Oracle® Hospitality Cruise Shipboard Property Management System

PA-DSS 3.2. Implementation Guide

Release 20.2
F44455-04
December 2023

Oracle Hospitality Cruise Shipboard Property Management System PA-DSS 3.2. Implementation Guide, Release 20.2

F44455-04

Contents

4 Services and Protocols (PA-DSS 8.2.c)

5 Appendix A Inadvertent Capture of PAN

Preface

This document describes the steps needed for your Oracle Hospitality Cruise Shipboard Property Management System (SPMS) installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application - Data Security Standards program (version 3.2 dated June 2016). For reference, download the PCI PA-DSS 3.2

Requirements and Security Assessment Procedures from the PCI SSC Document Library.

The Oracle Hospitality Cruise Shipboard Property Management System instructs and advises its customers to deploy the application in a manner that adheres to the PCI Data Security Standards. (v3.2). Subsequent to this, follow the best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various benchmarks, in order to enhance system logging, reduce the chance of intrusion, increase the ability to detect intrusion, and other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, disabling infrequently used or frequently vulnerable networking protocols, and implementing certificate-based protocols for access to servers by users and vendors.

Follow the steps outlined in this Implementation Guide for Oracle Hospitality Cruise Shipboard Property Management System installation to support your PCI DSS compliance efforts.

Revision History

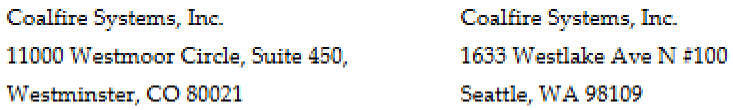
Table 1 Revision History

Date	Description of Change
September 2021	Initial publication.
March 2022	Made minor grammatical changes.
October 2022	Updated the document with correct format.
December 2023	Updated new customer portal.

This PA-DSS Implementation Guide is reviewed and updated on a yearly basis, when there are changes to the underlying application, or when there are changes to PA-DSS requirements. Go to the Hospitality documentation page at the Oracle Help Center at http://docs.oracle.com/en/industries/hospitality/cruise.html to view or download the current version of this guide, and see the Shipboard Property Management System Release Notes and this guide's Revision History to learn what has been updated or changed. In order to ensure your PCI DSS is compliance, subscribe to receive Oracle Security Alerts email by clicking the Critical Patch Updates link on the Oracle Technology Network at http://www.oracle.com/technetwork/index.html. This provides timely information on any possible updates to the PA-DSS Implementation Guide that you need to know about in order to continue to using SPMS in a PCI DSS compliant manner.

1 Executive Summary

Oracle Hospitality Cruise SPMS 20.x has been Payment Application - Data Security Standard (PA-DSS) validated, in accordance with PA-DSS Version 3.2. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):



Coalfire Systems, Inc.
11000 Westmoor Circle, Suite 450,
Westminster, CO 80021

Coalfire Systems, Inc.
1633 Westlake Ave N #100
Seattle, WA 98109

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document also provides specific installation, configuration, and ongoing management best practices for using Oracle Hospitality Cruise SPMS only, Oracle Hospitality Cruise Shipboard Property Management System Version 20.x as a PA-DSS validated application operating in a PCI DSS compliant environment.

PCI Security Standards Council Reference Documents

The following documents provides additional details surrounding the PCI SSC and related security programs:

- Payment Card Industry Payment Applications — Data Security Standard (PCI PA-DSS)

  https://www.pcisecuritystandards.org/security_standards/index.php
- Payment Card Industry Data Security Standard (PCI DSS)

  https://www.pcisecuritystandards.org/security_standards/index.php
- Open Web Application Security Project (OWASP)

  http://www.owasp.org
- Center for Internet Security (CIS) Benchmarks (used for OS Hardening)

  https://benchmarks.cisecurity.org/downloads/multiform/

Payment Application Summary

Table 1-1 Payment Application Summary

<table>
<tr><th>Payment Application Name</th><th>Oracle Hospitality Cruise SPMS</th><th>Payment Application Version</th><th>20.x</th></tr>
<tr><td><b>Payment Application Description</b></td><td colspan="3">Oracle Hospitality Cruise SPMS is a Cruise Property Management System that enables registration of the Guest/Crew payment type to its account. One of its supported payment types is by credit/debit card. To identify the type of Credit Card payment, you must read the card using a supported card swipe device that recognizes the card type from the Primary Account Number (PAN) number, or the information can be obtained directly from the card authorization processing system (EMV) when integrated with a third-party authorization system to provide batch authorization and settlement.</td></tr>
<tr><td><b>Typical Role of the Payment Application</b></td><td colspan="3">Oracle Hospitality Cruise SPMS is a payment application used on a cruise ship for processing credit card transactions and handling authorization and settlement. The authorization and settlement are sent to the merchant for processing using an online or a batch file format through a secured communication.</td></tr>
<tr><td><b>Target Market for Payment Application (check all that apply)</b></td><td colspan="3">□ Retail □ Processors □ Gas/Oil
□ e-Commerce □ Small/medium merchants
<b>X</b> Others (please specify): Hospitality Cruise</td></tr>
<tr><td><b>Stored Cardholder Data</b></td><td colspan="3">The following is a brief description of the files and tables that stores the cardholder data.
<table>
<tr><td>File or Table Name</td><td>Description of Stored Cardholder Data</td></tr>
<tr><td>CRD
CCA
CCT
POS
Authorization file
Settlement file</td><td>The following Cardholder Data is stored
• Full PAN capture include track 1 + track 2 (Track 1 + Track 2 can be disabled by parameter)
• Full PAN shows on screen
• Full PAN will be encrypted before saving into database</td></tr>
</table>
Individual access to cardholder data is logged as follows:
1. Every Card Registration is logged in the LOG Table under activity “GETCRD”.
2. Whenever there is any modification on the card transactions. It is logged in the LOG table.
3. Any access or modification to these tables throught the application is logged by the table’s trigger in Oracle 12c database.</td></tr>
<tr><td><b>Components of the Payment Application</b></td><td colspan="3"><b>The following application-vendor-developed components comprise the payment application:</b></td></tr>
</table>

Table 1-1 (Cont.) Payment Application Summary

Payment Application Name	Oracle Hospitality Cruise SPMS	Payment Application Version	20.x
	List all the components of the application suite that could be installed in a typical merchant network environment, and provide a short description of each component's functionality. Examples: • Management.exe – Main SPMS Guest Handling Module that records and manages the guest reservation details, posting, invoice and payment handling. • Quick Check In.exe – A Quick embarkation check-in module that allows capturing of credit card payment data of the guest, as well as an overview of all other guest-related activities. • Crew.exe – Main SPMS Crew Handling Module for Crew details management, posting, invoice and payment handling, as well as an overview of all other crew related activities. • Data Import.exe (flat file import module that allows importing of Guest/Crew data from a flat file including importing of credit card data. • DGS Res Online.exe – This program interacts directly with RES Online at shoreside and writes the data to the database • Credit Card Transfer.exe – Batch Credit Card Generation Interface that generates the Batch Authorization/Settlement file to various provider. • Tools – A program used to upload the PGP key and, change/update the database encryption key. • ADPI – A program used to purge the data/transaction from the database.		
Required Third Party Payment Application Software	**The following are additional third-party payment application components required by the payment application:** Not Applicable		
Supported Database Software	**The following are database management systems supported by the payment application:** The application utilizes Oracle 12c only		
Other Required Third Party Software	**The following are other third-party software components required by the payment application:** Not applicable.		
Supported Operating System(s)	**The following are Operating Systems supported or required by the payment application:** List Operating System(s) and versions/SP's supported. • Windows 10		
Payment Application Authentication	The application uses PBKDF method to apply pseudorandom function and hashes the user password using random SALT along with the hash value stored in the database.		

Table 1-1 (Cont.) Payment Application Summary

Payment Application Name	Oracle Hospitality Cruise SPMS	Payment Application Version	20.x
Payment Application Encryption	Define here the payment application’s encryption methodology, including key management, encryption used, encryption strength, data storage security and others, including encryption, access controls, truncation, and so on. Encryption Method: AES Encryption Method Key: SHA256 Hash Key Management: DEK stored in the database is encrypted using AES256. KEK is stored in the IIS Server local disk file and is protected using DPAPI. The user communicates with the IIS Server using a HTTPS protocol and authenticates with the user login + password before it is allowed to retrieve the KEK. Once the KEK is retrieved, it is stored in the local disk file protected with DPAPI. There is a hash of DEK store in DB, this is used to detect if the key had changed. Once the key changes, it will retrieve the new key from IIS again. Encryption Length: 256bits Padding method: PKCS7 Mode: CBC BlockSize: 128 Note: When the encryption key is due to expire in 14 days, the system prompts a warning to the user to change the encryption key using Tools.		
Supported Payment Application Functionality	□ Automated Fuel Dispenser	□ POS Kiosk	□ Payment Gateway/ Switch
	□ Card-Not-Present	□ POS Specialized	□ Payment Middleware
	□ POS Admin	□ POS Suite/ General	□ Payment Module
	□ POS Face-to-Face/POI	□ Payment Back Office	□ Shopping Card & Store Front

Table 1-1 (Cont.) Payment Application Summary

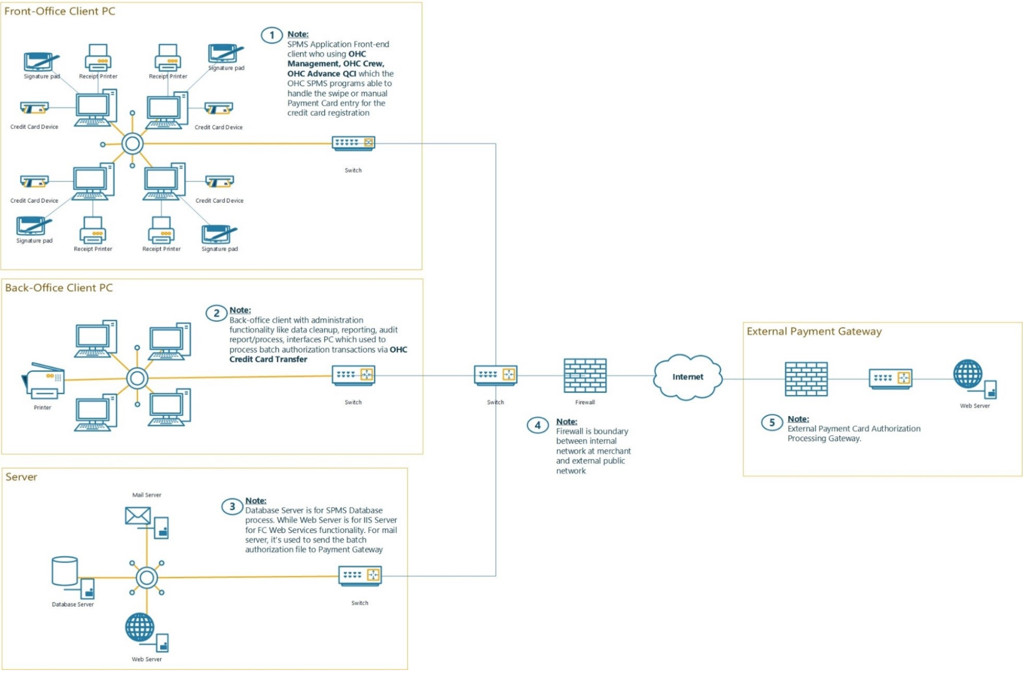
Payment Application Name	Oracle Hospitality Cruise SPMS	Payment Application Version	20.x
Payment Processing Connections	Under online scenario: Initial Authorization is captured during Credit Card registration. The card is inserted into the card reader (normally provided by payment processor). If the authorization is successful, a valid token or reference details with approval code details are returned to SPMS. This token or cc reference will be stored and used for subsequent request of incremental authorization for the same card. The same token/ref is used for settlement at a later stage. Currently supported payment processors are: 1. Servebase/PXP 2. Paypoint 3. Ingenico Under batch authorization scenario: Initial authorizations are generated using the Credit Card Transfer after Credit Card registration. The response authorization file from the merchant is read using the Credit Card Transfer. This response file corresponds to the initial authorization request to approve or decline the transaction. Posting is performed in the Management module. If the posting amount is less than the initial authorization amount, no incremental authorization is required, or else the authorization is generated using the Credit Card Transfer. Once the settlement completes in the Management module, a settlement authorization transaction can be generated using the Credit Card Transfer module. The authorization file is encrypted with PGP encryption. The Authorization File is handled by the user with care to transmit to the merchant accordingly. The response file given by merchant is encrypted with PGP encryption as well. SPMS program will decrypt the response file using the PGP encryption, and insert into SPMS.		

Table 1-1 (Cont.) Payment Application Summary

Payment Application Name	Oracle Hospitality Cruise SPMS	Payment Application Version	20.x
Description of Listing Versioning Methodology	Oracle Hospitality Cruise SPMS versioning follows Oracle versioning methodology. It has four levels, Major, Minor, Patch and Build: <Major>.<Minor>.<Patch> .<Build Number> • Major Version indicates Fiscal Year (Last two digits). For year 2020, Major Version to be 20. • Minor Version indicates Nth of release for this Year. If that is the first release for 2020, minor version will be 1. Minor Version will be represented as wildcard x. Changes at this level will not affect PA-DSS requirements or the security of the application indicated by PA-DSS. • Patch Version only deploy to address production bug fixes. Patch version will be represented as wildcard x. Changes at this level will not affect PA-DSS requirements or the security of the application indicated by PA-DSS. • Build number is changed on every internal compile for testing/ deployment. Every single compile has a unique build number for every version and not customer facing. Based on the above versioning methodology, the application version listed with the PCI SSC is: 20.x		

Typical Network Implementation

Figure 1-1 Typical Network Implementation



Note:
SPMS Application Front-end client who using **OHC Management, OHC Crew, OHC Advance QCI** which the OHC SPMS programs able to handle the swipe or manual Payment Card entry for the credit card registration

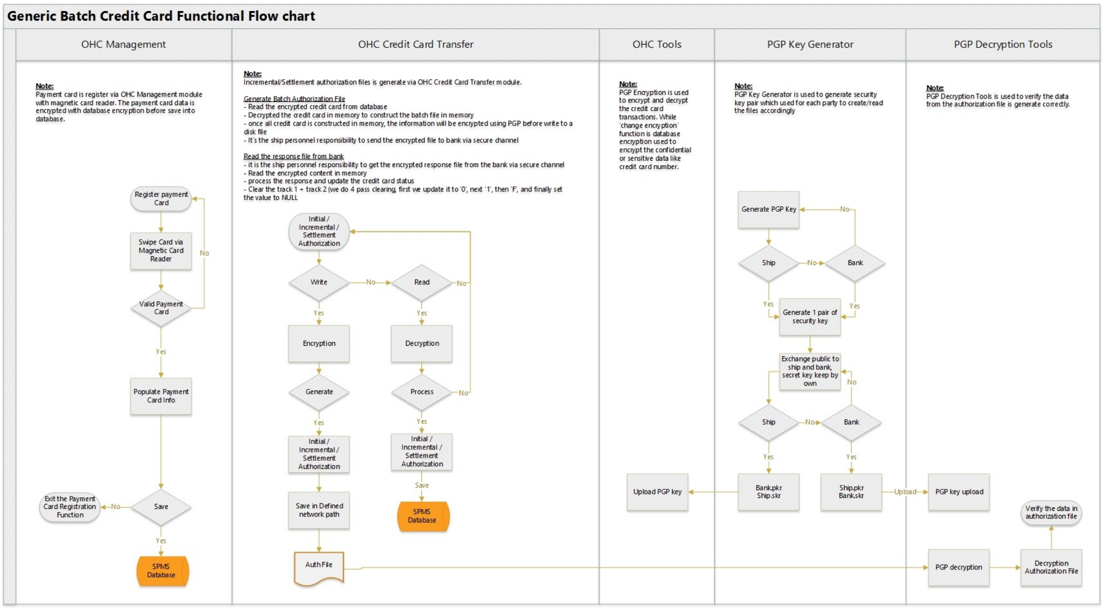
Note:
Back-office client with administration functionality like data cleanup, reporting, audit report/process, interfaces PC which used to process batch authorization transactions via **OHC Credit Card Transfer**

Note:
Database Server is for SPMS Database process. While Web Server is for IIS Server for FC Web Services functionality. For mail server, it's used to send the batch authorization file to Payment Gateway

Note:
Firewall is boundary between internal network at merchant and external public network

Note:
External Payment Card Authorization Processing Gateway.

Figure 1-2   Credit/Debit Cardholder Dataflow Diagram


Generic Batch Credit Card Functional Flow chart
OHC Management
OHC Credit Card Transfer
OHC Tools
PGP Key Generator
PGP Decryption Tools
Register payment Card
Swipe Card via Magnetic Card Reader
No
Valid Payment Card
Yes
Populate Payment Card Info
Save
No
Exit the Payment Card Registration Function
Yes
SPMS Database
Initial / Incremental / Settlement Authorization
Write
No
Read
No
Yes
Yes
Encryption
Decryption
Generate
Process
No
Yes
Yes
Initial / Incremental / Settlement Authorization
Initial / Incremental / Settlement Authorization
Save
SPMS Database
Save in Defined network path
Auth File
Upload PGP key
Generate PGP Key
No
Ship
No
Bank
Yes
Yes
Generate 1 pair of security key
Exchange public to ship and bank, secret key keep by own
No
Ship
No
Bank
Yes
Yes
Bank.pkr Ship.skr
Ship.pkr Bank.skr
Upload
PGP key upload
Verify the data in authorization file
PGP decryption
Decryption Authorization File

Note:
Payment card is register via OHC Management module with magnetic card reader. The payment card data is encrypted with database encryption before save into database.

Note:
Incremental/Settlement authorization files is generate via OHC Credit Card Transfer module.

Generate Batch Authorization File
- Read the encrypted credit card from database
- Decrypted the credit card in memory to construct the batch file in memory
- once all credit card is constructed in memory, the information will be encrypted using PGP before write to a disk file
- It's the ship personnel responsibility to send the encrypted file to bank via secure channel

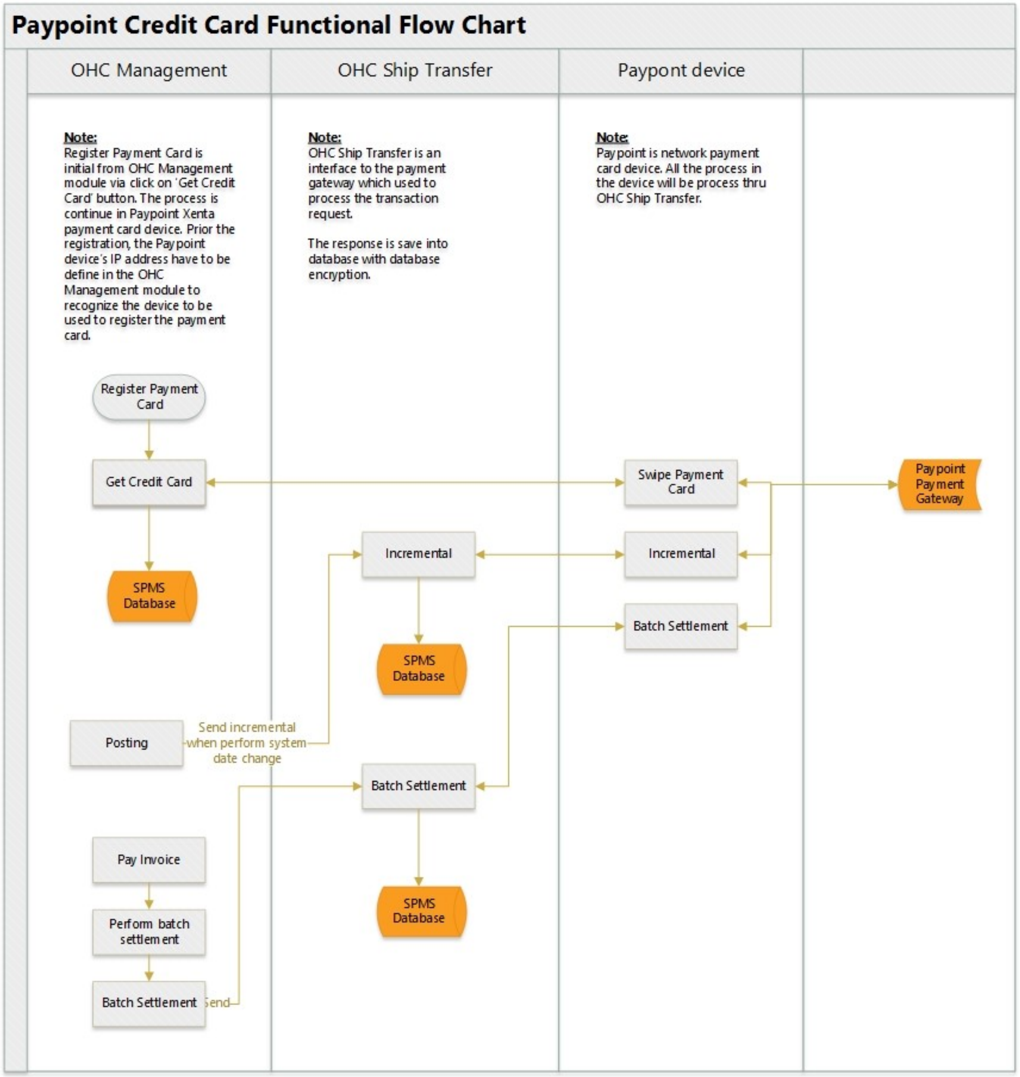
Read the response file from bank
- it is the ship personnel responsibility to get the encrypted response file from the bank via secure channel
- Read the encrypted content in memory
- process the response and update the credit card status
- Clear the track 1 + track 2 (we do 4 pass clearing, first we update it to '0', next '1', then 'F', and finally set the value to NULL

Note:
PGP Encryption is used to encrypt and decrypt the credit card transactions. While 'change encryption' function is database encryption used to encrypt the confidential or sensitive data like credit card number.

Note:
PGP Key Generator is used to generate security key pair which used for each party to create/read the files accordingly

Note:
PGP Decryption Tools is used to verify the data from the authorization file is generate correctly.

Figure 1-3 Paypoint Credit Card Functional Flow Chart



Note:
Register Payment Card is initial from OHC Management module via click on 'Get Credit Card' button. The process is continue in Paypoint Xenta payment card device. Prior the registration, the Paypoint device's IP address have to be define in the OHC Management module to recognize the device to be used to register the payment card.

Note:
OHC Ship Transfer is an interface to the payment gateway which used to process the transaction request.

The response is save into database with database encryption.

Note:
Paypoint is network payment card device. All the process in the device will be process thru OHC Ship Transfer.

Difference between PCI Compliance and PA-DSS Validation

As the software and payment application developer, our responsibility is to be PA-DSS validated. We have tested, assessed, and validated the payment application against PA-DSS Version 3.2 with our independent assessment firm (PAQSA) to ensure that our platform conforms to industry best practices when handling, managing, and storing payment-related information.

The PA-DSS Validation is intended to ensure that Oracle Hospitality Cruise SPMS will help you facilitate and maintain PCI Compliance with respect to how the payment application handles user accounts, passwords, encryption, and other payment data related information.

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process, or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment, which is defined as any network device, host, or application, included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

PCI Compliance is an assessment of your actual server (or hosting) environment called the Cardholder Data Environment (CDE). It is the responsibility of you, as the merchant, and your hosting provider to work together to use PCI compliant architecture with proper hardware and software configurations and access control procedures.

The 12 Requirements of the PCI DSS:

Build and Maintain a Secure Network and Systems

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

   Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

   Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

   Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data

   Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

    Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel

2

Considerations for the Implementation of Payment Application in a PCI-Compliant Environment

The following areas must be considered for proper implementation in a PCI-Compliant environment.

- Remove Historical Sensitive Authentication Data
- Handling of Sensitive Authentication Data
- Secure Deletion of Cardholder Data
- All Primary Account Number (PAN) is masked by default
- Cardholder Data Encryption & Key Management
- Removal of Historical Cryptographic Material

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4)

Sensitive Authentication Data (SAD) includes security-related information, including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks used to authenticate cardholders and/or authorize payment card transactions. See the Glossary of Terms, Abbreviations, and Acronyms in the PCI SSC for the definition of Sensitive Authentication Data

The previous versions of Oracle Hospitality Cruise SPMS stored SAD, including

- 7.30.x

Historical SAD stored by previous versions of Oracle Hospitality Cruise SPMS must be securely deleted and removal is absolutely necessary for PCI DSS compliance. Oracle Hospitality Cruise SPMS includes capabilities to securely delete historical SAD as follows:

When authorization response is received from Credit Card authorization server, the track data is automatically removed by the Credit Card Interface.

Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

Oracle Hospitality Cruise SPMS store SAD. The following guideline must be followed when dealing with SAD used for pre-authorization (swipe data, validation values or codes, PIN or PIN block data):

- Collect SAD only when needed to solve a specific problem
- Store such data only in specific, known locations with limited access
- Collect only the limited amount of data needed to solve a specific problem
- Encrypt such data while stored
- Securely delete such data immediately after use

Oracle Hospitality Cruise SPMS securely deletes Cardholder Data automatically by:

- Removing Track Data automatically when initial Authorization is received from Credit Card provider. (It performs 4 pass clearing, first update it to ALL ‘0’, next all ‘1’, then ‘F’, finally the value set to NULL)
- Authorization/settlement file is encrypted with PGP encryption. The file is handled by the user with care.
- We do not perform memory clearance for cardholder data.

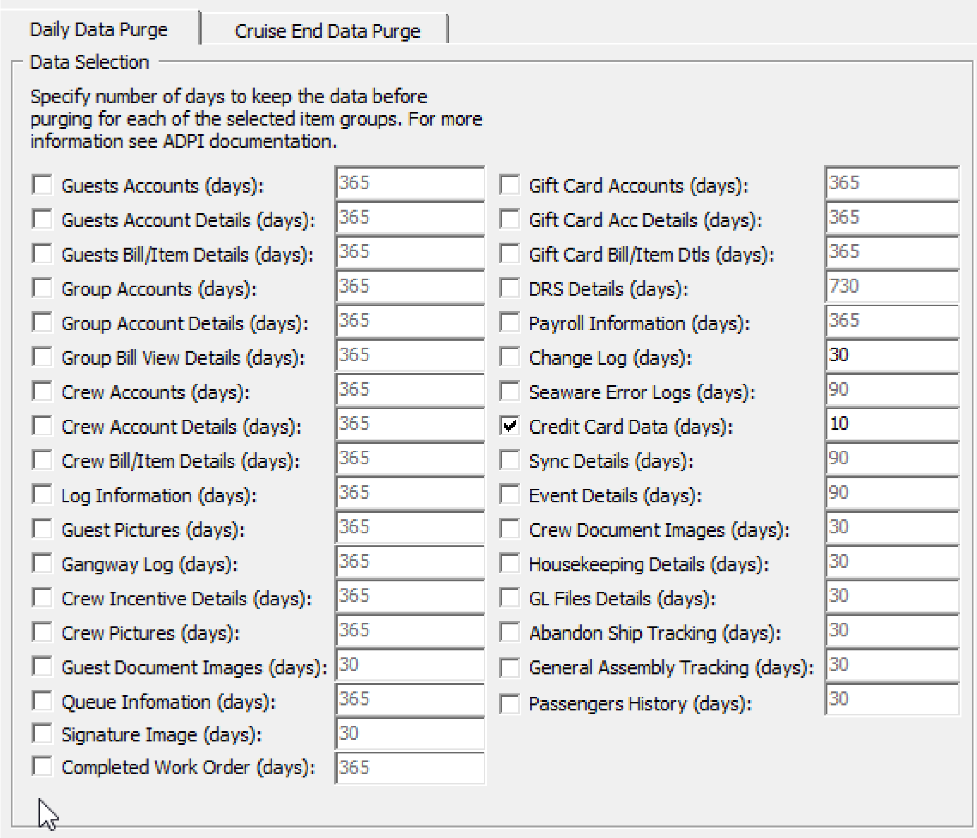
It is against Oracle Hospitality Cruise’s policy to collect any SAD (including any track data, card validation codes or PIN data) or Cardholder Data for any reason. Our troubleshooting processes do not require the collection of SAD or Cardholder Data, nor should it be accepted from a customer.

Secure Deletion of Cardholder Data (PA-DSS 2.1)

The following guidelines must be followed when dealing with Cardholder Data (Primary Account Number (PAN); Cardholder Name; Expiration Date; or Service Code):

- A customer-defined retention period must be defined with a business justification.

Figure 2-1 ADPI Configuration Screen



Data Selection

Specify number of days to keep the data before purging for each of the selected item groups. For more information see ADPI documentation.

☐ Guests Accounts (days):	365	☐ Gift Card Accounts (days):	365
☐ Guests Account Details (days):	365	☐ Gift Card Acc Details (days):	365
☐ Guests Bill/Item Details (days):	365	☐ Gift Card Bill/Item Dtls (days):	365
☐ Group Accounts (days):	365	☐ DRS Details (days):	730
☐ Group Account Details (days):	365	☐ Payroll Information (days):	365
☐ Group Bill View Details (days):	365	☐ Change Log (days):	30
☐ Crew Accounts (days):	365	☐ Seaware Error Logs (days):	90
☐ Crew Account Details (days):	365	☑ Credit Card Data (days):	10
☐ Crew Bill/Item Details (days):	365	☐ Sync Details (days):	90
☐ Log Information (days):	365	☐ Event Details (days):	90
☐ Guest Pictures (days):	365	☐ Crew Document Images (days):	30
☐ Gangway Log (days):	365	☐ Housekeeping Details (days):	30
☐ Crew Incentive Details (days):	365	☐ GL Files Details (days):	30
☐ Crew Pictures (days):	365	☐ Abandon Ship Tracking (days):	30
☐ Guest Document Images (days):	30	☐ General Assembly Tracking (days):	30
☐ Queue Infomation (days):	365	☐ Passengers History (days):	30
☐ Signature Image (days):	30		
☐ Completed Work Order (days):	365		

- Cardholder data exceeding the customer-defined retention period or when no longer required for legal, regulatory, or business purposes must be securely deleted.

- Here are the locations of the cardholder data you must securely delete: SPMS Database Schema, CRD, CCA, CCT, POS table.
- In order to remove the Credit Card related data from the database schema:
  - Select ‘Credit Card Data’ – this option is to remove CRD, CCA, and CCT table’s data.
  - Then, define the business operation justified retention period. After the purge process completes, Data is retained per the duration defined in the application.
- To securely delete Cardholder Data, you must do the following:

  Oracle Hospitality Cruise SPMS securely deletes Cardholder Data by:
  - Removing Track data automatically when initial Authorization is received from Credit Card provider. (It perform 4 pass clearing, first update it to ALL’0’, next all ‘1’, then ‘F’, and finally the record is removed).
  - Authorization/settlement file is encrypted with PGP encryption. The file is handled by the user with care.
  - We do not perform memory clearance for cardholder data.
- All underlying software (this includes operating systems and/or database systems) must be configured to prevent the inadvertent capture of PAN. Instructions for configuring the underlying operating systems and/or databases can be found in Appendix A.

All PAN is Masked by Default (PA-DSS 2.2)

Oracle Hospitality Cruise SPMS masks all PAN by default in all locations that displays PAN (screens, paper receipts, printouts, reports, etc.) by displaying only:

ALL but the last four digits of the PAN numbers is masked.

The payment application displays PAN in the following locations:

- printed receipts — optional
- all generated card reports in the reports menu; these include the following reports: customer invoice report with payment — optional
- all PAN is masked by Default and, the PAN is controlled by access right.

Select wether your application displays full PAN or not and then update based on the functionality of your application. Below are the modules/screen to view the masked PAN.

- Card Entry Screen (Manual and Swipe Entry) — Full PAN is displayed, which uses as verification against the credit card given on registration.
- Invoice Payment Screen — Full PAN/Masked PAN
- Quick Check-In Reservation Screen — Full PAN or Masked PAN
- Pop-up message Guest Reservation Screen — Full PAN
- Credit Card Authorization Screen — Full PAN/Masked PAN
- Credit Card Settlement Screen — Full PAN/Masked PAN
- Passenger Invoices Report (Final Statement Invoice, Detail Statement Invoice)
- User Log File Output — Truncated to show Last four

Oracle Hospitality Cruise SPMS does not have the ability to display full PAN and this is controlled by the user access rights

Cardholder Data Encryption & Key Management (PA-DSS 2.3, 2.4 and 2.5)

Oracle Hospitality Cruise SPMS stores cardholder data and can output PAN data for storage outside of the payment application. All PAN must be rendered unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs. The payment application uses an encryption methodology with statically generated keys to automatically encrypt all locations/methods where cardholder data is stored.

A list of all locations where PAN can be output by the merchant includes:

- Interface Log for debugging purposes — All PAN output is encrypted.

> **Note:**
>
> All PAN output by the merchant, to be stored in the merchant environment must be rendered unreadable using strong cryptographic methods.

The following key management activities must be performed per PCI DSS:

- You must restrict access to encryption keys to the fewest number of custodians necessary.
- You must store encryption keys securely in the fewest possible locations and forms.
- Key custodians must sign the Key Custodian form provided in Appendix A to acknowledge that they understand and accept their key-custodian responsibilities.
- Generation of strong cryptographic keys. The application uses AES 256 bit with SHA hashing.
- Secure cryptographic key distribution. They key is not distributed outside the system.
- DEK is stored in the database and encrypted using AES256.

KEK is stored in an IIS Server local disk file protected using DPAPI. The Client will communicate with the IIS Server using HTTPS and authenticates with a user login + password before it is allowed to retrieve the KEK.

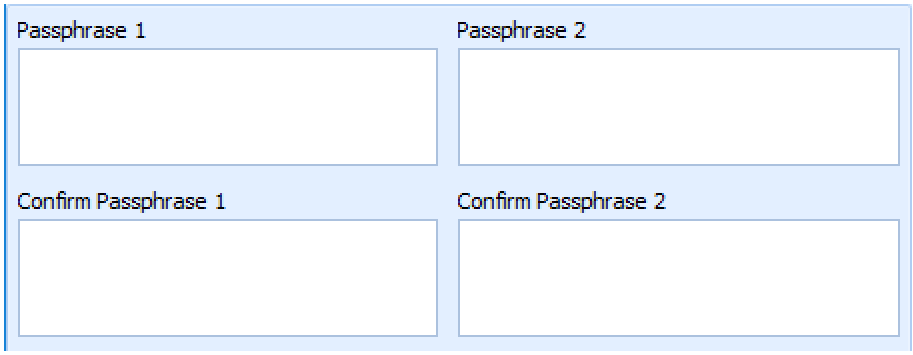
Once the KEK is retrieved, it will store it in a local disk file protected with DPAPI. There is a hash of DEK store in DB: this is used to detect if the key has changed. Once the key is found to have changed, it will retrieve a new key from IIS again.

- Cryptographic key changes for keys that have reached the end of their crypto period.
  - The defined crypto period for each key type is
    - The key will expire after one year and is hard-coded.
  - Oracle Hospitality Cruise SPMS enforces key changes at the end of the defined crypto period by

    - All applications will stop loading when the key is expired, except for the key changed application tool.

- Retire or replace keys when the integrity of the key has been weakened and/or when known or suspected compromise. If retired or replaced cryptographic keys are retained, the application cannot use these keys for encryption operations. The key is destroyed upon change; the application does not keep a history of the key.
- Manual clear-text cryptographic key-management procedures require split knowledge and dual control of keys.
  - The following key types are manual clear-text cryptographic keys: None.
- In order to enforce split knowledge and dual control, the key is split into two entries by two individuals.
  1. One person is to enter first part of the Key in Passphrase 1 and confirm Passphrase 1.
  2. Second person is to enter the key in Passphrase 2 and confirm Passphrase 2.
  3. No one person knows the complete key.

Figure 2-2 Passphrase Input Field



Prevention of unauthorized substitution of cryptographic keys. DEK is protected with KEK using AES256. KEK is protected with DPAPI. Hash of DEK is stored in DB to prevent unauthorized modification.

The following is PGP key management functionality (PGP is an encryption program that provides cryptographic privacy and authentication for data communication).

- The Public and Private PGP key is upload into database through the Oracle Hospitality Cruise SPMS program, and the key is encrypted with AES methodology before being stored in the database.
- The physical Public and Private PGP key is deleted and removed from the local folder and recycling bin once the keys are uploaded into the database.

Removal of Historical Cryptographic Material (PA-DSS 2.6)

Oracle Hospitality Cruise SPMS has the following versions that previously encrypt the cardholder data:

- 7.30x

If the historical Cardholder data is no longer needed, the following must be completed to ensure it is PCI Compliant:

- All cryptographic material for previous versions of the payment application (encryption keys and encrypted cardholder data) must be rendered irretrievable when no longer needed.
- To render historical encryption keys and/or cryptograms irretrievable you must do the following to decrypt and re-encrypt the data with new encryption keys:
  - Oracle Hospitality Cruise SPMS uses previously validated encryption algorithms that are PCI Compliant. Therefore, there is no need to render historical cryptographic keys or cryptograms irretrievable as they are still in use by the payment application.

Set up Strong Access Controls (PA-DSS 3.1 and 3.2)

The PCI DSS requires that access to all systems in the payment processing environment be protected through the use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by more than one user or process.

The following roles and default accounts within the application have administrative access:

- Internal Administrator Account for debugging purpose only

All authentication credentials are generated and managed by the application. Secure authentication is enforced automatically by the payment application for all credentials by the completion of the initial installation and for any subsequent changes (for example, any changes that result in user accounts reverting to default settings, any changes to existing account settings, or changes that generate new accounts or recreate existing accounts). To maintain PCI DSS compliance the following 11 points must be followed per the PCI DSS:

- The payment application must not use or require the use of default administrative accounts for other necessary or required software (for example, database default administrative accounts) (PCI DSS 2.1 / PA-DSS 3.1.1)
- The payment application must enforce the changing of all default application passwords for all accounts that are generated or managed by the application, by the completion of installation and for subsequent changes after the installation (this applies to all accounts, including user accounts, application and service accounts, and accounts used by Oracle Hospitality Cruise SPMS only for support purposes) (PCI DSS 2.1 / PA-DSS 3.1.2)
- The payment application must assign unique IDs for all user accounts. (PCI DSS 8.1.1 / PA-DSS 3.1.3)
- The payment application must provide at least one of the following three methods to authenticate users: (PCI DSS 8.2 / PA-DSS 3.1.4)
  1. Something you know, such as a password or a passphrase.
  2. Something you have, such as a token device or smart card.
  3. Something you are, such as a biometric.
- The payment application must NOT require or use any group, shared, or generic accounts and passwords (PCI DSS 8.5 / PA-DSS 3.1.5)

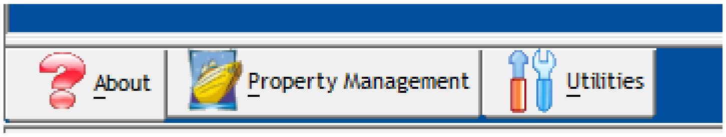
- The payment application requires passwords to be at least seven characters and to include both numeric and alphabetic characters (PCI DSS 8.2.3 / PA-DSS 3.1.6)
- The payment application requires passwords to be changed at least every 90 days (PCI DSS 8.2.4 / PA-DSS 3.1.7)
- The payment application keeps password history and requires that a new password is different from any of the last four passwords used (PCI DSS 8.2.5 / PA-DSS 3.1.8)
- The payment application limits repeated access attempts by locking out the user account after not more than six logon attempts (PCI DSS 8.1.6 / PA-DSS 3.1.9)
- The payment application sets the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (PCI DSS 8.1.7 / PA-DSS 3.1.10)
- The payment application requires the user to re-authenticate to re-activate the session if the application session has been idle for more than 15 minutes. (PCI DSS 8.1.8 / PA-DSS 3.1.11)

PCI Compliant Password in Oracle Hospitality Cruise Shipboard Property Management System

To comply with the PCI Data Security Standard, change your Oracle Hospitality Cruise SPMS's Username and Password.

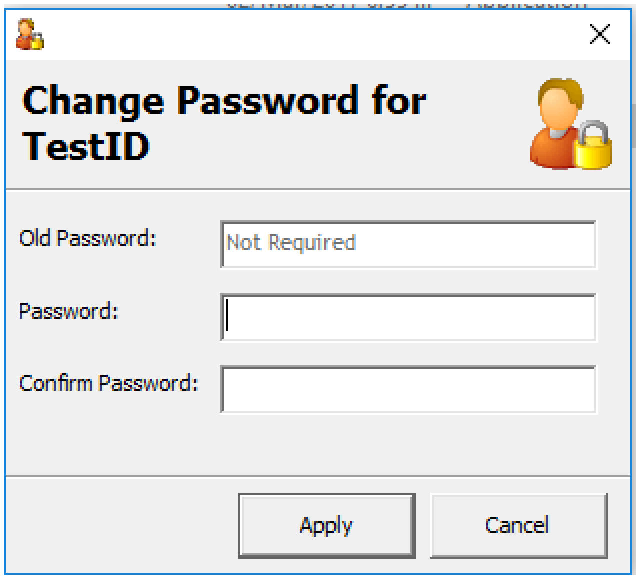
1. Navigate to the **Utilities tab** in the Launch Panel module.

Figure 2-3 Launch Panel Tabs



2. Double-click **User Security** to open the User Security program.
3. Click the **Change Password** to change the user password and then click **Apply**.

Figure 2-4 User Password Change Screen



Change Password for TestID

Old Password: Not Required

Password:

Confirm Password:

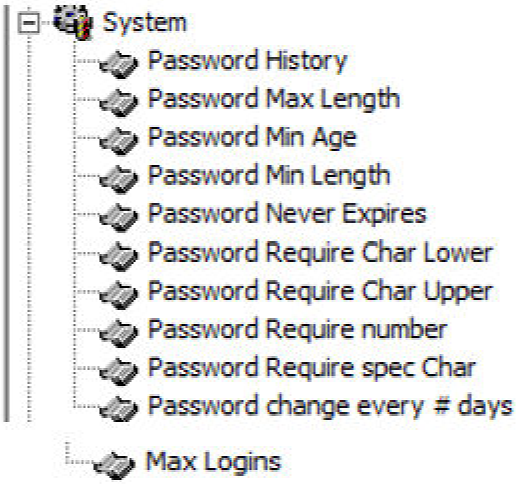
You must assign a strong password to any default accounts (even if they will not be used), and then disable or do not use the accounts.

To ensure strict access control of the Oracle Hospitality Cruise SPMS application, always assign unique usernames and complex passwords to each account. Oracle Hospitality Cruise mandates applying these guidelines to not only program password but to Microsoft Windows operating system passwords as well. Furthermore, Oracle Hospitality Cruise advises users to control access, using unique usernames and PCI-Compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

Creating Secure Password

To comply with PCI Data Security Standard, ensure the following options in the Oracle Hospitality Cruise SPMS program are configured as shown below:

Figure 2-5 Creating Secure Password



- System
  - Password History
  - Password Max Length
  - Password Min Age
  - Password Min Length
  - Password Never Expires
  - Password Require Char Lower
  - Password Require Char Upper
  - Password Require number
  - Password Require spec Char
  - Password change every # days
  - Max Logins

In the Oracle Hospitality Cruise SPMS program, Administrative module, from the main menu, navigate to **Administration, System Setup, Database Parameters**. Ensure these available options are configured per the following:

1. Ensure the Password History is at least four.
2. Ensure the Password Max Length is at least 14 characters.
3. Ensure the Password Min Age is one.
4. Ensure the Password Min Length is at least eight characters.
5. Ensure the Password Never Expires is zero (disabled).
6. Ensure the Password Require Char Lower is at least one character.
7. Ensure the Password Require Char Upper is at least one character.
8. Ensure the Password Require number is at least one number.
9. Ensure the Password Require spec char is at least one character.
10. Ensure the Password change every # days not greater than 90 days.
11. Ensure the Max Login is not greater than six.

Properly Train and Monitor Admin Personnel

It is your responsibility to institute proper personnel management techniques for allowing administrator user access to cardholder data, site data, and so on. You can control whether each individual administrator user can see credit card PAN (or only last four).

In most systems, a security breach is the result of unethical personnel. Pay special attention to whom you entrust your administration site to and who you allow to view full decrypted and unmasked payment information.

Log Settings Must be Compliant (PA-DSS 4.1.b and 4.4b)

4.1.b: Oracle Hospitality Cruise SPMS has PA-DSS compliant logging enabled by default. This logging is not configurable and may not be disabled.

Implement automated assessment trails for all system components to reconstruct the following events:

- 10.2.1 All individual user accesses to cardholder data from the application.
- 10.2.2 All actions taken by any individual with administrative privileges in the application.
- 10.2.3 Access to application audit trails managed by or within the application.
- 10.2.4 Invalid logical access attempts.
- 10.2.5 Use of the application’s identification and authentication mechanisms (including but not limited to creation of new accounts, elevation of privileges, and so on) and all changes, additions, and deletions to application accounts with root or administrative privileges.
- 10.2.6 Initialization, stopping, or pausing of the application audit logs.
- 10.2.7 Creation and deletion of system-level objects within or by the application record at least the following assessment trail entries for all system components for each event from 10.2.x above:

Record at least the following assessment trail entries for all system components for each event from the 10.2.x above:

- 10.3.1 User identification.
- 10.3.2 Type of event.
- 10.3.3 Date and time.
- 10.3.4 Success or failure indication.
- 10.3.5 Origination of event.
- 10.3.6 Identity or name of affected data, system component or resource.

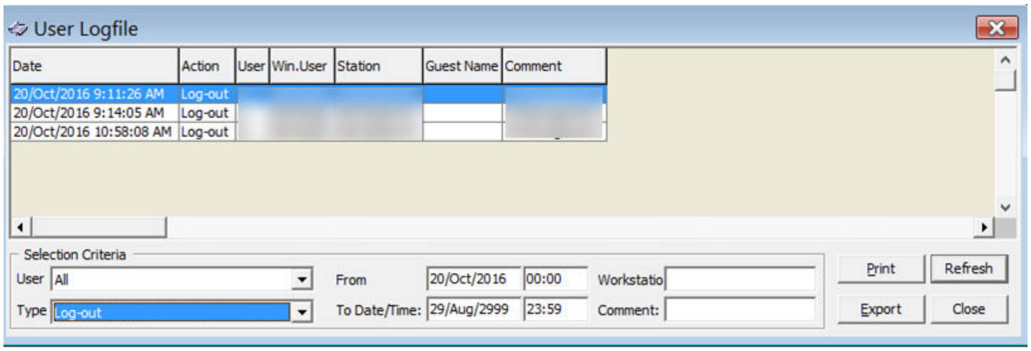
Disabling or subverting the logging function of Oracle Hospitality Cruise SPMS in any way will result in non-compliance with PCI DSS. You can access logs by:

Oracle provides a comprehensive audit trail within SPMS that allows privileged users to track Oracle Hospitality Cruise specific activities. The open database structure allows anyone with system level access to access the database server (Oracle) and system components covered under this requirement, and thus would require logging of user access and activity. Oracle Hospitality Cruise strongly recommends logging of activity on the database server. The log accessibility depends on the user access right.

4.4.b: Oracle Hospitality Cruise SPMS facilitates centralized logging.

The Oracle Hospitality Cruise User Activity Log records a ‘history’ of user activity in the Oracle Hospitality Cruise SPMS database and is accessed using **Security>User Logfile**. This logs data related to credit card registration, authorization, settlement, batch authorization, batch settlement and other transactions. The log file can be exported to support the workstation’s format (for example, if the workstation is installed with Microsoft Office is able to export the file to the Office file format.

Figure 2-6   User Log File Screen



User Logfile

Date	Action	User	Win.User	Station	Guest Name	Comment
20/Oct/2016 9:11:26 AM	Log-out	[redacted]	[redacted]	[redacted]		[redacted]
20/Oct/2016 9:14:05 AM	Log-out	[redacted]	[redacted]	[redacted]		[redacted]
20/Oct/2016 10:58:08 AM	Log-out	[redacted]	[redacted]	[redacted]		[redacted]

Selection Criteria

User All

Type Log-out

From 20/Oct/2016 00:00

To Date/Time: 29/Aug/2999 23:59

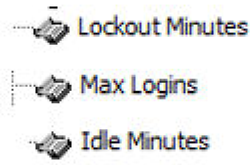
Workstatio

Comment:

Lockout Duration Configuration (PCI DSS 8.1.6 / PA-DSS 3.1.9)

To comply with PCI Data Security Standard, ensure the following options in the Oracle Hospitality Cruise SPMS program are configured as shown below:

Figure 2-7 Lockout Duration



In the Oracle Hospitality Cruise SPMS program, Administrative module, from the main menu, navigate to Administration, System Setup, Database Parameters. Ensure these available options are configured as below:

1. Ensure the Lockout Minutes is 30
2. Ensure the Max Login at 6
3. Ensure the Idle Minutes is 15

Test Data and Accounts: (PA-DSS 5.1.2 & 5.1.3)

Oracle Hospitality Cruise removes all test data and test accounts before the application is released to customers. In addition, all custom payment application accounts, user ID's and passwords are removed before the payment application is released to customers.

During a new/upgrade deployment, installer will run the PL/SQL script to remove all older test data from the database.

3

PCI-Compliant Wireless Settings (PA DSS 6.1.a and 6.2.b)

Oracle Hospitality Cruise SPMS does not support wireless technologies. However, should the merchant implement wireless access within the cardholder data environment, the following guidelines for secure wireless settings must be followed per PCI Data Security Standard 1.2.3, 2.1.1 and 4.1.1:

1.2.3: Perimeter firewalls must be installed between any wireless networks and systems that store cardholder data, and these firewalls must deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

2.1.1: Change wireless vendor defaults per the following 5 points:

1. Encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions.
2. Default SNMP community strings on wireless devices must be changed.
3. Default passwords/passphrases on access points must be changed..
4. Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks.
5. Other security-related wireless vendor defaults, if applicable, must be changed.

4.1.1: Industry best practices (for example, IEEE 802.11i) must be used to implement strong encryption for authentication and transmission of cardholder data.

> **Note:**
>
> The use of WEP as a security control was prohibited as of June 30, 2010.

4

Services and Protocols (PA-DSS 8.2.c)

The application must only use or require the use of necessary and secure e-services, protocols, daemons, and components. PCI requires that you list all required protocols, services and dependent software and hardware that are necessary for any functionality of the payment application, including those provided by third parties.

Oracle Hospitality Cruise SPMS does not require the use of any insecure services or protocols. Here are the services and protocols that Oracle Hospitality Cruise SPMS does require:

TLS1.1/TLS1.2 — Depending on IIS configuration by customer site.

HTTPS — Used in Web Service

Never Store Cardholder Data on Internet-Accessible Systems (PA-DSS 9.1.c)

Never store cardholder data on Internet-accessible systems (for example, the web server and database server must not be on the same server).

PCI-Compliant Remote Access (PA-DSS 10.1)

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment, access should be authenticated using a two-factor authentication mechanism. The means two of the following three authentication methods must be used:

1. Something you know, such as a password or passphrase — user id/password for remote access.
2. Something you have, such as token device or smart card — Token Device.
3. Something you are, such as biometric — Not used.

PCI-Compliant Delivery of Updates (PA-DSS 7.2.3, 10.2.1.a)

- How you communicate the availability of new patches and updates to customers.
- Normally, email notification is sent to the customer.
- Timely development and deployment of patches and updates. Patches are delivered in an average of twice a year.
- Delivery in a secure manner with a known chain-of-trust. Customers are required to download patches themselves from MOS: https://support.oracle.com/
- Delivery in a manner that maintains the integrity of the deliverable MOS.
- Integrity testing of the patch or update by the target system prior to installation: There is a small tool program written to make sure all modules/interfaces are compiled correctly and

no zero (0) size assembly is detected. As a development company, Oracle keeps abreast of the relevant security concerns and vulnerabilities in areas of development and expertise.

Oracle does this by using a Code Scanning Tool such as Fortify, doing code review, and extensive testing by QA team.

Once Oracle identifies a relevant vulnerability, the company works to develop and test a patch that helps protect Oracle Hospitality Cruise SPMS against the specific or new vulnerability. Oracle attempts to publish a patch within 30 days of the identification of the vulnerability and contact vendors and dealers to encourage them to install the patch. Typically, merchants are expected to respond quickly to and install available patches within 30 days.

We do not deliver software and/or updates by way of remote access to customer networks. Instead, software and updates are available by uploading them onto approved Oracle Automatic Release Update.

My Oracle Support employs the following security controls:

- My Oracle Support is an HTTPS extranet website service using Secure Socket Layer (SSL) encryption.
- Your registration on My Oracle Support uses a unique Customer Support Identifier (CSI) linked to your Support contract(s).
- Delivery in a manner that maintains the integrity of the deliverable. When a patch is downloaded from My Oracle Support's Automated Release Updates (ARU) page, the patch's digital signature should be verified. This is a relatively simple manual process. There are several free file integrity validation tools available on the web that can verify the Message Digest 5 (MD5) or Secure Hash Algorithm (SHA-1) checksum for the downloaded patch file. You can use a tool like the Microsoft File Checksum Integrity Verifier, or a similar MD5 and SHA-1 checksum utility. Choose and download the validation tool that you want to use. Once a patch is downloaded, run your file integrity validation tool against it and compare the hash value generated by the validation tool to the hash value that corresponds to the patch on the ARU page. Both hash values should exactly match each other to confirm the file's integrity. Once you have validated the patch file integrity, deploy the patch as soon as possible.

PCI-Compliant Remote Access (PA-DSS 10.3.2.a)

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate),

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited.

If users and hosts within the payment application environment may need to use third-party remote access software such as Remote Desktop (RDP)/Terminal Server and so on to access other hosts within the payment processing environment, special care must be taken.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). For <RDP/Terminal Services> this means using the high encryption setting on the server, and for <PCAnywhere> it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements will apply to these access methods as well.

When requesting support from a vendor, reseller, or integrator, customers are advised to take the following precautions:

- Change default settings (such as usernames and passwords) on remote access software (for example, VNC)
- Allow connections only from specific IP and/or MAC addresses.
- Use strong authentication and complex passwords for logins according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS 8.1, 8.3, and 8.5.8-8.5.15.
- Enable encrypted data transmission according to PA-DSS 12.1 and PCI DSS 4.1.
- Enable account lockouts after a certain number of failed login attempts according to PA-DSS 3.1.8 and PCI DSS 8.5.13.
- Require that remote access takes place over a VPN throught a firewall as opposed to allowing connections directly from the internet.
- Enable logging for auditing purposes.
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

Data Transport Encryption (PA-DSS 11.1.b)

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128-bit encryption strength (either at the transport layer with TLS or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard cardholder data during transmission over public networks (this includes the Internet and the Internet accessible DMZ network segments).

PCI DSS Requirement 4.1: Use strong cryptography and security protocols such as transport layer security (TLS 1.1/TLS 1.2) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in scope of the PCI DSS are:

- The Internet
- Wireless technologies
- Global System for Mobile Communications (GSM)
- General Packet Radio Service (GPRS)

See Credit/Debit Cardholder Dataflow Diagram in Typical Network Implementation for an understanding of the flow of encrypted data associated with Oracle Hospitality Cruise SPMS.

PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2.b)

Oracle Hospitality Cruise SPMS does not allow or facilitate the sending of a Primary Account Number (PAN) from any end user messaging technology (for example, e-mail, instant messaging, and chat).

Non-Console Administration and Multi-Factor Authentication (PA-DSS 12.1,12.2)

Although Oracle Hospitality Cruise SPMS does not support non-console administration and we do not recommend using non-console administration, should you ever choose to do this, you must use SSH, VPN, or TLS 1.1 or higher for encryption of this non-console administrative access along with a multi-factor authentication solution.

Network Segmentation

The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

See the standardized Network diagram for an understanding of the flow of encrypted data associated with Oracle Hospitality Cruise SPMS.

Maintain an Information Security Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self-Assessment Questionnaire.

- Call in outside experts as needed.

Application System Configuration

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

- Microsoft Windows 10 Professional. All latest updates and hot-fixes should be tested and applied.
- 4Gb of RAM minimum, 8GB or higher recommended for Payment Application.
- 128Gb of available hard-disk space.
- TCP/IP network connectivity.
- Oracle 12c. All latest updates and hot-fixes should be tested and applied.

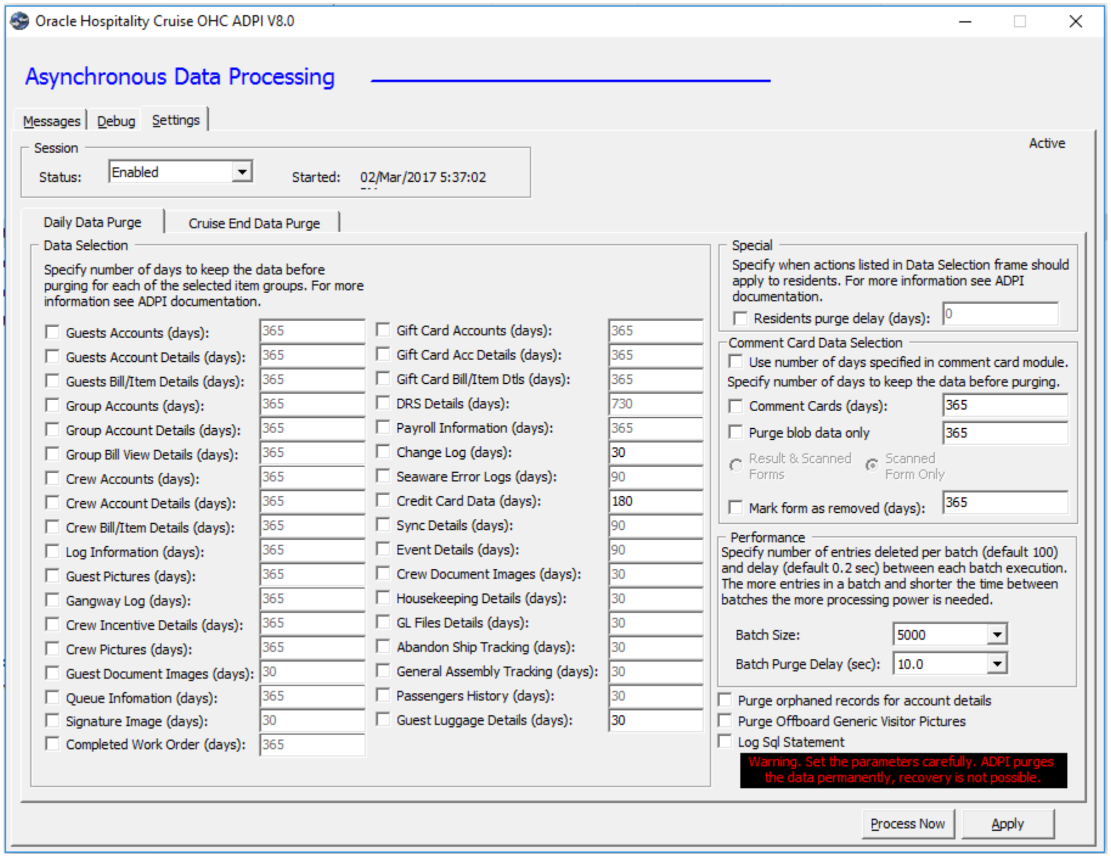
Payment Application Initial Setup & Configuration

Performing Maintenance

We use ADPI tool to pre-select how long historical data are to be kept.

- Credit Card Data is checked default which to compliance with PA-DSS.
- The Credit Card Data purges the orphaned credit card data, authorization and settlement that were entered a specific number of days ago.

Figure 4-1 ADPI Setting Window



Oracle Hospitality Cruise OHC ADPI V8.0

Asynchronous Data Processing

Active

Session

Status: Enabled

Started: 02/Mar/2017 5:37:02

Data Selection

Specify number of days to keep the data before purging for each of the selected item groups. For more information see ADPI documentation.

□ Guests Accounts (days):	365	□ Gift Card Accounts (days):	365
□ Guests Account Details (days):	365	□ Gift Card Acc Details (days):	365
□ Guests Bill/Item Details (days):	365	□ Gift Card Bill/Item Dtls (days):	365
□ Group Accounts (days):	365	□ DRS Details (days):	730
□ Group Account Details (days):	365	□ Payroll Information (days):	365
□ Group Bill View Details (days):	365	□ Change Log (days):	30
□ Crew Accounts (days):	365	□ Seaware Error Logs (days):	90
□ Crew Account Details (days):	365	□ Credit Card Data (days):	180
□ Crew Bill/Item Details (days):	365	□ Sync Details (days):	90
□ Log Information (days):	365	□ Event Details (days):	90
□ Guest Pictures (days):	365	□ Crew Document Images (days):	30
□ Gangway Log (days):	365	□ Housekeeping Details (days):	30
□ Crew Incentive Details (days):	365	□ GL Files Details (days):	30
□ Crew Pictures (days):	365	□ Abandon Ship Tracking (days):	30
□ Guest Document Images (days):	30	□ General Assembly Tracking (days):	30
□ Queue Infomation (days):	365	□ Passengers History (days):	30
□ Signature Image (days):	30	□ Guest Luggage Details (days):	30
□ Completed Work Order (days):	365		

Special

Specify when actions listed in Data Selection frame should apply to residents. For more information see ADPI documentation.

□ Residents purge delay (days): 0

Comment Card Data Selection

□ Use number of days specified in comment card module.

Specify number of days to keep the data before purging.

□ Comment Cards (days): 365

□ Purge blob data only 365

○ Result & Scanned Forms ● Scanned Form Only

□ Mark form as removed (days): 365

Performance

Specify number of entries deleted per batch (default 100) and delay (default 0.2 sec) between each batch execution. The more entries in a batch and shorter the time between batches the more processing power is needed.

Batch Size: 5000

Batch Purge Delay (sec): 10.0

□ Purge orphaned records for account details

□ Purge Offboard Generic Visitor Pictures

□ Log Sql Statement

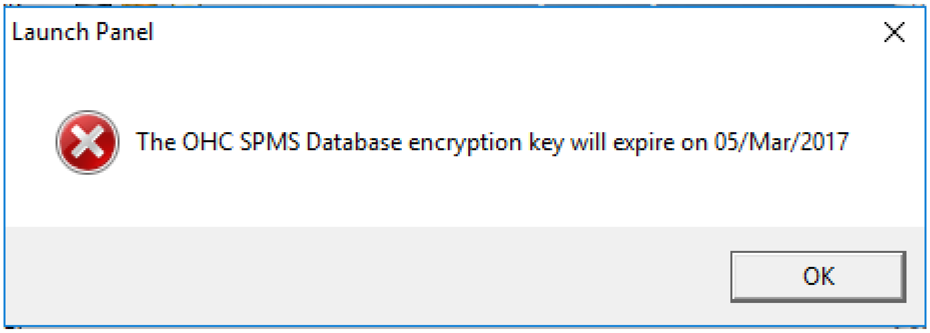
Warning. Set the parameters carefully. ADPI purges the data permanently, recovery is not possible.

1. Start the application **ADPI.exe**.
2. Check on the respective date to be purged.
3. Define the retention duration for the data.
4. Click **Process Now** to purge the selected data.

Updating your Encryption Key on a Periodic Basis

1. When the encryption key is due to expire in 14 days, the system prompts below warning, informing the shipboard user to renew the encryption key.

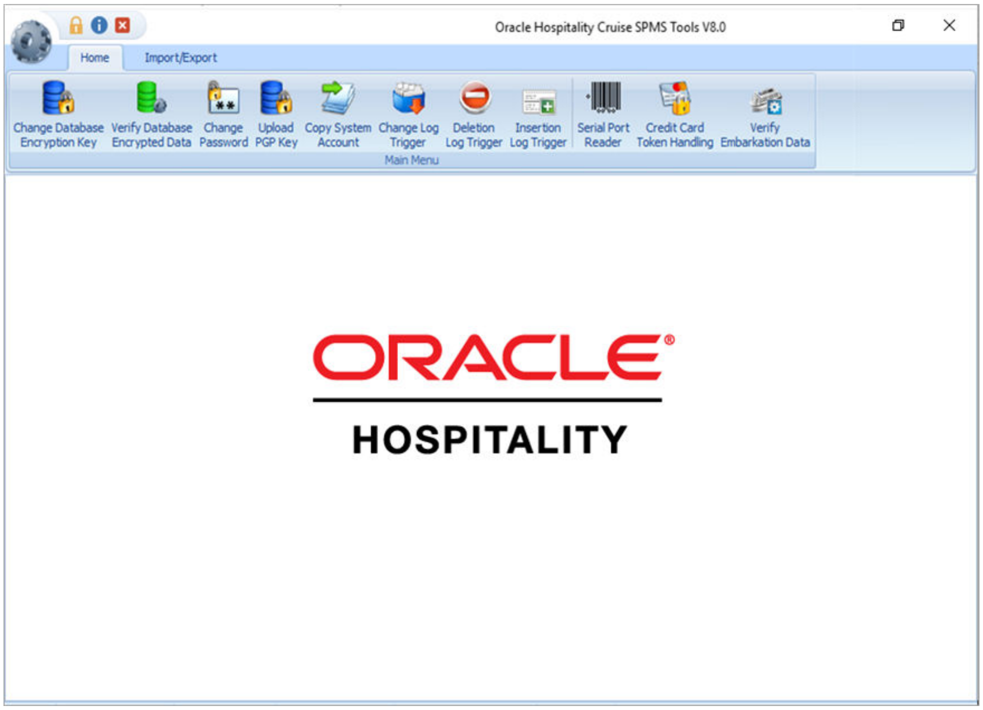
Figure 4-2 Day Encryption Key Expiry Warning



The OHC SPMS Database encryption key will expire on 05/Mar/2017

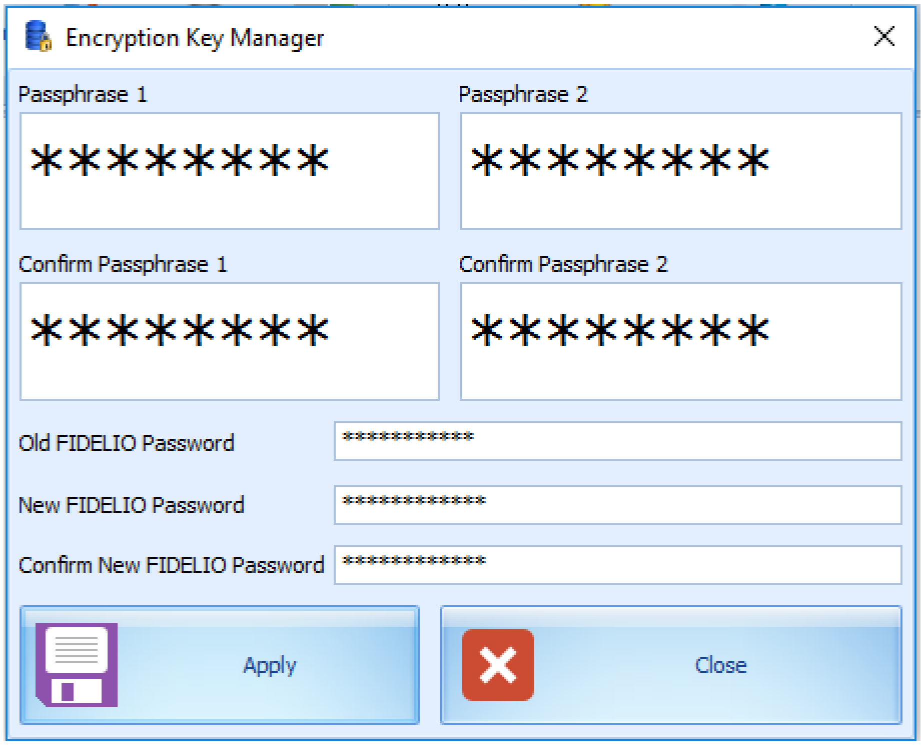
2. Launch the **Tools.exe**.
3. At the login screen, enter your login credentials.
4. After a successful authentication, a user with access to the application will see the main screen as shown in below figure.

Figure 4-3 Tools Main Screen



5. Click the **Change Database Encryption Key**. The Encryption Key Manager screen opens.
6. The key custodians must enter their part of the passphrase in the text boxes labeled **Passphrase 1** and **Passphrase 2**. They must confirm the input and the application will validate the passphrases.
7. Once the passphrase is entered and validated, another login to the database is required. The user needs to know the name of the Oracle connection and have a user ID and a password that grant necessary permissions to the targeted Oracle schema. See Figure 4–4 below.

Figure 4-4 Encryption Key Manager



Encryption Key Manager

Passphrase 1: ********

Passphrase 2: ********

Confirm Passphrase 1: ********

Confirm Passphrase 2: ********

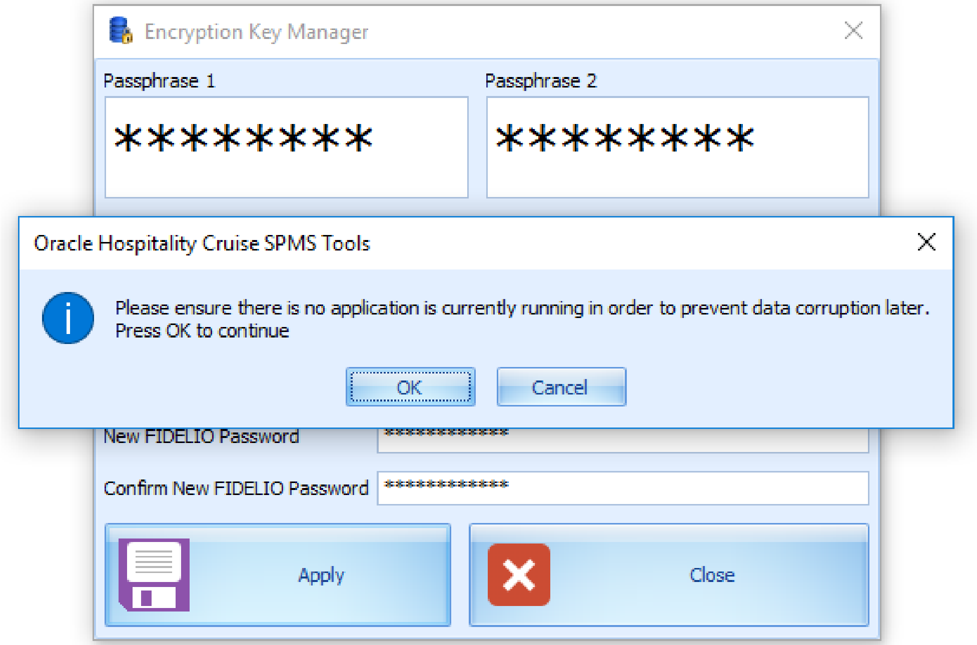
Old FIDELIO Password: ***********

New FIDELIO Password: ************

Confirm New FIDELIO Password: ************

8. Once all information is filled, click **Apply** and the system prompts a reminder window. See Figure 4–5 below.

Figure 4-5 Encryption Key Manager Prompt



Passphrase 1 ********

Passphrase 2 ********

Oracle Hospitality Cruise SPMS Tools

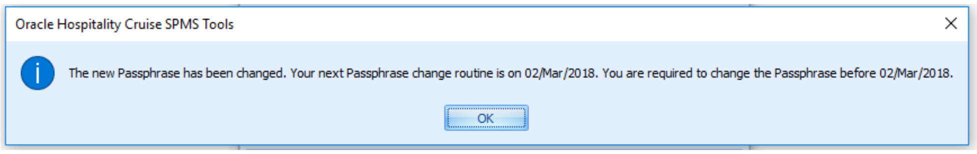
Please ensure there is no application is currently running in order to prevent data corruption later.
Press OK to continue

New FIDELIO Password ************

Confirm New FIDELIO Password ************

9. During the rotation of the keys, all the database infrastructure is in place and the cardholder data information residing in the database will be unencrypted using the soon-to-be replaced DEK (old) and once the new DEK is in place the information will be encrypted using the new DEK. These processes takes place in memory, and the newly encrypted cardholder data is written to the database. The following screen appears once the process completes.

Figure 4-6 Encryption Completes Notification



Oracle Hospitality Cruise SPMS Tools

The new Passphrase has been changed. Your next Passphrase change routine is on 02/Mar/2018. You are required to change the Passphrase before 02/Mar/2018.

5

Appendix A Inadvertent Capture of PAN

The appendix provides instruction for addressing the inadvertent capture of a Primary Account NUmber (PAN) on the following supported operating systems:

- Microsoft Windows 10

Microsoft Windows 10

Disable System Restore

1. Right-click **Computer** and select **Properties**.
2. On the System dialog box, click **Advanced system settings**.
3. On the **System Protection** tab, click **Configure**.
4. Select **Disable system protection**, click **Apply**, and then click **OK** until you return to the System dialog box.
5. Restart the computer.

Encrypt PageFile.sys

1. Your hard disk must be formatted using NTFS to perform this operation.
2. Click the **Start** button and enter **CMD**
3. Right-click **Command Prompt** and select **Run as Administrator**
4. Enter the command: `fsutil behavior set EncryptPagingFile 1`. To disable encryption, enter 0 instead of 1.
5. Enter the command: `fsutil behavior query EncryptPagingFile`. To disable encryption, enter 0 instead of 1.
6. Verify that the command prompt returns: `EncryptPagingFile = 1`

Clear the System PageFile.sys on Shutdown

You can enable the option to clear the PageFile.sys during system shutdown that will purge the temporary data. This is to ensure that information such as system and application passwords and cardholder data is not inadvertently kept in the temporary files. Enabling this feature may increase the time for the system to shutdown.

1. Click the**Start** button and enter **Regedit**.
2. Right-click **Registry Editor** and select **Run as Administrator**.
3. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\`
4. Right-click **ClearPageFileAtShutdown** and select **Modify**. If ClearPageFileAtShutdown does not exist, right-click the Memory Management folder, select **New**, and select **DWORD (32-bit) Value**.
5. Set the **Value data** field to 1 and click **OK**.

Disable System Management of PageFile.sys

1. Right-click on **My Computer** and select **Properties**.
2. On the System dialog box, click **Advanced system settings**.
3. On the **Advanced** tab, Performance section, click **Settings**.
4. On the **Advanced** tab, Virtual memory section, click **Change**.
5. Deselect Automatically manage page file size for all drives, select Custom size, and set the following fields:
   - **Initial Size:** the amount of Random-Access Memory (RAM) available.
   - **Minimum Size:** 2x the amount of RAM.
6. Click **Set** to save the entry.
7. Click **OK** until you return to the System dialog box.
8. Restart the computer.

Disable Error Reporting

1. Navigate to **Control Panel**.
2. Select **Security and Maintenance**
3. Select **Maintenance** and then click **Check for solutions**.
4. Select **Never check for solutions**, then click **OK**.
5. Click the **Start** button and enter **Regedit** in the search field.
6. Right-click Regedit.exe an select **Run as Administrator**.
7. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management`.
8. Right-click **ClearPageFileAtShutdown** and select **Modify**. If **ClearPageFileAtShutdown** does not exist, right-click the `Memory Management` folder, select **New**, then **DWORD (32-bit) Value**.
9. Select the **Value data** field to 1 and click **OK**.