THE CONCIERGE ASSISTANT® (CA) - CISP IMPLEMENTATION GUIDELINES

As of December 2006, The Concierge Assistant® is a Visa CISP and PABP validated solution.

Build and Maintain a Secure Network

Install and maintain a secure firewall configuration to protect data.

The Database folder Network share must not be connected to the Internet. All access by individuals with root or administrative privileges should be audited. All access to the logging file (TheCAS.mdb) should be audited. The creation or deletion of system-level objects should be audited. These audit logs should be reviewed on a regular basis.

In addition to writing out log events into the database, the Concierge Assistant also writes out log events to a file named 'TheCAS.mdb'. This file contains a log of deleted records, credit card views, user logons, and password changes. This log file is located in the shared network path originally set up. We highly recommend that you frequently back up this file to read-only media (CD or DVD). We also recommend that you turn on Windows Auditing to log all access to this file which will allow your organization to track all changes to this file.

Remove all unnecessary and insecure services and protocols (e.g., NetBIOS, filesharing, Telnet, unencrypted FTP, and others) from the Network Share and the workstations.

If wireless transmission is used encrypt the transmissions by using Wi-Fi Protected Access (WPA) technology if WPA capable, or VPN or SSL at 128-bit. Never rely exclusively on WEP to protect confidentiality and access to a wireless LAN. Use one of the above methodologies in conjunction with WEP at 128 bit, and rotate shared WEP keys quarterly and whenever there are personnel changes.

If employees, administrators, or vendors can access the application remotely, access should be authenticated using a 2-factor authentication mechanism. The application should allow for technologies such as RADIUS or TACACS with tokens, or VPN with individual certificates.

Do not use vendor-supplied defaults for system passwords and other security parameters. Logon to the network and database should require a unique username and strong password.

Strong Passwords are defined as follows:

Minimum of 7 characters; Maximum of 10 characters; Must contain at least one alphabetic character; Must contain at least one numeric character; Must not contain the User Logon Name; Must not reuse four previous passwords

Gold Key highly recommends that the user configures Safe Passwords and incorporates the same above password characteristics that we recommend for the CA passwords.

In The Concierge Assistant we supply you with a Generic Logon: Concierge/Manager



Effective with version 9.0.3, CA uses a default username and password when it is initially sent to the client. CA detects the first time CA is opened and CA forces the user to change the password.

Prior to version 9.0.3 CA worked as follows. After initial installation the password for Concierge had to be changed manually to a strong password or deleted. The Concierge logon/password should never be used by the concierge staff.

The recommended security settings can be found in the Administration Tab of The Concierge Assistant on the Security Options panel:

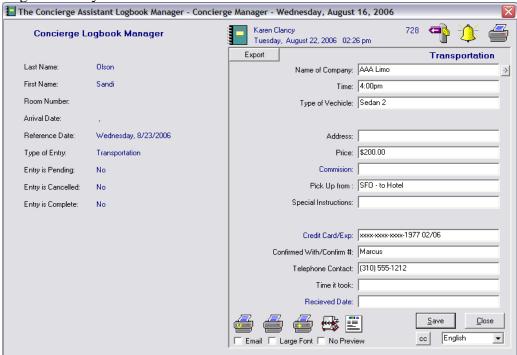


Protect Cardholder Data:

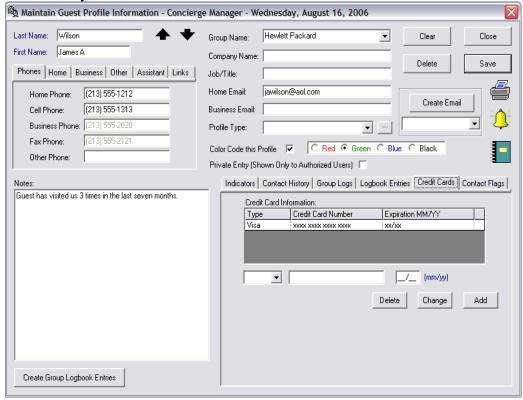
All Credit Card information is encrypted using Triple DES or AES encryption methods with the encrypted value converted to a hexadecimal string.

In The Concierge Assistant credit card information is found only in the Logbook and Profiles subsystems of CA. The credit card information is encrypted and is password protected:

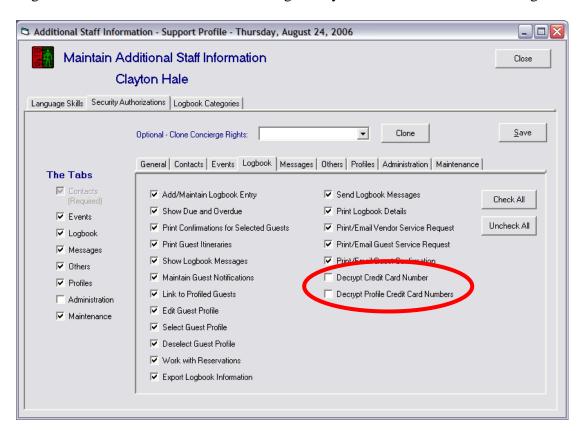
Logbook Entry:

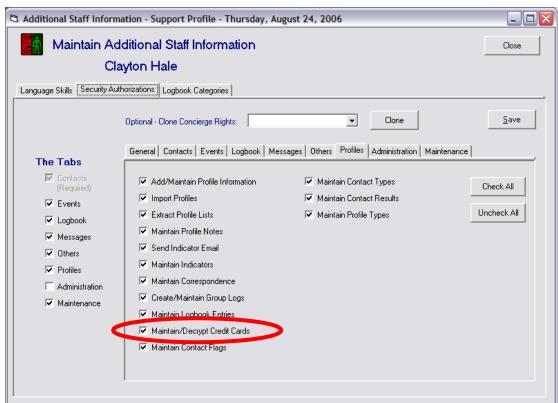


Profile Entry:



Rights to the Credit Card information are given by the Administrators of the Program:





The Administrators can give individual rights to each employee based on their need to know basis.

Maintain a Vulnerability Management Program:

Use and regularly update anti-virus software.

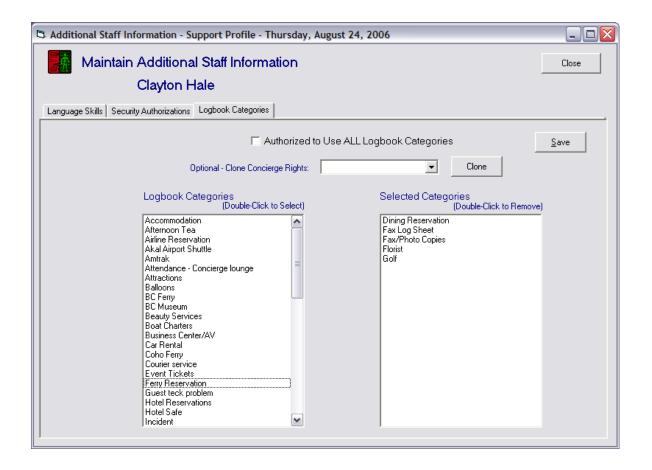
Develop and maintain secure systems, if Remote Access is allowed implement appropriate security and encryption procedures. This includes two-factor authentication (username and password).

Implement Strong Access Control Measures:

Restrict access to data by business need-to-know.

All Logbook categories and Profile information is restricted by the Administrators for each individual employee.

For a regular user, Administrators can restrict even the logbook categories that each employee can see:

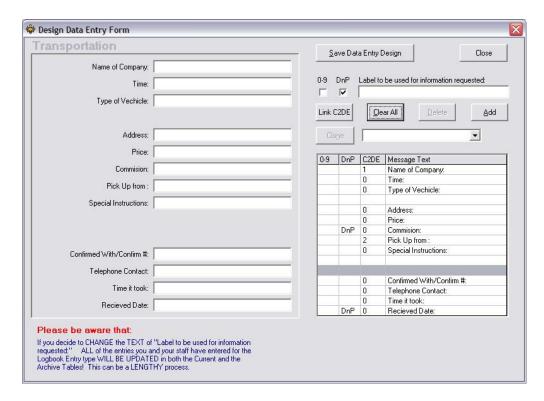


Administrators can also make the data entry panels contain or not contain credit card information:

With Credit Card Information:

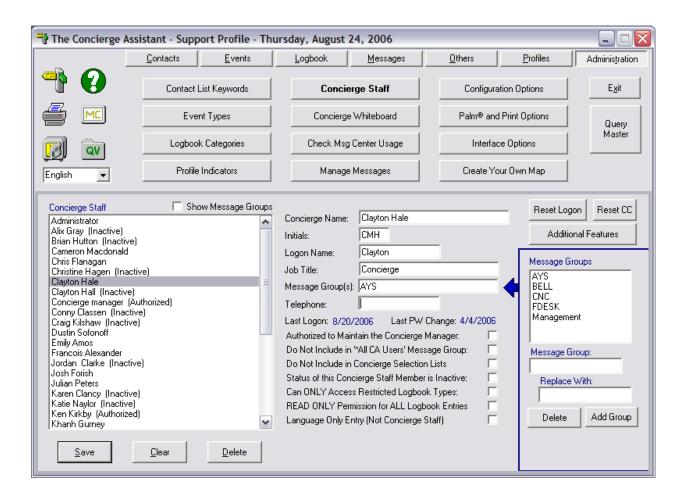
nsportation	Save Data Entry Design	Close	
Name of Company:			
Time:	0-9 DnP Label to be used for inform.	ation requested:	
Type of Vechicle:	Link C2DE <u>C</u> lear All <u>D</u> ele	Link C2DE Clear All Delete Ad	
Address:	Clone	·	
Price:	0-9 DnP C2DE Message Text		
Commision:	1 Name of Compan	y:	
Pick Up from :	0 Time:		
Pick op IIoIII.	0 Type of Vechicle.		
Special Instructions:	0 Address:		
	0 Address.		
-	DnP 0 Commission:		
Credit Card/Exp:	2 Pick Up from :	Pick Up from:	
Confirmed With/Confirm #:	0 Special Instruction	ns:	
Telephone Contact:	DnP 0 Credit Card/Exp:	Credit Card/Exp:	
-	0 Confirmed With/0		
Time it took:	0 Telephone Conta	ct:	
Recieved Date:	0 Time it took:		
	DnP 0 Recieved Date:		
se be aware that:			
decide to CHANGE the TEXT of "Label to be used for inform	ation		
sted:" ALL of the entries you and your staff have entered it lok Entry type WILL BE UPDATED in both the Current and the	or the		

Without Credit Card Information:



Assign a unique ID to each person with computer access.

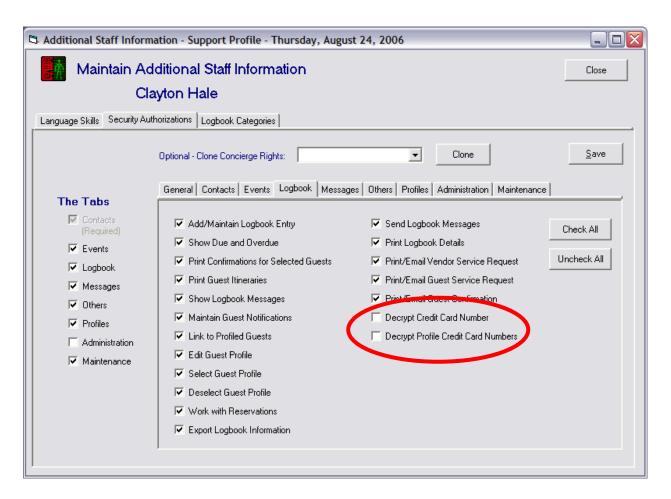
The Concierge Assistant does not provide for group logons. All employees have unique logons and passwords:



To make the passwords even more secure, in the Security Options set up by the Administrators, you can make users inactive; log users off after a pre-determined amount of time of not using the application, Inactivate the user after "X" number of failed logon attempts, and have the password change after "X" amount of days.



Each employee can be restricted to what they can or cannot see. If a certain employee should not have access to credit card information, by going into the employees profile the Administrator will be able to take that access away from the employee:



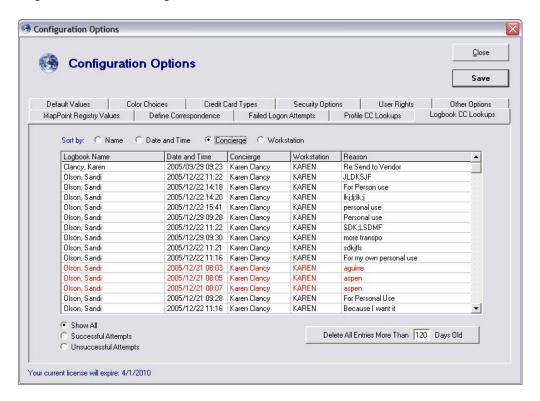
This is to ensure that all employees only have access to the information that they require.

Regularly Monitor and Test Networks

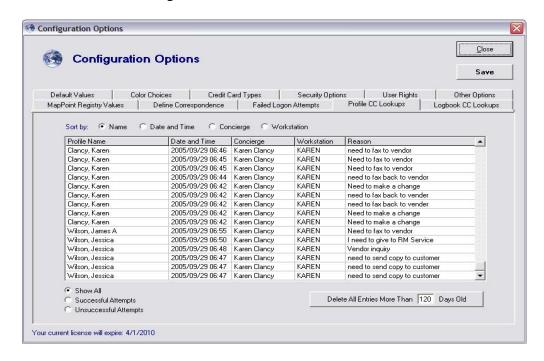
Track and monitor all access to network resources and cardholder data.

In the Concierge Assistant, all credit card information from both Logbook and Profiles is traced to the employee who retrieved the information from the system.

Logbook Credit Card Log:



Profile Credit Card Log:



Maintain an 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 and maintain a firewall configuration to protect data 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 CISP information please refer to our Best Practices - Credit Card Encryption, which can be, used as a training document for your staff members.

For more technical information regarding The Concierge Assistant, please refer to our IT Memo.