

THE CONCIERGE ASSISTANT® (CA) - CISP IMPLEMENTATION DOC

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.

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:

The screenshot shows the 'Configuration Options' dialog box with the 'Security Options' tab selected. The dialog has a title bar with a close button (X) and two buttons: 'Close' and 'Save'. Below the title bar is a tabbed interface with the following tabs: 'MapPoint Registry Values', 'Define Correspondence', 'Failed Logon Attempts', 'Profile CC Lookups', 'Logbook CC Lookups', 'Default Values', 'Color Choices', 'Credit Card Types', 'Security Options' (selected), 'User Rights', and 'Other Options'. The 'Security Options' tab contains the following settings:

Setting	Value	Checked
Inactivate User if No Logon in Last	21 days	<input checked="" type="checkbox"/>
Range is from 10 to 90 days		
Logoff User if No Activity in the Last	15 Minutes	<input checked="" type="checkbox"/>
Range is from 10 to 60 Minutes		
Inactivate User after	3 Failed Logon Attempts	<input checked="" type="checkbox"/>
Enforce Strong Passwords		<input checked="" type="checkbox"/>
A Strong Password is defined as:		
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		
Password must be changed every	90 days	<input checked="" type="checkbox"/>
Range is from 30 to 180 days		

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: (see next page)

Logbook Entry:

The Concierge Assistant Logbook Manager - Concierge Manager - Wednesday, August 16, 2006

Concierge Logbook Manager

Last Name: Olson
First Name: Sandi
Room Number:
Arrival Date:
Reference Date: Wednesday, 8/23/2006
Type of Entry: Transportation
Entry is Pending: No
Entry is Cancelled: No
Entry is Complete: No

Transportation

Name of Company: AAA Limo
Time: 4:00pm
Type of Vehicle: Sedan 2
Address:
Price: \$200.00
Comission:
Pick Up from: SFO - to Hotel
Special Instructions:
Credit Card/Exp: xxxx-xxxx-xxxx-1977 02/06
Confirmed With/Confirm #: Marcus
Telephone Contact: (310) 555-1212
Time it took:
Recieved Date:

☐ Email ☐ Large Font ☐ No Preview

Save Close
cc English

Profile Entry:

Maintain Guest Profile Information - Concierge Manager - Wednesday, August 16, 2006

Last Name: Wilson
First Name: James A

Group Name: Hewlett Packard
Company Name:
Job/Title:
Home Email: jawilson@aol.com
Business Email:
Profile Type:
Color Code this Profile ☒ Red ☒ Green ☐ Blue ☐ Black
Private Entry (Shown Only to Authorized Users) ☐

Home Phone: (213) 555-1212
Cell Phone: (213) 555-1313
Business Phone: (213) 555-2020
Fax Phone: (213) 555-2121
Other Phone:

Notes:
Guest has visited us 3 times in the last seven months.

Indicators Contact History Group Logs Logbook Entries Credit Cards Contact Flags

Credit Card Information:

Type	Credit Card Number	Expiration MM/YY
Visa	xxxx xxxx xxxx	xx/xx

____/____ (mm/yy)

Delete Change Add

Create Group Logbook Entries

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

Additional Staff Information - Support Profile - Thursday, August 24, 2006

Maintain Additional Staff Information
Clayton Hale

Language Skills | Security Authorizations | Logbook Categories

Optional - Clone Concierge Rights: [Dropdown] [Clone] [Save]

The Tabs

- ☒ Contacts (Required)
- ☒ Events
- ☒ Logbook
- ☒ Messages
- ☒ Others
- ☒ Profiles
- ☐ Administration
- ☒ Maintenance

General | Contacts | Events | Logbook | Messages | Others | Profiles | Administration | Maintenance

<input checked="" type="checkbox"/> Add/Maintain Logbook Entry	<input checked="" type="checkbox"/> Send Logbook Messages	[Check All]
<input checked="" type="checkbox"/> Show Due and Overdue	<input checked="" type="checkbox"/> Print Logbook Details	
<input checked="" type="checkbox"/> Print Confirmations for Selected Guests	<input checked="" type="checkbox"/> Print/Email Vendor Service Request	[Uncheck All]
<input checked="" type="checkbox"/> Print Guest Itineraries	<input checked="" type="checkbox"/> Print/Email Guest Service Request	
<input checked="" type="checkbox"/> Show Logbook Messages	<input checked="" type="checkbox"/> Print/Email Guest Confirmation	
<input checked="" type="checkbox"/> Maintain Guest Notifications	<input type="checkbox"/> Decrypt Credit Card Number	
<input checked="" type="checkbox"/> Link to Profiled Guests	<input type="checkbox"/> Decrypt Profile Credit Card Numbers	
<input checked="" type="checkbox"/> Edit Guest Profile		
<input checked="" type="checkbox"/> Select Guest Profile		
<input checked="" type="checkbox"/> Deselect Guest Profile		
<input checked="" type="checkbox"/> Work with Reservations		
<input checked="" type="checkbox"/> Export Logbook Information		

Additional Staff Information - Support Profile - Thursday, August 24, 2006

Maintain Additional Staff Information
Clayton Hale

Language Skills | Security Authorizations | Logbook Categories

Optional - Clone Concierge Rights: [Dropdown] [Clone] [Save]

The Tabs

- ☒ Contacts (Required)
- ☒ Events
- ☒ Logbook
- ☒ Messages
- ☒ Others
- ☒ Profiles
- ☐ Administration
- ☒ Maintenance

General | Contacts | Events | Logbook | Messages | Others | Profiles | Administration | Maintenance

<input checked="" type="checkbox"/> Add/Maintain Profile Information	<input checked="" type="checkbox"/> Maintain Contact Types	[Check All]
<input checked="" type="checkbox"/> Import Profiles	<input checked="" type="checkbox"/> Maintain Contact Results	
<input checked="" type="checkbox"/> Extract Profile Lists	<input checked="" type="checkbox"/> Maintain Profile Types	[Uncheck All]
<input checked="" type="checkbox"/> Maintain Profile Notes		
<input checked="" type="checkbox"/> Send Indicator Email		
<input checked="" type="checkbox"/> Maintain Indicators		
<input checked="" type="checkbox"/> Maintain Correspondence		
<input checked="" type="checkbox"/> Create/Maintain Group Logs		
<input checked="" type="checkbox"/> Maintain Logbook Entries		
<input checked="" type="checkbox"/> Maintain/Decrypt Credit Cards		
<input checked="" type="checkbox"/> Maintain Contact Flags		

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:

The screenshot shows a web application window titled "Additional Staff Information - Support Profile - Thursday, August 24, 2006". The main heading is "Maintain Additional Staff Information" for "Clayton Hale". There are three tabs: "Language Skills", "Security Authorizations", and "Logbook Categories", with the last one being active. The window contains a checkbox for "Authorized to Use ALL Logbook Categories" (unchecked), a "Save" button, and a section for "Optional - Clone Concierge Rights" with a dropdown menu and a "Clone" button. Below this are two lists: "Logbook Categories (Double-Click to Select)" and "Selected Categories (Double-Click to Remove)". The first list contains 25 items, with "Ferry Reservation" highlighted. The second list contains 5 items: "Dining Reservation", "Fax Log Sheet", "Fax/Photo Copies", "Florist", and "Golf".

Logbook Categories (Double-Click to Select)	Selected Categories (Double-Click to Remove)
Accommodation	Dining Reservation
Afternoon Tea	Fax Log Sheet
Airline Reservation	Fax/Photo Copies
Akal Airport Shuttle	Florist
Amtrak	Golf
Attendance - Concierge lounge	
Attractions	
Balloons	
BC Ferry	
BC Museum	
Beauty Services	
Boat Charters	
Business Center/AV	
Car Rental	
Coho Ferry	
Courier service	
Event Tickets	
Ferry Reservation	
Guest teck problem	
Hotel Reservations	
Hotel Safe	
Incident	

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

With Credit Card Information:

The screenshot shows the 'Design Data Entry Form' window for 'Transportation'. The left panel contains input fields for: Name of Company, Time, Type of Vehicle, Address, Price, Commission, Pick Up from, Special Instructions, Credit Card/Exp, Confirmed With/Confirm #, Telephone Contact, Time it took, and Received Date. The right panel has a 'Save Data Entry Design' button, a 'Close' button, and a section for 'Label to be used for information requested' with checkboxes for '0-9' and 'DnP'. Below this are buttons for 'Link C2DE', 'Clear All', 'Delete', and 'Add'. A 'Close' button is also present. At the bottom, a table lists the message text for each field, including 'Credit Card/Exp'. A red warning message is at the bottom left.

Please be aware that:
If you decide to CHANGE the TEXT of "Label to be used for information requested:" ALL of the entries you and your staff have entered for the Logbook Entry type WILL BE UPDATED in both the Current and the Archive Tables! This can be a LENGTHY process.

Without Credit Card Information:

The screenshot shows the 'Design Data Entry Form' window for 'Transportation' without the credit card information fields. The left panel contains input fields for: Name of Company, Time, Type of Vehicle, Address, Price, Commission, Pick Up from, Special Instructions, Confirmed With/Confirm #, Telephone Contact, Time it took, and Received Date. The right panel has a 'Save Data Entry Design' button, a 'Close' button, and a section for 'Label to be used for information requested' with checkboxes for '0-9' and 'DnP'. Below this are buttons for 'Link C2DE', 'Clear All', 'Delete', and 'Add'. A 'Close' button is also present. At the bottom, a table lists the message text for each field, excluding 'Credit Card/Exp'. A red warning message is at the bottom left.

Please be aware that:
If you decide to CHANGE the TEXT of "Label to be used for information requested:" ALL of the entries you and your staff have entered for the Logbook Entry type WILL BE UPDATED in both the Current and the Archive Tables! This can be a LENGTHY process.

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:

The Concierge Assistant - Support Profile - Thursday, August 24, 2006

Contacts Events Logbook Messages Others Profiles Administration

Contact List Keywords Concierge Staff Configuration Options Exit

Event Types Concierge Whiteboard Palm® and Print Options Query Master

Logbook Categories Check Msg Center Usage Interface Options

Profile Indicators Manage Messages Create Your Own Map

English

Concierge Staff ☐ Show Message Groups

Administrator
Alix Gray (Inactive)
Brian Hutton (Inactive)
Cameron Macdonald
Chris Flanagan
Christine Hagen (Inactive)
Clayton Hale
Clayton Hall (Inactive)
Concierge manager (Authorized)
Conny Classen (Inactive)
Craig Kilshaw (Inactive)
Dustin Sofonoff
Emily Amos
Francois Alexander
Jordan Clarke (Inactive)
Josh Forish
Julian Peters
Karen Clancy (Inactive)
Katie Naylor (Inactive)
Ken Kirkby (Authorized)
Khanh Gurney

Concierge Name: Clayton Hale
Initials: CMH
Logon Name: Clayton
Job Title: Concierge
Message Group(s): AYS
Telephone:
Last Logon: 8/20/2006 Last PW Change: 4/4/2006
Authorized to Maintain the Concierge Manager: ☐
Do Not Include in "All CA Users" Message Group: ☐
Do Not Include in Concierge Selection Lists: ☐
Status of this Concierge Staff Member is Inactive: ☐
Can ONLY Access Restricted Logbook Types: ☐
READ ONLY Permission for ALL Logbook Entries: ☐
Language Only Entry (Not Concierge Staff): ☐

Reset Logon Reset CC
Additional Features

Message Groups
AYS
BELL
CNC
FDESK
Management
Message Group:
Replace With:
Delete Add Group

Save Clear Delete

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.

The screenshot shows the 'Configuration Options' dialog box with the 'Security Options' tab selected. The dialog has a title bar with a globe icon and a close button. Inside, there's a header with a globe icon and the text 'Configuration Options', followed by 'Close' and 'Save' buttons. Below the header is a tabbed interface with six tabs: 'MapPoint Registry Values', 'Define Correspondence', 'Failed Logon Attempts', 'Profile CC Lookups', 'Logbook CC Lookups', and 'Default Values'. The 'Security Options' tab is active, showing several security settings with checkboxes and numeric input fields.

MapPoint Registry Values	Define Correspondence	Failed Logon Attempts	Profile CC Lookups	Logbook CC Lookups
Default Values	Color Choices	Credit Card Types	Security Options	User Rights
			Other Options	

Inactivate User if No Logon in Last <input type="text" value="21"/> days <small>Range is from 10 to 90 days</small>	<input checked="" type="checkbox"/>
Logoff User if No Activity in the Last <input type="text" value="15"/> Minutes <small>Range is from 10 to 60 Minutes</small>	<input checked="" type="checkbox"/>
Inactivate User after <input type="text" value="3"/> Failed Logon Attempts	<input checked="" type="checkbox"/>
Enforce Strong Passwords <small>A Strong Password is defined as:</small> 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	<input checked="" type="checkbox"/>
Password must be changed every <input type="text" value="90"/> days <small>Range is from 30 to 180 days</small>	<input checked="" type="checkbox"/>

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:

Additional Staff Information - Support Profile - Thursday, August 24, 2006

Maintain Additional Staff Information
Clayton Hale

Language Skills | Security Authorizations | Logbook Categories

Optional - Clone Concierge Rights: [Dropdown] [Clone] [Save]

The Tabs

- ☒ Contacts (Required)
- ☒ Events
- ☒ Logbook
- ☒ Messages
- ☒ Others
- ☒ Profiles
- ☐ Administration
- ☒ Maintenance

General | Contacts | Events | **Logbook** | Messages | Others | Profiles | Administration | Maintenance

<input checked="" type="checkbox"/> Add/Maintain Logbook Entry	<input checked="" type="checkbox"/> Send Logbook Messages	[Check All]
<input checked="" type="checkbox"/> Show Due and Overdue	<input checked="" type="checkbox"/> Print Logbook Details	
<input checked="" type="checkbox"/> Print Confirmations for Selected Guests	<input checked="" type="checkbox"/> Print/Email Vendor Service Request	[Uncheck All]
<input checked="" type="checkbox"/> Print Guest Itineraries	<input checked="" type="checkbox"/> Print/Email Guest Service Request	
<input checked="" type="checkbox"/> Show Logbook Messages	<input checked="" type="checkbox"/> Print/Email Guest Confirmation	
<input checked="" type="checkbox"/> Maintain Guest Notifications	<input type="checkbox"/> Decrypt Credit Card Number	
<input checked="" type="checkbox"/> Link to Profiled Guests	<input type="checkbox"/> Decrypt Profile Credit Card Numbers	
<input checked="" type="checkbox"/> Edit Guest Profile		
<input checked="" type="checkbox"/> Select Guest Profile		
<input checked="" type="checkbox"/> Deselect Guest Profile		
<input checked="" type="checkbox"/> Work with Reservations		
<input checked="" type="checkbox"/> Export Logbook Information		

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:

Configuration Options

Close Save

Default Values Color Choices Credit Card Types Security Options User Rights Other Options
MapPoint Registry Values Define Correspondence Failed Logon Attempts Profile CC Lookups Logbook CC Lookups

Sort by: ☐ Name ☐ Date and Time ☒ Concierge ☐ Workstation

Logbook Name	Date and Time	Concierge	Workstation	Reason
Clancy, Karen	2005/09/29 09:23	Karen Clancy	KAREN	Re Send to Vendor
Olson, Sandi	2005/12/22 11:22	Karen Clancy	KAREN	JLDKSJF
Olson, Sandi	2005/12/22 14:18	Karen Clancy	KAREN	For Person use
Olson, Sandi	2005/12/22 14:20	Karen Clancy	KAREN	lkjlkjlkj
Olson, Sandi	2005/12/22 15:41	Karen Clancy	KAREN	personal use
Olson, Sandi	2005/12/29 09:28	Karen Clancy	KAREN	Personal use
Olson, Sandi	2005/12/22 11:22	Karen Clancy	KAREN	SDK.LSDMF
Olson, Sandi	2005/12/29 09:30	Karen Clancy	KAREN	more transpo
Olson, Sandi	2005/12/22 11:21	Karen Clancy	KAREN	sdkjfls
Olson, Sandi	2005/12/22 11:16	Karen Clancy	KAREN	For my own personal use
Olson, Sandi	2005/12/21 08:03	Karen Clancy	KAREN	aguirre
Olson, Sandi	2005/12/21 08:05	Karen Clancy	KAREN	aspen
Olson, Sandi	2005/12/21 08:07	Karen Clancy	KAREN	aspen
Olson, Sandi	2005/12/21 09:28	Karen Clancy	KAREN	For Personal Use
Olson, Sandi	2005/12/22 11:16	Karen Clancy	KAREN	Because I want it

☒ Show All
☐ Successful Attempts
☐ Unsuccessful Attempts

Delete All Entries More Than 120 Days Old

Your current license will expire: 4/1/2010

Profile Credit Card Log:

Configuration Options

Close Save

Default Values Color Choices Credit Card Types Security Options User Rights Other Options
MapPoint Registry Values Define Correspondence Failed Logon Attempts Profile CC Lookups Logbook CC Lookups

Sort by: ☒ Name ☐ Date and Time ☐ Concierge ☐ Workstation

Profile Name	Date and Time	Concierge	Workstation	Reason
Clancy, Karen	2005/09/29 06:46	Karen Clancy	KAREN	need to fax to vendor
Clancy, Karen	2005/09/29 06:45	Karen Clancy	KAREN	Need to fax to vendor
Clancy, Karen	2005/09/29 06:45	Karen Clancy	KAREN	Need to fax to vendor
Clancy, Karen	2005/09/29 06:44	Karen Clancy	KAREN	need to fax back to vendor
Clancy, Karen	2005/09/29 06:42	Karen Clancy	KAREN	Need to make a change
Clancy, Karen	2005/09/29 06:42	Karen Clancy	KAREN	need to fax back to vender
Clancy, Karen	2005/09/29 06:42	Karen Clancy	KAREN	need to fax back to vender
Clancy, Karen	2005/09/29 06:42	Karen Clancy	KAREN	Need to make a change
Clancy, Karen	2005/09/29 06:42	Karen Clancy	KAREN	Need to make a change
Wilson, James A	2005/09/29 06:55	Karen Clancy	KAREN	Need to fax to vendor
Wilson, Jessica	2005/09/29 06:50	Karen Clancy	KAREN	I need to give to RM Service
Wilson, Jessica	2005/09/29 06:48	Karen Clancy	KAREN	Vendor inquiry
Wilson, Jessica	2005/09/29 06:47	Karen Clancy	KAREN	need to send copy to customer
Wilson, Jessica	2005/09/29 06:47	Karen Clancy	KAREN	need to send copy to customer
Wilson, Jessica	2005/09/29 06:47	Karen Clancy	KAREN	need to send copy to customer

☒ Show All
☐ Successful Attempts
☐ Unsuccessful Attempts

Delete All Entries More Than 120 Days Old

Your current license will expire: 4/1/2010

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