AutoClerk User Guide
ACAdmin

Table of Contents

TABLE OF CONTENTS **2**

COPYRIGHT INFORMATION **3**

1. INTRODUCTION **4**

ACADMIN FUNCTIONS 4
ACAdmin, PA-DSS and PCI DSS *4*
USER GROUPS 4
USER ACCOUNTS 5
User Account Passwords *5*
FIRST TIME USE 5
Running ACAdmin and Station #1 ..... *5*
Default Passwords Required for Initial Use *5*
General Manager Account and AC Administration Group *5*
Number of Managers and Owners Using ACAdmin *6*
Managers/Owners Creating User Accounts for Staff *6*
Employees Forgetting Passwords *7*

2. ADMIN FUNCTIONS **8**

1. ENCRYPTION KEYS 8
Resetting a Key *9*
Common Keys *10*
License 10
Backupkey 1 and 2 10
bw2/rw 11
Credit Card Keys 11
2. CLERK SET UP 12
Creating a New User *12*
Active 14
Clerk Name - Initials 15
Level 15
User Groups 16
Final Steps 17
Password Details *17*
CLERK PASSWORDS 18
Resetting Clerks Passwords *18*
USER-GROUPS SETUP 19
Adding a New User Group *21*
Assigning Functions to a User Group *21*

3. ADDITIONAL ACADMIN FUNCTIONS **22**

RE-ENCRYPT DATA SET 22
VIEW LOGS 23
BACKUP 25

LIST OF FIGURES **26**

INDEX OF AUTOCLERK V9 ACADMIN ICONS, MENUS, AND COMMANDS **27**

Copyright Information

AutoClerk, Inc.

Address: 1981 North Broadway, Suite 430, Walnut Creek, CA 94596

Phone: 925.284.1005

Fax: 925.284.3423

URL: www.autoclerk.com

1. Introduction

AutoClerk has developed a user management program, ACAdmin, to comply with the Payment Card Industry's (PCI) Payment Application Data Security Standard (PA-DSS). ACAdmin is a completely separate application from the AutoClerk PMS client program.

AutoClerk, Inc. does *not* maintain any property's user names or passwords for an AutoClerk client, ACAdmin, or for Windows. This includes the two (2) backup keys needed to restore your dataset with encrypted credit card numbers should you have a fatal hardware crash. It also includes any interface startup passwords set in ACAdmin.

ACAdmin Functions

ACAdmin functions include setup, maintenance, and deletion of AutoClerk PMS user accounts and user groups as well as management of PMS Backup Encryption keys and Interface Login keys.

ACAdmin stores AutoClerk Server and Interface logs according to PA-DSS requirements. Through ACAdmin, a manager can view these logs for troubleshooting purposes, backup the AutoClerk PMS data, or re-encrypt the AutoClerk PMS data.

ACAdmin, PA-DSS and PCI DSS

AutoClerk clerk IDs and passwords comply with PA-DSS and PCI DSS requirements. Passwords are mandatory for *all* users' clerk IDs for the AutoClerk PMS. In addition, the property can set up different types of AutoClerk PMS users with various functions and permissions. For example, you can assign permissions to those specific users who need to perform backups, restore from backups, and view full credit card numbers.

Since credit card numbers used to guarantee reservations are encrypted and truncated, only employees assigned the specific function are able to see full credit card numbers within AutoClerk. (Note: There are few places where a full number might not be visible at all.)

If your property has credit card tokenization enabled, then once a credit card has been tokenized, the only way to see the complete number is to go through your processor.

All access and use of ACAdmin is logged automatically within the AutoClerk Server logs as required by PA-DSS.

To comply with PA-DSS and PCI DSS requirements, each clerk should log out and/or log in to change the current user before doing any work in AutoClerk. In addition, AutoClerk will automatically log the existing user out of an AutoClerk session if the station has been idle for more than 15 minutes.

User Groups

There are 4 default user groups. The first 3 user groups relate to performing functions in the AutoClerk PMS. The fourth user group is the AC Administration group.

- The AC Administration group deals solely with ACAdmin and is separate from anything to do with AutoClerk PMS usage.
- No identical user account may belong to the AC Administration group in addition to another group.
    - There must be a separate user account for the non-AC Administration group.

User Accounts

- A user is required to belong to at least one of the user groups.
- A user account consists of the following:
    - Clerk ID
    - Clerk Name
    - Initials

User Account Passwords

1. When you create a user, a one-time use password is generated by ACAdmin.
2. Users login with this password the first time to create their own unique password.
3. The password created by the user is only known by that user, since it is not created or entered into the system by anyone else.

First Time Use

This section contains an overview of details related to the first time you run and login to ACAdmin.

Running ACAdmin and Station #1

You can run ACAdmin from a shortcut on any AutoClerk station. However, when ACAdmin is in use, it takes over as Station #1. Station #1 must be logged out in order for ACAdmin to run. Other stations can continue to use AutoClerk while ACAdmin is running.

Default Passwords Required for Initial Use

1. After ACAdmin is installed, AutoClerk gives the GM (or another key staff member) a default clerk ID and password for access to the module.
2. This default password (but not Clerk ID) is past its expiration date. Therefore, the GM must create a new password immediately upon the first use of ACAdmin.
    a. All other users will follow this procedure when they first access AutoClerk PMS or ACAdmin.

General Manager Account and AC Administration Group

1. Once logged into ACAdmin for the first time, the GM creates his or her own ACAdmin user account.

2. This account (like any other) requires the following:
    - Clerk ID
    - Clerk Name
    - Initials
3. This account is required to belong only to the AC Administration' group. The AC Administration group is designed for key management roles consisting of owners, GMs, or property managers.
4. The user login credentials you use for the AutoClerk PMS cannot be used for ACAdmin.
5. The AC Administration group (owners and key employees) typically do not use ACAdmin on a daily basis. Make sure to choose new and unique components for your ACAdmin account identifiers (ID, Name, and Initials).

Number of Managers and Owners Using ACAdmin

1. You are permitted more than 1 user in the AC Administration group.
2. It is prudent to assign more than 1 key employee, owner or user to the ACAdmin Administration group, since the AutoClerk Support staff is not able to gain access or assist hotel staff to gain access to either AutoClerk or ACAdmin once the initial setup is completed.
    a. You might want to assign both the owner(s) and the GM to the AC Administration group, so both have access. Or you might assign the GM and the Front Desk Manager (this is especially helpful if these two positions often work different regular hours).
    b. Thus, if one of the parties leaves the property, then the other has rights to get into ACAdmin and make any necessary changes.
3. If you forget your user name and/or password and cannot log into ACAdmin, we can reset the user name and password three times for no fee. The current fee is $135.00 per reset.

Managers/Owners Creating User Accounts for Staff

1. GM’s need to create their own ACAdmin user account. This ACAdmin account is assigned permissions for the ACAdmin Administration group. This gives the GM the ability to create, modify, and delete other user accounts.
    a. The GM then creates user accounts for every employee using the AutoClerk PMS.
2. If you are a GM (or the key employee) creating these user accounts, remember you must also create an AutoClerk PMS user account for yourself. You will then have 2 user accounts:
    a. ACAdmin user account with ACAdmin Administration group permissions
    b. AutoClerk PMS user account

3. A staff member cannot use the AutoClerk PMS program until you set up their user account and password.

Employees Forgetting Passwords

1. If a clerk forgets their Clerk ID and/or password, only someone onsite with access to ACAdmin can reset it.
2. AutoClerk Support and Techs *cannot* reset passwords.
3. It is practical to give more than one person at your property ACAdmin Administration group permissions. So if one key employee is not onsite, another designated key employee can reset a password.
4. If a GM or key employee loses their own ACAdmin password, and are unable to have another ACAdmin user at the hotel reset your ACAdmin password, you need to contact AutoClerk Support staff during regular business hours and arrange to have your account reset to the default. (Remember, this may require a fee.)

2. Admin Functions

This section describes different ACAdmin administration functions.

1. Once you login to ACAdmin, the Home page appears as shown in Figure 1.

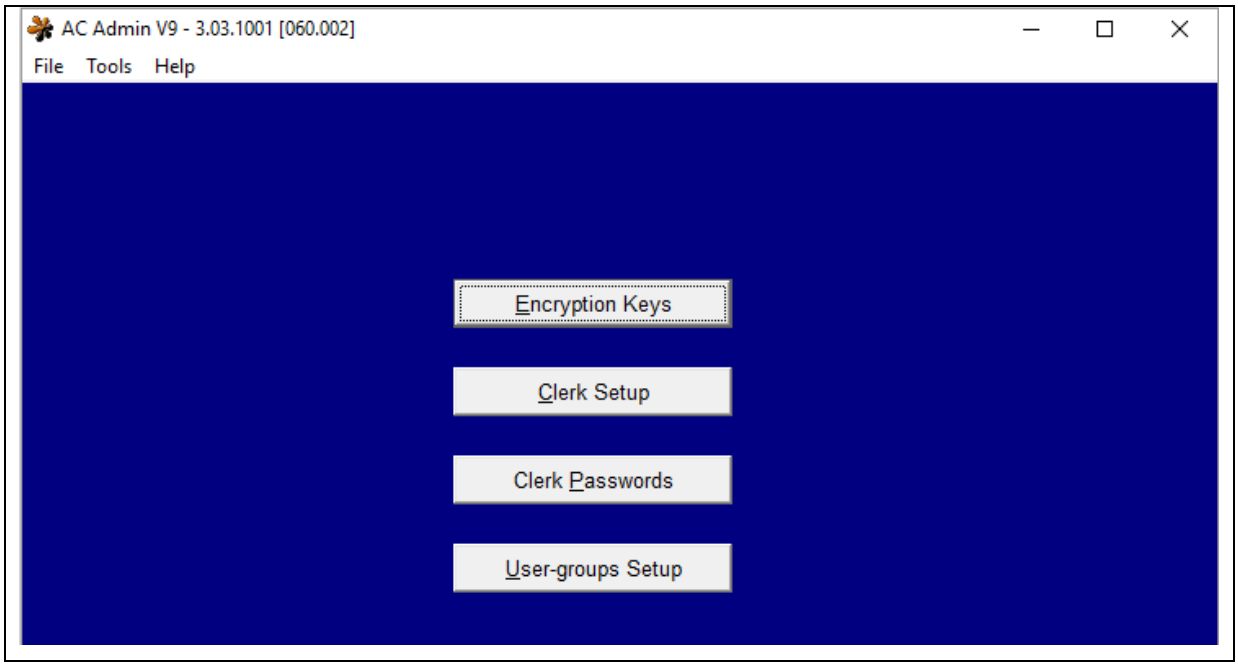

Figure 1: ACAdmin Homepage

1. Encryption Keys

1. On the ACAdmin Home page, click the Encryption Keys button.
    a. The Reset Encryption Keys window appears as shown in Figure 2.

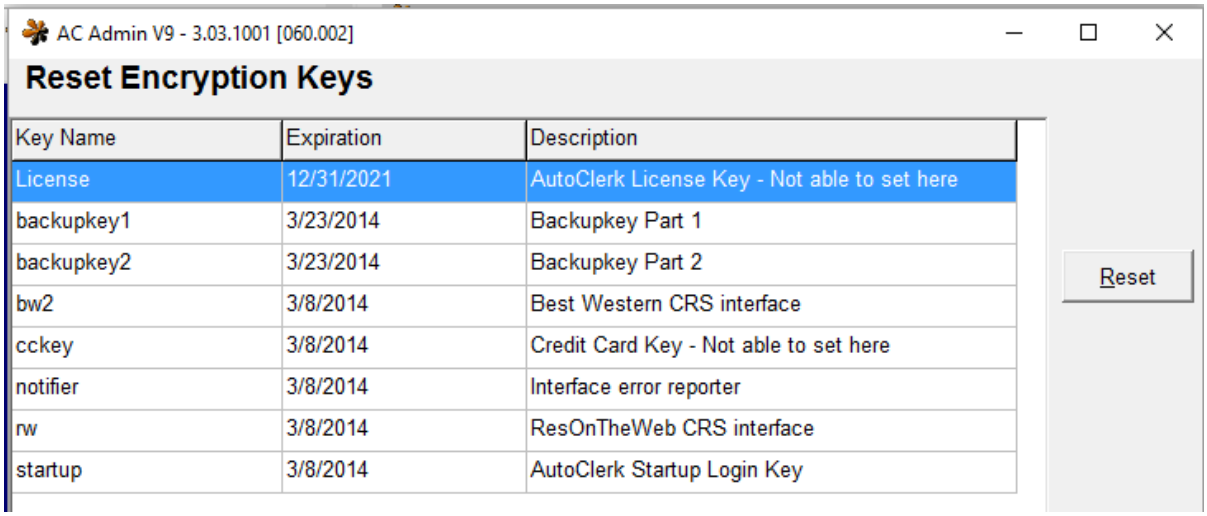

Figure 2: Reset Encryption Keys Window

   b. The number of keys and logins shown varies, as each hotel will have a different number of interfaces that require its own login.

2. The Reset Encryption Keys window displays the Key Name, the Expiration (date) for the encryption keys and logins, and a Description.
3. This is where you set and reset various encryption and login keys used by the AutoClerk PMS and its interfaces.
   a. An Encryption key tells a program how to encode data. Only someone, or program, who has the key is able to see (decode) the full data.
   b. Login keys can be thought of as passwords used by programs to invisibly login and run on the AutoClerk server. For example, interfaces such as an online booking agent, as well as the AutoClerk start-up routine use Login keys in order to function.
4. Encryption and Login keys MUST be changed at least once a year.
5. When you reset the Encryption and Login keys, you must also reset the Backup keys and re-encrypt the data.
6. The Night Audit automatically prints a report which lists any Encryption and/or Login keys due to expire within the next 14 days.
   a. This report is generated each night for those 14 nights or until the key is changed.
   b. The report can also be generated at will from View Past Night Audit Reports in the Utilities icon on the AutoClerk main menu.

Resetting a Key

1. To reset a key, highlight the line on which the Key Name appears

2. Click the Reset button. The Encryption Key [key name] window opens.
3. Enter the new key. Repeat the entry and click ok. AutoClerk updates the registry with the new key.
4. Resetting the Backupkeys is VERY important and mandatory for your PCI compliance.
    a. Please see the specific instructions below for resetting those keys.

Common Keys

Below is a list of common keys you will see in at your property. Remember that your specific list may be longer or shorter depending on the number of interfaces you have.

The first listing is always License. After that, the keys are listed in alphabetic order.

License

1. The AutoClerk License key can only be reset by AutoClerk Tech staff.
2. Computer stations added to the AutoClerk network cannot access the AutoClerk PMS until AutoClerk Support increases the number of licenses.
3. Users will get a pop-up each time they log onto Station #1 for 14 days prior to a license expiring, informing them to contact AutoClerk to have it reset.

Backupkey 1 and 2

1. Backupkey1 and Backupkey2 are the 2 separate keys (passwords) which are used by the system when zipping and unzipping AutoClerk data during shift change backups and the Night Audit. This data includes the encrypted credit card information.
    a. These keys are also used to restore AutoClerk data if there is a server crash.
    b. If AutoClerk Support or Tech needs to obtain a copy of the hotel's data in order to troubleshoot an issue, they cannot access that data without getting the two Backupkeys from hotel management.
2. Setting 2 separate Backupkeys by 2 different management-level employees is mandatory per PCI DSS.
    a. The Backupkeys also must to be recorded in a secure manner per the property's security policy.
3. Whenever you change the Backupkeys, all old backups become unreadable and cannot be restored unless you keep a record of previous Backupkeys and their effective dates.
4. AutoClerk, Inc. does *not* record and/or maintain the two (2) backupkeys needed to restore your dataset with encrypted credit card numbers should you have a fatal hardware crash. They are solely your responsibility.

   a. Should you have a fatal hardware crash and you do not have your backup keys, when your data is restored, your reservations will *not* have credit information in them.

5. The Backupkeys you decide upon should be complex but also ones you can remember.
   a. The keys are not visible, even as they are typed.
   b. A key must be between 12 and 16 characters and should follow Best Practices.
   c. It should contain at least one letter and one number.
   d. Keys are case sensitive and may contain special characters.
6. An AutoClerk technician will ask the management to type in the hotel's Backupkeys at the time of conversion/upgrade and/or installation.
7. Always the backup the AutoClerk data both before *and* after a Backupkey change. This way, if there are any problems, there is backed up data to which you can revert.

bw2/rw

1. These are the Best Western and ResOnWeb CRS interfaces.
2. They require a 'key' to log in behind the scenes and run.
3. When you change the keys, you MUST inform AutoClerk.

Credit Card Keys

1. Cckey is used to reset the credit card encryption key.
   a. Once the key has been reset, AutoClerk re-encrypts the credit card data with the new key.
2. To reset this key, go to the ACAdmin Main menu and select Tools on the title bar.
   a. Re-encrypting the credit card data may take a long time, depending on the number of records.
      i. It also requires that all stations be out of AutoClerk.
      ii. It is advisable to do this at a quiet time.
   b. Select Backup. You MUST backup your data prior to resetting this key.
   c. Once the backup is complete, select Re-encrypt Data Set from the Tools menu.
      i. Say Yes when asked if you have done a backup.
      ii. Say Yes at the warning that it could take hours.
   d. When complete, you will return to the ACAdmin Main menu.
3. Per your PCI compliance, you MUST reset your key at least once a year; of if you think your data may have been compromised.

2. Clerk Set Up

1. On the ACAdmin Home page, click on the Clerk Setup button. The Clerk Setup window appears as shown in Figure 3.
2. The Clerk Setup window contains all of the property's AutoClerk PMS and ACAdmin users.
3. Each user record consists of a Clerk ID, Clerk Name, Initials, (Permission) Level and a list of User Groups to which the user is a member.
4. A user's password is set once this form has been completed. See Clerk Passwords, below for more information.

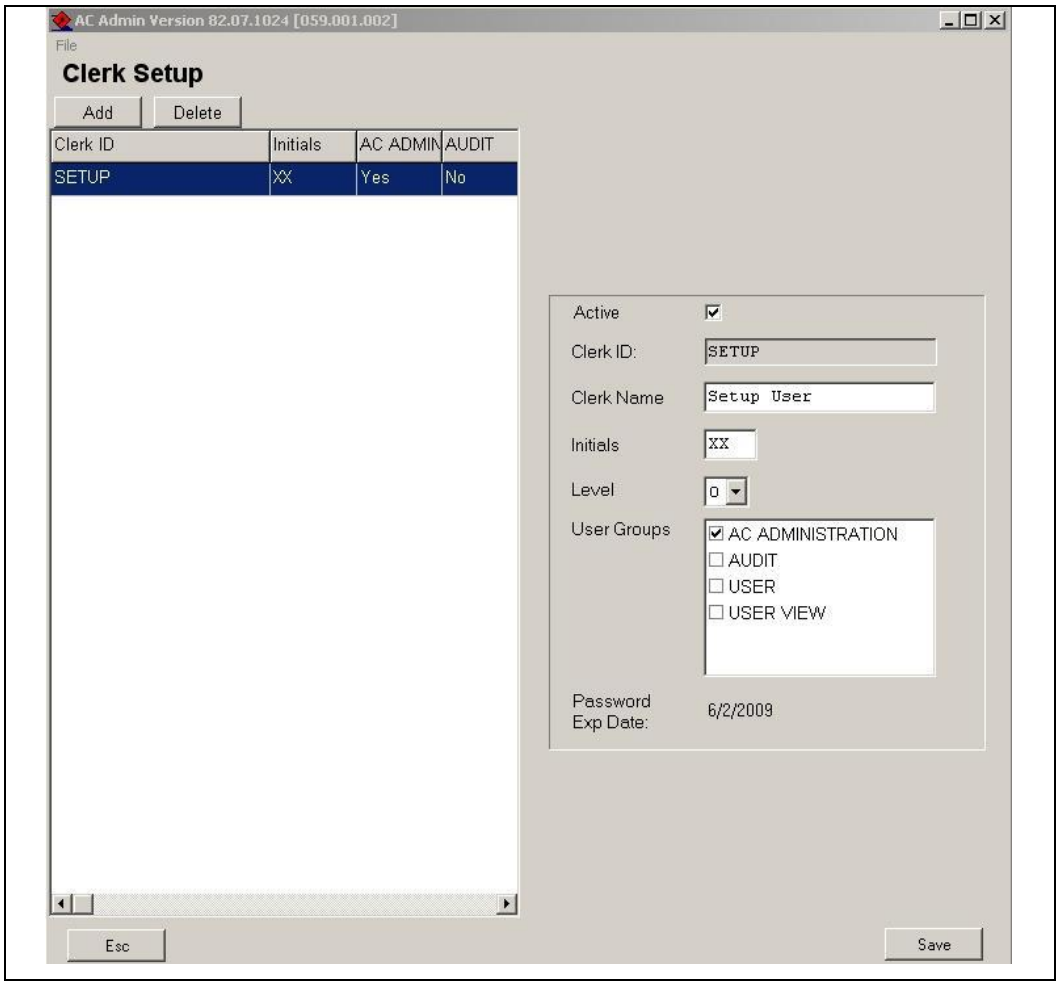

Figure 3: Clerk Setup Window

Creating a New User

1. On the Clerk Setup window, click on the 'Add' button to add a new user. The New Clerk box appears, as shown in Figure 4.

Figure 4: New Clerk Window

2. Enter the clerk's name in the Clerk ID field. (We will be using ANNE as our example.)
    a. Each user must have a unique Clerk ID of at least 4 characters.
        i. The Clerk ID cannot contain spaces within it. For example, JAY P (space between letters) is not accepted, but JAYP (no space between letters) will be.
        ii. Duplicate Clerk IDs are not permitted. This field is not case sensitive.
        iii. The same Clerk ID cannot be part of the AC Administration group as well as non-AC Administration group(s). You must set up a separate Clerk ID.
    b. Once the Clerk ID is entered, click the Save button.
3. Figure 5 is an example of a list of several Clerk IDs as they would appear in ACAdmin.

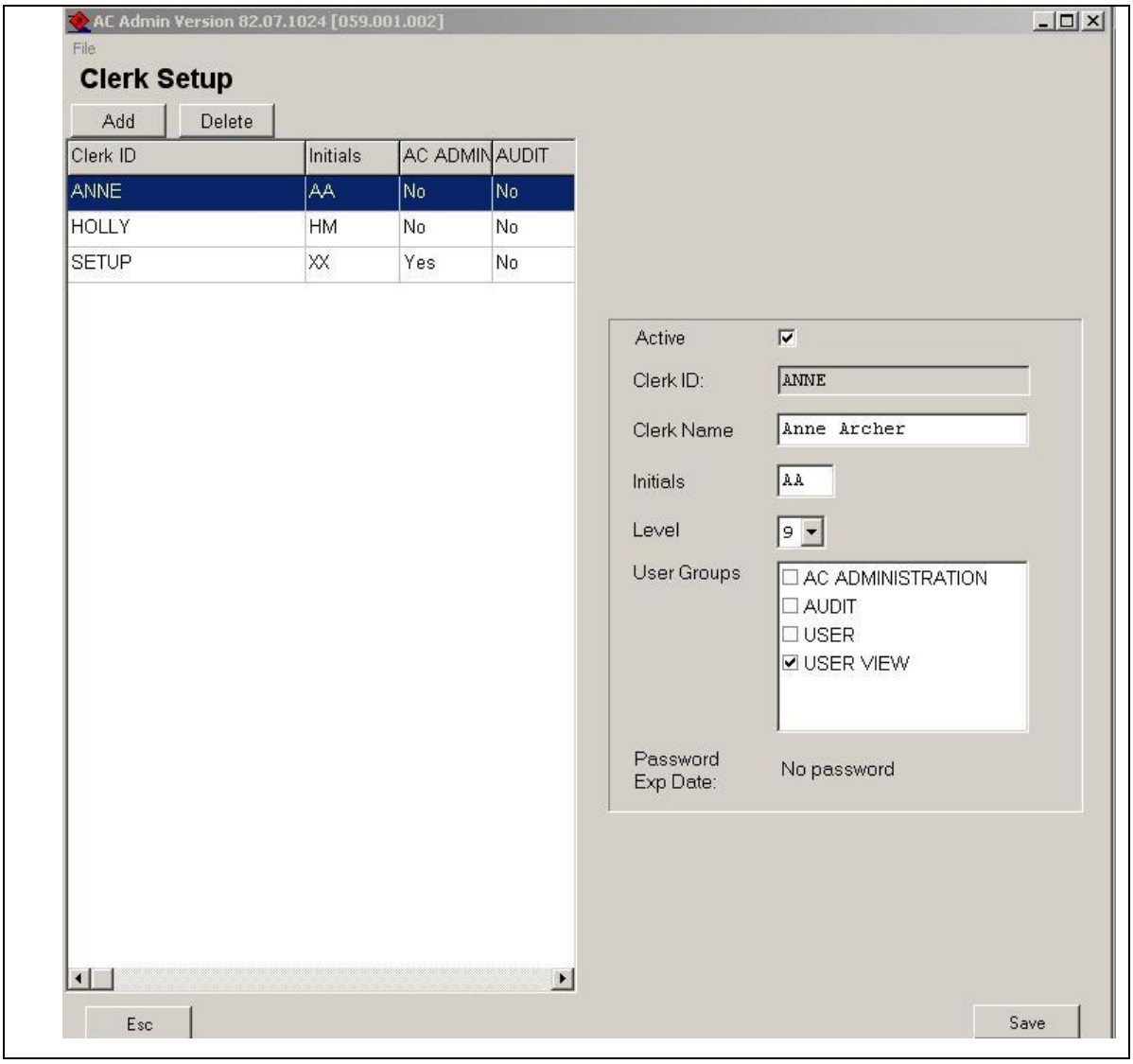

Figure 5: Clerk Setup Window

4. Complete the rest of the form referring to the sections below for details on their use and function.

Active

1. The 'Active' box is checked by default once you save the new user's Clerk ID.
2. Uncheck the Active box to temporarily disable a staff member from logging into the system.

a. For example, rather than permanently deleting a staff member taking an annual vacation, highlight the user name and uncheck the 'Active' box. When the staff member returns to work, re-check the Active checkbox.

Clerk Name - Initials

1. Enter the user's full name in the Clerk Name field.
2. Enter the clerk's first and last name initials in the Initials field.
    a. Clerk's initials appear on AutoClerk PMS reports as well as in some log files. These initials identify who is logged into the PMS and/or on a particular station when a transaction is processed, or a credit card number is viewed.

Level

1. Level is also referred to as Permission Level.
2. Permission levels are not interrelated to user groups or their functions. For example, a user may have a Level 9 permission level and still not be able to view a full credit card number if the user is not part of that group.
3. Select a permission level from the Level drop down.
4. The following is a list of current permission level restrictions:
    a. A user must be a Level 3 or above to access Guest Letters through the Utilities icon in the Main menu. However, if a user is above a Level 3 and does not know the Utilities access code, that user still cannot access Guest Letters.
    b. A user must be a Level 4 or above to get into some areas of the Housekeeping reports, such as Setting up Housekeepers, Lookup Housekeepers, Setup Room Order and Suppression, and Assign Rooms to Housekeepers.
    c. A user must be a Level 5 or above in order to access the Room Allocation Monitor.
        i. This is used mostly by properties with a CRS.
    d. You must be at least a Level 7 to access ACConfig. Once in ACConfig, your permission level determines which menu items you can then access.
        i. A Level 7 can only access parts of Rates and parts of GTD/Cancel Setup.
        ii. A Level 8 can access of Rates and parts of GTD/Cancel Setup.
            1. If you have a Revenue Manager, they should be a Level 8.
        iii. A Level 9 has full access to ACConfig.
    e. You can enable a Configuration Option regarding the ability to put rooms out of order.

i. If this option is enabled, a user must be above a Level 3 to put a room out of order.

ii. The user also needs a password, which is given to the GM at the time the option is enabled.

f. You can enable a Configuration Option to lock an assigned room in a reservation.

i. When the option is enabled, a user with a permission level of less than 4 makes a reservation.

ii. When making the reservation, the user assigns a room number and also checks the Requested box.

iii. Once the reservation has been saved, if the guest calls back and wants a different room number, the only person who can change it is a user with permission Level 4 or above.

1. This only applies if the reservation has a room number assigned, and the requested box is checked.

g. In ACConfig – Defaults/Options – Options, you can set a permission level that will allow users to Void a Transaction.

i. If set, a user must be above the set level to Void a Transaction.

h. If you are a Best Western property, a user with a Level 9 permission level can remove the BWR number from a reservation by hitting the F11 key on the keyboard

A good rule of thumb for setting permission levels is to set clerks to 1 and managers to 9. Keep in mind that being a level 9 does not give a clerk the right to view credit cards or access areas that may be access code protected if they do not know the code.

User Groups

1. A User Group is a collection of functions, such as view credit cards and backup. (See User-Group for more details.)
2. Select a group(s) to which the employee belongs by checking the appropriate User Groups checkboxes.
    a. A user must belong to at least one group.
3. Any user who is created to belong to the AC Administration group *must* have 2 user accounts:
    a. One user account in the AC Administration group to access ACAdmin.
    b. One user account for day-to-day use of the AutoClerk PMS.
4. If you need or want to create a new User Group, see that section in this document.

Final Steps

1. If you need to create several users, do not click on the Save button until you have created all of the user accounts.
    a. When you have completed one clerk's setup, click the Add button.
    b. Then create the next user account.
    c. When you are finished creating all of the new users, click the Save button.
2. ACAdmin generates a unique password for each new user. This unique password appears on the screen, as shown in Figure 6.

Figure 6: Password Confirmation Box

    a. Although this password may seem overly complex, users only need it to log into the system the first time. Users need to enter the unique system-generated password twice, so, copy it down carefully before you give it to the new user. It is automatically set to expire, so each user is forced to create their own complex password the first time they log into AutoClerk.
    b. If, for some reason, you do not want to use that particular password, click the No button, and the system generates and offers you another unique password to give to the new user.
    c. For security purposes, if you click the Escape button, no password is set and that user cannot log into AutoClerk.
        i. If by mistake you hit the Escape button please see Clerk Passwords below to force reset a password.

Password Details

Password management is solely the responsibility of the property. Neither the AutoClerk PMS nor AutoClerk, Inc., stores or maintains user passwords.

1. All AutoClerk PMS and ACAdmin users are required to have a unique user name and password.
2. User accounts and passwords must *never* be shared, and there must *not* be any kind of generic user account.
3. The first time a user logs into log into the AutoClerk PMS after being created, a pop-up window appears informing you that your password is expired. This is different than an invalid user name or password message.

4. Click the OK button.
5. On the next screen, re-enter the randomly generated password.
6. Enter and confirm a new password of your choosing.
    a. AutoClerk PMS user passwords are case sensitive.
    b. All users *must* follow these rules when creating new passwords:
        i. Contain at least 7 characters
        ii. Contain at least one letter
        iii. Contain at least one numeric digit
    c. In addition, an AutoClerk password *may* have any of the following for added security of passwords:
        i. Contain at least one uppercase letter
        ii. Contain at least one lowercase letter
        iii. Contain at least one non-alphanumeric character. Usable AutoClerk password characters are: ` ~ @ ^ _ = \ | { } [ ] : ; < > ?

Clerk Passwords

When you click on Clerk Passwords from the Home screen you are directed to the Reset Clerks Passwords form, shown in Figure 7. It lists the Clerk ID, Initials, Clerk name, and the date on which the Password Expires.

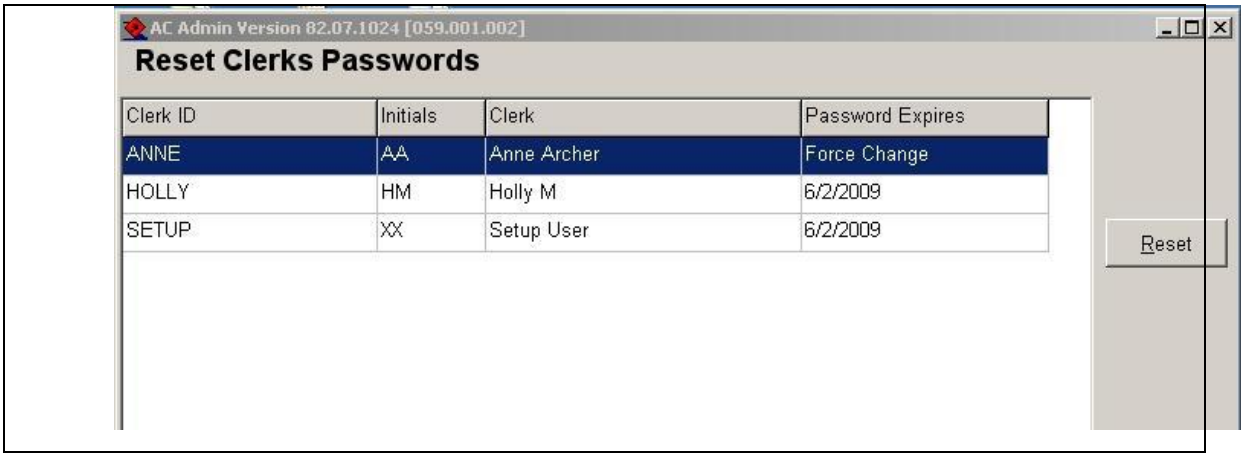

Figure 7: Reset Clerk Passwords Window

Resetting Clerks Passwords

1. An ACAdmin user can reset any user's password.
    a. Resetting a password forces a user to change their password at their next login.

2. To reset a user's password:
    a. Highlight the user's name.
    b. Click the Reset button.
    c. ACAdmin generates a random password.
    d. Give this new password to the user for their next login.
3. If a user forgets his password, an ACAdmin user MUST reset it. AutoClerk Support cannot reset any user's password.
4. User passwords automatically expire every 90 days and must be changed.
    a. When a user logs into AutoClerk, they will receive a pop-up that their password is going to expire.
        i. The pop-up starts five (5) days prior to the expiration and will continue to appear until the password is changed.
    b. A user can change their current password in AutoClerk.
        i. While logged into AutoClerk, click on Xtra – Reset Current User Password.
        ii. Enter the new password, confirm the password, and click OK.
        iii. Be sure to follow the password requirements or it will not be accepted.
            1. In addition, when changing passwords, you cannot use any of the last four (4) passwords.

User-Groups Setup

In this section, you can add and define what functions a User Group can perform.

1. User Groups define user functions.
    a. A group record consists of a Group ID/Name and a list of functions, as shown in Figure 8.

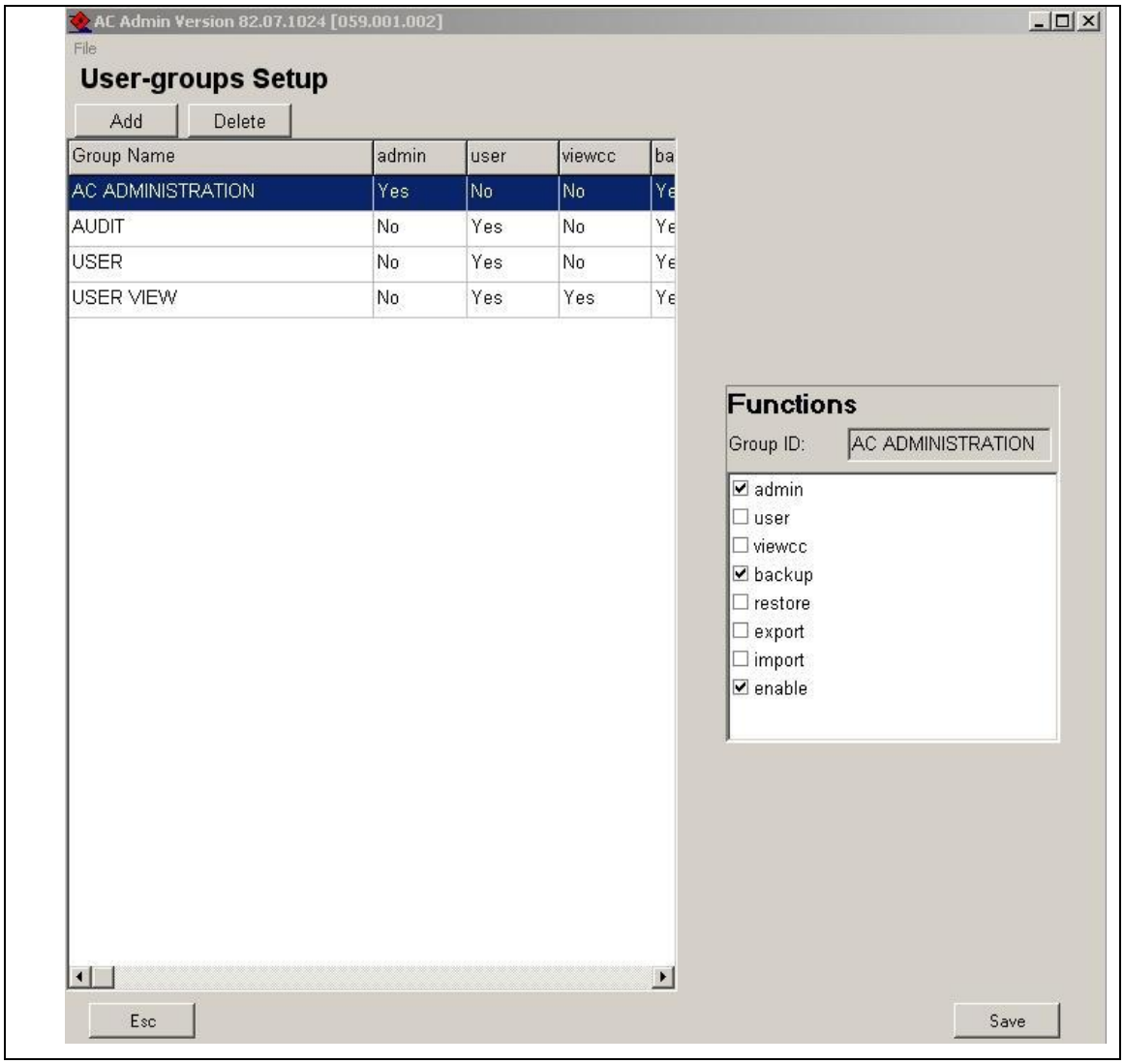

Figure 8: User Groups Setup

2. Upon installation, there is a default set of 4 user groups: AC Administration, Audit, User and User View. The purposes of these groups are as follows:
    a. AC Administration: This group is strictly for those accessing ACAdmin.
        i. Any user who is part of this group must also have an additional user account, which is not part of this group.
        ii. Assigning a user to the Admin group locks them out of using the PMS with that user profile.
        iii. Admin group functions are strictly admin, backup, and enable.
    b. Audit: This is typically the Night Auditor who may or may not have more permissions than a desk clerk.

i. A user can run the Night Audit in AutoClerk and not be part of the Audit group.

c. Users: These are day-to-day AutoClerk users.

i. This group might include desk staff, sales, accounting, and the concierge.

ii. They do not have permission to view full credit-card numbers in reservations.

d. User view: Day-to-day AutoClerk users who you allow to also view untruncated (for example, no XXX's in the number) credit card numbers in current reservations.

i. If your property has enabled credit card tokenization, then no user will be able to see a full credit card number in AutoClerk, regardless of user-group and/or function.

Adding a New User Group

1. To add a new group, click the Add button.
2. Enter a Group ID or name.
    a. Click the Save button.
3. Assign functions to the new group by checking the functions you want this group to perform.
    b. For example, you can add a group called Operations.
        i. Users assigned to this group might be housekeeping or maintenance.
        ii. These employees need to use AutoClerk, but they do not need to perform data backups.
        iii. The only function assigned to this group would be 'user'.

Assigning Functions to a User Group

There are currently 8 functions you can assign to user groups:

1. Admin: This group member can carry out administrative functions within ACAdmin.
    a. It does *not* mean this person has access to configuration within the PMS.
    b. It should only be assigned to the AC Administration group
2. User: This group member is an AutoClerk PMS user.
3. View cc: This group member is an AutoClerk PMS user and can view full credit card numbers.
    a. All cc access is logged in AutoClerk.

4. Backup: This group member can backup the dataset. (User, User View and Audit must have the ability to perform backups at shift change and Night Audit.)
5. Restore: This group member can restore from a backed up dataset.

   The restore function would only be performed by an AutoClerk technician.
6. Export: This group member can export data. For example, this group member can copy outside the AutoClerk data structure.
7. Import: This group member can import data.
8. Enable: This group member can enable or disable logins for other users.
   a. This should only be assigned to the AC Administration group.)

3. Additional ACAdmin Functions

1. On the ACAdmin Homepage, as shown in Figure 1, select the Tools menu from the Title bar.
2. Under the Tools menu, you can view addition functions:
   a. Re-encrypt Data set
   b. View Logs
   c. Backup
   d. Refresh License

Re-Encrypt Data Set

1. This tool sets a new Encryption key (Cckey as discussed earlier) for your credit cards and then re-encrypts the data using the new key.
2. Per PCI, you MUST run this tool as least once per year or anytime you believe your data has been compromised.
3. All users must be logged out of AutoClerk for the Re-encrypt to run.
4. Click on the Tools menu and select Re-encrypt data.
   a. The system asks if you have done a backup of the property's data.
      i. You MUST perform a backup prior to re-encrypting your data.
      ii. To perform a backup, click on Tools, then on Backup.
      iii. Backing up the dataset will kick all users out of AutoClerk.
   b. If you click No, you are returned to the ACAdmin Home page.
5. Once you have done a backup, go back to Tools → Re-encrypt data and click the Yes button.
   a. The AutoClerk Confirm box appears confirming your decision, as shown in Figure 9:

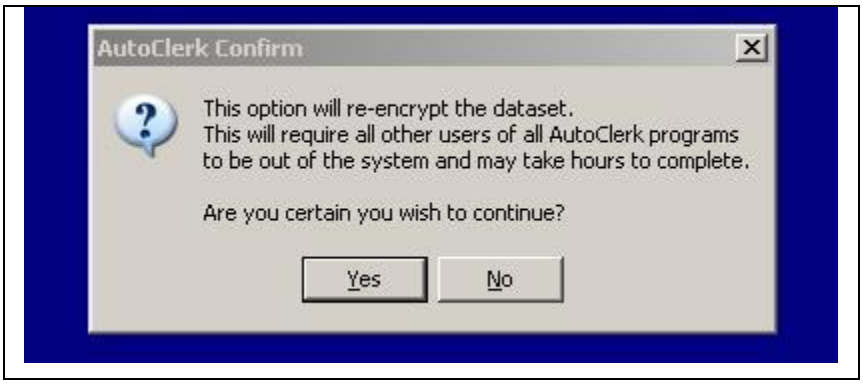

Figure 9: Re-Encrypt Data AutoClerk Confirmation Box

6. Click the Yes button.
    a. The data is re-encrypted.
    b. You get a confirmation box when it is complete.

View Logs

PA-DSS requires the PMS (AutoClerk) to log all activities that pertain to credit cards. For example, when a clerk views a full credit card number in a reservation in order to charge a no-show guest; this is logged.

Each installed interface also creates a log regardless of whether or not credit card and/or security are involved. Depending on the PCI and PA DSS requirements, the AutoClerk PMS retains the logs files for up to a year. Logs can also be viewed to troubleshoot problems and/or research issues.

1. On the ACAdmin Homepage, as shown in Figure 1, select the Tools menu from the Title bar.
2. Under the Tools menu, select View Logs. The View Logs For box appears, as shown in Figure 10.

Figure 10: View Logs For Box

3. Enter the appropriate dates in the Start Date and End Date fields. The default date range is for the past 30 days.

4. From the Log Type drop-down menu, pick the type of log you wish to view.
5. Log Types are as follows:
    a. AutoServe
    b. Startup: These perform a ledger check each time the AutoServ program is restarted.
    c. Rekey: This resets the credit card encryption key and re-encrypts your data.
    d. Interface Scheduler: This manages the property's various interfaces.
    e. Log files for each of the hotel's installed interfaces.
        i. Examples of interfaces are:
            1. Phone switch
            2. Movies
            3. CRS (Central reservation system) such as Best Western
6. In this example, we chose AutoClerk Server (asv). The display appears as shown in Figure 11.

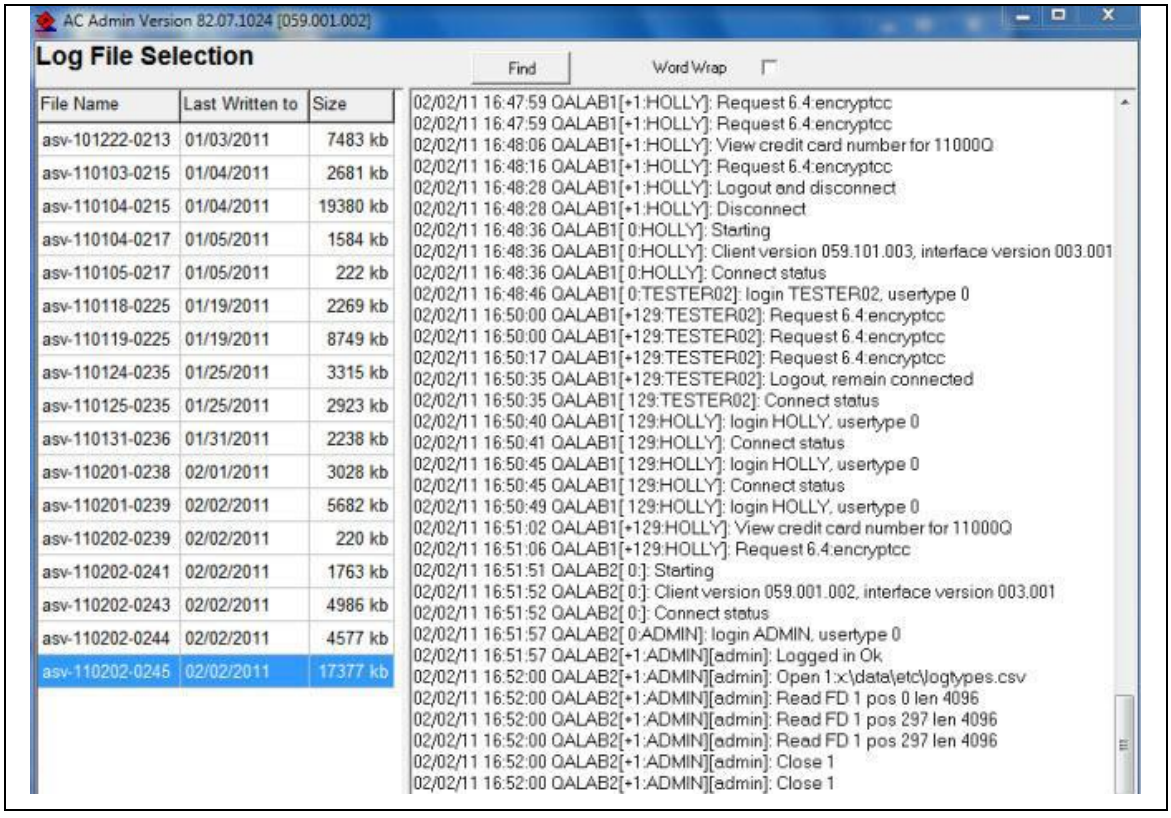

Figure 11: Log File Selection

7. The left hand column is the list of logs in the date span requested.

8. On the right is the log file for the highlighted date.
9. Each log entry consists of the date, time (military), name of the computer, station number and clerk name, and then the action.
10. In the example log, shown in Figure 11, you can see that on 02/02/11 at 16:50:49, Holly logged on and then viewed the credit card number on AutoClerk reservation 11000Q.

Backup

1. On the ACAdmin Homepage, as shown in Figure 1, select the Tools menu from the Title bar.
    a. Select Backup.
2. This is where you perform a backup of the data.
    a. A backup must done before the data can be re-encrypted.
    b. It is a good idea to do a backup afterwards as well.
3. An extra backup should be done before and after a reset of the Backup Encryption keys.
4. Remember that when a backup is performed, all PMS users must be logged out of the system.

List of Figures

Figure 1: ACAdmin Homepage 8
Figure 2: Reset Encryption Keys Window 9
Figure 3: Clerk Setup Window 12
Figure 4: New Clerk Window 13
Figure 5: Clerk Setup Window 14
Figure 6: Password Confirmation Box 17
Figure 7: Reset Clerk Passwords Window 18
Figure 8: User Groups Setup 20
Figure 9: Re-Encrypt Data AutoClerk Confirmation Box 23
Figure 10: View Logs For Box 23
Figure 11: Log File Selection 24

Index of AutoClerk V9 ACAdmin Icons, Menus, and Commands

A

ACAdmin Functions, 4
ACAdmin, PA-DSS and PCI-DSS, 4
Active, 14
Adding a New User Group, 21
Additional ACAdmin Functions, 22
Admin Functions, 8
Assigning Functions to a User Group, 21
AutoClerk, 3

B

Backup, 25
Backupkey 1 and 2, 10
bw2/rw, 11

C

Clerk Name - Initials, 15
Clerk Passwords, 18
Clerk Set Up, 11
Common Keys, 10
Credit Card Keys, 11

D

Default Passwords Needed for Initial Use, 5

E

Employees Forgetting Passwords, 7
Encryption Keys, 8

F

Final Steps, 17
First Time Use, 5

G

General Manager Account and AC Administration Group, 5

I

Introduction, 4

L

Level, 15
License, 10

M

Managers/Owners Creating User Accounts for Employees, 6

N

Number of Managers and Owners Using ACAdmin, 6

R

Re-Encrypt Data Set, 22
Resetting a Key, 9
Resetting Clerks Passwords, 18
Running ACAdmin and Station #1, 5

U

User Account Passwords, 5
User Accounts, 5
User Groups, 4, 16
User-Groups Setup, 19

V

View Logs, 23