CA Web
Best Practices
Administration
PCI Standards for
Implementation and

Contents

Revision History

Date	Version	Description	Author
8/26/09	1.0	FINAL	Karen Neumeier
09/01/09	1.1	Update	Karen Neumeier
10/09/09	1.2	Update – Firewall 1.4a and 1.4b	Karen Neumeier

Introduction

CA Web is a PCI - DSS compliant software application and follows the PCI-DSS recommendations that credit card information be limited to as few locations as possible and that only employees who are on a "business need to know" should be given permission to review or decrypt credit card information. This document will cover those aspects of CA Web as they relate to its' users and PCI-DSS compliance.

NOTE: Only properties who have specifically requested the ability to store credit card data in CA Web will be given capability to do so. A signed "Enable Credit Card Processing" form 43 from each property must be received by Gold Key Solutions requesting the ability to store and retrieve credit card data in their property's version of CA Web.

Implementation

Protect Cardholder Data

All credit card numbers are encrypted with a symmetric key using the Triple-DES algorithm and a 128-bit key, and then hex-encoded prior to transmission and storage in the database.

In CA Web, credit card information is found only in the Logbook and Profiles features.

NOTE: Credit card information must NEVER be sent via end-user messaging technologies such as Instant Messaging, Reminders or Messaging features within CA Web. To do so is in violation of PCI standards and their function and purpose.

Passwords

Upon implementation of CA Web, each property will determine their "Site Administrators" (Refer to Roles & Rights) and provide Gold Key Solutions with the names of these individuals. These individuals will be established as the initial users of the software. GKS will provide these designated users with their initial logon names and passwords to allow them access into CA Web.

For your own security, assign a unique ID to each person with computer access. Do NOT USE group, shared, or generic accounts and passwords.

Immediately upon entering their logon name and password, CA Web will request that a new user password be entered. The password requirements include: a minimum of 7 characters; at least one alpha and one numeric character; may not contain the User Logon Name and may not reuse four previous passwords.

CA Web requires each user to enter a new password every 90 days.

If a user has not been active within CA Web for 15 minutes the user will be logged out. At one (1) minute remaining the user will get a message warning them of their imminent logout with a "seconds remaining" countdown and the option to Continue or Log out.

It is the responsibility of each individual client using CA Web, to review the status of all employees on a regular basis and to ensure that inactive or terminated staff members have no access to CA Web or the information contained therein.

Logbook

All Logbook Categories must be created by the Site Administrator(s) for your property. When creating these categories, fields are identified to determine the type of data that will be entered by the users. It can also be determined at this time whether credit card information will be entered into the Logbook entries for various guest requests. All credit card information can be kept in the Profile feature of CA Web to use without the necessity of entering the number again into each request the guest has made. (Refer to Profiles).

One of these selections is specifically for the purpose of defining credit card numbers and credit card expiration date fields. To define these logbook fields the Site Administrator must select the field type "Credit Card Number" and "Credit Card Exp" in the corresponding Logbook Category in Administration>Logbook Categories.

When a vendor requires a credit card number for orders and or reservations, this information may be entered into CA Web's previously defined credit card fields as a convenience for future orders, reservations or historical data for this guest.

When the transaction is saved by clicking on the Save button, the system will encrypt the credit card number and mask the first 11 or 12 numbers of the credit card by replacing them with *****, showing only the last 4 numbers of the credit card number. Also at that time, a small lock icon will appear next to the masked number.

Decrypting the credit card requires an additional password used only for this purpose. Simply start by clicking on the lock. You will see the following screen.

The very first time you are decrypting the credit card number, you will enter your logon name, exactly like the first time you entered into CA Web, and the reason you are decrypting the credit card number. Click on the button "Display". You will be asked to change your password first.

To change your password, go to the welcome link in the upper right of your screen. It will say "Welcome, (User Name)".

Clicking on this link will take you to "Administration>My Profile". Click the "Change my Password for Viewing Credit Card" in the upper right area above the label "Change My Password for Login"

You will see this screen. Enter the current password (your logon name) and your new password then verify it in the third space provided. You may choose any password you desire as long as it is not the same as your logon password and a minimum of 7 characters containing at least one alpha or numeric character. Click OK.

When you click on the OK button, your screen will return to the "Administration>My Profile" screen. Click on the Logbook link to return to the entry that you were working on. Now click the lock again.

Enter the new password you just created and click on "Display". The system will present the encrypted number. NOTE: If the password is entered incorrectly 6 times within 30 minutes, CA Web will inactivate the user who must be reactivated by the Site Administrator or another designated person.

Once the screen is closed, the credit card information will remain masked on the Logbook entry.

If the associate forgets his/her credit card password, the Site Administrator must reset the password in Administration>User Management. After clicking on the associate's name click the button labeled "Reset Their Password for Viewing Credit Cards" above the label "Reset Their Logon Password".

Profiles

Credit Card information may also be stored in the "Profiles" feature of CA Web for each guest for easy retrieval.

To decrypt a credit card in this area, click on the "Show CC Number" of the desired credit card and you will get the following screen.

You must enter your password and the reason for decrypting this credit card. (If this is your first time decrypting you will need to follow the steps described in the section for Logbook entries.) Now click on the button labeled "Display".

If the Logbook entry is generated from the Profile feature,

The Guest profile information comes over too.

If you wish to decrypt the credit card information, simply click on the link,"Show CC Number".

You will get this screen

Enter your password and click on the "Display" button. The screen will now reflect the decrypted credit card information.
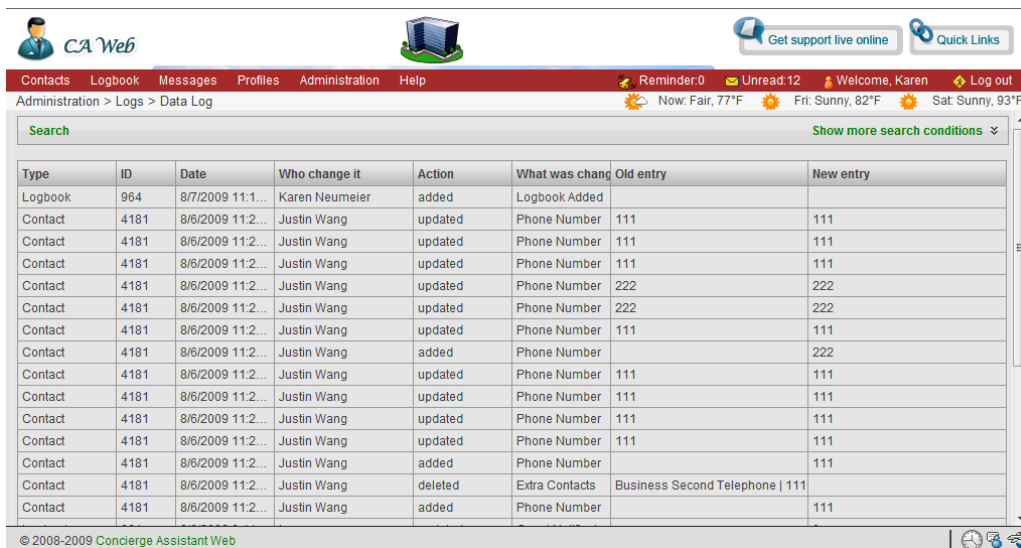

Once the screen is closed, the credit card information will remain masked in the Profile.

Regularly Monitor

Another security precaution for credit card information entered into CA Web is the ability to know who is looking up credit card information and why.
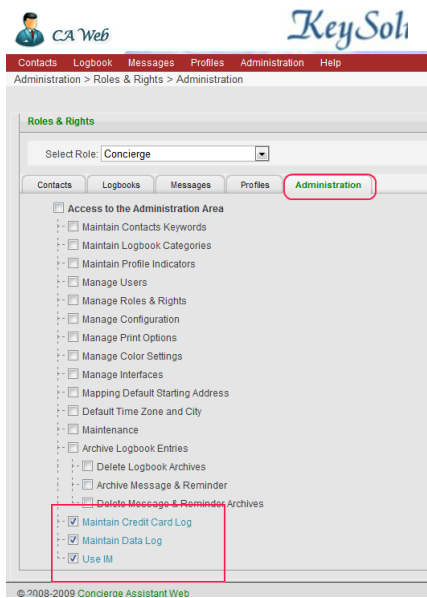
In CA Web, through the use of logon names and passwords, we have provided a means to create an "audit trail" of staff associates who are accessing this information via Logbook entries and the Profile feature.(Refer to Roles and Rights) This log may be deleted on a regular basis by the Site Administrator or someone designated by the Site Administrator. (Refer to Purging Old Credit Card Information)

This information is available under Administration>Logs>Credit Card Logs and is only accessible to "Site Administrators" and those authorized by the Site Administrator to see this information thru Administration> Roles and Rights.

Roles & Rights

Who Is Authorized to Decrypt Credit Card Information?

Site Administrators are given the responsibilities of the foundational controls in CA Web. They have access to all aspects of the application. This includes the capabilities of decrypting credit card data as well as the authorization to grant specific associates, determined to be in the "need to know" access to decrypt credit card data as well.   (Refer to User Management Section)

Do NOT USE group, shared, or generic accounts and passwords.

To establish the Site Administrator each property must provide Gold Key Solutions (GKS) with the name of the person or person's they want authorized for this capacity.   GKS will establish in the initial setup, this individual(s) and their initial password as the only user(s).

It will then be the Site Administrator's responsibility to establish all other users and their parameters within CA. Only "Site Administrators" can assign the rights to decrypt credit card information under Administration>Roles & Rights.
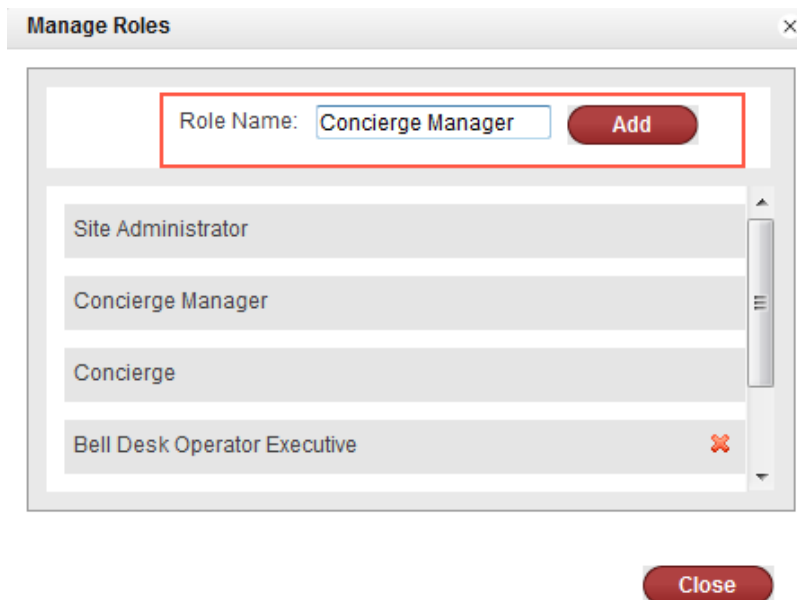
The Site Administrator must establish the Roles that each of the users will qualify under such as; Concierge Manager, for associates in a supervisory capacity with the need to manage activities of the staff; Concierge, who will be interacting with guests and their requests requiring the need to decrypt credit card information for orders and reservations; and PBX may need to access Contact information for directions to assist an off property guest and so on. These Roles are designed to the specifics of each property and its' users.

Under Administration>Roles & Right, click on the button "Manage Roles".
.
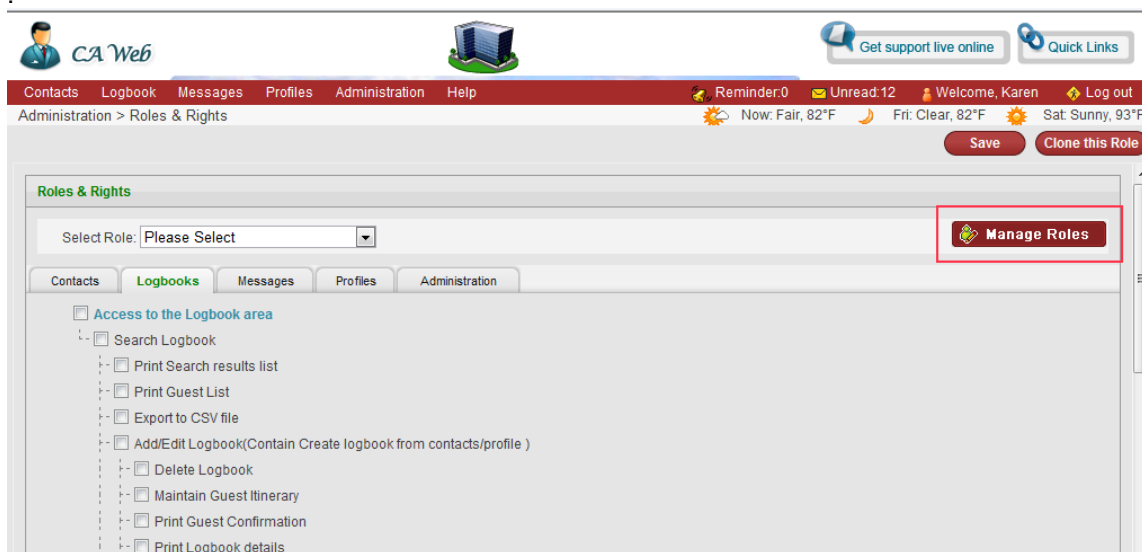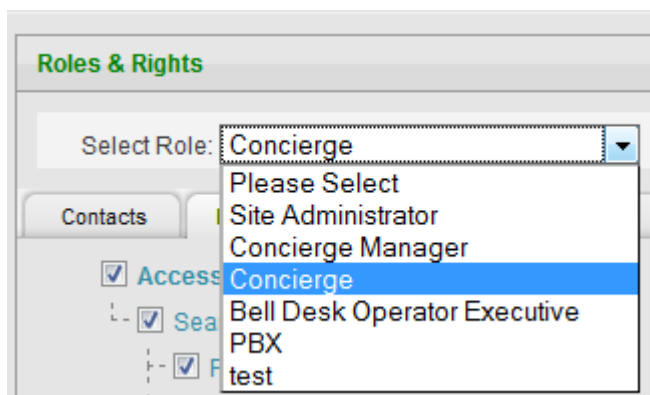
Enter the label of the Role you will be establishing, such as Concierge Manager, Concierge, PBX etc and click "Add". You can enter all of the Roles at one time so you may have them available as you are establishing the Rights for each.

Click on Close when you have completed entering your list of Roles.
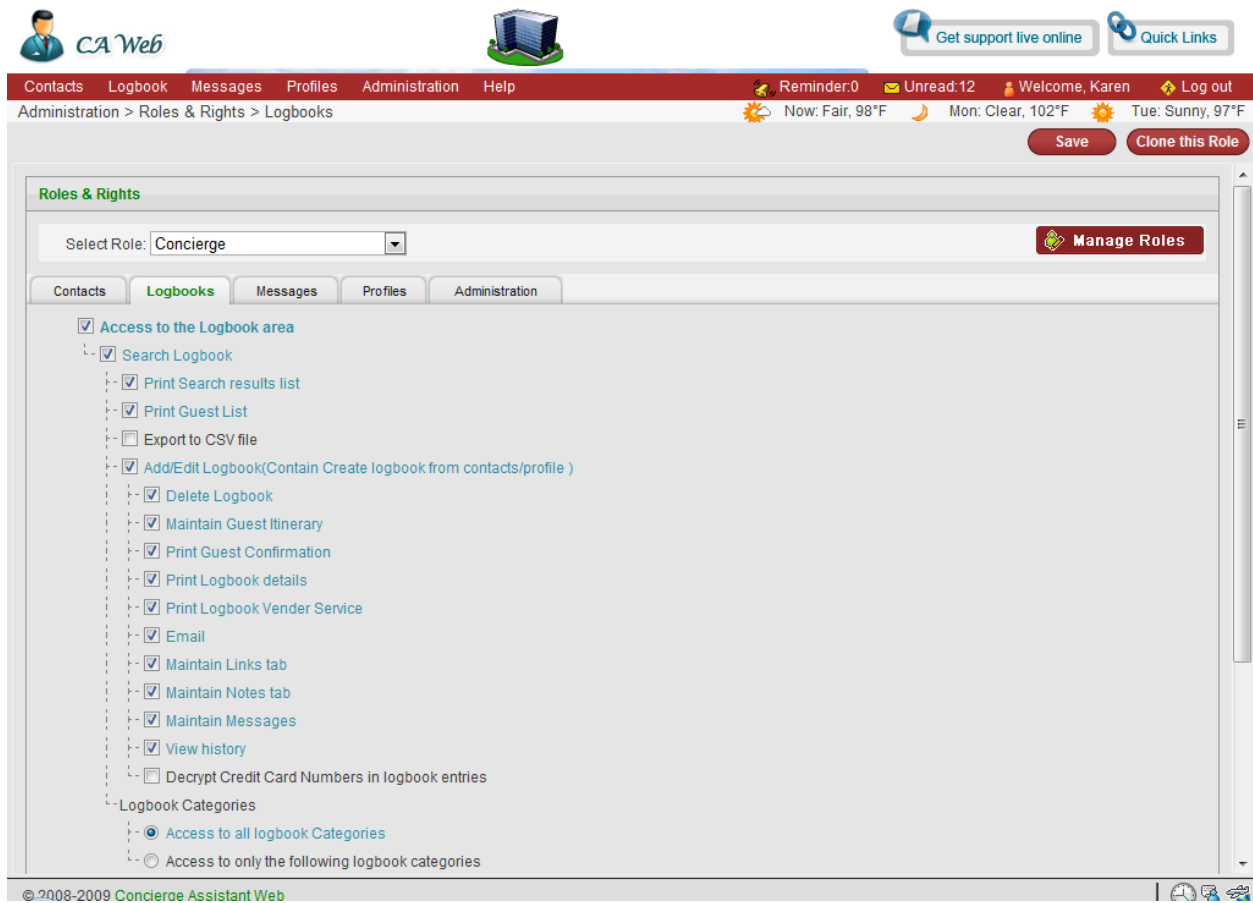
Now select a Role you want to establish the Rights for.

There are tabs for each of the major features in CA Web. These are the Rights or permissions relating to those features in CA Web that you will be assigning to the various Roles.

For each Role created in CA Web, you must give permission by checking or not checking each box provided for these various permissions as in this sample for the role "Concierge".

In the Logbook and Profile features you will want to pay particular attention to the authorization to "Decrypt Credit Card in Numbers in Logbook Entries" and "Decrypt Credit Card Number in Profiles" respectively.
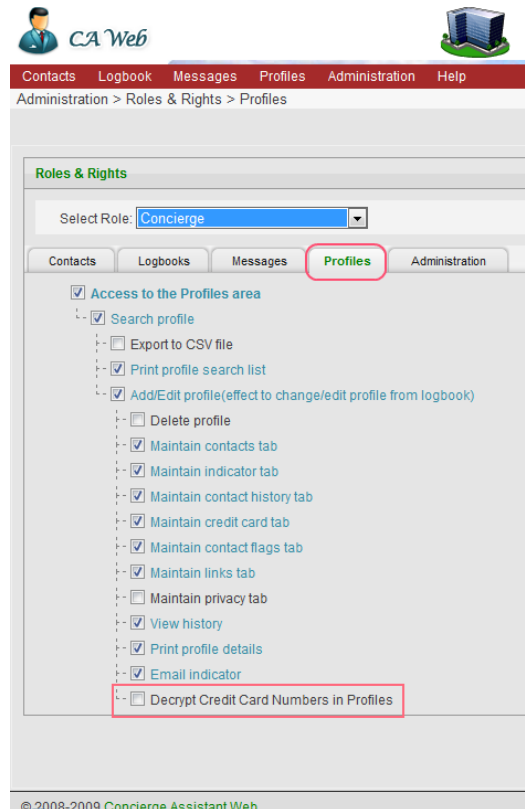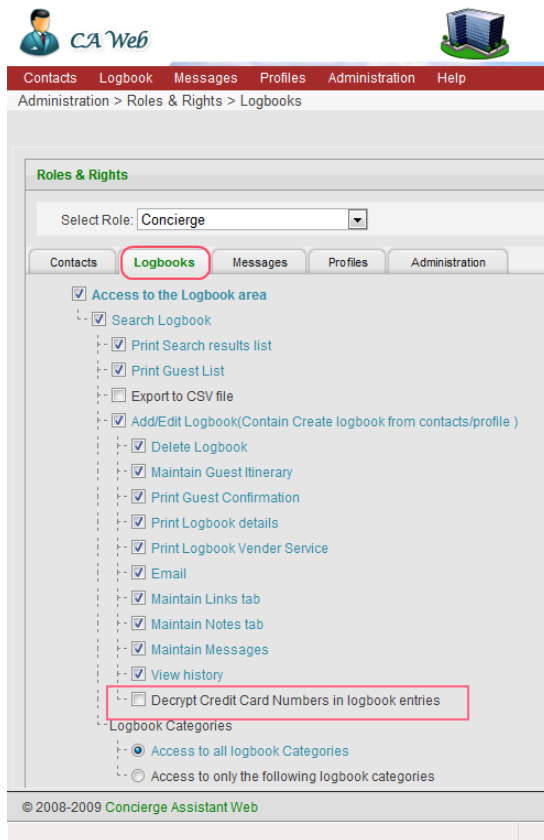
In these examples, the Role "Concierge" do NOT have permission to Decrypt Credit Card Numbers in Logbook Entries or in Profiles. That permission is only given if the boxes are checked.

You will continue this process for each of the Roles created for your property.

User Management

Now that the Roles and the Rights associated with those Roles has been established, a Site Administrator (or an associate given those rights) will need to assign those Roles to various staff associates. This is done under Administration>User Management.

Select the ADD tab to enter your first staff member.

Fill in the applicable information relating to the associate in the space provided, like this. Continue to do this for the remainder of the associates who will be authorized to have access to CA Web.

You will have a Search screen that looks like this, providing you with a list of associates and their assigned Roles. You will note that you have the ability to label associates as "Inactive" and to "Edit" information or Roles for each individual.

Purging Old Credit Card Information

If your property has requested the ability and is entering credit card information into CA Web, it is a PCI requirement that each property be responsible for deleting old credit card information in Logbooks and Profiles to reduce exposure for both yourself and your guests. To assist you with this responsibility, CA Web allows you to determine your own retention policy and create the schedule for the system to delete your credit card information based on your own standards. Only Site Administrators and those they grant permission can access this area.

Go to Administration>Options>Archive Settings
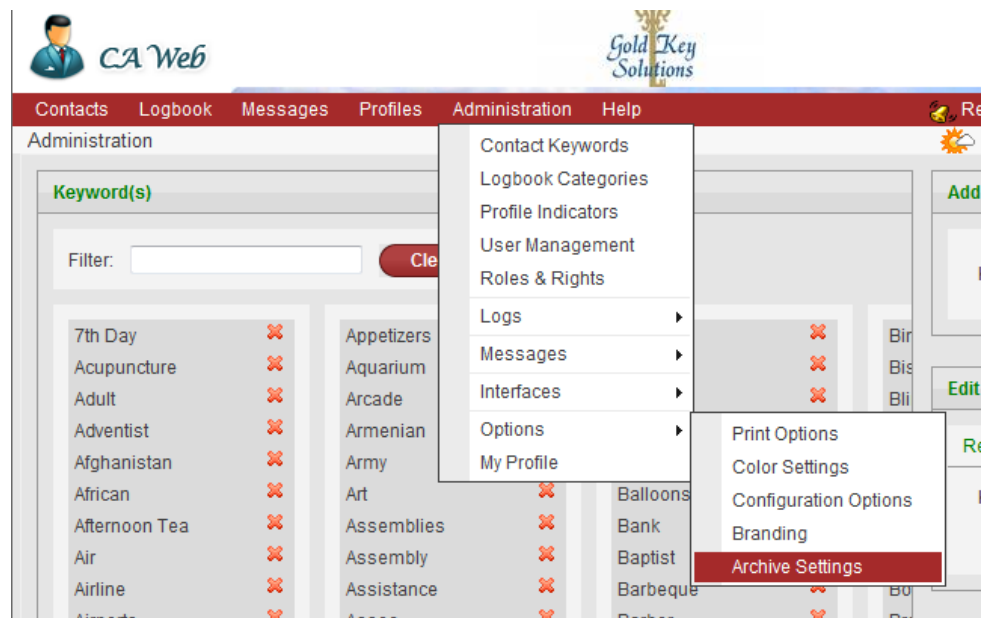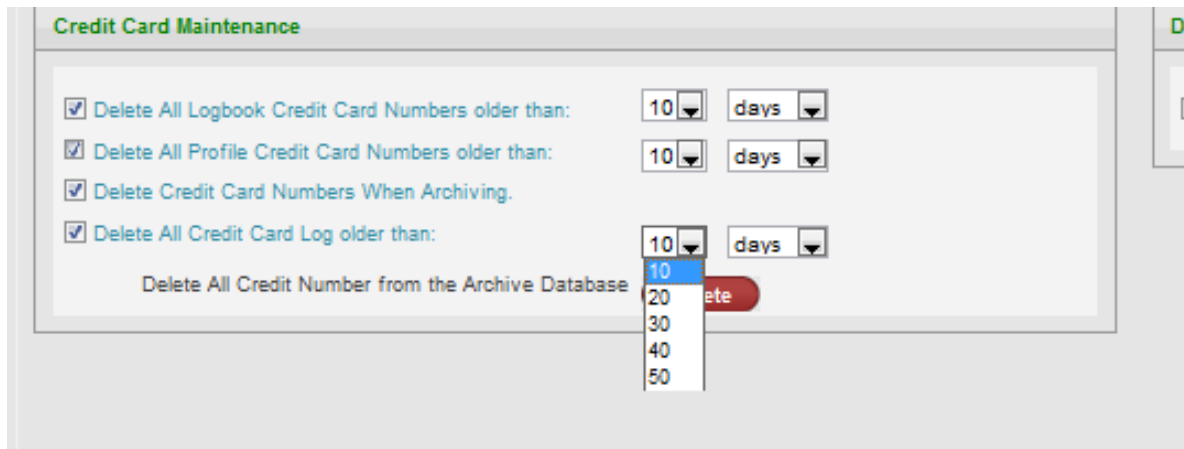
You will see this screen.
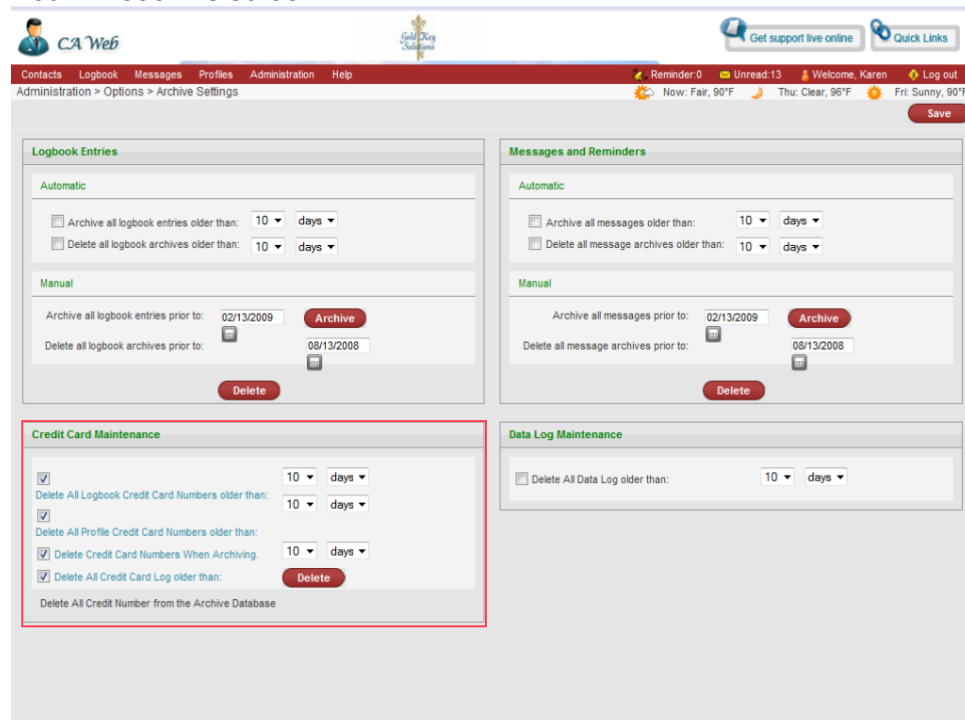
It is through this feature that old Logbook entries and Messages will either be Archived (for historical reference of guest activities) or Deleted (when it is no longer necessary for business need to know).

For credit card information you will be dealing with this portion of the screen. You will simply check the applicable boxes and establish within CA Web the number of days you wish for the credit card information retention within Logbook and Profiles, anything older than (10days, 20 days, etc) will be deleted automatically by the system.

There are also the options to; "Delete Credit Card Numbers when Archiving", "Delete All Credit Card Logs" and to "Delete All Credit Card Numbers from the Archive Database". This last option is a manual transaction created by clicking on the Delete button next to the verbiage.

Maintain as Information Security Policy:

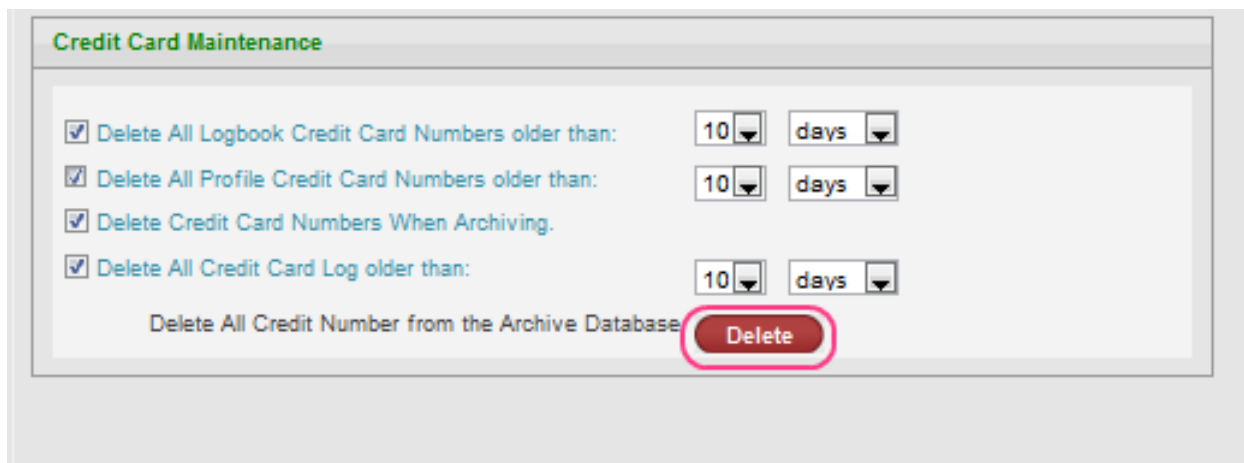The following is a list of the basic elements of a good information security policy.

PCI Data Security Standard	
Build and Maintain a Secure Network	Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (e.g. laptops used by employees), which are used to access the organization's network. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	Protect stored data Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	Use and regularly update anti-virus software Develop and maintain secure systems and applications
Implement Strong Access Control Measures	Restrict access to data by business need-to-know Assign a unique ID to each person with computer access Restrict physical access to cardholder data
Regularly Monitor and Test Networks	Track and monitor all access to network resources and cardholder data Regularly test security systems and processes
Maintain an Information Security Policy	Maintain a policy that addresses information security

For more information on PCI standards or the PCI Council, visit their website at
https://www.pcisecuritystandards.org/