run 24/7. It is recommended that you select a hardware vendor who can provide support for the computers, network, operating system, and other software during the hours your property needs such support.

acPMS technicians will *not* install the acPMS software on computers that do not meet acPMS' Specifications. This can delay an installation and increase costs. To avoid costly repairs and delays*, please be absolutely sure* that your hardware vendor reads and follows *acPMS' PA-DSS Implementation Guide* and acPMS' "System Specifications"; you order the correct equipment from your vendor, and your vendor delivers and properly installs the equipment you ordered.

General Installation Requirements

1. High-speed Internet access is required. It must be persistent and static and be accessible via a public (not private) address. Examples of acceptable broadband services would be DSL, T1, or cable modem.
2. External Hardware Firewall (PCI DSS Req. 1): This is a dedicated device placed between your Internet connection and Local Area Network (LAN). It is not sufficient to rely exclusively on personal software firewalls co-resident on your LAN. Examples of software firewalls are Windows Firewall, Zone Alarm, BlackIce, and Panda. If present, software firewalls must be configured to allow acPMS internal LAN traffic (tcp/udp ports 11193). Shift4's (credit card gateway) internal LAN traffic uses port 17477, and it uses tcp ports 26880 and 26881 for its outbound traffic. Depending on what, if any, Internet reservation interfaces you have with acPMS, additional(s) ports will need to be opened.

3. acPMS support uses a system/product called Bomgar, which requires ports open for the hotel staff to get out on the Internet to initiate a support session. See Support - Establishing a Connection below for the necessary ports.
4. The 1000 Base T Network Switch is made by one of the following manufacturers:
   - 3Com http://www.3com.com (Now part of HP)
   - HP http://www.hp.com
   - CISCO http://www.cisco.com (including Linksys http://www.linksys.com)
   - Edimax http://www.edimax.com
   - Dell http://www.dell.com
   - Netgear ProSafe http://www.netgear.com/

   In addition:

   a. All equipment must be connected to mains power via a surge suppressor or an uninterruptible power supply (UPS) of sufficient capacity. All surge suppressors used should be supplied with an insurance policy.

   b. Serial ports are RS232C with male DB9 connectors.

   c. All serial interfaces require one serial port (RS232C DB9). Interfaces run on the acPMS server. If you are not sure how many interfaces the property is purchasing, please contact Adam Williams at adam.williams@autoclerk.com.

   d. If you need to add a serial port, the acPMS approved extenders are:
      - Digi Neo for low profile solutions https://www.digi.com/products/usb-and-serial-connectivity/serial-cards/digineo
      - Digi AccelePort Xr920
      - Edgeport USB to multi-port RS232C. https://www.digi.com/products/usb-and-serial-connectivity/usb-over-serial-hubs/edgeport

   e. All system clocks must be synchronized (PCI DSS Req. 10.4). This is imperative for the Best Western 2 Way Reservation Interface.

   f. Each station that processes physical credit cards must have a separate card swipe or EMV chip reader.

      a. Card swipes *must* be a MagTek MiniUSB Magnetic Stripe Card Reader: Part# 21040110.

      b. acPMS highly recommends you switch to EMV technology.

         i. You will need to purchase EMV readers.

         ii. acPMS has only certified specific EMV machines to work in conjunction with the three (3) certified credit card processors.

         iii. Contact Adam Williams at adam.williams@autoclerk.com for more information on where/how to purchase the card swipes and/or EMV readers.

All Computers

All computers must meet at minimum, the following specifications. (Note: Dedicated servers have additional requirements that override those given here.)

Permitted Operating Systems are Windows 10 Pro or Microsoft Server 2019.

1. Processor speed: Use Intel Pentium 4 or compatible processor, 2.0 GHz minimum.
2. RAM: You need 4 Gig RAM (minimum).
3. Video Card capable of supporting a display resolution of 1024 x 768 with 16-bit color.
4. Monitors: Monitors need to have a resolution of 1024 x 768 minimum. If it is a touch screen monitor, a serial port may be needed for the touch screen. Monitors may *not* be shared.
5. Keyboard and mouse: Use a standard keyboard and mouse. However, these may *not* be shared.
6. At least one (1) dedicated USB Port.
7. Network Interface Card (NIC): Use a 100mb/sec or Gigabit Network Interface Card (NIC) from these manufacturers:
   - 3Com http://www.3com.com (Now part of HP)
   - Intel http://www.intel.com or
   - Broadcom https://www.broadcom.com/products/
8. Anti-virus software: The software must be current, actively running and set to generate assessment logs (PCI DSS Req. 5.2). It should also be capable of detecting, removing, and protecting against all known types of malicious software such as worms, adware, and spyware (PCI DSS Req. 5.1.1).
9. Screen savers and computer lock-out screens: Set screen savers and computer lockout to require a user to re-enter their password to re-activate the terminal if it has been idle for more than 15 minutes (PCI DSS Req. 8.1.8).
10. User names and passwords: There must be unique user names and passwords for *all* users (PCI DSS Req. 8). (See the section in this system specification, “Installation” for more details on users and password requirements.)
11. Browsers: A browser *must* be installed for staff to see reports within acPMS as well as to get remote support.
12. If the Internet is blocked on computers, you *must* allow access to esupport.autoclerk.com so the property can get support from acPMS Support staff. Hotel staff will also need the ability to download an applet for the support session. You should also consider allowing access to http://www.autoclerk.com and http://www.myautoclerk.com.

Dedicated Server (Required for our Best Western Customers)

acPMS recommends that ALL properties have a dedicated server network. If you are an existing acPMS client and do not have a dedicated server network, consider switching to one. It will provide better security and system dependability. A dedicated server network can better support strong enterprise-level enforcement of operating system, anti-virus, and anti-spyware updates, while keeping user stations restricted to non-administrative access. If you are a Best Western (BW) property, a dedicated file server is required.

If your computer configuration is one -three computers, then you do not have to have a dedicated server. However, if you have four (4) or more stations and/or are a Best Western property, you MUST have a dedicated server network.

Specifications for the acPMS dedicated server are:

Note: If a specification is listed above for ALL computers, then it also applies to the dedicated server, unless a variation and/or addition is listed below.

1. Microsoft Operating Systems Server 2019. You can use Windows 10 Pro ONLY if the server network has three or fewer acPMS stations.

2. Intel Pentium 4 or compatible processor.
3. CD-ROM or DVD drive
4. 20GB Disk storage available for acPMS. It is highly desirable that redundant (RAID 1 or higher) disk storage be used. It may be SCSI or Serial ATA.
5. A server class Smart UPS with messaging enabled.
6. A serial port extender as specified above may be required depending on how many serial interfaces the property is purchasing.
7. The server must have a keyboard, mouse, and monitor but cannot share them with a workstation.
8. Speakers are not necessary for a dedicated server.
9. If the property is getting the credit card interface through acPMS, they MUST use Shift4, a payment gateway; Heartland Payment Systems, or Elavon Payment Services. (More on credit cards and the interface below.)

Station #1 and any station designated as a backup station #1

If you have an acPMS dedicated server, Station #1 is your main acPMS station. If you only have 1 - 3 stations and are opting to not have an acPMS dedicated server, then Station #1 will also act as a non-dedicated server. In both cases, Station #1 is usually located at the front desk. These are additional requirements for Station #1 (and the designated backup #1 only)

1. 40 GB Disk storage
2. CD-ROM or DVD drive
3. UPS

Credit Card Data Capture Security Requirements

ALL hoteliers that store, process and/or transmit confidential credit cardholder data, regardless of whether they process credit cards through acPMS MUST comply with the PCI DSS Requirements found at: https://www.pcisecuritystandards.org. A summary of the current requirements is:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Protect all systems against malware and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

If a property is purchasing the credit card interface through acPMS, they MUST use Shift4, a third-party payment gateway provider, Heartland Payment Services, or Elavon Payment Services. For information on switching payment processors or general information on the credit card interface, please contact Adam Williams at adam.williams@autoclerk.com or (623) 780-6174.

Notes:

acPMS does not endorse other application programs such as Microsoft Office or system services such as IIS, Apache or MSSQL, and cannot determine whether they may cause any incompatibilities.

If you choose to run other programs on a computer that is also running acPMS, you may need to increase RAM and disk capacities.

The primary front desk computer (Station #1) and the acPMS dedicated server, if you have one, are critical computers. Most properties require these computers to function 24 hours a day, seven days a week. These computers are responsible for creating a proper backup of hotel data.

Business grade computers and other business grade components must be used throughout the system. Consumer grade computers as found in many discount stores

are NOT suitable. Computers with Windows 10 Home or Media edition pre-installed are not business grade computers.

Installation Specifications

Network

While this section is aimed at dedicated server networks, acPMS is a client/server application. Even on a single computer, many parts of acPMS act as a network. Please make sure you cover all portions of this section.

It is the responsibility of the hotelier to establish, ensure and maintain their own security in regard to not only the physical access to computers but to the data and in particular, the credit card data through the network.

To view a PDF of our Network Topology, go to http://www.myautoclerk.com/ and look under the Specifications header.

1. Cabling CAT 5E (Minimum) - Cabling is the most critical part of any network. acPMS requires that all network cabling be wired to the Category 5E (minimum) specifications as defined by the EIA/TIA-T568-B standard.

If the property already has cabling in place, have your network administrator scan the line with a 1 GB CAT 6 Cable Certification Scanner. If the cabling passes at CAT 5E performance or better, have the administrator sign off on the scan certification and retain it at the property. If not, then make the necessary changes.

Sub-standard cabling is very difficult and expensive to diagnose. Many times, it will start out fine and decay over time. When it does have problems, the problems may mimic other types of software and hardware problems.

acPMS requires that the entire cabling hardware AND installation specifications be followed. This includes, but is not limited to:

- The quality of the cable
- Cable runs must be from a "Patch Panel" at the server location to a jack at the station locations.
- RJ-45 Patch Cords must be used to connect the actual computers to the jacks and patch panel.
- Patch Cords must be machine pressed. No handmade patch cords. No ‘Home Runs’.
- Cable runs must avoid appliances that can cause interference such as florescent lights.
- Jacks must be punch down, no screw connectors.
- Jacks and the Patch Panel are to be clearly marked and a wiring diagram posted at the server.

2. Wireless - Wireless connections to the acPMS network segment must NEVER be used.

If your property has ANY type of public wireless Ethernet accessibility, such as from guest rooms, it MUST be on a separate network segment. In addition, you MUST follow PCI DSS Reqs. 2.1.1 and 4.1.1. These requirements include but are not limited to configuring a perimeter firewall to deny traffic from any public access wireless environment to the acPMS Client environment; not using any default WEP keys; not using any default passwords; and enabling WPA technology, if applicable. (See Section 6 of the Implementation Guide for more information.)

3. Network Switch - acPMS requires the network to be at least 1000 Base T. If the acPMS dedicated server should fail, the PMS is designed so the server program can be installed on another computer and the network can continue to operate while the server is being repaired or replaced if the network switch and cabling are intact. The network switch must be plugged into the UPS so it will continue to function during a power outage.
4. Power, UPS, and Smart communications - Computers will not run without power and will not run well without proper power.

   Like cabling, clean power is critical! Each computer must have clean power. The file server must have a dedicated line with an isolated ground.

   Station #1 must have a battery backup (UPS). Make sure all components of Station #1 are plugged into the battery, the CPU and monitor. Laser printers may overload a UPS and therefore should not be plugged into one. Printers should be plugged into a surge protector. Some UPSs have surge protector outlets that are not UPS protected.

   The acPMS dedicated server requires a UPS with Smart messaging software. All components (CPU, Monitor, Network Switches ...etc.) must be plugged into this UPS. APC and PowerChute have proven to be reliable, and our staff are familiar with these products.

   As batteries age, the amount of power and the amount of time they can provide emergency power declines. The typical life expectancy is about 3 years. This life expectancy can be substantially shortened if the battery is used often. Depending on the quality of the power in your area, you may want a larger capacity UPS and may even need to consider installing a line conditioner to assure that the power is clean.
5. Server Location - The acPMS server must not be in a heavy traffic area. It should be in a well-ventilated, easily accessible but in/on a locked cabinet or rack. As your credit card data is transmitted through the server, you MUST restrict and control physical access to the server location. (PCI DSS Req. 9)
6. Server Operating System (If dedicated on a network of four (4) or more computers) - Must run Windows Microsoft Server 2019 as a Primary Domain Controller. Set it to automatically download updates so the system always has the latest updates and patches. Installation should be managed by your network administrator.
7. Drive Mapping - acPMS requires a "V:" drive map, sharing the acPMS Client install bin directory.
   a. acPMS will be installed in the file server's largest hard drive partition.
   b. Right click on the directory /autoclerk/bin and share it as "autoclerk"

c. Click on the "Permissions" button and set as follows:

d. Everyone = read only

e. This is the ONLY acPMS directory that users can see

8. We suggest using a Domain Login Script called otto.bat to set the drive mapping with the contents:

   net use v: \\192.168.0.100\bin /p:y

   If this is a Peer-to-Peer network, or a dedicated server running Window 8 Pro or Windows 10 on the non-sever station(s), we suggest you map the drive by creating an autostart.bat file to be placed in the all users startup folder. The contents should be: net use v: \\192.168.0.100\bin /p:y

9. User Accounts - Administrator(s)

   Create an Administrator user with a unique user name and complex/strong password. Do NOT use any vendor supplied defaults for any system passwords or other security parameters. (PCI DSS Req. 2) See Section 11 below for password requirements for ALL users. Make sure the hotel's General Manager/Owner knows the Administrative user name and password for the server and station #1.

   Create another administrative user, again with a unique user name and complex/strong password that will ONLY be used by acPMS. Call acPMS (925-284-1005) with that user name and password. acPMS technicians will need it to install our software and interfaces. Once the acPMS installation is complete and ALL interfaces have been installed and tested, you MUST disable that account. The account must be re-enabled "only during the time period needed and disabled when not in use and monitored when in use". (PCI DSS Req. 8.1.5)

   Those employees that need administrative level access to a computer must have a separate user and “complex” password with administrative access, which must only be used when that access level is needed.

   Property management must either disable or not use ANY users with Administrative rights on a day-to-day basis. (PCI DSS Req. 8.5)

10. User Accounts - Everyone

    ALL USERS MUST HAVE THEIR OWN UNIQUE ID (PCI DSS Req. 8)

    Your network vendor must get a list all current users from the hotel General Manager and set them up in Windows with a unique user name. These users must NOT have administrative rights. There must be an additional method of login authentication. Accepted methods include: a password, token device or biometrics. If the property chooses to use passwords, then the passwords MUST follow the requirements listed below.

    Customers are strongly advised to control access, via a unique user ID and PCI DSS-compliant secure authentication, to any PCs, servers, and databases with payment applications and cardholder data. (PA-DSS 3.2)

11. Network and Computer Password Requirements

a. any vendor supplied defaults must be changed prior to installing a system on the network (PCI DSS Req. 2.1)

b. control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.

c. verify the user's identity before resetting a password

d. set first-time passwords to a unique value for each user and set so it must be changed immediately after the first use

e. revoke access for any terminated users immediately upon their dismissal

f. remove/disable any inactive user accounts within 90 days

g. enable accounts used by vendors for remote maintenance only during the time needed; disable when not in use; and monitor when in use

h. hotel management must communicate password procedures and policies to all users who have access to cardholder data

i. do not use any group, shared, or generic accounts and passwords

j. users must change their passwords at least every 90 days

k. contains at least 7 characters

l. contains both letters and numbers

m. cannot duplicate any of the last 4 passwords

n. lockout ANY user after 6 failed attempts. This includes an administrator.

o. set the lockout duration to 30 minutes or until an administrator enables the user ID

p. authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users

q. Many of these requirements also apply to acPMS users. Please see separate documentation 'User Guide – ACAdmin' for details on setting up acPMS users.

12. Assign Login Script to Users - this is so the v: drive is mapped when they log onto stations and can use acPMS.

13. Disable Automatic Logon - Windows allows you to automate the logon process by storing your password and other pertinent information in the Registry database. Automatic logon MUST be disabled on EVERY computer on the network.

14. If a computer session has been idle for more than 15 minutes, require the user to re-enter their Windows user and password to re-activate the terminal. (PCI DSS 8.1.8)

15. Windows Components - On the acPMS dedicated server running Windows Server 2019, you must disable all unnecessary and insecure services and protocols. You must also remove all unnecessary functionality. (PCI DSS Reqs. 2.2.2 and 2.2.5)

Workstations

1. All non-server network computers must use Windows 10 Pro. Ensure your network administrator is managing the OS updates, so the system always has the latest updates and patches by enabling automatic download.
2. Check for maverick applications.
3. Make computers as basic as possible. Remove all icons from the desktop except 'My Computer', 'Network Neighborhood', and 'Recycle'. Consider a desktop lockdown policy.
4. Install anti-virus software on all computers. (PCI DSS Req. 5) Be sure the anti-virus programs are capable of detecting, removing, and protecting against other forms of malware. Also be sure the programs are current, actively running, and capable of generating assessment logs. They must be set to automatically update so they are always current with the program patches.
5. Remote acPMS stations (also known as Regional PMS) MUST be via Windows Terminal Services. When implementing the remote stations, be sure to follow best practices. Best practices include but is not limited to proper implementation of the hardware and personal software firewalls (PCI DSS Req. 1.3), not using any vendor supplied defaults (PCI DSS Req. 2.1.1), implementing session timeouts, idle timeouts, using non-standard RDP ports wrapped in a VPN tunnel and enabling auditing/logging.

   You should always use a ‘high’ level of encryption which encrypts data transmission in both directions using a 128-bit key for Terminal Services.

   Multi-factor authentication must be used when connecting to the acPMS network segment from a remote station. Multi-factor authentication requires users to produce a minimum of two (2) separate authentication methods to access a system. Credentials consist of something the user has in their possession (for example, smartcards or hardware tokens) and something they know for example, a password). To access a system, the user must produce both factors. (See PCI DSS Req. 8.2 and 8.3 for more details)

   Review PCI DSS Req. 12.3 for additional restrictions for remote access such as not allowing cut and paste. acPMS only allows remote access using Terminal Services that has been properly and securely set up by the hotel’s network administrator.

   acPMS recommends you use VPN or SSL/TLS for encryption for your Terminal Services, as you must "Encrypt all non-console administrative access." (PCI DSS Req. 2.3)
6. Disable or remove any unnecessary and insecure services and protocols (e.g., NetBIOS, file-sharing, Telnet, unencrypted FTP, and others).

TCP/IP

Set individual (static) TCP/IP addresses for each computer as 192.168.0.N, Subnet Mask 255.255.255.0.

N is replaced by the number:

Server, N = 100.

Station 1, N = 101;

Station 2, N = 102, and so on.

The Server and Domain should have unique names for each property. In addition, each computer must have a unique name. HOTELNAME_SRVR, STATION1, STATION2, etc. is a good naming convention. The names may NOT have spaces.

Test for TCP/IP connectivity on every computer.

acPMS Data Backup

acPMS backs up acPMS data, storing a copy on the internal hard disk of the acPMS server in [c]:\autoclerk\ [hotelid]\backup. It also places a copy of the backup on the internal hard disk of Station #1 in [C]:\ProgramFiles\AutoClerk\backup. These backups are performed by default at each shift change and during the night audit.

acPMS has an option to place a data backup on an extra directory or drive on the hotel's dedicated server or Station #1. This extra location may be an internal or external device but must be referenced as a drive letter or path (no UNC) from Station #1. The default location will be c:\autoclerk\ [hotelid]\backup\extra. The 'extra' backup is in lieu of the removable backup and takes place during the night audit. We strongly suggest the contents of this extra directory/drive then be copied by any third-party backup software product of hotel management's choice and stored offsite. An extra backup is disabled by default.

While there are many different third-party backup software solutions, one product in particular – IPVault by ipVAULT Storage Technologies has successfully proven itself at several acPMS hotel sites since 2006. Online backup is available as an additional service and cost. Please contact acPMS sales for more information.

acPMS automatically performs rolling purges of the acPMS backup folders on a nightly basis after a backup file has aged beyond a certain set point, as determined by hotel management. The number of backups kept on the drive is configurable.

Warning: If hotel management chooses to have no external backup service or removable media, the hotel is at risk of catastrophic data loss in the event of a hard disk crash (on the server and/or station #1).

Printers

A laser printer and acPMS' plain paper registration slips and folios, also known as stylesheets, are required for use with acPMS. There is also an option to have eRegistration slips and you can email folios.

There must be a default printer configured on Station #1. This printer will be used for night audit.

Printers should be connected directly to the network via TCP/IP. Any printer connected via USB will be for local (NOT shared) use only.

acPMS Support

acPMS support sessions are facilitated by known secure solutions: Bomgar and secure tokens.

Bomgar is a security cloud application. acPMS has its own dedicated and protected segment on the application. Each acPMS Support employee has their own hardware (or software) token which generates a unique number every 60 seconds and is used to initiate a Bomgar session and then connect with a property. Only authorized acPMS employees with a valid token generated number can access our segment.

Support and/or tech sessions with our customers can be conducted in the following ways:

4. Customers initiate an acPMS support session by visiting esupport.autoclerk.com from a browser and entering the session key the support agent gives them or clicking on a support agent's name. The pin code is only valid for that support session.
5. An acPMS support agent may email a link to the customer.
6. From within acPMS, on the Main Menu, customers click on Help, then click on Support. This redirects them to esupport.autoclerk.com where they can enter a session key given to them by the Support agent, or they can click on a Support agent's name.
7. The client software may be permanently installed on hotel computers, such as dedicated server computers, or others. If the property is interested in having this installed, please contact acPMS Technical support at (925) 284-1005 during regular business hours.

Establishing a Connection

A browser MUST be installed for staff to access the Internet to then get interactive support from acPMS staff. If the Internet is blocked on computers, you MUST allow access to esupport.autoclerk.com. Staff will also need the ability to download an applet for the support session.

Bomgar solutions are designed to work transparently through firewalls, enabling a connection with any computer with internet connectivity, anywhere in the world. However, with certain highly secured networks, some configuration may be necessary.

- Ports 80, 443, and 8200 need to be open for outbound TCP traffic.
- NOTE: Port 8200 is used as a rollover for port 443 and is not strictly required, though it is recommended.
- Internet Security software such as software firewalls must not block Bomgar executable files from downloading. Some examples of software firewalls include MacAfee Security, Norton Security, and Zone Alarm.

Architecture

The architecture of Bomgar solutions lends built-in security to the support process. Because session traffic is outbound from both directions, both the customer and the support representative can work from behind corporate firewalls providing a barrier to any potentially malicious traffic.

In addition, each Bomgar session is initiated by the remote customer when the support issue occurs and is then discontinued automatically when the session is complete, allowing only a small, irregular period wherein Bomgar traffic is crossing the Internet. This secure architecture provides the first level of Bomgar security, obscuring the entire support session by leaving existing security structures in place and spontaneously generating each support session.

Network Administrator Responsibilities

As the property's network administrator, you are responsible in training ALL staff on the following:

1. How to properly startup the system and log into the network.
2. How to properly shut down the system and the network.
3. Label and show them where all components of the system are including, but not limited to CPU, Monitor, UPS, Server, Network Switch, and Cable connections.
4. Windows Basics including but not limited to logging onto a computer, mouse use, active window, switching windows, and displaying the taskbar.
5. All non-acPMS programs. I.e., Word, Excel
6. How to check the battery level on the UPS.
7. How to set up, delete, enable, disable, and maintain Windows users and authentication.

While acPMS is the first point of contact for all acPMS related problems, you will be called upon when needed to provide support for the following:

1. Hardware
2. Operating system
3. Network Communication(TCP/IP) Problems
4. Non-acPMS programs (I.e., Word, Excel, Internet)
5. Printing
6. Data Security

If acPMS determines that you need to be brought in, the customer will normally contact you directly. You should then contact us, and we will go over the problem together and lay out a plan of attack. The idea is that by the customer calling you, you know you have the authorization needed to act. By talking to us, rather than the customer, you get accurate information on a technical level and the customer is not brought into the middle.

Should the customer contact you directly to work on the system, even if it seems non-acPMS related, we must be contacted ahead of time so we can determine if an acPMS technician will need to be available or is required. Upon arriving at the property, we need to be contacted so we can make sure proper steps are done to assure the smooth operation of the property. Once finished, contact us again, so we can run tests to make sure acPMS is running properly.

Security

As the network administrator, you are responsible for supporting the property's data security as stated in the PCI DSS. This includes but is not limited to:

1. Antivirus - Many of our customers use McAfee or Norton. (ALL computers on the network MUST have an antivirus program installed. It must be kept always running and be enabled for automatic updates to ensure they are current with security patches. They must also be capable of detecting, removing, and protecting against other forms of malware.(PCI DSS Req. 5)
2. Internet Firewall - acPMS requires a hardware firewall, however if you enable a software firewall in addition, then port 11193 MUST be opened for acPMS to run. (PCI DSS Req. 1)
3. Physical security of the dedicated server, if used. (PCI DSS Req. 9)
4. Regular testing of the security of the entire network (PCI DSS Req. 11)
5. Internal network security, including, but not limited to unique user names and passwords for ALL users; password rules and maintenance; user permissions; and enabling logs to track access.

The property's PCI DSS compliance depends, in part, on the set up and installation of the network hardware and software. Deviation from the above Specifications will make the property NON-PCI DSS compliant as well as vulnerable to breaches. It is the property's responsibility to see that their system is set up and installed in a PCI DSS complaint manner and that it is maintained to continue its compliancy.

Appendix B: Sample Key Custodian Form

The following is a sample of the Key Custodian form that must be signed by all Key Custodians:

The signee of this document acknowledges that he or she has been afforded access to key management devices, software, and equipment. I understand I have been chosen as a key custodian for one (1) acPMS backup encryption key.

I hereby agree that I:

1. Have read and understood the policies and procedures associated with key management and agree to comply with them to the best of my ability. I have been trained in security awareness and have had the ability to raise questions and have had those questions satisfactorily answered.
2. Agree to never divulge to any third party, especially including personnel who maintain the other half of the key management or related security systems, passwords, processes, security hardware, or secrets associated with the acPMS system, unless authorized by a manager, owner, or required to do so by law enforcement officers.
3. Agree 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 the following: Phone requests from unidentifiable callers for access to secure information, unidentifiable files found on computers, and unusual activity recorded in log files.
4. My duties are to generate my half of the acPMS backup encryption key when necessary and to always protect the integrity of this password. If it is written down, then the written password must be secured within a secure, locked area, preferably a safe, per my property's security policy

_____

Signature Date

_____

Print Name