



CA Web Best Practices Administration PCI Standards for Implementation and

Contents

Introduction.....	ii
Implementation	3
Protect Cardholder Data.....	3
Passwords.....	3
Logbook	5
Profiles	12
Regularly Monitor.....	16
Roles & Rights	17
User Management	22
Purging Old Credit Card Information	24
Maintain as Information Security Policy:	26

This document contains information from Gold Key Solutions, Inc. that may be confidential. Except for personal use by the intended recipient, or as expressly authorized by the sender, any person who receives this information is prohibited from disclosing, copying, distributing, and/or using it.

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.

Gold Key Solutions CA Web Best Practices Rev 09/01/09

The screenshot shows the 'Add' user management page in the CA Web application. The interface includes a top navigation bar with links like 'Contacts', 'Logbook', 'Messages', 'Profiles', 'Administration', and 'Help'. A sidebar on the left contains sections for 'Login Information', 'Role(s)', 'Message Group(s)', and 'GUI Preferences'. The main content area is divided into 'User Profile' and 'Interface Setting' sections. The 'User Profile' section contains fields for personal and contact information, while 'Interface Setting' includes fields for 'Open Table ID' and 'Network ID'. A 'Status' dropdown menu is set to 'Active'. Buttons for 'Clear' and 'Save' are located at the top right of the form.

Login Information

- User Name: JBrown
- Password: [masked]
- Confirm Password: [masked]

Role(s):

- ☐ Bell Desk Operator Exe...
- ☒ Concierge
- ☐ Concierge Manager
- ☐ Loss Prevention
- ☐ PBX
- ☐ Site Administrator
- ☐ test

Message Group(s):

- ☒ Concierge
- ☐ Front Desk
- ☐ Housekeeping
- ☐ Management
- ☐ Open table group
- ☐ Spa
- ☐ The One

GUI Preferences:

- ☒ Search panels collapsed upon login
- Default page: Logbook

User Profile

- First Name: John
- Last Name: Brown
- Initials: JB
- Job Title: Concierge
- Email: vn@goldkeyhotel.com
- Phone: 123-456-7890
- Fax: [empty]
- Zip Code: [empty]
- Address: [empty]
- City: [empty]
- State: [empty]
- Country: [empty]

Interface Setting

- Open Table ID: 123456
- Network ID: [empty]

Status: Active

Clear Save

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.

The screenshot shows the login page for the Concierge Assistant Web application. It features the CA Web logo on the left and a login form on the right. The form includes fields for 'User Name' (pre-filled with 'JBrown') and 'Password' (masked with dots). A 'Login' button is positioned below the password field. A link for 'Forgot Your Password' is located at the bottom of the form.

Concierge Assistant Web

User Name: JBrown

Password: [masked]

Login

Forgot Your Password

The screenshot shows the password change page for the Concierge Assistant Web application. It features the CA Web logo on the left and a form on the right. The form has a heading 'Please Change your password' and two input fields: 'New Password' and 'Confirm'. 'OK' and 'Cancel' buttons are at the bottom of the form.

Concierge Assistant Web

Please Change your password

New Password: [empty]

Confirm: [empty]

OK Cancel

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.

The screenshot shows the CA Web Administration interface. The top navigation bar includes links for Contacts, Logbook, Messages, Profiles, Administration, and Help. The main content area is titled "Logbook Categories" and shows a list of categories on the left, including Car Rental, Carey Limousine, Che Frontiere, Credit card, Dining Reservations, Floral (selected), Golf, Guest Request, Hotel Reservations, Inquiry/Guest Request, Jazz, Leon's categories, Logbook categories for test, and Messenger Service. The right pane shows the "Edit Selected Category" form for the "Floral" category. It includes fields for Category, Rename, and a table of roles. The table has columns for Label, Type, Link to Contact Field, Do not Print, Required Field, and Operations. The "Credit Card" and "CC Exp" rows have "Credit Card Number" and "Credit Card Exp" selected in the Type column, which are highlighted with a red box.

Label	Type	Link to Contact Field	Do not Print	Required Field	Operations
Company:	Text	Contact Name	<input type="checkbox"/>	<input type="checkbox"/>	+ -
Caller Name:	Text	Do Not Link this Element	<input type="checkbox"/>	<input type="checkbox"/>	+ -
Phone:	Text	Do Not Link this Element	<input type="checkbox"/>	<input type="checkbox"/>	+ -
Credit Card:	Credit Card Number	Do Not Link this Element	<input checked="" type="checkbox"/>	<input type="checkbox"/>	+ -
CC Exp:	Credit Card Exp	Do Not Link this Element	<input checked="" type="checkbox"/>	<input type="checkbox"/>	+ -
Note Card:	Text	Do Not Link this Element	<input type="checkbox"/>	<input type="checkbox"/>	+ -
Price:	Text	Do Not Link this Element	<input type="checkbox"/>	<input type="checkbox"/>	+ -
Room Charge (Yes or No):	Text	Do Not Link this Element	<input type="checkbox"/>	<input type="checkbox"/>	+ -

Gold Key Solutions CA Web Best Practices Rev 09/01/09

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.

The screenshot shows the CA Web interface. At the top, there's a navigation bar with links like Contacts, Logbook, Messages, Profiles, Administration, and Help. Below this, a status bar shows weather forecasts for Now, Fri, and Sat. The main content area is divided into two sections: 'Guest Information' and 'Entry'. In the 'Guest Information' section, fields for Salutation, Arrival, Guest Notification, Last Name, Departure, Group Name, First Name, Primary Email, Room Number, and Primary Phone are visible. In the 'Entry' section, fields for Reference Date, Time, Entry Type, Company, CC Exp, Note Card, Description/Arrang., Caller Name, Price, Deliver to, Phone, Confirmed with, Credit Card, and Room Charge are visible. The 'Save' button in the top right corner is highlighted with a red border. The 'Credit Card' field in the 'Entry' section is also highlighted with a red border, showing the number 4356890040265494.

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.

This screenshot shows a close-up of the 'Credit Card' field in the CA Web interface. The field is now masked with asterisks, showing only the last four digits '5494'. A small lock icon is visible next to the masked number, indicating that the credit card information has been encrypted. The field is highlighted with a red border.

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.

Show Credit Card Number

Please change your password first.

* Password:

* Reason:

Type	Credit Card Number	Expiration MM/YY

Display

Cancel

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

Get support live online

Quick Links

Reminder:2

Unread:0

Welcome, Leo

Log out

udy, 62°F

Thu: AM Clouds/PM Sun, 59°F

Fri: AM Clouds/PM Sun, 61°F

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”

The screenshot shows the 'Administration > My Profile' page in the CA Web interface. The page has a red navigation bar at the top with links like 'Contacts', 'Logbook', 'Messages', 'Profiles', 'Administration', and 'Help'. Below the navigation bar, there's a weather widget and a 'Save' button. The main content area is divided into several sections: 'Login Information' (User Name: leo), 'Role(s)' (Site Administrator), 'Message Group(s)' (Concierge, Management, Open table group, Spa), and 'GUI Preferences' (Search panels collapsed upon login, Default page: Logbook). The 'User Profile' section contains fields for First Name, Last Name, Initials, Job Title, Email, Phone, Fax, Zip Code, Address, City, State, and Country. The 'Interface Setting' section contains fields for Open Table ID and Network ID. On the right side, there are two 'Change Password' buttons: 'Change Password' for Viewing Credit Card (highlighted with a blue box) and 'Change 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.

The screenshot shows a dialog box titled 'Change My Password for Viewing Credit Card'. It contains three password input fields: '*Your Current Password:', '*Your New Password:', and '*Verify New Password:'. Below the fields are 'OK' and 'Cancel' buttons.

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.

The screenshot shows the CA Web interface. The top navigation bar includes links for Contacts, Logbook, Messages, Profiles, Administration, and Help. The Logbook tab is active, showing a list of entries. The entry for ID 960 is selected. The entry details are displayed in a form with fields for Guest Information, Entry, and a sidebar with various action buttons. The credit card number is masked with a red padlock icon, indicating it is locked.

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.

The screenshot shows a dialog box titled "Show Credit Card Number". It contains a password field, a text area for "Book floral arrangement", and a "Reason" field. Below these fields is a table showing the credit card information:

Type	Credit Card Number	Expiration MM/YY
	4356890040265494	12/12

At the bottom of the dialog are "Display" and "Cancel" buttons.

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".

The screenshot displays the 'User Management' interface for a user named 'leo'. The interface is divided into several sections:

- Login Information:** Contains a 'User Name' field with the value 'leo'.
- Role(s):** A list of roles with checkboxes: 'Bell Desk Operator...', 'Concierge', 'Concierge Manager', 'PBX', 'Site Administrator' (checked), and 'test'.
- Message Group(s):** A list of message groups with checkboxes: 'Concierge' (checked), 'Front Desk', 'Housekeeping', 'Management' (checked), 'Open table group' (checked), and 'Spa'.
- GUI Preferences:** Includes a checkbox for 'Search panels collapsed upon login' (checked) and a 'Default page' dropdown set to 'Logbook'.
- User Profile:** Contains fields for 'First Name' (Leo), 'Last Name' (Aguirre), 'Initials', 'Job Title', 'Email' (leo@goldkeysolutions.o), 'Phone', 'Fax', 'Zip Code', 'Address', 'City', 'State', and 'Country'.
- Interface Setting:** Contains fields for 'Open Table ID' (308188) and 'Network ID'.
- Actions:** On the right side, there are buttons for 'Save', 'Delete', and 'Clone This User'. Below these, there is a 'Status' dropdown set to 'Active'. A red box highlights the 'Reset Password' button, which is labeled 'Reset Their Password for Viewing Credit Cards.' Below this, there is a 'Set Password' button labeled 'Reset Their Log On Password.'

Profiles

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

The screenshot shows the CA Web interface for a guest profile. The top navigation bar includes links for Contacts, Logbook, Messages, Profiles, Administration, and Help. The main content area displays the guest profile for Allen (ID: 367). The 'Credit Card Information' section is expanded, showing a table with two credit cards. The 'Show CC Number' link for the second card is circled in red.

Type	Credit Card Number	Expiration MM/YY	Operations
Visa	*****2606	**/**	Edit Delete Show CC Number
Visa	*****5494	**/**	Edit Delete Show CC Number

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.

The screenshot shows the 'Show Credit Card Number' dialog box. It contains fields for Password, Reason, and a text area for the credit card number. The 'Book Tour' text is highlighted in the text area.

Type	Credit Card Number	Expiration MM/YY

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".

Show Credit Card Number

* Password: [Masked]

* Reason: Book Tour

Type	Credit Card Number	Expiration MM/YY
Visa	4635890000112606	12/15

Display Cancel

If the Logbook entry is generated from the Profile feature,

CA Web

Get support live online Quick Links

Profiles > Profiles > Allen

Search Add Allen

ID: 367

Guest

Salutation: Please Select

* Last Name: Allen

* First Name: Mike

Company

Company Name:

Job/Title:

Picture

Image: [Image] Browse... Upload Image

Guest Group & Type

Group Name: Please Select

Profile Type: No Filter

Email

Home Email: Primary

Business Email: mike@goldkeysol

Notes

Color code: Black

Create Logbook

Set Reminder

Print

*All Indicators

Email

Contacts Indicators Contact History Logbook Entries Credit Cards Contact Flags Links Privacy History

Credit Card Information

Please Select / (MM/YY) Add Clear Set Password View History

Type	Credit Card Number	Expiration MM/YY	Operations
MC	*****1977	**/**	Edit Delete Show CC Number
Dsc	*****0298	**/**	Edit Delete Show CC Number

Page 1 of 1 Show 10 Items Displaying 1 to 2 of 2 items

© 2008-2009 Conclerge Assistant Web

Gold Key Solutions CA Web Best Practices Rev 09/01/09

The Guest profile information comes over too.

The screenshot displays the Gold Key Solutions CA Web interface. The top navigation bar includes links for Contacts, Logbook, Messages, Profiles, Administration, and Help. The main content area is divided into several sections:

- Guest Information:** Fields for Salutation, Last Name (Allen), First Name (Mike), Room Number (123), Arrival, Departure, Guest Notification, Group Name, and Primary Phone (22). Buttons for Change Profile and Edit Profile are present.
- Entry:** Fields for Reference Date (05/26/2009), Time (04:22 am), Entry Type (Dining Reservations), Restaurant (Cioppinos), Address (400 Jefferson Street San), Credit Card, Telephone ((415) 775-9311 X 56565), Number in Party, Special requests, Confirmation, Notes, Confirmed With, Smoking Preferences, and Special Comments. Buttons for Change Contact and Edit Contact are present.
- Guest Profile:** A section containing guest details and a table for Credit Card Information.

The Credit Card Information table is highlighted with a red box:

Type	Credit Card Number	Expires	Operations
Dsc	*****0298	**/**	Show CC Number
MC	*****1977	**/**	Show CC Number

The bottom of the page shows the copyright notice: © 2008-2009 Concierge Assistant Web.

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

This screenshot is identical to the one above, but with a red box highlighting the "Show CC Number" link in the Operations column of the Credit Card Information table. The link is underlined and green, indicating it is clickable.

You will get this screen

Dialog box titled "Show Credit Card Number" with a close button (X).

* Password: [Masked]

* Reason: Book Tour

Type	Credit Card Number	Expiration MM/YY

Buttons: Display, Cancel

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

Dialog box titled "Show Credit Card Number" with a close button (X).

* Password: [Masked]

* Reason: Book Tour

Type	Credit Card Number	Expiration MM/YY
Visa	4635890000112606	12/15

Buttons: Display, Cancel

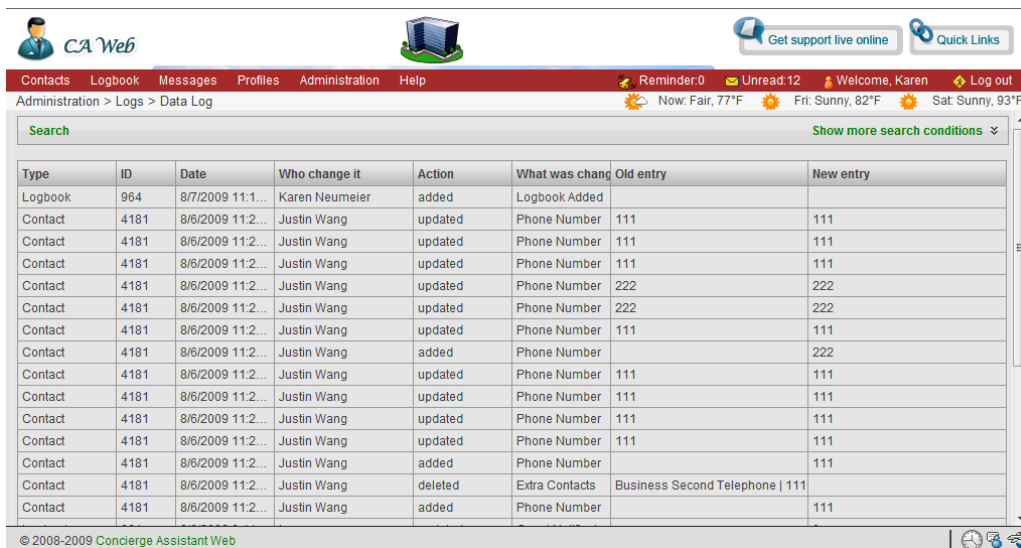
Once the screen is closed, the credit card information will remain masked in the Profile.

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.

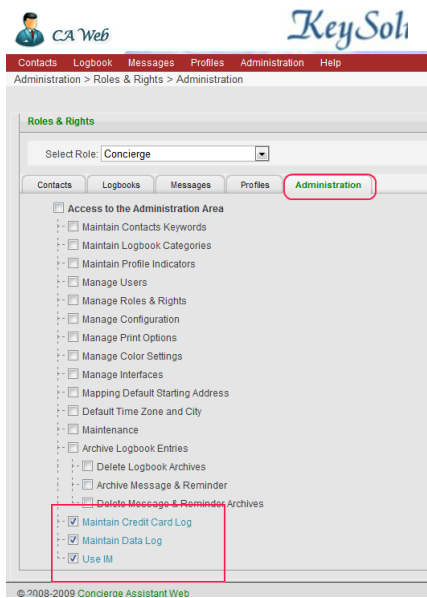
In CA Web, through the use of logon names and passwords, we have provided a means to create an “audit trail” of staff associates who are accessing this information via Logbook entries and the Profile feature. (Refer to Roles and Rights) This log may be deleted on a regular basis by the Site Administrator 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.



The screenshot shows the CA Web interface with a navigation bar at the top. The main content area displays a table titled "Data Log" under the "Administration > Logs > Data Log" path. The table has columns for Type, ID, Date, Who change it, Action, What was changed, Old entry, and New entry. The table lists various logbook and contact entries, including updates and deletions of phone numbers and extra contacts. A search bar and "Show more search conditions" link are at the top of the table. The footer shows the copyright notice "© 2008-2009 Concierge Assistant Web".

Type	ID	Date	Who change it	Action	What was changed	Old entry	New entry
Logbook	964	8/7/2009 11:1...	Karen Neumeier	added	Logbook Added		
Contact	4181	8/6/2009 11:2...	Justin Wang	updated	Phone Number	111	111
Contact	4181	8/6/2009 11:2...	Justin Wang	updated	Phone Number	111	111
Contact	4181	8/6/2009 11:2...	Justin Wang	updated	Phone Number	111	111
Contact	4181	8/6/2009 11:2...	Justin Wang	updated	Phone Number	222	222
Contact	4181	8/6/2009 11:2...	Justin Wang	updated	Phone Number	222	222
Contact	4181	8/6/2009 11:2...	Justin Wang	updated	Phone Number	111	111
Contact	4181	8/6/2009 11:2...	Justin Wang	added	Phone Number		222
Contact	4181	8/6/2009 11:2...	Justin Wang	updated	Phone Number	111	111
Contact	4181	8/6/2009 11:2...	Justin Wang	updated	Phone Number	111	111
Contact	4181	8/6/2009 11:2...	Justin Wang	updated	Phone Number	111	111
Contact	4181	8/6/2009 11:2...	Justin Wang	added	Phone Number		111
Contact	4181	8/6/2009 11:2...	Justin Wang	deleted	Extra Contacts	Business Second Telephone 111	
Contact	4181	8/6/2009 11:2...	Justin Wang	added	Phone Number		111



The screenshot shows the CA Web interface with a navigation bar at the top. The main content area displays the "Roles & Rights" configuration page. The "Selected Role" is "Concierge". The "Administration" tab is selected. The page lists various roles and rights, including "Access to the Administration Area", "Maintain Contacts Keywords", "Maintain Logbook Categories", "Maintain Profile Indicators", "Manage Users", "Manage Roles & Rights", "Manage Configuration", "Manage Print Options", "Manage Color Settings", "Manage Interfaces", "Mapping Default Starting Address", "Default Time Zone and City", "Maintenance", "Archive Logbook Entries", "Delete Logbook Archives", "Archive Message & Reminder", and "Delete Message & Reminder Archives". The "Maintain Credit Card Log", "Maintain Data Log", and "Use IM" options are checked and highlighted with a red box. The footer shows the copyright notice "© 2008-2009 Concierge Assistant Web".

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).

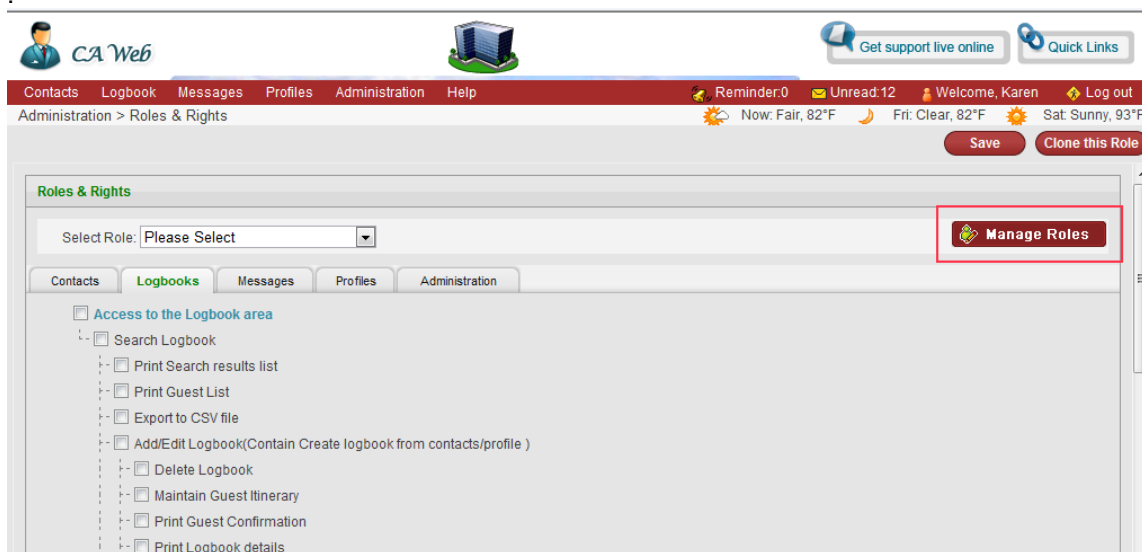
The screenshot displays the CA Web User Management interface. The top navigation bar includes links for Contacts, Logbook, Messages, Profiles, Administration, and Help. The user is logged in as 'leo'. The main content area shows the 'User Profile' for 'leo'. The 'Role(s)' section is highlighted with a red box, showing a list of roles: Bell Desk Operator..., Concierge, Concierge Manager, PBX, Site Administrator (selected), and test. The 'User Profile' section includes fields for First Name (Leo), Last Name (Aguirre), Initials, Job Title, Email (leo@goldkeysolutions.), Phone, Fax, Zip Code, Address, City, State, and Country. The 'Interface Setting' section shows Open Table ID (308186) and Network ID. The bottom status bar indicates the copyright is © 2008-2009 Concierge Assistant Web.

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.

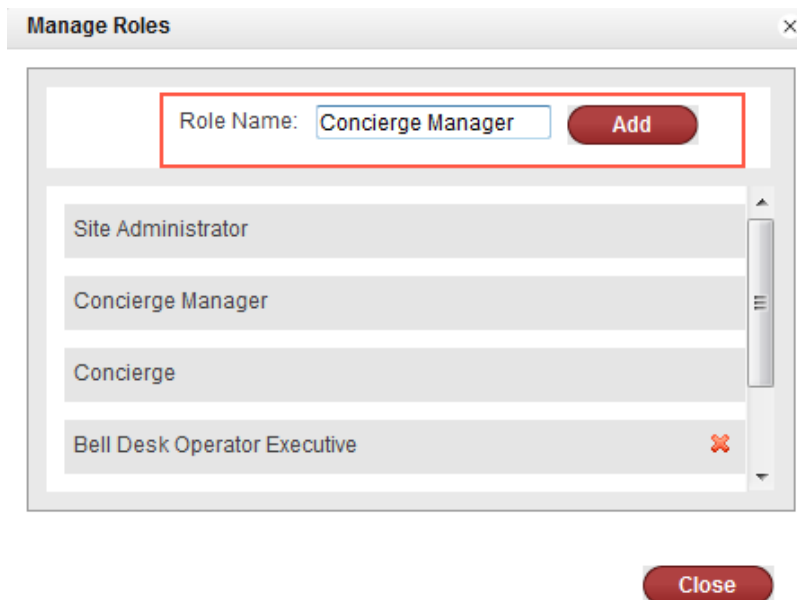


The Site Administrator must establish the Roles that each of the users will qualify under such as; Concierge Manager, for associates in a supervisory capacity with the need to manage activities of the staff; Concierge, who will be interacting with guests and their requests requiring the need to decrypt 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".



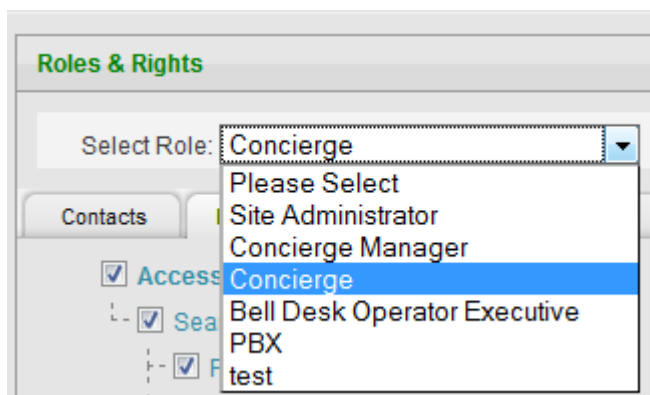
Enter the label of the Role you will be establishing, such as Concierge Manager, Concierge, PBX etc and click “Add”. You can enter all of the Roles at one time so you may have them available as you are establishing the Rights for each.



The image shows a 'Manage Roles' dialog box. At the top, there is a text input field labeled 'Role Name:' containing the text 'Concierge Manager', followed by a red 'Add' button. Below this is a list of roles: 'Site Administrator', 'Concierge Manager', 'Concierge', and 'Bell Desk Operator Executive'. The 'Bell Desk Operator Executive' role has a red 'X' icon next to it. At the bottom of the dialog is a red 'Close' button.

Click on Close when you have completed entering your list of Roles.

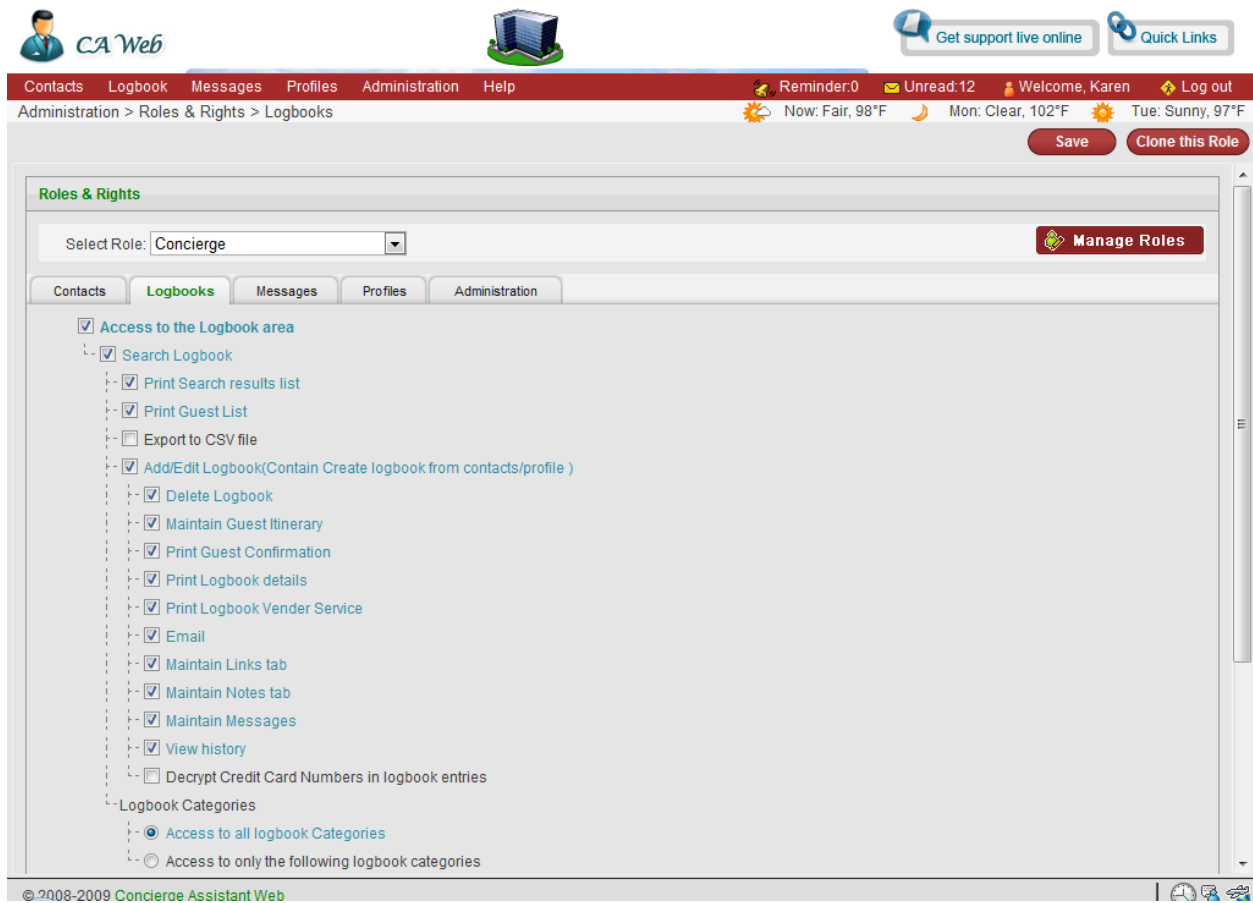
Now select a Role you want to establish the Rights for.



The image shows a 'Roles & Rights' dialog box. It has a 'Select Role:' dropdown menu with a list of roles: 'Please Select', 'Site Administrator', 'Concierge Manager', 'Concierge' (highlighted in blue), 'Bell Desk Operator Executive', 'PBX', and 'test'. To the left of the dropdown is a 'Contacts' tab and a list of checkboxes for 'Access', 'Sea', and 'F'.

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”.



The screenshot shows the CA Web interface with the 'Roles & Rights' section active. The role 'Concierge' is selected. The 'Logbooks' tab is chosen, showing a list of permissions with checkboxes. Most permissions are checked, indicating they are granted to the Concierge role.

Roles & Rights

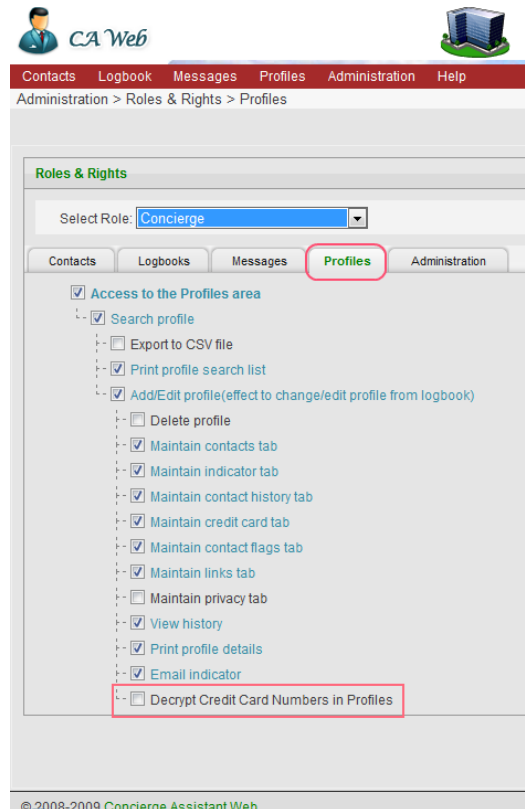
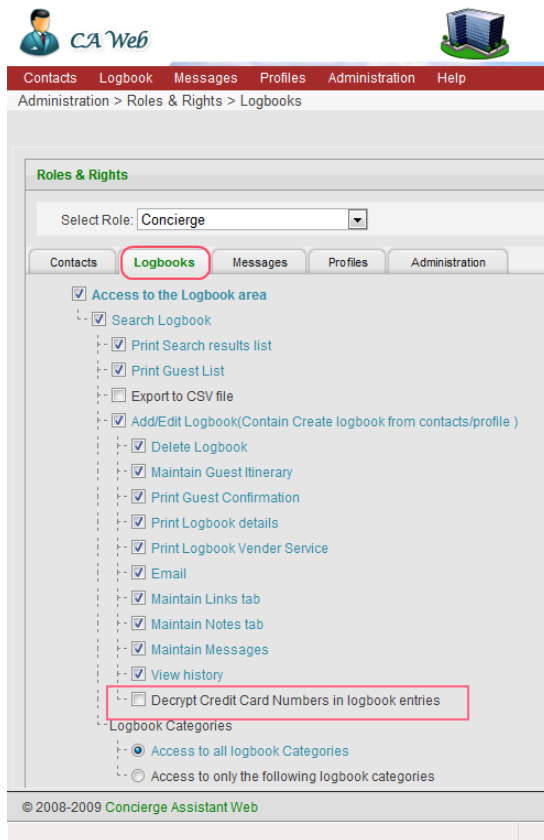
Select Role: **Concierge** Manage Roles

Contacts **Logbooks** Messages Profiles Administration

- ☒ **Access to the Logbook area**
 - ☒ Search Logbook
 - ☒ Print Search results list
 - ☒ Print Guest List
 - ☐ Export to CSV file
 - ☒ Add/Edit Logbook(Contain Create logbook from contacts/profile)
 - ☒ Delete Logbook
 - ☒ Maintain Guest Itinerary
 - ☒ Print Guest Confirmation
 - ☒ Print Logbook details
 - ☒ Print Logbook Vender Service
 - ☒ Email
 - ☒ Maintain Links tab
 - ☒ Maintain Notes tab
 - ☒ Maintain Messages
 - ☒ View history
 - ☐ Decrypt Credit Card Numbers in logbook entries
 - Logbook Categories**
 - ☒ Access to all logbook Categories
 - ☐ Access to only the following logbook categories

© 2008-2009 Concierge Assistant Web

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.

Gold Key Solutions CA Web Best Practices Rev 09/01/09

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.

Search Users

Search

First Name: Last Name: Role: Status: User Name:

Set as default search Run default search Clear Search

Select All Selected All Export to CSV file Print

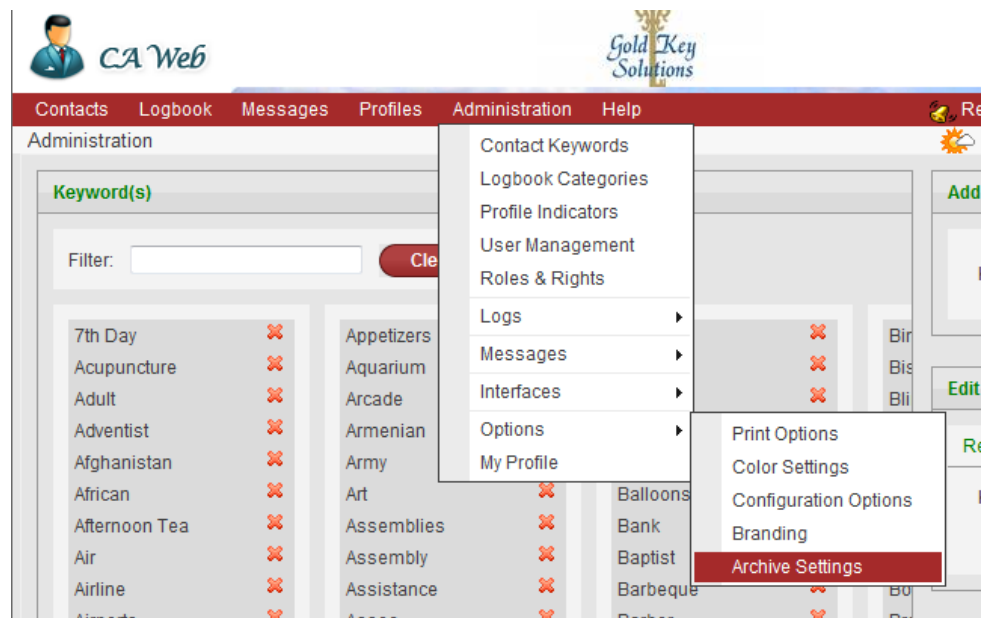
First Name	Last Name	User Name	Role	Status	Operations
<input type="checkbox"/> admin	admin	admin	Site Administrator	Active	Edit
<input type="checkbox"/> Ann	Taylor	Ann	Concierge	Active	Edit
<input type="checkbox"/> betty	wu	betty	Site Administrator	Active	Edit
<input type="checkbox"/> Charles	Dickens	charles	Site Administrator	Active	Edit
<input type="checkbox"/> Concierge	Goldkey	concierge	Concierge	Active	Edit
<input type="checkbox"/> concierge manager	manager	manager	Concierge Manager	Active	Edit
<input type="checkbox"/> Cris	Dovich	cris	Site Administrator	Active	Edit
<input type="checkbox"/> CrisTest	Test	CrisTest	Concierge	Active	Edit
<input type="checkbox"/> david	c	david	Site Administrator	Active	Edit
<input type="checkbox"/> eric	eric	eric	Site Administrator	Active	Edit
<input type="checkbox"/> Jane	Austen	Jane	Concierge	Active	Edit
<input type="checkbox"/> jerry	li	jerry	Site Administrator	InActive	Edit
<input type="checkbox"/> Joe	Blow	joe	PBX, Concierge	Active	Edit
<input type="checkbox"/> John	Doe	JDoe	Bell Desk Operator Exe...	Active	Edit
<input type="checkbox"/> John	rambo	rambo	Concierge Manager	Active	Edit

© 2008-2009 Concierge Assistant Web

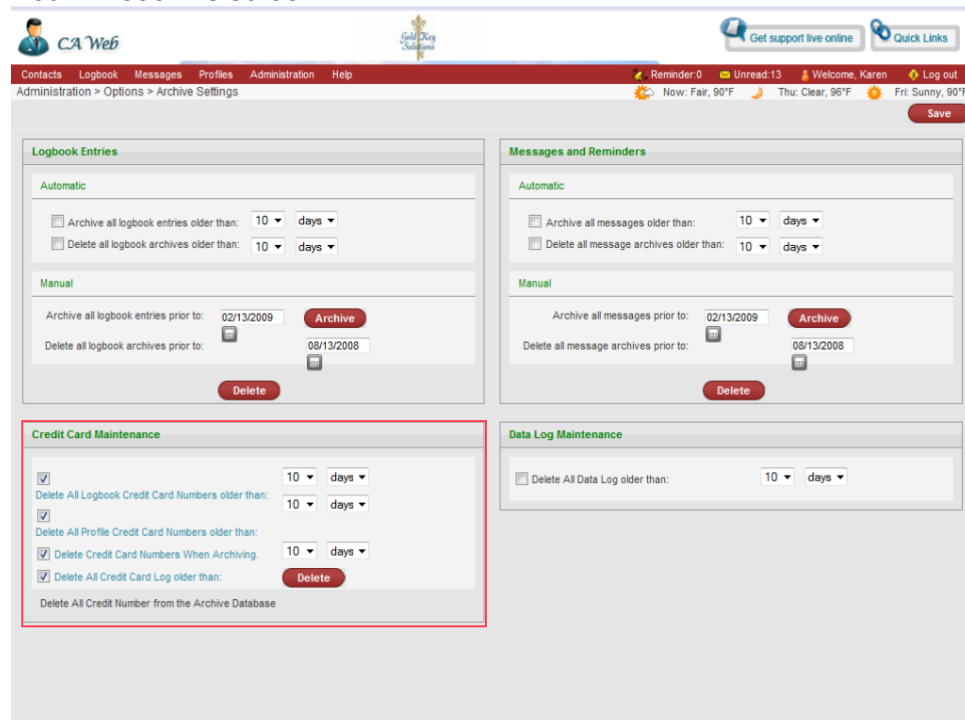
Purging Old Credit Card Information

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

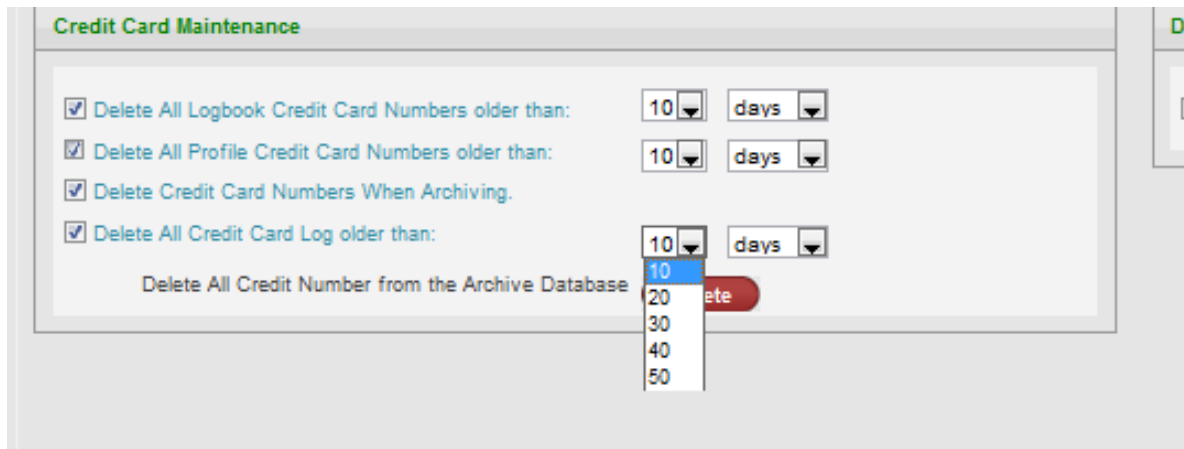


You will see this screen.



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.

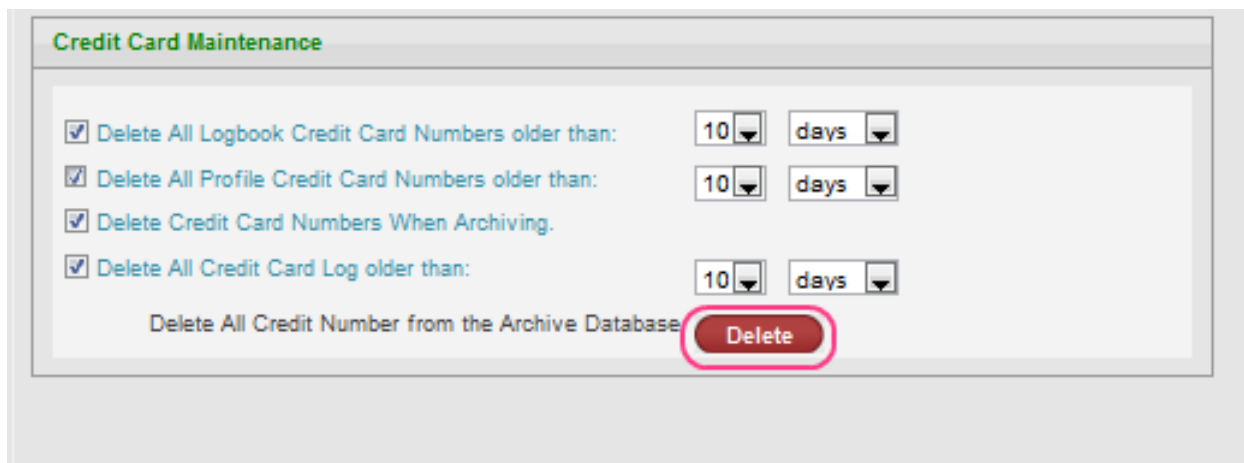


The screenshot shows the 'Credit Card Maintenance' interface. It contains four checked checkboxes with associated dropdown menus for retention periods:

- ☒ Delete All Logbook Credit Card Numbers older than: 10 days
- ☒ Delete All Profile Credit Card Numbers older than: 10 days
- ☒ Delete Credit Card Numbers When Archiving.
- ☒ Delete All Credit Card Log older than: 10 days

Below these is the text 'Delete All Credit Number from the Archive Database' followed by a red 'Delete' button. A dropdown menu is open for the last '10 days' setting, showing options: 10, 20, 30, 40, and 50.

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.



This screenshot shows the same 'Credit Card Maintenance' interface as the previous one, but with the red 'Delete' button next to the text 'Delete All Credit Number from the Archive Database' highlighted with a pink oval.

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	<p>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.</p> <p>Do not use vendor-supplied defaults for system passwords and other security parameters</p>
Protect Cardholder Data	<p>Protect stored data</p> <p>Encrypt transmission of cardholder data and sensitive information across public networks</p>
Maintain a Vulnerability Management Program	<p>Use and regularly update anti-virus software</p> <p>Develop and maintain secure systems and applications</p>
Implement Strong Access Control Measures	<p>Restrict access to data by business need-to-know</p> <p>Assign a unique ID to each person with computer access</p> <p>Restrict physical access to cardholder data</p>
Regularly Monitor and Test Networks	<p>Track and monitor all access to network resources and cardholder data</p> <p>Regularly test security systems and processes</p>
Maintain an Information Security Policy	<p>Maintain a policy that addresses information security</p>

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