

**Oracle Hospitality Suite8 Property**

**Version: 8.10.1.x**

**PA-DSS 3.2 Implementation Guide**

Date: 07/11/2017

**ORACLE**

## Table of Contents

Notice .....	3
About this Document.....	4
Revision Information.....	5
Executive Summary.....	6
Application Summary .....	7
Typical Network Implementation .....	10
Credit/Debit Cardholder Dataflow Diagram .....	11
Difference between PCI Compliance and PA-DSS Validation.....	13
Considerations for the Implementation of Payment Application in a PCI-Compliant Environment.....	15
Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4) .....	15
Handling of Sensitive Authentication Data (PA-DSS 1.1.5) .....	15
Secure Deletion of Cardholder Data (PA-DSS 2.1) .....	15
All PAN is Masked by Default (PA-DSS 2.2).....	16
Cardholder Data Encryption & Key Management (PA-DSS 2.3, 2.4, and 2.5) .....	17
Removal of Historical Cryptographic Material (PA-DSS 2.6).....	17
Set up Strong Access Controls (3.1 and 3.2) .....	18
Properly Train and Monitor Admin Personnel.....	20
Log settings must be compliant (PA-DSS 4.1.b, 4.4.b) .....	20
PCI-Compliant Wireless settings (PA-DSS 6.1.a and 6.2.b).....	23
Services and Protocols (PA-DSS 8.2.c).....	23
Never store cardholder data on internet-accessible systems (PA-DSS 9.1.c) .....	23
PCI-Compliant Remote Access (10.1) .....	23
PCI-Compliant Delivery of Updates (PA-DSS 10.2.1.a, 7.2.3).....	24
PCI-Compliant Remote Access (10.2.3.a) .....	24
Data Transport Encryption (PA-DSS 11.1.b) .....	24
PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2.b).....	25
Network Segmentation .....	25
Maintain an Information Security Program .....	25
Application System Configuration.....	26
Payment Application Initial Setup & Configuration .....	26
Appendix A: Addressing Inadvertent Capture of PAN .....	27
Addressing Inadvertent Capture of PAN on WINDOWS 7 .....	27
Addressing Inadvertent Capture of PAN on WINDOWS 10 .....	34

## Notice

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

## About this Document

This document describes the steps that must be followed in order for your Oracle Hospitality Suite8 Property 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)<sup>1</sup>.

Oracle instructs and advises its customers to deploy Oracle applications in a manner that adheres to the PCI Data Security Standard (v3.2). Subsequent to this, best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various “Benchmarks”, should be followed in order to enhance system logging, reduce the chance of intrusion and increase the ability to detect intrusion, as well as 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, the disabling of infrequently-used or frequently vulnerable networking protocols and the implementation of certificate-based protocols for access to servers by users and vendors.

**You must follow the steps outlined in this *Implementation Guide* in order for your Oracle Hospitality Suite8 Property installation to support your PCI DSS compliance efforts.**

---

<sup>1</sup> PCI [PA-DSS 3.2](#) can be downloaded from the PCI SSC Document Library.

## Revision Information

Name	Title	Date of Update	Summary of Changes
Marc Watermann	Oracle Hospitality Suite8 Property - PA-DSS Data Security Standard Implementation Guide - Version 8.10.1.X	04/11/2017	Initial Version
Marc Watermann		06/06/2017	Updated
Marc Watermann		07/03/2017	Updated footnote and legal notice

**Note:** This PA-DSS Implementation Guide must be reviewed on a yearly basis, whenever the underlying application changes or whenever the PA-DSS requirements change. Updates should be tracked and reasonable accommodations should be made to distribute or make the updated guide available to users. Oracle will distribute the IG to new customers via the Oracle Help Center. Go to the Hospitality documentation page on the Oracle Help Center at <http://docs.oracle.com> to view or download the current version of this guide, and refer to the Oracle Hospitality Suite8 Property Release Notes and this guide's Revision History to learn what has been updated or changed. In order to ensure your PCI DSS compliance, you need to subscribe to receive email Oracle Security Alerts by clicking the Critical Patch Updates link on the Oracle Technology Network at <http://www.oracle.com/technetwork/index.html>. This provides you timely information on any possible updates to the PA-DSS Implementation Guide that you need to know about in order to continue to use Oracle Hospitality Suite8 Property in a PCI DSS compliant manner.

## Executive Summary

Oracle Hospitality Suite8 Property 8.10.1.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 then provides specific installation, configuration, and ongoing management best practices for using Oracle Hospitality Suite8 Property Version 8.10.1.x as a PA-DSS validated Application operating in a PCI DSS compliant environment.

### PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs (PA-DSS, PCI DSS, etc):

- Payment Card Industry Payment Applications - Data Security Standard (PCI PA-DSS)  
[https://www.pcisecuritystandards.org/security\\_standards/index.php](https://www.pcisecuritystandards.org/security_standards/index.php)
- Payment Card Industry Data Security Standard (PCI DSS)  
[https://www.pcisecuritystandards.org/security\\_standards/index.php](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/>

## Application Summary

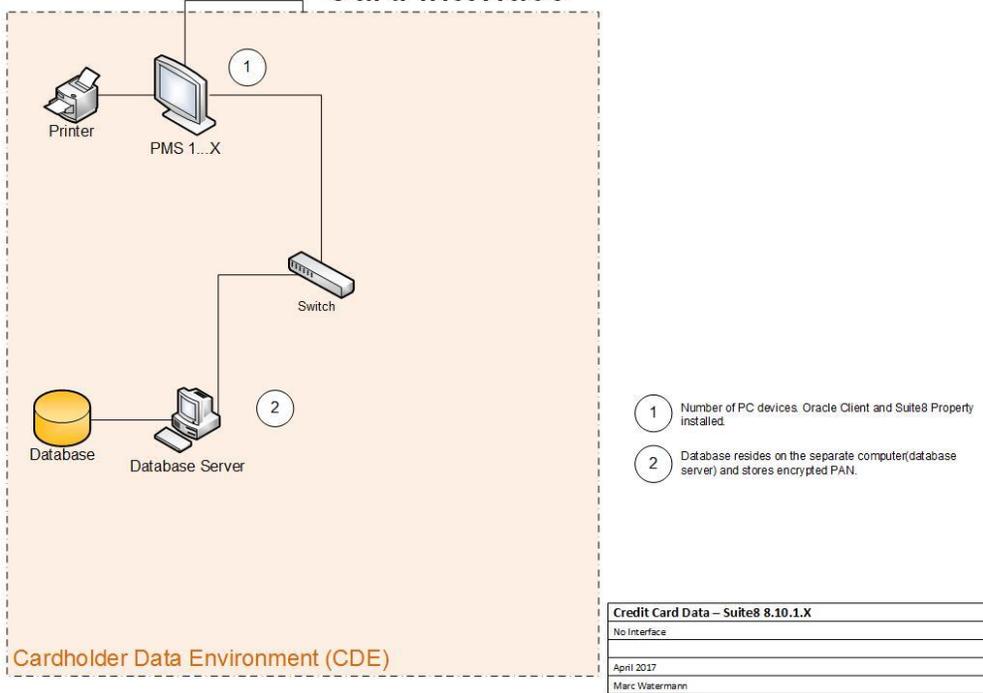
<b>Payment Application Name</b>	Oracle Hospitality Suite8 Property	<b>Payment Application Version</b>	8.10.1.x																
<b>Application Description</b>	Oracle Hospitality Suite8 Property is an on premise installed hotel property management system, which offers to manage guest profiles, guest reservations from check in to check out, conference bookings and more. Oracle Hospitality Suite8 Property needs additional payment providers to process online credit card transactions. Oracle Hospitality Suite8 Property offers individual hotels an economic solution that helps efficiently manage their operations.																		
<b>Typical Role of Application</b>	Oracle Hospitality Suite8 Property function as on premise based solution for hotels to manage guest information, reservations and check out.																		
<b>Target Market for Payment Application</b>	<table border="1"> <thead> <tr> <th colspan="4">Target Market for Payment Application (check all that apply):</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>Retail</td> <td><input type="checkbox"/></td> <td>Processors</td> </tr> <tr> <td><input type="checkbox"/></td> <td>e-Commerce</td> <td><input type="checkbox"/></td> <td>Small/medium merchants</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td colspan="3">Others (please specify): Hospitality Solution</td> </tr> </tbody> </table>			Target Market for Payment Application (check all that apply):				<input type="checkbox"/>	Retail	<input type="checkbox"/>	Processors	<input type="checkbox"/>	e-Commerce	<input type="checkbox"/>	Small/medium merchants	<input checked="" type="checkbox"/>	Others (please specify): Hospitality Solution		
Target Market for Payment Application (check all that apply):																			
<input type="checkbox"/>	Retail	<input type="checkbox"/>	Processors																
<input type="checkbox"/>	e-Commerce	<input type="checkbox"/>	Small/medium merchants																
<input checked="" type="checkbox"/>	Others (please specify): Hospitality Solution																		
<b>Stored Cardholder Data</b>	The following is a brief description of files and tables that store cardholder data:																		
	File or Table Name	Description of Stored Cardholder Data																	
	Database table XCCS	Primary Account Number (PAN) Cardholder Name Expiration Date																	
<b>Components of the Payment Application</b>	<b>Individual access to cardholder data is logged as follows:</b>																		
	In case the user has the right to access clear data the log table is updated i.e. gained access to clear credit card number 'XXXXXXXXXXXXXXXX9999'.																		
<b>Required Third Party Payment Application Software</b>	The following are the application-vendor-developed components which comprise the payment application:																		
	<ul style="list-style-type: none"> <li>Fideliov8.exe: Primary and only PMS application. Manage all functionality.</li> <li>Several additional DLL's used from fideliov8.exe</li> </ul>																		
<b>Database Software Supported</b>	The following are additional third party <u>payment application</u> components required by the payment application:																		
	No 3rd party payment applications are required by the payment application.																		
<b>Database Software Supported</b>	The following are database management systems supported by the payment application:																		
	<ul style="list-style-type: none"> <li>Oracle Database 11.2.0.4</li> <li>Oracle Database 12.1.0.2</li> </ul>																		

<b>Other Required Third Party Software</b>	The following are other required third party software components required by the payment application:																							
	<ul style="list-style-type: none"> <li>• Oracle Database Client 11.2.0.4 or</li> <li>• Oracle Database Client 12.1.0.2 in relation to the used database version</li> <li>• Crystal Reports Runtime 12.2.0 to run Crystal reports</li> </ul>																							
<b>Operating System(s) Supported</b>	The following are Operating Systems supported or required by the payment application:																							
	<p>Latest Supported Versions of:</p> <ul style="list-style-type: none"> <li>• Windows 7 SP1</li> <li>• Windows 10</li> <li>• Windows 2012 Server</li> </ul>																							
<b>Application Authentication</b>	<ul style="list-style-type: none"> <li>• The application using Username/password authentication.</li> <li>• The authentication can be done either using Suite 8 Password Management or external LDAP server</li> <li>• In case Suite8 Password Management is used, only PBKDF2 hash of the password is stored.</li> <li>• Stored passwords are rendered unreadable using a strong, one-way cryptographic algorithm, based on approved standards.</li> <li>• A unique input variable is concatenated with each password before the cryptographic algorithm is applied</li> </ul>																							
<b>Application Encryption</b>	<ul style="list-style-type: none"> <li>• Encryption algorithm use AES256.</li> <li>• Oracle Transparent Data Encryption (Oracle Wallet) used for additional sensitive data protection</li> </ul>																							
<b>Application Functionality Supported</b>	<b>Payment Application Functionality (check only one):</b>																							
	<table border="1"> <tr> <td><input type="checkbox"/></td> <td>Automated Fuel Dispenser</td> <td><input type="checkbox"/></td> <td>POS Kiosk</td> <td><input type="checkbox"/></td> <td>Payment Gateway/Switch</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Card-Not-Present</td> <td><input type="checkbox"/></td> <td>POS Specialized</td> <td><input type="checkbox"/></td> <td>Payment Middleware</td> </tr> <tr> <td><input type="checkbox"/></td> <td>POS Admin</td> <td><input checked="" type="checkbox"/></td> <td>POS Suite/General</td> <td><input type="checkbox"/></td> <td>Payment Module</td> </tr> <tr> <td><input type="checkbox"/></td> <td>POS Face-to-Face/POI</td> <td><input type="checkbox"/></td> <td>Payment Back Office</td> <td><input type="checkbox"/></td> <td>Shopping Cart &amp; Store Front</td> </tr> </table>	<input type="checkbox"/>	Automated Fuel Dispenser	<input type="checkbox"/>	POS Kiosk	<input type="checkbox"/>	Payment Gateway/Switch	<input type="checkbox"/>	Card-Not-Present	<input type="checkbox"/>	POS Specialized	<input type="checkbox"/>	Payment Middleware	<input type="checkbox"/>	POS Admin	<input checked="" type="checkbox"/>	POS Suite/General	<input type="checkbox"/>	Payment Module	<input type="checkbox"/>	POS Face-to-Face/POI	<input type="checkbox"/>	Payment Back Office	<input type="checkbox"/>
<input type="checkbox"/>	Automated Fuel Dispenser	<input type="checkbox"/>	POS Kiosk	<input type="checkbox"/>	Payment Gateway/Switch																			
<input type="checkbox"/>	Card-Not-Present	<input type="checkbox"/>	POS Specialized	<input type="checkbox"/>	Payment Middleware																			
<input type="checkbox"/>	POS Admin	<input checked="" type="checkbox"/>	POS Suite/General	<input type="checkbox"/>	Payment Module																			
<input type="checkbox"/>	POS Face-to-Face/POI	<input type="checkbox"/>	Payment Back Office	<input type="checkbox"/>	Shopping Cart & Store Front																			
<b>Payment Processing Connections:</b>	Oracle Hospitality Suite8 Property does not authorize credit/debit card transaction without external provider.																							
<b>Description of Listing Versioning Methodology</b>	Oracle Hospitality Suite8 Property versioning has three levels, Major, Minor, and Build: 8.<Major>.<Minor>.<Build>																							

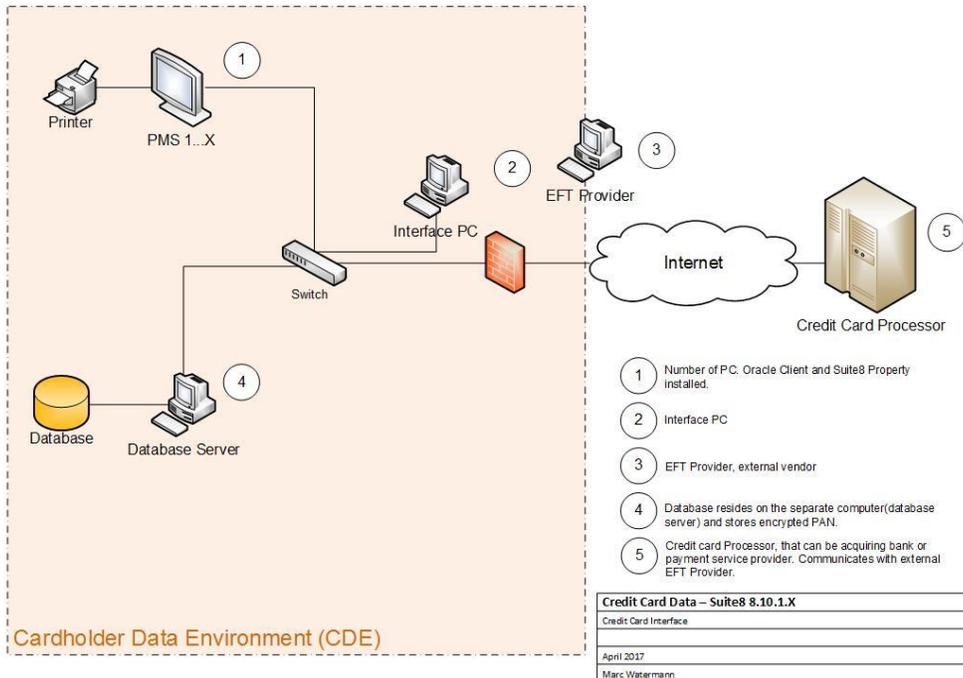
	<ul style="list-style-type: none"><li>• Major changes include significant changes to the application and would have an impact on PA-DSS requirements.</li><li>• Minor changes include small changes such as minor enhancements and may or may not have an impact on PA-DSS requirements.</li><li>• Build changes include bug fixes or rollups and would have no negative impact on PA-DSS requirements and are indicated by the WILDCARD (X).</li></ul> <p>Based on the above versioning methodology the application version being listed with the PCI SSC is: 8.10.1.X</p>
--	---

# Typical Network Implementation

## Suite8 Property Network Diagram without Credit Card Interface



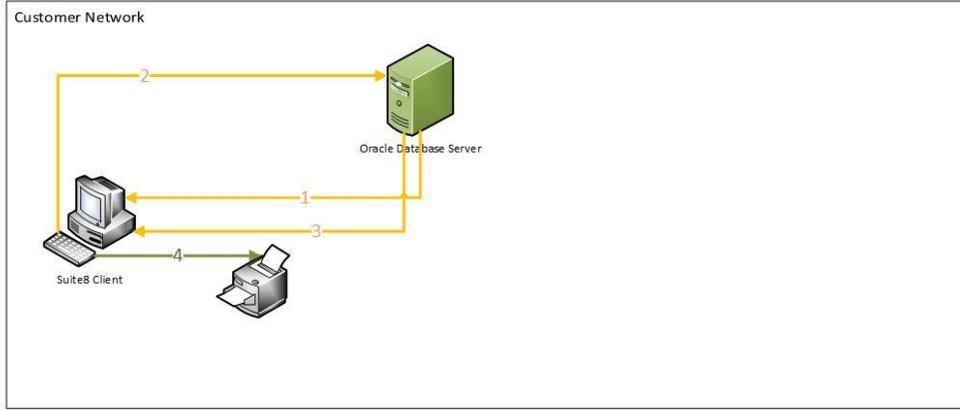
## Suite8 Property Network Diagram with Credit Card Interface



# Credit/Debit Cardholder Dataflow Diagram

## Oracle Hospitality Suite8 Property without CC Interface

Colored line represents the type of data in transit as follows  
 - Green represents data that is not considered Cardholder or Sensitive Authentication data  
 - Red, is up to the Pay-APP  
 - orange can contain card data, which would be encrypted in the PMS

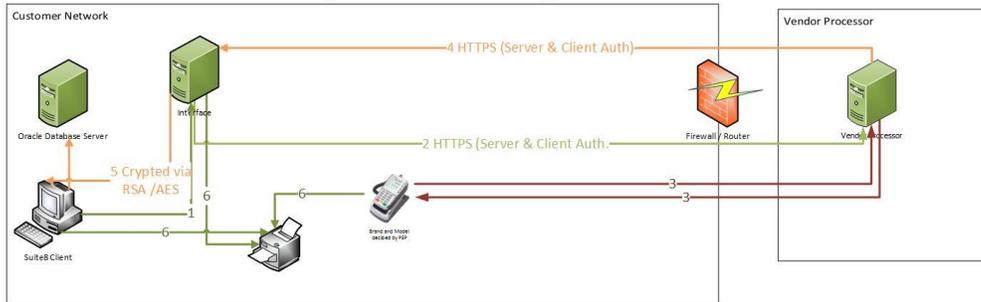


- Interprocess communication
  - Connection details up to PSP Vendor
  - Interprocess communication
1. Suite8 client enter credit card data (PAN, Name and valid until)
  2. Data is stored in the database. Encrypted PAN
  3. Suite8 Client could retrieve credit card data (PAN, Name and valid until)
  4. Suite8 could print

<b>Credit Card Data – Suite8 8.10.1.X</b>
No Interface
April 2017
Marc Watermann

## Oracle Hospitality Suite8 Property chip&pin SixCards HTTPS

Colored line represents the type of data in transit as follows  
 - Green represents data that is not considered Cardholder or Sensitive Authentication data  
 - Red, is up to the Pay-APP  
 - orange can contain card data, which would be encrypted in the PMS

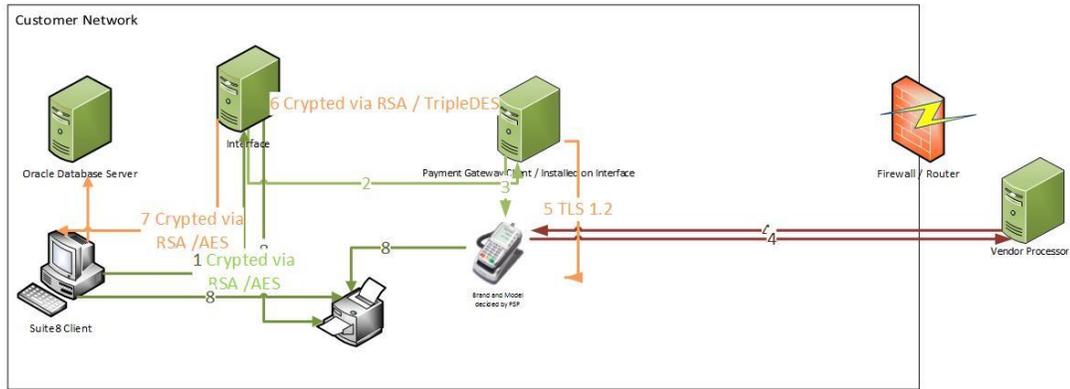


- Interprocess communication
  - Connection details up to PSP Vendor
  - Interprocess communication
1. Suite8 sends only payment request to interface. No card data.
  2. Interface forwards payment request
  3. Vendor will process request including prompting for card and communication with acquirer.
  4. Vendor provides final response to Suite8
  5. Suite8 saves transaction number / auth code received from vendor
  6. Optional. Suite8 / Interface prints CC receipt provided by Vendor, Mask CC data up to vendor

<b>Credit Card Driver Transaction Flow – Suite8 8.10.1.X</b>
1 Chip & Pin –
(SixCards via HTTPS)
April 2017
Marc Watermann

# Oracle Hospitality Suite8 Property chip&pin MPG Lan

Colored line represents the type of data in transit as follows  
 - Green represents data that is not considered Cardholder or Sensitive Authentication data  
 - Red, is up to the Pay-APP  
 - orange can contain card data, which would be encrypted in the PMS



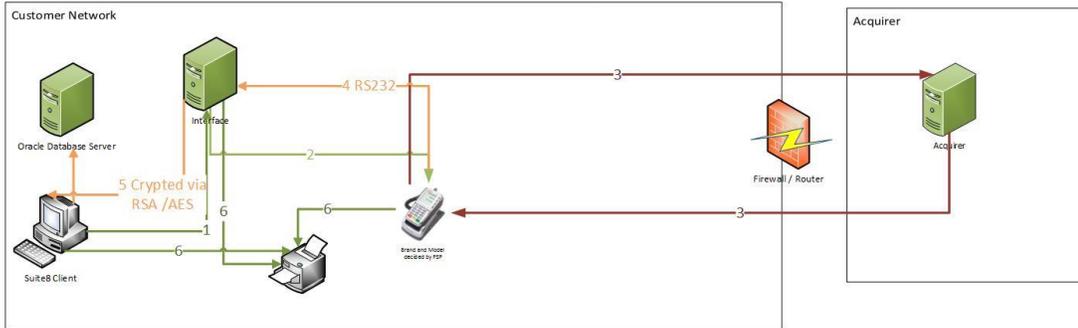
- Interprocess communication
- Connection details up to PSP Vendor
- Interprocess communication

1. Suite8 sends only payment request to interface. No card data.
2. Interface forwards payment request to Payment Gateway Client
3. Payment Gateway Client forward request to Pin Pad via TSL 1.2
4. Vendor will process request including prompting for card and communication with acquirer.
5. Pin Pad send response to Payment Gateway Client via TSL 1.2
6. Payment Gateway Client provides final response to Suite8
7. Suite8 saves transaction number / auth code and perhaps PAN received from vendor
8. Optional. Suite8 / Interface prints CC receipt provided by Vendor, Mask CC data up to vendor

<b>Credit Card Driver Transaction Flow – Suite8 8.10.1.X</b>
1. Chip & Pin –
(Micros Payment Gateway via LAN)
April 2017
Marc Watermann

# Oracle Hospitality Suite8 Property chip&pin NETS Manison SteriaPay

Colored line represents the type of data in transit as follows  
 - Green represents data that is not considered Cardholder or Sensitive Authentication data  
 - Red, is up to the Pay-APP  
 - orange can contain card data, which would be encrypted in the PMS



- Interprocess communication
- Connection details up to PSP Vendor
- Interprocess communication

1. Suite8 sends only payment request to interface. No card data.
2. Interface forwards payment request
3. Vendor will process request including prompting for card and communication with acquirer.
4. Vendor provides final response to Suite8
5. Suite8 saves transaction number / auth code received from vendor
6. Optional. Suite8 prints CC receipt provided by Vendor, Mask CC data up to vendor

<b>Credit Card Driver Transaction Flow – Suite8 8.10.1.X</b>
1. Chip & Pin –
(Manison, NETS, SteriaPAY, ZYT)
April 2017
Marc Watermann

## **Difference between PCI Compliance and PA-DSS Validation**

As a software vendor who develops payment applications, our responsibility is to be “PA-DSS Validated.” We have performed an assessment and payment application validation review with our independent assessment firm (PAQSA), to ensure that our platform does conform to industry best practices when handling, managing and storing payment related information.

PA-DSS Version 3.2 is the standard against which Payment Application has been tested, assessed, and validated.

PCI Compliance is then later obtained by the merchant, and is an assessment of your actual server (or hosting) environment called the Cardholder Data Environment (CDE).

Obtaining “PCI Compliance” is the responsibility of you the merchant and your hosting provider, working together, using PCI compliant architecture with proper hardware & software configurations and access control procedures.

The PA-DSS Validation is intended to ensure that Oracle Hospitality Suite8 Property 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.

### ***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*

## 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 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)

Previous versions of Oracle Hospitality Suite8 Property did not store sensitive authentication data. Therefore, there is no need for secure deletion of this historical data by the application as required by PA-DSS v3.2.

### Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

Oracle Hospitality does not store Sensitive Authentication Data for any reason, and we strongly recommend that you do not do this either. However, if for any reason you should do so, the following guidelines must be followed when dealing with Sensitive Authentication Data used for pre-authorization (swipe data, validation values or codes, PIN or PIN block data):

- Collect sensitive authentication data 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 sensitive authentication data while stored
- Securely delete such data immediately after use

### 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.
- 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:  
Database table XCCS
- To securely delete Cardholder Data you must do the following:
  - Oracle Hospitality Suite8 Property automatically securely deletes Cardholder Data by days defined in the configuration. The database record (XCCS\_NUMBER in the table XCCS) is not deleted for integrity reasons, but the encrypted number

is overwritten with a text-string which notifies the user accordingly should he try to access a deleted number at a later stage. Please do not adjust the default configuration of 10 days.

Setup -> Configuration -> Global Settings -> Interface ->Interface 2



Delete CC data after C/O (days)

- 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**.

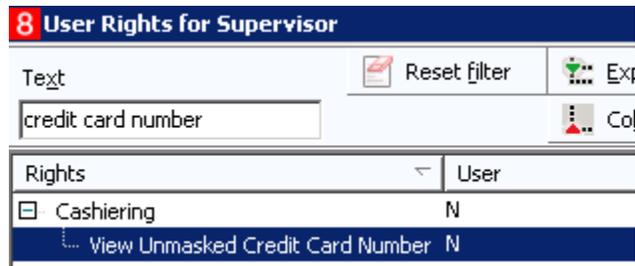
## All PAN is Masked by Default (PA-DSS 2.2)

Oracle Hospitality Suite8 Property masks all PAN by default in all locations that display PAN (screens, paper receipts, printouts, reports, etc. by displaying only the last four digits and the others are masked The payment application displays PAN in the following locations.

- PAN is displayed in Reservation -> Option -> Credit card
- PAN is displayed in Check Out -> Payment
- PAN is displayed in Check Out -> Payment -> Credit Card

Oracle Hospitality Suite8 Property does have the ability to display full PAN for users with legitimate business need. In order to configure the application to display full PAN for only personnel with a legitimate business need you must create a new user group or change an existing user group with the rights to 'View Unmasked Credit Card Number' and assign this user group to the relevant user:

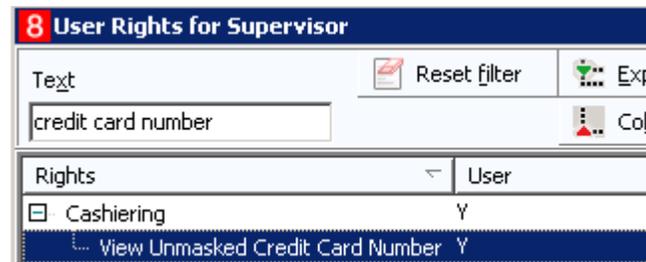
Setup -> Configuration -> Users -> User Group ->



**8 User Rights for Supervisor**

Text

Rights	User
<input type="checkbox"/> Cashiering	N
<input type="checkbox"/> View Unmasked Credit Card Number	N



**8 User Rights for Supervisor**

Text

Rights	User
<input type="checkbox"/> Cashiering	Y
<input type="checkbox"/> View Unmasked Credit Card Number	Y

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

The payment application uses an encryption methodology with dynamically generated keys to automatically encrypt all locations/methods where cardholder data is stored.

The payment application does not output PAN for use or storage in a merchants environment for any reason therefore there are no location or configuration details to provide as required by PA-DSS v3.2.

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.

The following key management functions are performed automatically using AES 256 dynamic encryption key methodology and there are no key custodians or intervention required by customers or resellers/integrators. The full Data-encrypting-key will be calculated during runtime using an additional part of the key which consist of the PBKDF2 mixed entropy and run time parameters. The data stored in the database is secured with Oracle Wallet.

- Generation of strong cryptographic keys.  
The cryptographic keys consists of the Data Encryption Key (DEK) and Initialization Vector (IV).  
The DEK is generated by adding up the Oracle Database ID and a System Generated Random Key (12 characters long).  
The IV is the taken from the Hotel Name.
- Secure cryptographic key storage.  
The Cryptographic Keys are first encrypted using a system generated 'Key encryption Key' (KEK) and then stored in data base, which is protected by Oracle Wallet.
- Cryptographic key changes for keys that have reached the end of their cryptoperiod.  
The cryptographic key handling is currently done in the code itself, the customer has no access to it.
- 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.

## **Removal of Historical Cryptographic Material (PA-DSS 2.6)**

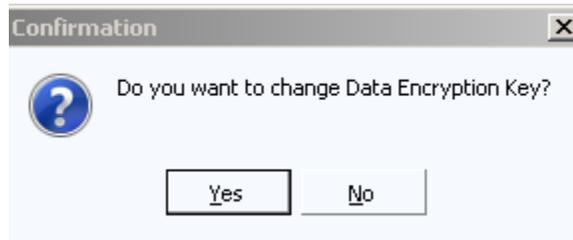
Oracle Hospitality Suite8 Property has the following versions that previously encrypted cardholder data:

- 8.7.X
- 8.8.X
- 8.9.X

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

- 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:

Setup -> Miscellaneous -> System Maintenance-> Cashiering -> Change Credit Card Encryption Key



## Set up Strong Access Controls (3.1 and 3.2)

The PCI DSS requires that access to all systems in the payment processing environment be protected through 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.

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:

1. 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)
2. 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 <<Company\_Name>> for support purposes) (PCI DSS 2.1 / PA-DSS 3.1.2)

3. The payment application must assign unique IDs for all user accounts. (PCI DSS 8.1.1 / PA-DSS 3.1.3)
4. 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)
  - a. Something you know, such as a password or passphrase
  - b. Something you have, such as a token device or smart card
  - c. Something you are, such as a biometric
5. 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)
6. The payment application requires passwords must to be at least 7 characters and includes both numeric and alphabetic characters (PCI DSS 8.2.3 / PA-DSS 3.1.6)
7. The payment application requires passwords to be changed at least every 90 days (PCI DSS 8.2.4 / PA-DSS 3.1.7)
8. The payment application keeps password history and requires that a new password is different than any of the last four passwords used (PCI DSS 8.2.5 / PA-DSS 3.1.8)
9. 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)
10. 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)
11. 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)

To fulfill all mentioned requirements please create for all employee an Oracle Hospitality Suite8 Property user. Do not change the default password expiry days to more than 90 per user:

Password expiry (days)

Before validate and proof the default Oracle Hospitality Suite8 Property settings:

Setup -> Configuration -> Global Settings -> Generic -> Generic3 -> Security

Security	
Auto log off (min)	<input type="text" value="30"/>
Minimum length of password	<input type="text" value="7"/>
<input checked="" type="checkbox"/> Psw must include number	
<input type="checkbox"/> Psw must include uppercase alphabet	
<input type="checkbox"/> Psw must include lowercase alphabet	
<input checked="" type="checkbox"/> Psw must include symbol	
Password history deepness	<input type="text" value="4"/>
Lock out user after # of tries	<input type="text" value="6"/>

- Auto log off (min): 30 (Requirement 10)
- Minimum length of password: 7 or higher (Requirement 6)
- Psw must include number: active (Requirement 6)
- Psw must include symbol: active (Requirement 6)
- Password history deepness: 4 or higher (Requirement 8)
- Lock out user after # of tries: 6 or smaller (Requirement 9)

You must assign strong passwords to any default accounts (even if they won't be used), and then disable or do not use the accounts.

**[Note:** These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to systems with cardholder data, and for access controlled by the application.

The requirements apply to the payment application and all associated tools used to view or access cardholder data.]

**PA-DSS 3.2:** Control access, via unique username and PCI DSS-compliant complex passwords, to any PCs or servers with payment applications and to databases storing cardholder data.

## **Properly Train and Monitor Admin Personnel**

It is your responsibility to institute proper personnel management techniques for allowing admin user access to cardholder data, site data, etc. You can control whether each individual admin user can see credit card PAN (or only last 4).

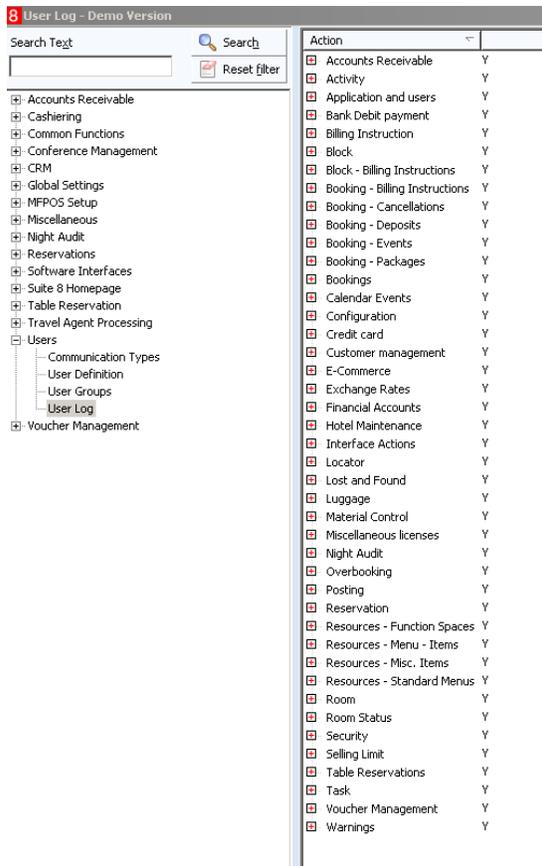
In most systems, a security breach is the result of unethical personnel. So pay special attention to whom you trust into your admin site and who you allow to view full decrypted and unmasked payment information.

## **Log settings must be compliant (PA-DSS 4.1.b, 4.4.b)**

**4.1.b:** Oracle Hospitality Suite8 Property logging is always turned on and cannot be deactivated per PCI DSS 10.2 and 10.3:

Setup -> Configuration -> Users -> User Log

All relevant log are turned on.



The format of the log file is not configurable and stores always the following information:

- User identification
- Type of event
- Date and time
- Action indication
- Origination
- Name and component or resources

**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, etc.) and all changes, additions, 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:**

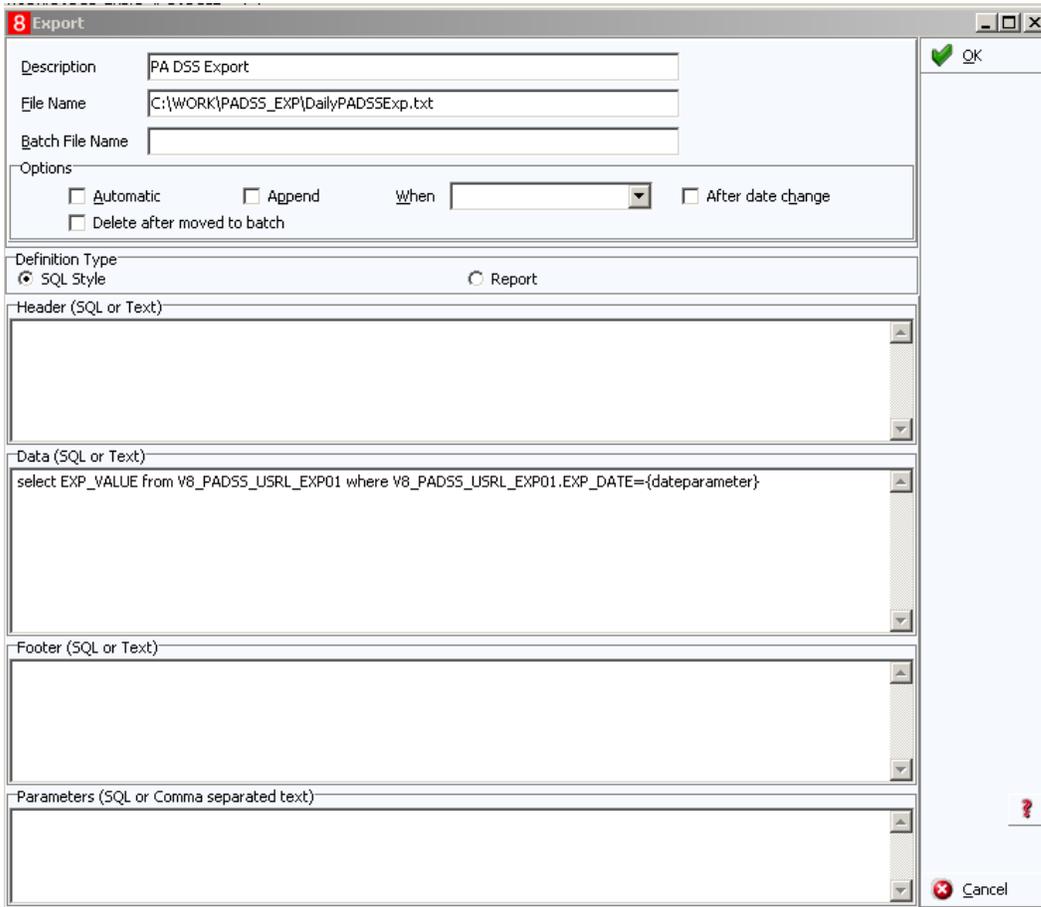
- 10.3.1 User identification
- 10.3.2 Type of event
- 10.3.3 Date and time
- 10.3.4 Success or failure indication
- 10.3.5 Origination of event
- 10.3.6 Identity or name of affected data, system component, or resource.

Disabling or subverting the logging function of Oracle Hospitality Suite8 Property in any way will result in non-compliance with PCI DSS.

**4.4.b:** Oracle Hospitality Suite8 Property facilitates centralized logging.

To use activate the predefined CSV export. Define folder and filename and adjust for your requirements. Activating the option 'Automatic' will export the data on a daily basis.

Miscellaneous → Export



## **PCI-Compliant Wireless settings (PA-DSS 6.1.a and 6.2.b)**

Oracle Hospitality Suite8 Property 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:

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
5. Other security-related wireless vendor defaults, if applicable, must be changed

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.

4.1.1: Industry best practices (for example, IEEE 802.11.i) 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.

## **Services and Protocols (PA-DSS 8.2.c)**

Oracle Hospitality Suite8 Property does not require the use of any insecure services or protocols. Here are the services and protocols that Oracle Hospitality Suite8 Property does require:

TCP / IP connection within local network.

TLS 1.1 or higher to connect to external systems.

## **Never store cardholder data on internet-accessible systems (PA-DSS 9.1.c)**

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

## **PCI-Compliant Remote Access (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:

Something you know, such as a user ID and password combination.

Something you have, such as a RSA token or radius server.

Something you are; this is most often associated with biometrics, such as a finger print scan.

Oracle Hospitality only supports by using Bomgar and WebEx as a connection tool. Connections through VPN or other means are not permitted.

A client needs to acknowledge each and every connection manually by selecting a Bomgar link or WebEx session ID which was provided by the support agent via mail.

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

We do not deliver software and/or updates via remote access to customer networks. Instead, software and updates are available by installation to be performed by an Oracle consultant on site or performed by the customer himself downloading the software and/or updates from the My Oracle Support portal on <https://support.oracle.com/>

### **PCI-Compliant Remote Access (10.2.3.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).

Oracle Hospitality only supports by using Bomgar and WebEx as a connection tool. Connections through VPN or other means are not permitted.

A client needs to acknowledge each and every connection manually by selecting a Bomgar link or WebEx session ID which was provided by the support agent via mail.

### **Data Transport Encryption (PA-DSS 11.1.b)**

Oracle Hospitality Suite8 Property never requires transferring of sensitive cardholder data over public networks. If there ever is a need, then follow these steps.

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 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)

Refer to the Dataflow diagram for an understanding of the flow of encrypted data associated with Oracle Hospitality Suite8 Property.

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

Oracle Hospitality Suite8 Property does not allow or facilitate the sending of PANs via 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 Suite8 Property does not support non-console administration and we do not recommend using non-console administration, should you ever choose to do this, 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.

- ☞ Refer to the standardized Network diagram for an understanding of the flow of encrypted data associated with Oracle Hospitality Suite8 Property.

## **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

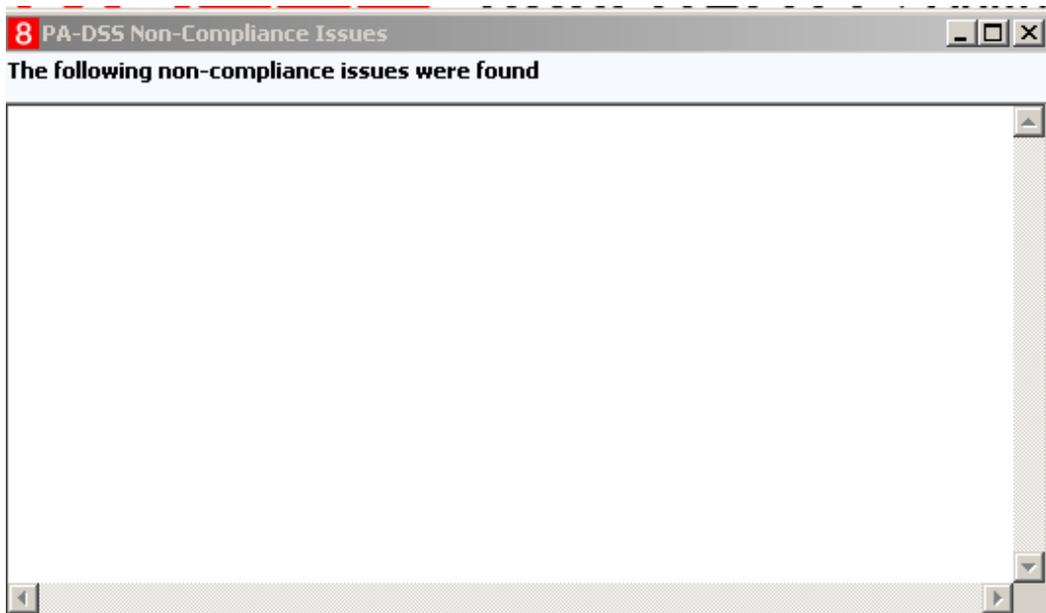
Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

- ✍ Microsoft Windows Server 2012
- ✍ Microsoft Windows Server 2008 R2
- ✍ Microsoft Windows 10
- ✍ Microsoft Windows 7 SP1
- ✍ 512 MB of RAM minimum, 2GB or higher recommended for Payment Application
- ✍ 1000 MB of available hard-disk space
- ✍ TCP/IP network connectivity
- ✍ Oracle Database 11.2.0.4 or Oracle Database 12.1.0.2

## Payment Application Initial Setup & Configuration

Please review the configuration within Oracle Hospitality Suite8 Property to verify the configuration.

Help -> Check PA DSS Compliance



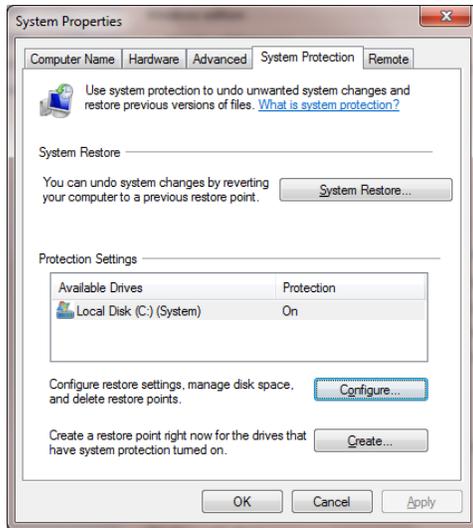
Any non-compliance issues must be resolved.

# Appendix A: Addressing Inadvertent Capture of PAN

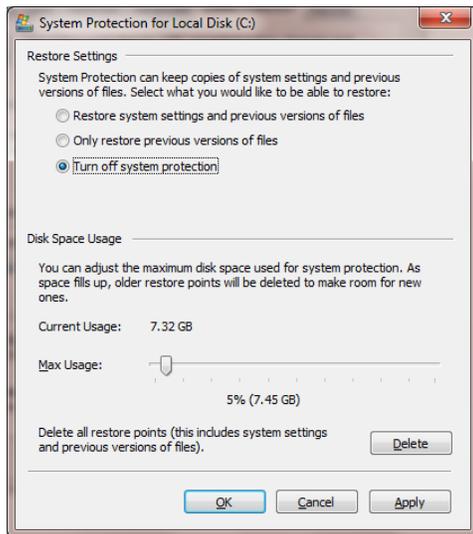
## Addressing Inadvertent Capture of PAN on WINDOWS 7

### Disabling System Restore – Windows 7

- Right Click on Computer > Select “Properties”
- Select “System Protection” on the top left list, the following screen will appear:



- Select Configure, the following screen will appear:

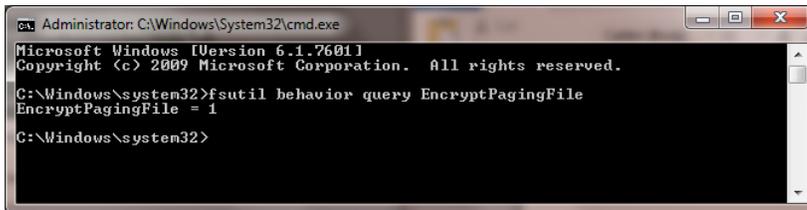


- Select “Turn off system protection”
- Click apply, and OK to shut the System Protection window
- Click OK again to shut the System Properties window
- Reboot the computer

## Encrypting PageFile.sys – Windows 7

\* Please note that in order to perform this operation the hard disk must be formatted using NTFS.

- Click on the Windows “Orb” and in the search box type in “cmd”.
- Right click on cmd.exe and select “Run as Administrator”
- To Encrypt the Pagefile type the following command: fsutil behavior set EncryptPagingFile 1

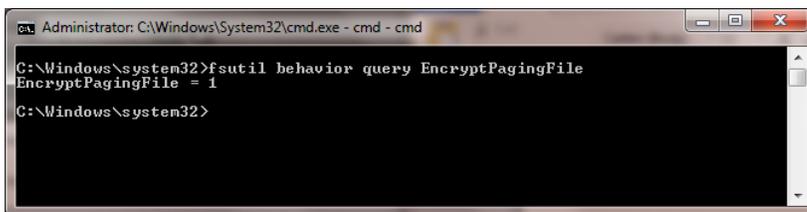


```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 1

C:\Windows\system32>
```

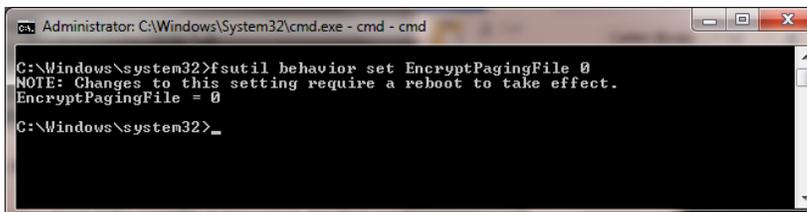
- To verify configuration type the following command: fsutil behavior query EncryptPagingFile



```
Administrator: C:\Windows\System32\cmd.exe - cmd - cmd
C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 1

C:\Windows\system32>
```

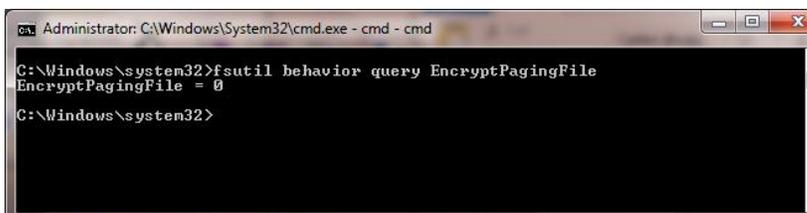
- If encryption is enabled EncryptPagingFile = 1 should appear
- In the event you need to disable PageFile encryption type the following command: fsutil behavior set EncryptPagingFile 0



```
Administrator: C:\Windows\System32\cmd.exe - cmd - cmd
C:\Windows\system32>fsutil behavior set EncryptPagingFile 0
NOTE: Changes to this setting require a reboot to take effect.
EncryptPagingFile = 0

C:\Windows\system32>_
```

- To verify configuration type the following command: fsutil behavior query EncryptPagingFile



```
Administrator: C:\Windows\System32\cmd.exe - cmd - cmd
C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 0

C:\Windows\system32>
```

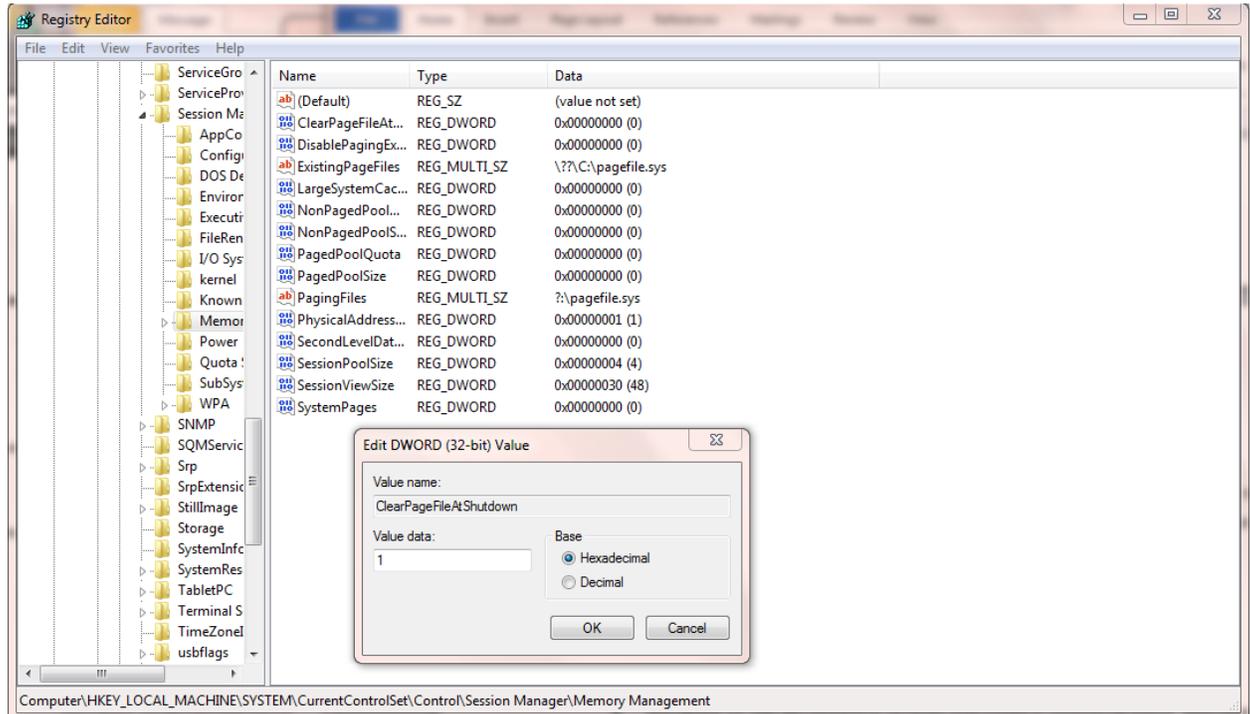
- If encryption is disabled EncryptPagingFile = 0 should appear

## Clear the System Pagefile.sys on shutdown

Windows has the ability to clear the Pagefile.sys upon system shutdown. This will purge all temporary data from the pagefile.sys (temporary data may include system and application passwords, cardholder data (PAN/Track), etc.).

NOTE: Enabling this feature may increase windows shutdown time.

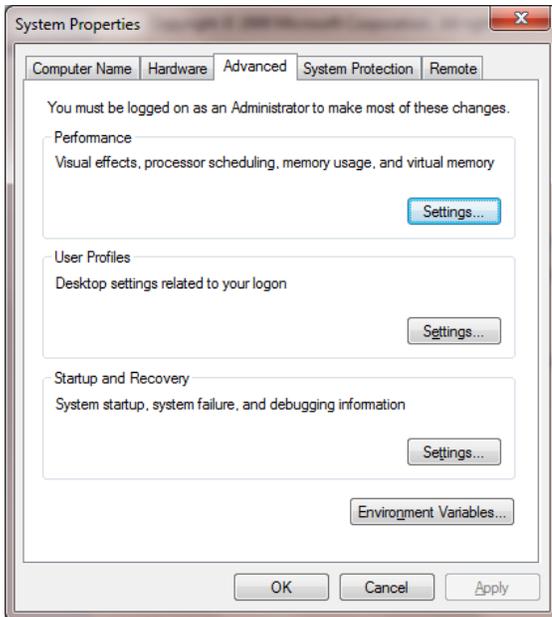
- Click on the Windows “Orb” and in the search box type in “regedit”.
- Right click on regedit.exe and select “Run as Administrator”
- Navigate to HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
- Change the value from 0 to 1
- Click OK and close Regedit



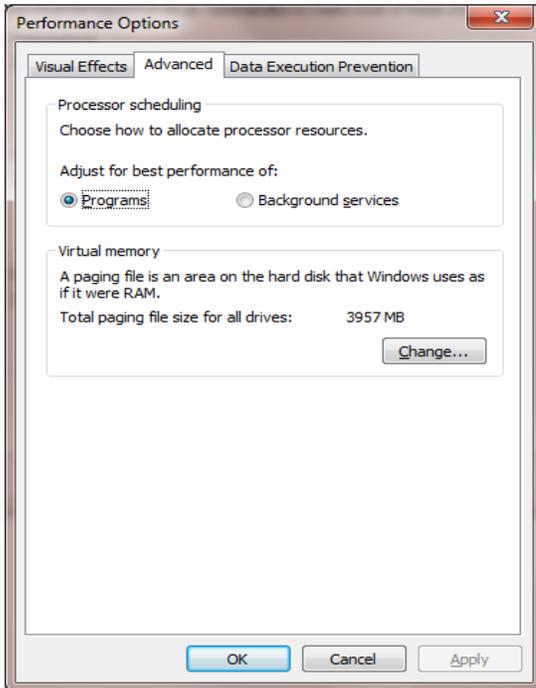
- If the value does not exist, add the following:
  - Value Name: ClearPageFileAtShutdown
  - Value Type: REG\_DWORD
  - Value: 1

## ***Disabling System Management of PageFile.sys – Windows 7***

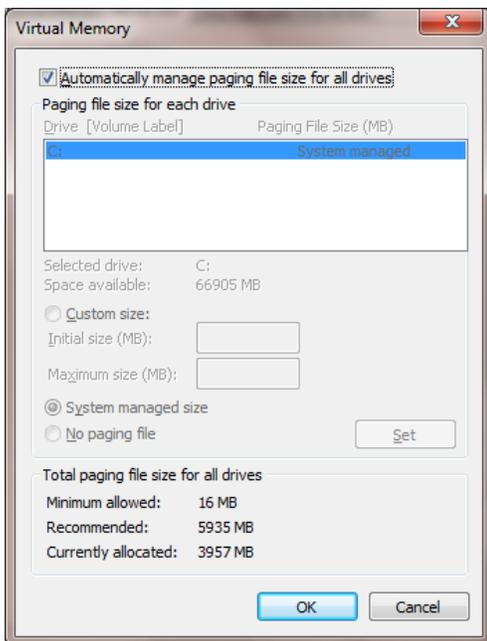
- Right Click on Computer > Select “Properties”
- Select “Advanced System Settings” on the top left list, the following screen will appear:



- Under performance select “Settings” and go to the “Advanced” tab, the following screen will appear:



- Select “Change” under Virtual Memory, the following screen will appear:

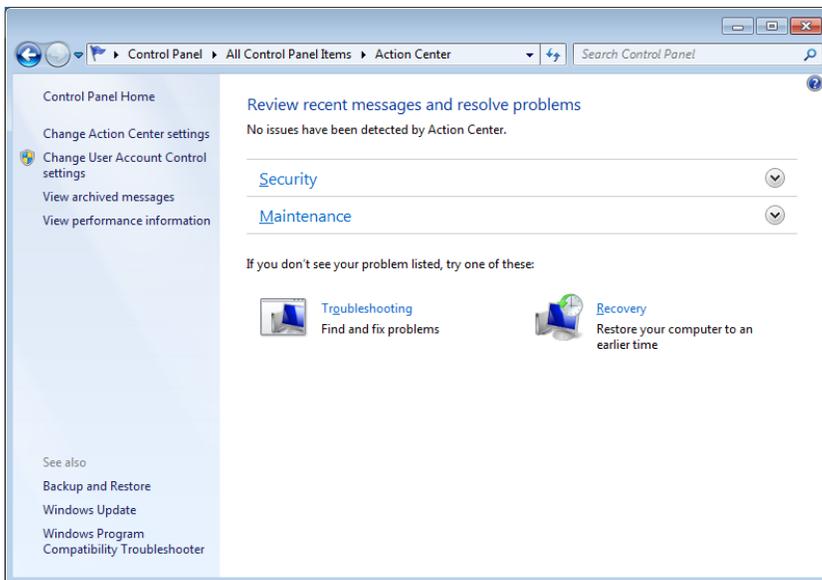


- Uncheck “Automatically manage page file size for all drives”
- Select “Custom Size”
- Enter the following for the size selections:

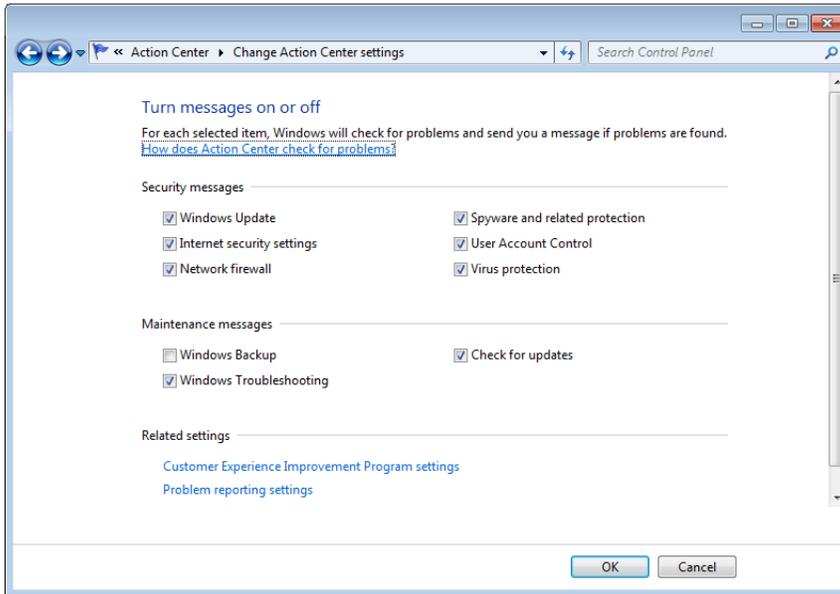
- Initial Size – as a good rule of thumb, the size should be equivalent to the amount of memory in the system.
- Maximum Size – as a good rule of thumb, the size should be equivalent to 2x the amount of memory in the system.
- Click “Ok”, “OK”, and “OK”
- You will be prompted to reboot your computer.

### ***Disabling Windows Error Reporting – Windows 7***

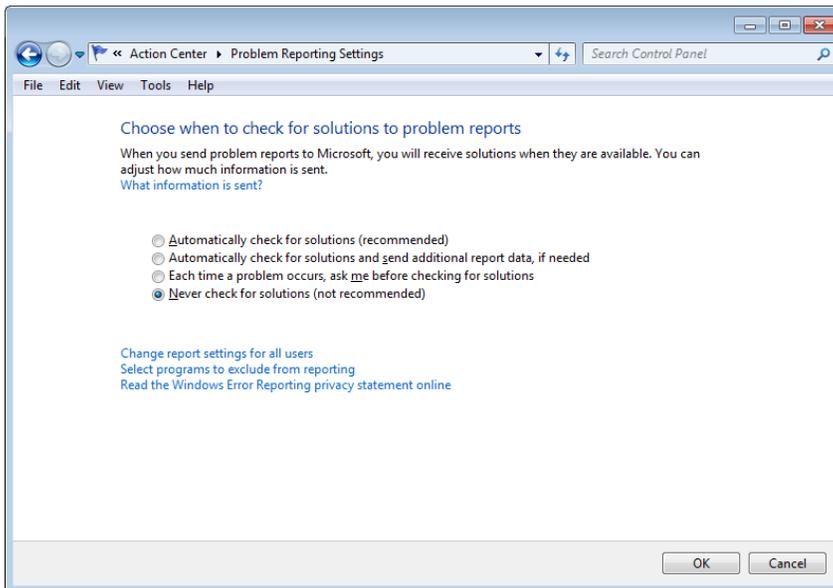
- Open the Control Panel
- Open the Action Center
- Select “Change Action Center Settings”



- Select “Problem Reporting Settings”



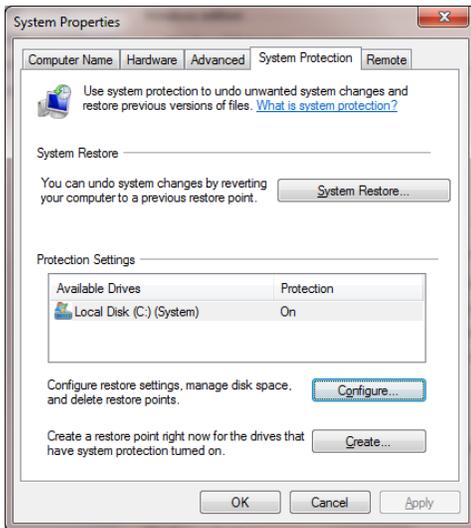
- Select “Never Check for Solutions”



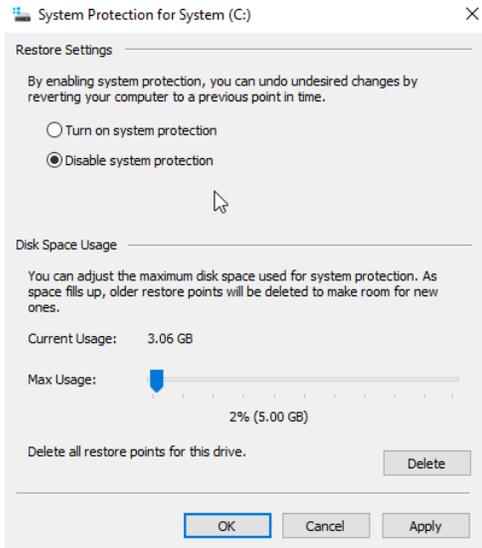
# Addressing Inadvertent Capture of PAN on WINDOWS 10

## Disabling System Restore – Windows 10

- Right Click on Computer > Select “Properties”
- Select “System Protection” on the top left list, the following screen will appear:



- Select Configure, the following screen will appear:

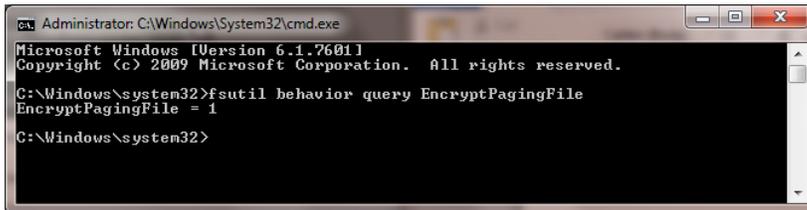


- Select “Disable system protection”
- Click apply, and OK to shut the System Protection window
- Click OK again to shut the System Properties window
- Reboot the computer

## Encrypting PageFile.sys – Windows 7

\* Please note that in order to perform this operation the hard disk must be formatted using NTFS.

- Right Click on the Windows “Orb” and select “Command Prompt (Admin)”.
- To Encrypt the Pagefile type the following command: `fsutil behavior set EncryptPagingFile 1`

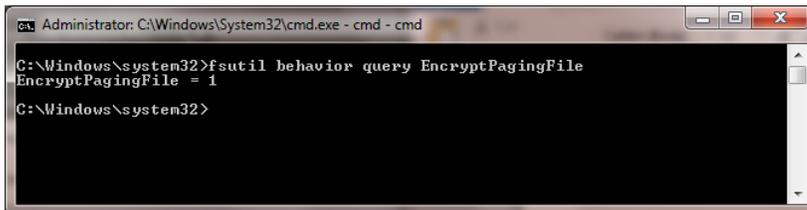


```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 1

C:\Windows\system32>
```

- To verify configuration type the following command: `fsutil behavior query EncryptPagingFile`

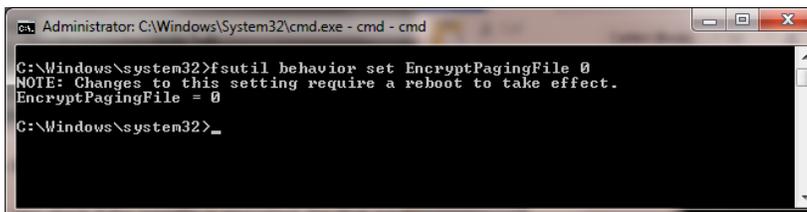


```
Administrator: C:\Windows\System32\cmd.exe - cmd - cmd

C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 1

C:\Windows\system32>
```

- If encryption is enabled `EncryptPagingFile = 1` should appear
- In the event you need to disable PageFile encryption type the following command: `fsutil behavior set EncryptPagingFile 0`

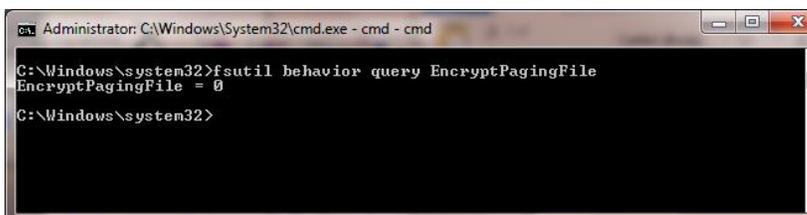


```
Administrator: C:\Windows\System32\cmd.exe - cmd - cmd

C:\Windows\system32>fsutil behavior set EncryptPagingFile 0
NOTE: Changes to this setting require a reboot to take effect.
EncryptPagingFile = 0

C:\Windows\system32>_
```

- To verify configuration type the following command: `fsutil behavior query EncryptPagingFile`



```
Administrator: C:\Windows\System32\cmd.exe - cmd - cmd

C:\Windows\system32>fsutil behavior query EncryptPagingFile
EncryptPagingFile = 0

C:\Windows\system32>
```

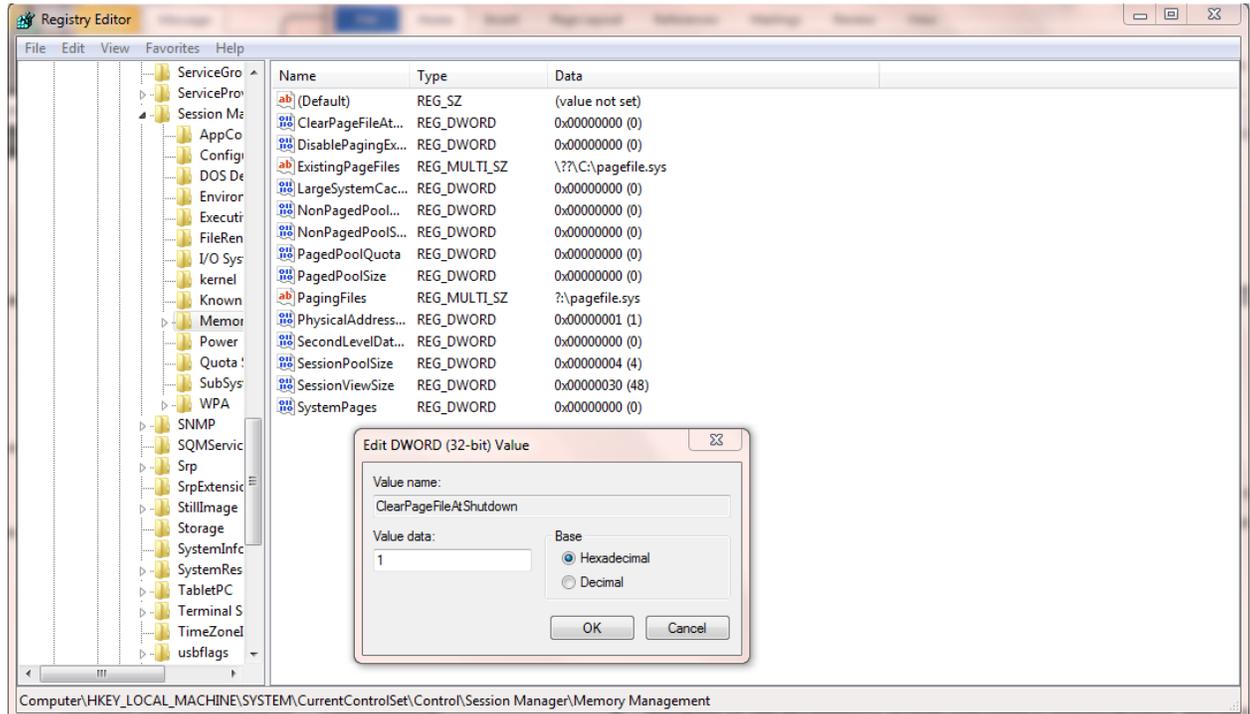
- If encryption is disabled `EncryptPagingFile = 0` should appear

## Clear the System Pagefile.sys on shutdown

Windows has the ability to clear the Pagefile.sys upon system shutdown. This will purge all temporary data from the pagefile.sys (temporary data may include system and application passwords, cardholder data (PAN/Track), etc.).

NOTE: Enabling this feature may increase windows shutdown time.

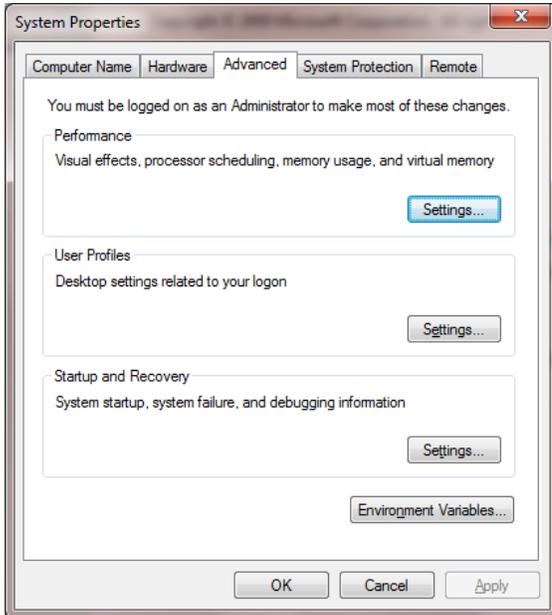
- Click on the Windows “Orb” and type in “regedit”.
- Right click on regedit.exe and select “Run as Administrator”
- Navigate to HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
- Change the value from 0 to 1
- Click OK and close Regedit



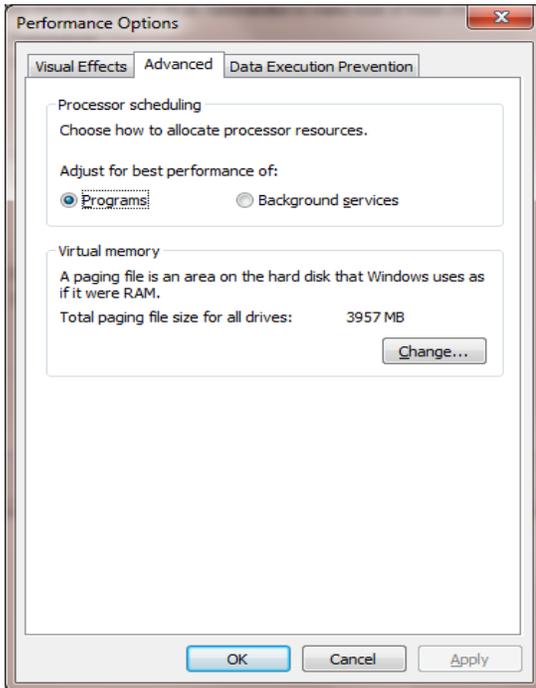
- If the value does not exist, add the following:
  - Value Name: ClearPageFileAtShutdown
  - Value Type: REG\_DWORD
  - Value: 1

## ***Disabling System Management of PageFile.sys – Windows 10***

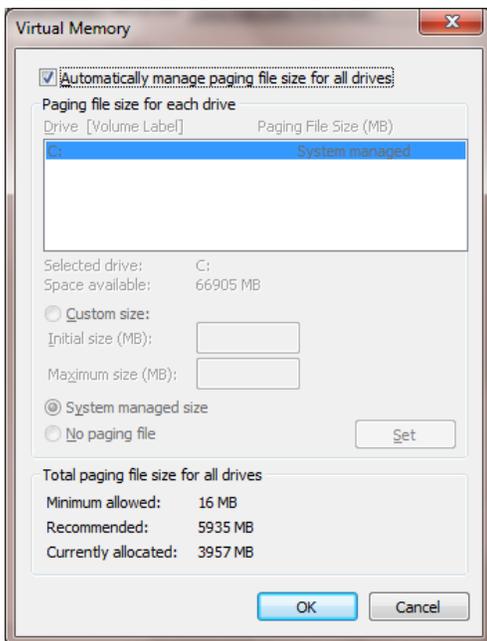
- Right Click on Computer > Select “Properties”
- Select “Advanced System Settings” on the top left list, the following screen will appear:



- Under performance select “Settings” and go to the “Advanced” tab, the following screen will appear:



- Select “Change” under Virtual Memory, the following screen will appear:

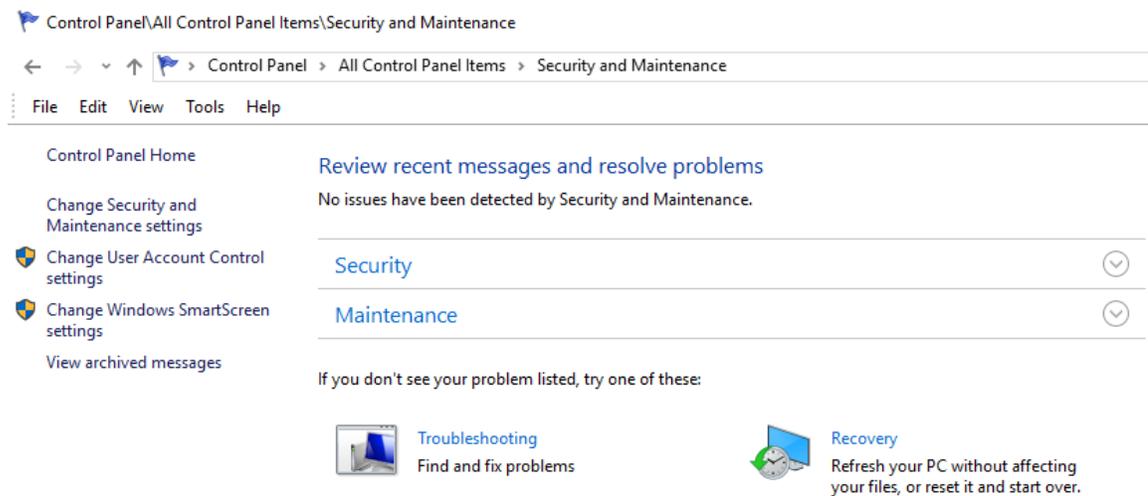


- Uncheck “Automatically manage page file size for all drives”
- Select “Custom Size”
- Enter the following for the size selections:

- Initial Size – as a good rule of thumb, the size should be equivalent to the amount of memory in the system.
- Maximum Size – as a good rule of thumb, the size should be equivalent to 2x the amount of memory in the system.
- Click “Ok”, “OK”, and “OK”
- You will be prompted to reboot your computer.

### ***Disabling Windows Error Reporting – Windows 10***

- Open the Control Panel
- Open “Security and Maintenance”
- Select “Change Security and Maintenance Settings”



- Select “Problem Reporting Settings”

e\Change Security and Maintenance

> Security and Maintenance > Change Security and Maintenance settings

### Turn messages on or off

For each selected item, Windows will check for problems and send you a message if problems are found.

[How does Security and Maintenance check for problems?](#)

#### Security messages

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Windows Update             | <input checked="" type="checkbox"/> Spyware and unwanted software protection |
| <input checked="" type="checkbox"/> Internet security settings | <input checked="" type="checkbox"/> User Account Control                     |
| <input checked="" type="checkbox"/> Network firewall           | <input checked="" type="checkbox"/> Virus protection                         |
| <input checked="" type="checkbox"/> Microsoft account          | <input checked="" type="checkbox"/> SmartScreen                              |
| <input checked="" type="checkbox"/> Windows activation         |  |

#### Maintenance messages

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> Windows Backup        | <input checked="" type="checkbox"/> Windows Troubleshooting |
| <input checked="" type="checkbox"/> Automatic Maintenance | <input checked="" type="checkbox"/> HomeGroup               |
| <input checked="" type="checkbox"/> Drive status          | <input checked="" type="checkbox"/> File History            |
| <input checked="" type="checkbox"/> Device software       | <input checked="" type="checkbox"/> Storage Spaces          |
| <input checked="" type="checkbox"/> Startup apps          | <input checked="" type="checkbox"/> Work Folders            |

OK

Cancel

- Select “Never Check for Solutions”

nance\Problem Reporting Settings

ems > Security and Maintenance > Problem Reporting Settings

### Choose when to check for solutions to problem reports

When you send problem reports to Microsoft, you will receive solutions when they are available. You can adjust how much information is sent.

[What information is sent?](#)

- Automatically check for solutions
- Automatically check for solutions and send additional report data, if needed
- Each time a problem occurs, ask me before checking for solutions
- Never check for solutions (not recommended)

[Change report settings for all users](#)

[Select programs to exclude from reporting](#)

[Read the Windows Error Reporting privacy statement online](#)