

Oracle® Hospitality OPERA Property Management
PA-DSS 3.2 Implementation Guide
Release 5.5.1.0 (5.5.X.X)
Part Number: E72248-02

February 2020

Copyright © , 2020, 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.

Contents

1	Preface	5
	Revision History.....	6
2	Executive Summary	8
	PCI Security Standards Council Reference Documents.....	8
	Payment Application Summary.....	9
	Typical Network Implementation	12
	Credit/Debit Cardholder Dataflow Diagram	13
	Difference between PCI Compliance and PA-DSS Validation	14
	The 12 Requirements of the PCI DSS:	15
3	Considerations for the Implementation of Payment Application in a PCI-Compliant Environment.....	16
	Removal of Historical Sensitive Authentication Data (PA-DSS 1.1.4).....	16
	Handling of Sensitive Authentication Data (PA-DSS 1.1.5).....	17
	Secure Deletion of Cardholder Data (PA-DSS 2.1).....	17
	All PAN is Masked by Default (PA-DSS 2.2)	19
	Cardholder Data Encryption & Key Management (PA-DSS 2.3, 2.4, and 2.5).....	19
	Removal of Historical Cryptographic Material (PA-DSS 2.6).....	20
	Set up Strong Access Controls (PA-DSS 3.2)	20
	Properly Train and Monitor Admin Personnel	22
	Log Settings must be Compliant (PA-DSS 4.1.b and 4.4.b)	22
4	PCI-Compliant Wireless Settings (PA-DSS 6.1.a and 6.2.b).....	23
5	Services and Protocols (PA-DSS 8.2.c)	24
	Never Store Cardholder Data on Internet-Accessible Systems (PA-DSS 9.1.b).....	24
	PCI-Compliant Remote Access (PA-DSS 10.1).....	24
	PCI-Compliant Delivery of Updates (PA-DSS 10.2.1.a).....	25
	PCI DSS 1	25
	PCI DSS 12.3.9	25
	PCI-Compliant Remote Access (PA-DSS 10.3.2.a).....	26
	Data Transport Encryption (PA-DSS 11.1.b)	27
	PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2.b)	27
	Non-Console Administration (PA-DSS 12.1)	28
	Network Segmentation	28
	Maintain an Information Security Program	28
	Application System Configuration.....	28
	Payment Application Initial Setup & Configuration	29
Appendix A	Inadvertent Capture of PAN.....	1
	Microsoft Windows 8	3
	Disable System Restore	3

Encrypt PageFile.sys.....	Error! Bookmark not defined.
Clear the System PageFile.sys on Shutdown	3
Disable System Management of PageFile.sys	Error! Bookmark not defined.
Disable Error Reporting.....	7
Microsoft Windows 7	9
Disable System Restore	9
Encrypt PageFile.sys.....	9
Clear the System PageFile.sys on Shutdown	10
Disable System Management of PageFile.sys	10
Disable Error Reporting.....	10

Notice

THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. ORACLE HOSPITALITY MAKES NO REPRESENTATION OR WARRANTY AS TO THE ACCURACY OR THE COMPLETENESS OF THE INFORMATION CONTAINED HEREIN. YOU ACKNOWLEDGE AND AGREE THAT THIS INFORMATION IS PROVIDED TO YOU ON THE CONDITION THAT NEITHER ORACLE HOSPITALITY NOR ANY OF ITS AFFILIATES OR REPRESENTATIVES WILL HAVE ANY LIABILITY IN RESPECT OF, OR AS A RESULT OF, THE USE OF THIS INFORMATION. IN ADDITION, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR MAKING YOUR OWN DECISIONS BASED ON THE INFORMATION HEREIN.

Nothing herein shall be construed as limiting or reducing your obligations to comply with any applicable laws, regulations or industry standards relating to security or otherwise including, but not limited to PCI PA-DSS and DSS.

The retailer may undertake activities that may affect compliance. For this reason, Oracle Hospitality is required to be specific to only the standard software provided by it.

Preface

This document describes the steps that you must follow in order for your OPERA Property Management 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). You can download the PCI [PA-DSS 3.2 Requirements and Security Assessment Procedures](#) from the PCI SSC Document Library.

Oracle Hospitality instructs and advises its customers to deploy Oracle Hospitality applications in a manner that adheres to the PCI Data Security Standard (v3.2). Subsequent to this, you should 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.

You must follow the steps outlined in this Implementation Guide in order for your OPERA Property Management installation to support your PCI DSS compliance efforts.

You must follow the steps outlined in this Implementation Guide in order for your OPERA Property Management installation to support your PCI DSS compliance efforts.

Revision History

Date	Description of Change
July 2015	<ul style="list-style-type: none">Initial publication.
January 2017	<ul style="list-style-type: none">Oracle Hospitality OPERA Property Management Versioning Number updated throughout the document along with the Description of Listing Versioning Methodology section to update the new versioning definitions that have been implemented in the product.
August 2017	<ul style="list-style-type: none">Added a new section about the OPERA automated installation wizard before the '12 Requirements of the PCI DSS' list.
September 2017	<ul style="list-style-type: none">Updated last subsections within section 3.
February 2020	<ul style="list-style-type: none">Updated language to PCI PA-DSS 3.2.

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 on the Oracle Help Center at <http://docs.oracle.com/en/industries/hospitality/> to view or download the current version of this guide, and refer to the OPERA Property Management's 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 OPERA Property Management in a PCI DSS compliant manner.

1 Executive Summary

OPERA Property Management Version 5.5.1.0 (5.5.X.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 OPERA Property Management Version 5.5.1.0 (5.5.X.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
- 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

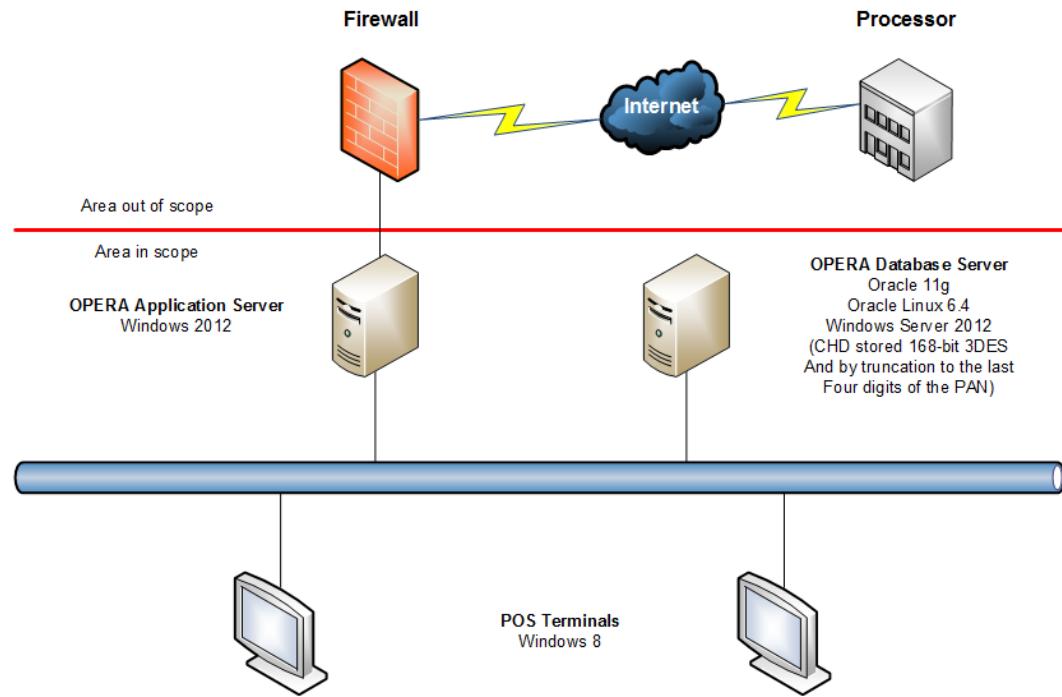
Payment Application Name	OPERA Property Management	Payment Application Version	5.5.1.0 (5.5.X.X)			
Payment Application Description	<p>OPERA Property Management is a Windows-based software application used to process payment card payments. The application can accept both card present and card-not-present transactions. OPERA Property Management Version 5.5.1.0 does not support PIN-based debit transaction nor does it include the capability to perform chargebacks. For the purpose of settling transactions, the application retains the PAN, expiry date, and cardholder name in an Oracle 11g database, using AES256 encryption for the data at rest. The application also stores the truncated card number with just the last four digits of the PAN, if needed for reference by the merchant employee. Cardholder data can be either swiped or manually entered into the application. When manually entered, card validation codes are requested. All sensitive authentication data collected during a transaction, including PAN, magnetic track data and card validation codes, CVV2, is stored in VRAM prior to authorization. Subsequent to authorization, data is purged from VRAM. OPERA Property Management Version 5.5.1.0 is only sold as a software package with the responsibility of hardware purchase up to the customer. Oracle provides functionality within OPERA Property Management to enter sensitive personal information (including passport, date of birth, and credit card numbers) in specific fields on the user interface. The form fields that are intended to receive this information are clearly labeled, and are designed with heightened security controls such as data masking in the form and encryption of at rest. Entering this sensitive personal information in any other field (for example, in a Notes or Comments field), does not provide it with these heightened security controls and is not consistent with the requirements for protecting cardholder data as detailed in the Payment Card Industry Data Security Standards (PCI DSS).</p>					
Typical Role of the Payment Application	<p>OPERA Property Management is a payment application used in hotels for processing credit card transactions and handling authorization and settlement. OPERA Property Management can handle card-present and card-not-present transactions but not debit or other PIN-based transactions. The application consists of a PC-based POS terminal client, an application server, and a database server. The application accepts cardholder data, including PAN, magnetic track and CVV2 codes, directly through the POS terminal client, which passes the cardholder data to the application server, which is used to facilitate the authorization of transactions through communications with the merchant's processor. The database stores cardholder data, including the PAN, cardholder name and expiry date only for the purpose of settlement of transactions, using AES256 encryption. The OPERA software resides on both the POS terminal clients and the application server.</p>					
Target Market for	<input type="checkbox"/>	Retail	<input type="checkbox"/>	Processors	<input type="checkbox"/>	Gas/Oil

Payment Application (check all that apply)	<input type="checkbox"/>	e-Commerce	<input type="checkbox"/>	Small/medium merchants		
	<input checked="" type="checkbox"/>	Hospitality Industry				
Stored Cardholder Data	The following is a brief description of files and tables that store cardholder data.					
	File or Table Name		Description of Stored Cardholder Data			
	name_credit_card		Full PAN, cardholder name, expiry date			
	name_credit_card		Truncated PAN			
	Individual access to cardholder data is logged as follows: Access to this table is logged by the Oracle 11g database software.					
Components of the Payment Application	The following are the application-vendor-developed components which comprise the payment application:					
	OPERA Property Management is designed to be run on Microsoft Windows-based systems. The application is comprised of an application server, a database server running Oracle 11gR2 and PC-based POS terminal clients. All components are meant to be installed within the customer's corporate network. The application server provides all communication to the processing bank as well as reporting and management functions. The POS terminal client component runs on Microsoft Windows 7 or 8.1. The application server runs on Windows Server 2012 R2 and the database server component runs on Windows Server 2012 R2 and Oracle Linux 6.4. The application requires the database server to run Oracle 11gR2 on any platform that is supported by Oracle for that version.					
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 the Oracle 11gR2 database server. Encrypted cardholder data, including PANs, expiry date, and cardholder name are stored in the database located on the back office server using AES256 encryption.					
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:					
	Linux x86-64		Oracle Linux 6.4			
	Microsoft Windows x64 (64-bit)		8.1 7 2012 R2 2008 R2			
Payment Application Authentication	Authentication to the POS application is handled separately from the operating system. Authentication credentials are held within the application's database. These credentials are stored in the					

	<p>database using DBMS_CRYPTO.Hash_SH1 in Database 11g and DBMS_CRYPTO.SH512 in Database 12c. During the authentication process, clear text credentials are not sent over the network. When the POS terminal client initiates a connection to the application server, an HTTPS/TLS 1.2 tunnel is opened between the two. All communication including authentication traffic is encrypted.</p>					
Payment Application Encryption	<p>The database server provides back-end storage for application data including cardholder data, the PAN, cardholder name, and expiry date encrypted using AES256. The POS software can be installed on a standard PC with a cash drawer. The application is not designed to be implemented in a web-based environment.</p>					
Supported Payment Application Functionality	<input type="checkbox"/>	Automated Fuel Dispenser	<input type="checkbox"/>	POS Kiosk	<input type="checkbox"/>	Payment Gateway/ Switch
	<input type="checkbox"/>	Card-Not-Present	<input checked="" type="checkbox"/>	POS Specialized	<input type="checkbox"/>	Payment Middleware
	<input type="checkbox"/>	POS Admin	<input type="checkbox"/>	POS Suite/General	<input type="checkbox"/>	Payment Module
	<input checked="" type="checkbox"/>	POS Face-to-Face/POI	<input type="checkbox"/>	Payment Back Office	<input type="checkbox"/>	Shopping Card & Store Front
Payment Processing Connections	<p>OPERA Property Management uses the standard Microsoft TCP/IP stack that is included with the Windows Operating system when deployed on an Ethernet network. All communications between the application's components (POS terminal client, application server, and database server) are performed via HTTPS/TLS 1.2 tunnels.</p>					
Description of Listing Versioning Methodology	<p>Oracle uses a major.minor.patchset.patchset update scheme for Oracle Hospitality OPERA Property Management versioning. Here is a common example:</p> <p>Oracle Hospitality OPERA Property Management versioning has four levels, Major, Minor, Patchset, and Patchset update:</p> <p><Major>.<Minor>.<Patchset>.<Patchset Update></p> <ul style="list-style-type: none"> • Major includes substantial modification to the application in both operational functionality and appearance would have an impact on PA-DSS requirements. • Minor identifies the milestone steps towards the next major release and may or may not have an impact on PA-DSS requirements. • Patchset contains moderate enhancements and fixes that will not have an impact on Security or PA-DSS requirements and is reflected with the Wildcard. • Patchset Update contains minor enhancements and fixes that will not have an impact on Security or PA-DSS requirements and is reflected with the Wildcard. 					

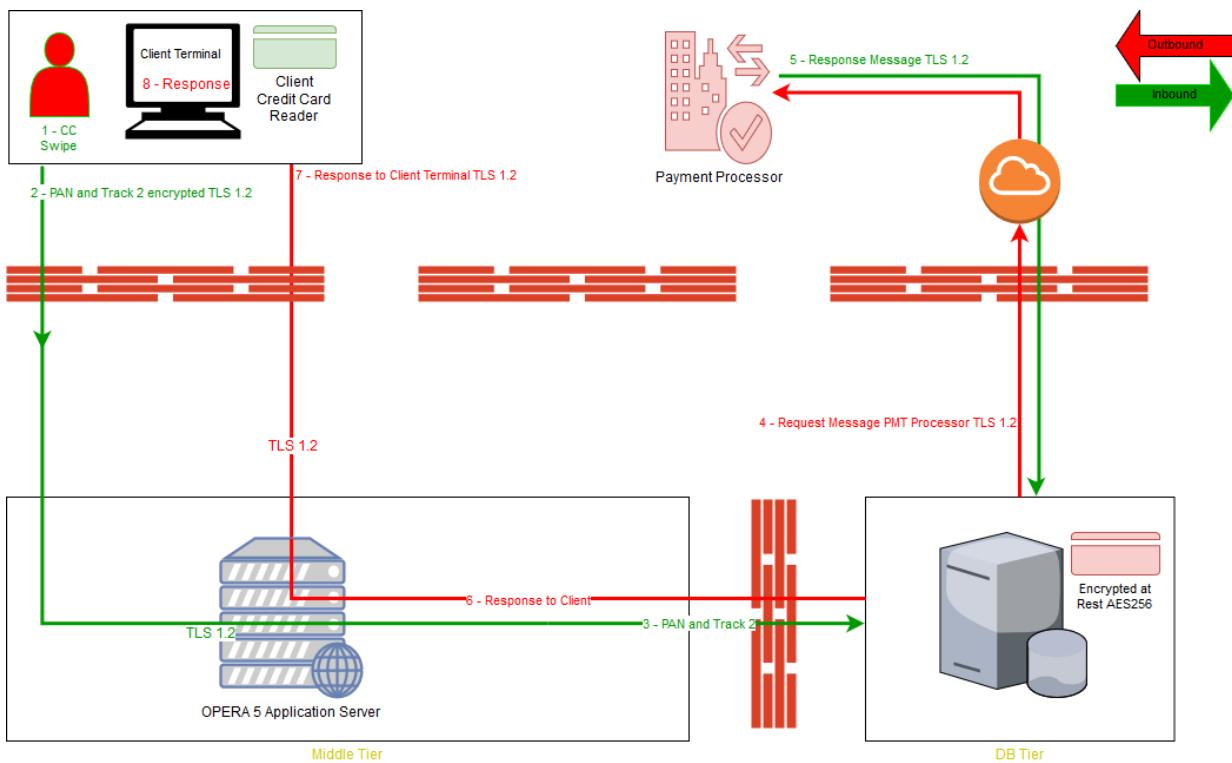
	Based on the above versioning methodology the application version being listed with the PCI SSC is: 5.5.1.0 (5.5.X.X)
--	-----------------------------------------------------------------------------------------------------------------------

Typical Network Implementation



Credit/Debit Cardholder Dataflow Diagram

OPERA Property Management Services Data Flow Diagram Example



1. Client swipes card for card present or enters card data manually for card not present transactions in the browser on the Client Terminal.
2. PAN and Track 2 (if swiped) is sent via HTTPS/TLS1.2 from the Client Terminal browser to the OPERA Application Server.
3. The OPERA Application Server sends this data to the OPERA Database Server.
4. The OPERA Database formats the data into a request message and sends the transaction to the Payment Processor.
5. The Processor responds with the approval or decline of the transaction. The PAN and Expiration Date are stored encrypted for any future use related to the original transaction.
6. The OPERA Database sends the response to the OPERA Application Server.
7. The OPERA Application Server directs the response to the correct Client Terminal.
8. The response is displayed to the user to action if needed or to complete the business transaction.

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 performed an assessment and payment application validation review with our independent assessment firm (PAQSA) to ensure that our platform conforms to industry best practices when handling, managing, and storing payment-related information.

PA-DSS Version 3.2 is the standard against which the 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 OPERA Property Management 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 & software configurations and access control procedures.

The OPERA Application is delivered with an automated installation wizard and “secure by default” with all default passwords removed from the installation.

The administrator/installer establishes passwords during the automated wizard installation for key system components during the installation, set up and configuration of the database and OPERA system.

OPERA Application parameters are set automatically to a secure by default setting.

Even though the automated installation wizard is performing the installation, there are certain elements out of scope for the wizard and need additional action.

As part of building and maintaining a secure network and systems the following manual steps are required:

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.

- Removal of 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

Removal of 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. Refer to the Glossary of Terms, Abbreviations, and Acronyms in the PCI SSC for the definition of [Sensitive Authentication Data](#).

The following previous versions of OPERA stored Sensitive Authentication Data (SAD) including Track 2 data:

- OPERA Version 3
- OPERA Version 2
- Below OPERA Version 2

Sensitive Authentication Data 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.

Historical SAD stored by previous versions of OPERA must be securely deleted and removal is absolutely necessary for PCI DSS compliance. Oracle Hospitality provides a secure deletion tool that includes capabilities to securely delete historical SAD as follows:

After the release of OPERA Version 4, no historical credit card data is stored. But should an upgrade from a version previous to 4 be required, OPERA offers a solution to deleting any sensitive data.

To stay in compliance with the Payment Card Industries – Security Standards Council requirements, when upgrading from a version of OPERA previous to Version 4.0, the CC_TRACK2 parameter must first be turned off in the previous version. This deletes the Track 2 data from the OPERA database. To turn off the parameter in OPERA Version 3.2, select **Setup**, then **Application Settings**, and set the IFC Group Application Parameter to **No**, as shown below.

If you do not currently use a secure delete tool; you can use one of the following:

Windows:

Heidi Eraser can be obtained from <http://www.heidi.ie/eraser/>

Microsoft SDelete can be obtained from <http://technet.microsoft.com/en-us/sysinternals/bb897443>

UNIX:

Wipe can be obtained from <http://wipe.sourceforge.net/>

Shred is included with many distributions of Linux.

Unishred Pro is a commercial tool available at <http://www.lat.com/>

Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

OPERA Property Management stores Sensitive Authentication Data (SAD) for troubleshooting purposes only and only during the time we are supporting a customer issue. The following guidelines are 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.

We strongly recommend that you do not store SAD for any reason. However, if you should do so, the preceding guidelines must be followed when dealing with SAD used for pre-authorization (swipe data, validation values or codes, PIN or PIN block data).

Oracle provides functionality within OPERA Property Management to enter sensitive personal information (including passport, date of birth, and credit card numbers) in specific fields on the user interface. The form fields that are intended to receive this information are clearly labeled, and are designed with heightened security controls such as data masking in the form and encryption of at rest. Entering this sensitive personal information in any other field (for example, in a Notes or Comments field), does not provide it with these heightened security controls and is not consistent with the requirements for protecting cardholder data as detailed in the Payment Card Industry Data Security Standards (PCI DSS).

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:
name_credit_card (Full PAN, cardholder name, expiry date)
name_credit_card (Truncated PAN).

Cardholder Data must be securely deleted within the payment applications and databases. Oracle recommends activating the **GENERAL > PURGE UNNECESSARY CREDIT CARDS** application setting and entering the number

of days to use to determine which credit cards are eligible for removal from the database, provided the credit card is not attached to any other current or future reservations in any property (in multi-property environments). Actual removal is handled by the Purge Credit Cards procedure, which is included in the OPERA Data Purge Routine, and is implemented at the next scheduled run of that routine. Here is how this setting affects credit card information removal. The procedure executes each time the OPERA Data Purge Routine is scheduled. The procedure refers to the Days to Remove Unnecessary Credit Cards setting only to determine all the valid credit card information that is older than that many days.

- Days entered are the days after the departure date of the reservation that was settled by credit card. For example, if Days is set to 5, and the reservation departure date is April 7, the credit card information is eligible to be removed on April 12 (regardless of whether the reservation was cancelled or was no show).
- Days entered are the days after the folio close date (when the **CASHIERING > OPEN FOLIO** application parameter is set to Y) if payment was made by credit card and the reservation is checked out with open folio. For example, if Days is set to 5, and the guest checks out on April 7 with open folio, if the folio is closed on April 11, the credit card information is eligible to be removed on April 16.
- Days entered are the days after reconciliation if the reservation is checked out to a credit card payment method having an AR account attached. For example, if Days is set to 5, and a reservation checks out paying by credit card, an AR invoice is created in the associated AR account. If this AR invoice is reconciled on May 12, the credit card information is eligible to be removed on May 17 provided this reconciled AR invoice has already been purged. If the invoice is not purged even after reconciliation, the credit card information will NOT be removed.
- Days entered are the days after the credit card information has been added to the profile (available when the **PROFILES > PROFILE CREDIT CARD** application function is set to Y), provided the credit card has not been attached to any current or future reservations. For example, if Days is set to 5, and the credit card information is attached to a profile on April 7, the credit card information is eligible to be removed on April 12.
- Credit card information will NOT be removed in case there is a pending batch/offline settlement for the credit card.

For all users, credit card information is only available in truncated format (e.g., XXXXXXXXXXXX4317, expiration date XX/XX) once it has been removed from the database. (After the purge routine runs, all that actually remains of the credit card number in the OPERA database is the last four digits; all other credit card information, including the expiration date, is entirely removed.) The truncated format information is displayed, as required, in screens and in response to requests for reports and historical information.

- 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)

OPERA Property Management masks all PAN by default in all locations that display PAN (screens) and truncates PAN in all outputs (screens, paper receipts, printouts, reports, etc.) by displaying only the last 4 digits of the credit card number. The payment application displays the truncated PAN in the following locations:

- All printed receipts.
- All generated card reports in the reports menu; these include the following reports: AR Credit Invoice (arcrdlist), AR Credit Card Transfer (arcrtransfer), AR Ledger (arledger), Membership Pre-Check In (arrprecheckinmem), Check Report (check_rep), Credit Card History (creditcard_history), Credit Card Rebates (creditcard_rebates), Credit Card Authorization History (cc_auth_history), Journal by Cashier and Article Code (finjrnl_articles), Journal by Foreign Currency (finjrnlbyforcurr), Financial Transactions by Tax Type (finjrnlbytax), Journal By Cashier and Transaction Code (finjrnlbytrans), Financial Transactions with Generates (finjrnlbytrans2), Cashier Audit (finpayments), Credit Limit Report- All Payment Methods (gi_authlimit), Rate Variance (giratevariance), Group Rooming List (grprmlist), Night Audit Credit Card Authorization (nacc_authorization), No Shows of the Day (nanoshow), Paid Outs (napaidout), No Show Extended Reservations (noshow_ext), and Arrivals: Detailed (res_detail).

OPERA Property Management does have the ability to display full PAN for users with legitimate business needs. In order to configure the application to display full PAN, you must have the permission **Credit Card Information View**. Users can double-click on the masked PAN details and view the full unmasked PAN details within OPERA. But when a user completes this action, it is logged in the User Activity Log as described later in the document in the Logging section.

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

OPERA Property Management does store cardholder data and does not have the ability to 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 dynamically generated keys to automatically encrypt all locations/ methods where cardholder data is stored.

OPERA Property Management does not have a debugging mode that could write PAN to debugging logs.

The following key management functions are performed automatically using AES256 dynamic encryption key methodology and there are no key custodians or intervention required by customers or resellers/integrators.

- Generation of strong cryptographic keys.
- Secure cryptographic key distribution.
- Secure cryptographic key storage.
- Cryptographic key changes for keys that have reached the end of their cryptoperiod.
- 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.

- Manual clear-text cryptographic key-management procedures require split knowledge and dual control of keys.
- Prevention of unauthorized substitution of cryptographic keys.

Removal of Historical Cryptographic Material (PA-DSS 2.6)

OPERA has the following versions that previously encrypted cardholder data:

- OPERA 4

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 decrypt and re-encrypt the data with new encryption keys.
- You must manually re-encrypt all historical cardholder data by selecting **Utilities** and then **Change CC Encryption Key**. This utility allows OPERA users with appropriate permissions to change the encryption key that is used to secure customer credit card data. This utility should be used with extreme caution. The following permissions are required to run this utility: Select **Reservations**, then **Credit Card Information Edit** and **Utilities**, and then select **Change Encrypt Key**.
- Previous historical credit card data (no longer needed) must be securely deleted within the payment applications and databases by setting the **GENERAL > PURGE UNNECESSARY CREDIT CARDS** application setting that will run with the OPERA Scheduler.

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 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.

-Supervisor

-Member of OPERA Supervisor Role

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 3.1.12)

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 Oracle Hospitality 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 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)

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.

These same account and password criteria from the above 11 requirements must also be applied to any applications or databases included in payment processing to be PCI compliant. OPERA Property Management, as tested in our PA-DSS validation, meets, or exceeds these requirements.

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).

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

4.1.b: OPERA Property Management has PA-DSS compliant logging enabled by default. This logging is not configurable and may not be disabled. Disabling or subverting the logging function of OPERA Property Management in any way will result in non-compliance with PCI DSS.

Oracle provides a comprehensive audit trail utility within OPERA that allows privileged users to track OPERA specific activities. The advent of open database structure means that anyone with system level access to the database server (Oracle) has access to system components covered under this requirement, and requires logging of user access and activity. ORACLE strongly recommends logging of activity on the database server.

4.4.b: OPERA Property Management facilitates centralized logging. The OPERA User Activity Log records a "history" of user activity in the OPERA database and is accessed via selecting **Miscellaneous**, and then **User Activity Log**. This logs data related to credit card authorizations, settlements, credit card information entry and deletion, and other transactions. This includes offline settlements taking place for a reservation due to interface time out or when user performs the settlement of temporarily stored offline settlements by opening **Cashiering**, then **Credit Cards**, and then selecting the **Settlement** option, or when End of Day attempts to perform the settlement of temporarily stored offline settlements.

Note: Each time any user who is granted the permission via selecting **RESERVATIONS** and then **CREDIT CARD INFORMATION VIEW** to access an OPERA screen to view credit card information (i.e., credit card numbers and expiration dates), the activity is recorded in the User Activity Log. Users without this permission will only see last 4. These screens include the Reservation screen, the Payment screen, the Profile screen, the Group Rooming List, and others.

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 OPERA Property Management in any way will result in non-compliance with PCI DSS.

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

OPERA Property Management does support wireless technologies and 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 802.11.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.

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

OPERA Property Management does not require the use of any insecure services or protocols. Here are the services and protocols that OPERA Property Management does require:

- SSL PROTOCOLS UTILIZED
- SFTP
- HTTPS
- IPSec

Oracle recommends that all sensitive information that is transmitted over the Internet be secured using a form of encryption such as SSL Protocols; this includes all wireless transmissions, email and use of services such as Telnet and FTP.

Additionally Oracle recommends using IPSec between the Application and Database servers to secure communications. The IPSEC tunnel is also the proposed solution for all other non-strictly app servers that connect directly to the DB (OWS, ADS, GDS, OXI).

Oracle strongly suggests that when using our web-based credit card interface, it is set up to use SSL Protocol communication. To configure this, do the following: Select **Configuration**, then **Setup**, then **Property Interfaces**, and then select **Interface Configuration** and edit the active EFT Interface. On this form you will see a section to configure the URL that you are to connect to. Be sure that this URL starts with HTTPS. This will ensure a secure SSL Protocol connection is made to the vendor prior to transmitting credit card data.

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

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 (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. This means two of the following three authentication methods must be used:

1. Something you know, such as a password or passphrase
2. Something you have, such as a token device or smart card
3. Something you are, such as a biometric

OPERA Property Management utilizes this two-factor authentication by having the user have to sign into the OPERA application itself with a User ID and Password and then another User ID and Password must be entered to get into other sections within OPERA, such as Cashiering.

And when swiping a credit card on an encrypted credit card reader from within the MICROS Payment Application (widget), OPERA reads the configuration of the credit card reader and passes this configuration information on to the MICROS Payment Application. The widget then parses the credit card information. The Expiration Date,

Name of the Credit Card holder, the last 4 digits of the credit card number, and encrypted track data are extracted and sent to the Credit Card Vendor, based on the credit card reader device configuration. The Credit Card Vendor then decrypts the data and returns a token to OPERA to be used with any following credit card transactions.

Also, OPERA supports the Chip and PIN method of credit card and membership card authorization for both offline and online transactions. In addition, OPERA Kiosk supports Chip and PIN credit card payments to be made through a hotel kiosk system. Chip and PIN relies on a microchip inserted into the card; the chip stores cardholder authentication information. When the card is inserted into a specially designed reader, the microchip is accessed and the cardholder is prompted to enter a PIN (Personal Identification Number) to authorize the card.

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

OPERA Property Management delivers patches and updates in a secure manner:

PCI DSS 1

Install and maintain a firewall configuration to protect cardholder data.

PCI DSS 12.3.9

Activate remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.

As a development company, we keep abreast of the relevant security concerns and vulnerabilities in our area of development and expertise.

Once we identify a relevant vulnerability, we work to develop and test a patch that helps protect OPERA Property Management against the specific new vulnerability. We attempt to publish a patch within 10 days of the identification of the vulnerability. We then 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 deliver software and/or updates via remote access to customer networks. These are made available on the Oracle website < <http://support.oracle.com> > for download.

For receiving updates via remote access, merchants must adhere to the following guidelines:

Secure remote access technology use, per PCI Data Security Standard 12.3.9:

12.3 *Activation of remote access technologies for vendors only when needed by vendors, with immediate deactivation after use.*

To receive e-mail notifications of the release of Critical Patch Updates and Security Alerts, please follow the steps outlined below.

1. If you do not have an Oracle Technology Network account, click on the *Account* link at the top of this page to create an account.
2. If you already have an Oracle Technology Network account, click on the *Account* link at the top of this page and login to your account.
3. Once logged in, click *account name* to see profile.
4. Click *Subscriptions* and select the checkbox for *Security Alerts*.

To unsubscribe, login, click *Subscriptions* and uncheck the *Security Alerts* checkbox.

Critical Patch Updates (CPU) information is available on the Oracle website:
<https://www.oracle.com/security-alerts/>

PCI-Compliant Remote Access (PA-DSS 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).

1. Something you know, such as a password or passphrase
2. Something you have, such as a token device or smart card
3. Something you are, such as a biometric

OPERA Property Management utilizes this two-factor authentication by having the user have to sign into the OPERA application itself with a User ID and Password and then another User ID and Password must be entered to get into other sections within OPERA, such as Cashiering.

And when swiping a credit card on an encrypted credit card reader from within the MICROS Payment Application (widget), OPERA reads the configuration of the credit card reader and passes this configuration information on to the MICROS Payment Application. The widget then parses the credit card information. The Expiration Date, Name of the Credit Card holder, the last 4 digits of the credit card number, and encrypted track data are extracted and sent to the Credit Card Vendor, based on the credit card reader device configuration. The Credit Card Vendor then decrypts the data and returns a token to OPERA to be used with any following credit card transactions.

Also, OPERA supports the Chip and PIN method of credit card and membership card authorization for both offline and online transactions. In addition, OPERA Kiosk supports Chip and PIN credit card payments to be made through a hotel kiosk system. Chip and PIN relies on a microchip inserted into the card; the chip stores cardholder authentication information. When the card is inserted into a specially designed reader, the microchip is accessed and the cardholder is prompted to enter a PIN (Personal Identification Number) to authorize the card.

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, Oracle Support, etc. 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 Oracle Support it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements 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 (e.g. VNC).
- Allow connections only from specific IP and/or MAC addresses.
- Use strong authentication and complex passwords for logins according to PA-DSS 3.2 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 3.2 and PCI DSS 8.5.13.
- Require that remote access take place over a VPN via 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 3.2 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 AES256) 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 OPERA Property Management

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

OPERA Property Management facilitates/enables the sending of PANs via end user messaging technology by ensuring that PAN is always masked on materials that can be printed, emailed, and faxed, which makes the PAN unreadable to any person viewing the item.

PCI requires that cardholder information sent via any end user messaging technology must use strong encryption of the data.

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

OPERA Property Management or server allows non-console administration, so you must use SSH, VPN, or TLS 1.1 or higher for encryption of this non-console administrative access. Because OPERA Property Management allows such access, multi-factor authentication (at least 2 of something you know, something you have, or something you are) must be utilized when accessing OPERA Property Management over these technologies.

Follow the setup instructions for your selected MFA solution to implement that solution with OPERA

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 OPERA Property Management.

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.

Linux x86-64	Oracle Linux 6.4
Microsoft Windows x64 (64-bit)	8.1

	7 2012 R2 2008 R2
--	-------------------------

Payment Application Initial Setup & Configuration

The Credit Card Vault feature is used to eliminate the storage of credit card numbers in OPERA. When this feature is active, instead of storing credit card numbers, unique ID's (tokens) provided by the EFT system replace credit card numbers for all of the guest's credit card transactions. With this feature active, a card number can only be entered on the Payment Application to retrieve the token. The Payment Application is an external component (JAVA) that communicates the card data out to the EFT system and only the token in to OPERA. The token is saved in the OPERA database and used for all the guest's payment transactions. E2EE devices can also be utilized to further reduce the entry of clear card data in the Payment Application.

When initially configuring OPERA to function with the external Credit Card Vault application, the following application settings must be considered for configuration within OPERA:

- IFC > CREDIT CARD VAULT
- IFC > CREDIT CARD VAULT ID
- IFC > CREDIT CARD VAULT MAX CC PROCESSED
- IFC > CREDIT CARD VAULT TIMEOUT
- IFC > CREDIT CARD VAULT CHAIN CODE
- IFC > CREDIT CARD VAULT WEB SERVICE URL
- IFC > WALLET PASSWORD

The CcHttpLib.dll allows client side certificates utilizing mutual authentication to be imported on workstations at a Computer Account level in order to be scalable to all North American properties and viable for franchised workstations. The CcHttpLib.dll is placed on the OPERA Application Server for automatic deployment to the workstations when accessing OPERA.

The .crt and .p12 certificates and password (needed to import the certificate) are supplied by the credit card vendor.

The workstations that will access OPERA and conduct credit card transactions must have Microsoft Management Console (MMC) and Microsoft Windows HTTP Services certificate configuration tool (WinHttpCertCfg.exe) installed.

The following steps must be performed by an administrator on each workstation or a similar process followed to push the certificates to the workstation.

- A. Save the vendor provided **.crt** and **.p12** on the workstation.
- B. Run **MMC** and import the certificate using the following steps.
 1. Go to **File > Add or Remove Snap-ins**.
 2. Select **Certificates** under the *Available snap-ins* section and add it to the *Selected snap-ins* section.
 3. On the *Certificates snap-ins* screen, select **Computer account** and then click **Next**.
 4. Keep the option **Local computer** and click **Finish**.
 5. Click **OK** to go back to the main **MMC** window.

6. Right-click on a folder under the *Certificates* folder and select **All Tasks** followed by **Import...**
7. Click **Next** on the **Import Wizard** and **Browse** to find the **.crt** that was saved on the workstation in step A.
8. Click **Next** and select the option **Automatically select the certificate store based on the type of certificate.**
9. Click **Next** and **Finish**. The message '*The import was successful.*' appears.
10. Right-click again on a folder under the *Certificates* folder and select **All Tasks** followed by **Import...**
11. Click **Next** on the **Import Wizard** and **Browse** to find the **.p12** that was saved on the workstation in step A.
12. Click **Next** and enter the password provided by the vendor.
13. Click **Next** and select the option **Automatically select the certificate store based on the type of certificate.**
14. Click **Next** and **Finish**. The message '*The import was successful.*' appears.

The certificate can now be found in three Stores.

C. Open a cmd window and run the following command:

`WinHttpCertCfg.exe -g -c LOCAL_MACHINE\MY -s "www.micros.com" -a everyone`

A successful response is similar to this:

Microsoft (R) WinHTTP Certificate Configuration Tool

Copyright (C) Microsoft Corporation 2001.

Matching certificate:

CN=www.micros.com

OU=ODH

O=TARPON

L=Silver Spring

S=Maryland

C=US

OID.1.3.6.1.4.1.99999.10.1=UAT Opera Transaction Vault

Granting private key access for account:

\Everyone

An unsuccessful response may be similar to this:

Unable to update security info for key container, error = 0x5

If this occurs, initialize cmd with *Run as administrator* and execute the command again.

D. Log out of the workstation and log in as a regular user to access OPERA and conduct credit card transactions.

Any user account that has the permissions to log on to the domain and workstation has access to the certificate to successfully conduct business.

- Installing the Payment Application – the needed DLLs and jar files are automatically downloaded with the OPERA installation. With the above application settings active and certificates installed, the Payment App will be available from the icon on the OPERA forms.

- Defining the Payment Gateway - use an SSL connection for communication between OPERA and the EFT system. The vendor provided .p12 is used as the Server side certificate and imported to the Oracle Wallets folder on the OPERA database server.
- Obtaining and Installing the 128 bit SSL Protocol Certificate.
- Conducting Test Transactions - can be completed only if Vendor supports test card data.
- Special Instructions for Upgrades – existing card numbers in the OPERA database can be converted to tokens from the EFT system in a process initiated through OPERA Utilities.
- Resetting Administrator Passwords - OPERA User Passwords have mandatory expiry every 30 days.
- Performing Maintenance - recommend setup purge of historical data.
- Updating your Encryption Key on a Periodic basis - recommend setup purge of historical data and execute the Encryption Utility on a scheduled basis as mentioned in above section 'Removal of Historical Cryptographic Material (PA-DSS 2.6)'. Not needed when Vault is active.

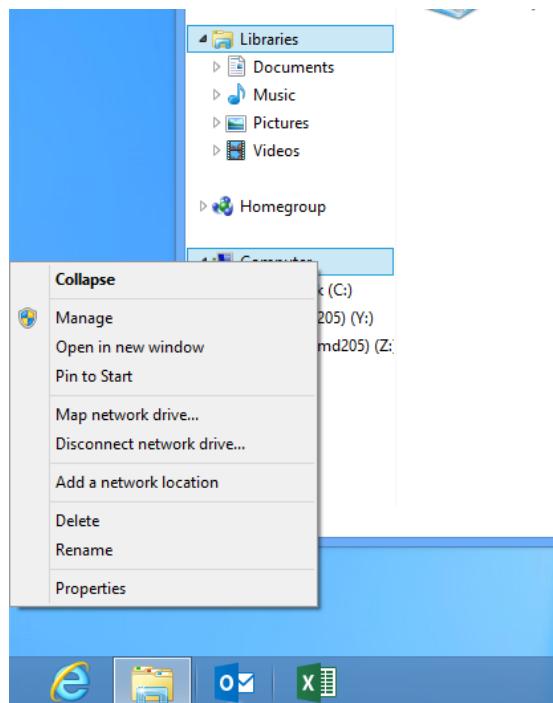
Appendix A Inadvertent Capture of PAN

This appendix provides instructions for addressing the inadvertent capture of PAN on the following supported operating systems:

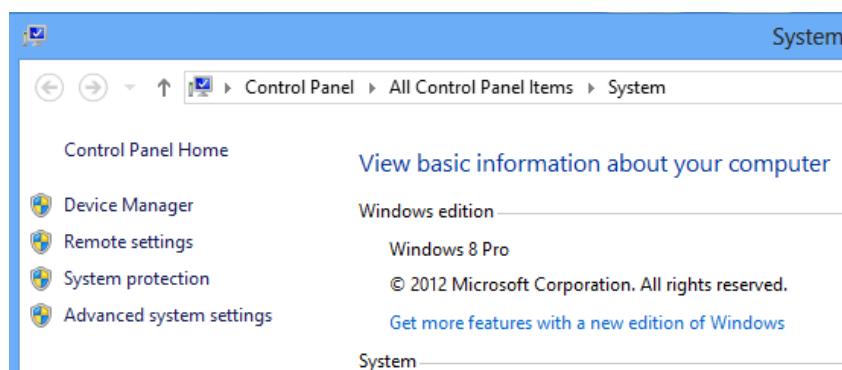
- Microsoft Windows 8
- Microsoft Windows 7

Disabling System Restore – Microsoft Windows 8

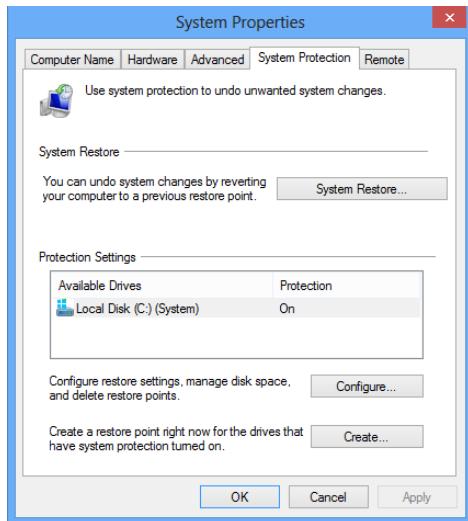
- Right Click on Computer > Select “Properties”:



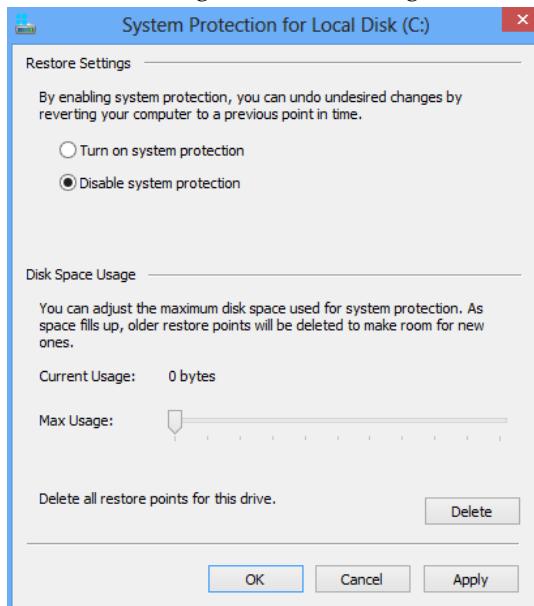
- Select “Advanced System Settings” from the System screen:



- Select “System Protection” on the top left list, the following screen will appear:



- Select Configure, the following screen will appear:

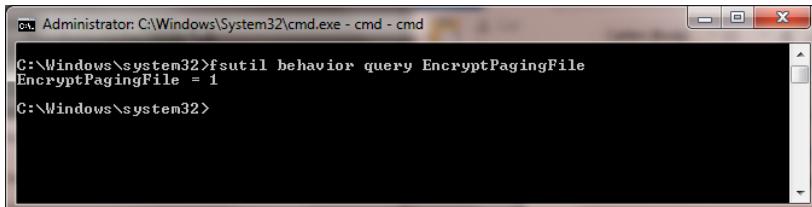


- Select “Disable system protection”
- Click apply, and OK to shut the System Protection window
- Click OK again to shut the System Properties window
- Reboot the computer

Encrypting PageFile.sys – Microsoft Windows 8

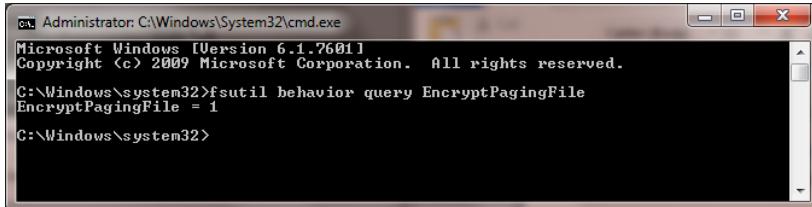
* Please note that in order to perform this operation the hard disk must be formatted using NTFS.

- From the desktop hold down the “Windows” key and type “F” to bring up the “Search” charm, select “Apps” in the “Apps” box type in “cmd”.
- 1. Rightclick on “**Command Prompt**” icon located on the left side of your screen, a selection bar will appear at the bottom of the screen, select “**Run as Administrator**”
- 2. 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>
```

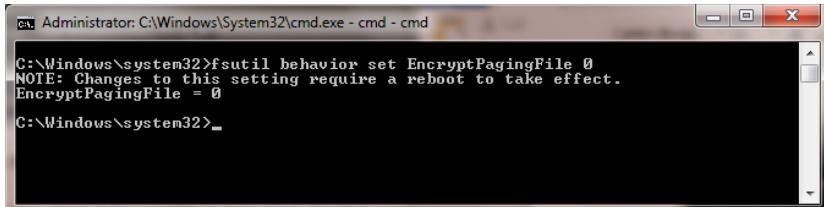
- If encryption is enabled `EncryptPagingFile = 1` should appear
- 3. If encryption is disabled `EncryptPagingFile = 0` should appear
- To Encrypt the Pagefile type the following command: `fsutil behavior set EncryptPagingFile 1`



```
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>
```

- 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>
```

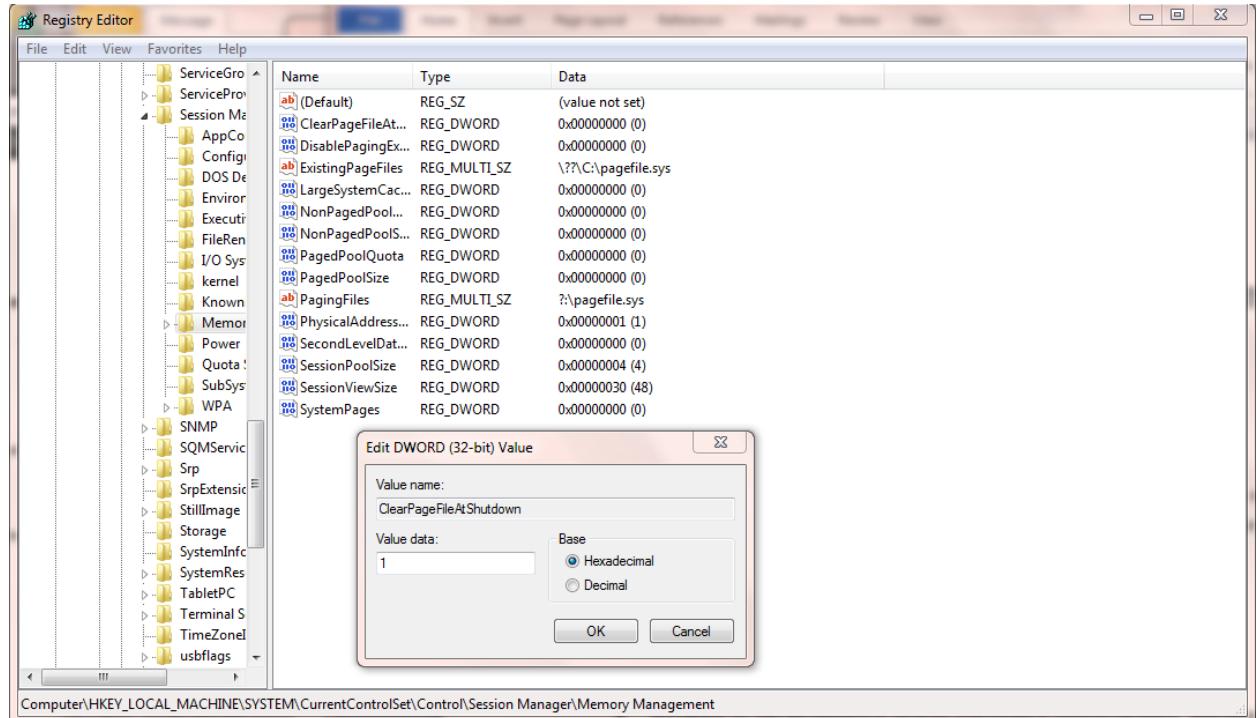
Clear the System PageFile.sys on Shutdown

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.

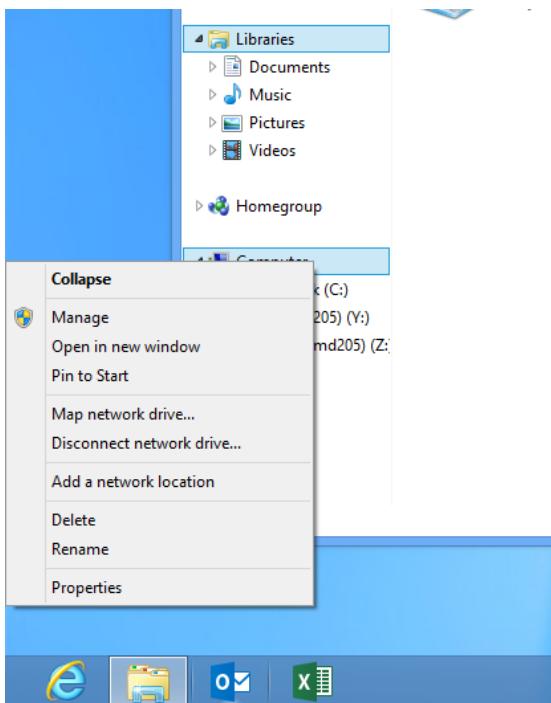
- From the desktop hold down the “Windows” key and type “F” to bring up the “Search” charm, select “Apps” in the “Apps” box type in “regedit”.

1. Rightclick on regedit.exe and select “Run as Administrator”
2. Navigate to HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
- Change the value from 0 to 1 on the “ClearPageFileAtShutdown” DWORD.
- Click OK and close Regedit

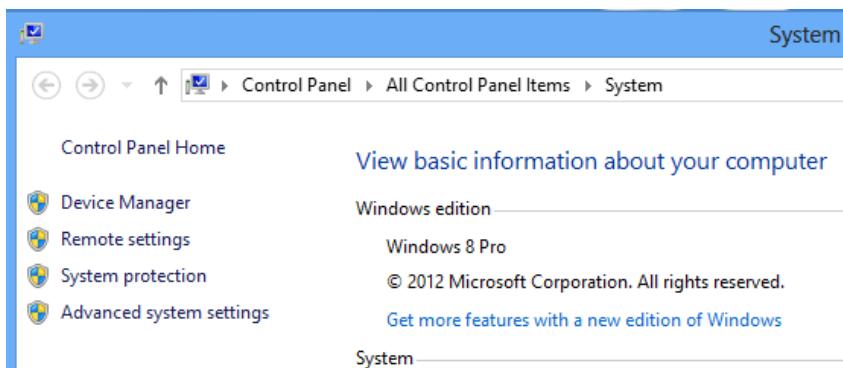


- If the value does not exist, add the following:
 - o Value Name: ClearPageFileAtShutdown
 - o Value Type: REG_DWORD
 - o Value: 1

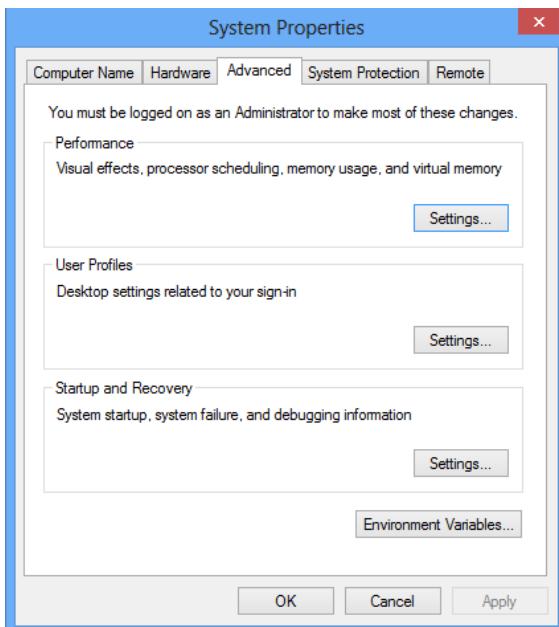
3. Disabling System Management of PageFile.sys – Microsoft Windows 8
1. Right Click on **Computer** > Select “**Properties**”:



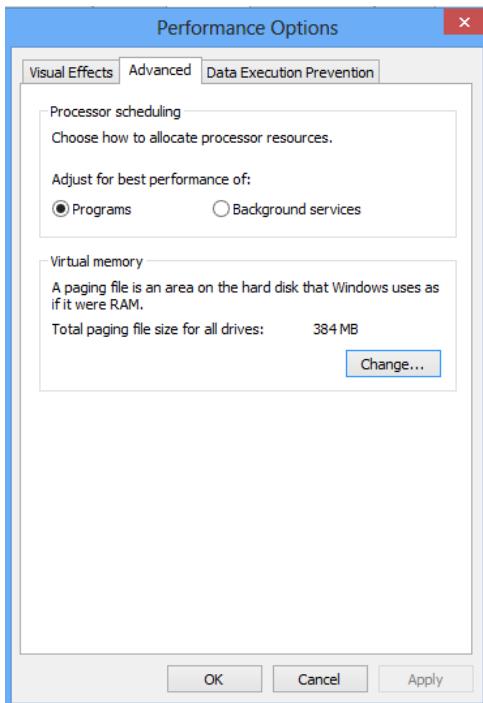
2. Select “**Advanced system settings**” from the System screen:



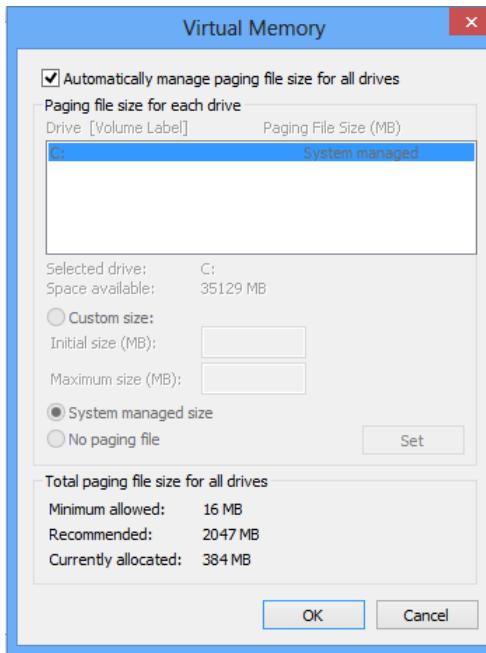
- Select the “**Advanced**” tab:



3. 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”

4. Enter the following for the size selections:

- a. Initial Size – as a good rule of thumb, the size should be equivalent to the amount of memory in the system.
- b. Maximum Size – as a good rule of thumb, the size should be equivalent to 2x the amount of memory in the system.

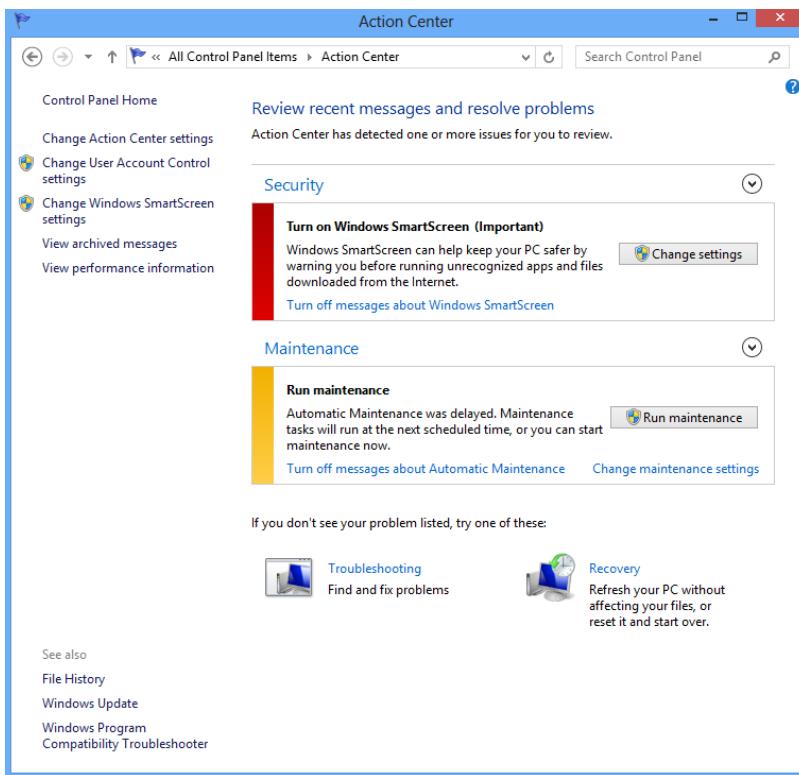
- Click “Ok”, “OK”, and “OK”

5. You will be prompted to reboot your computer.

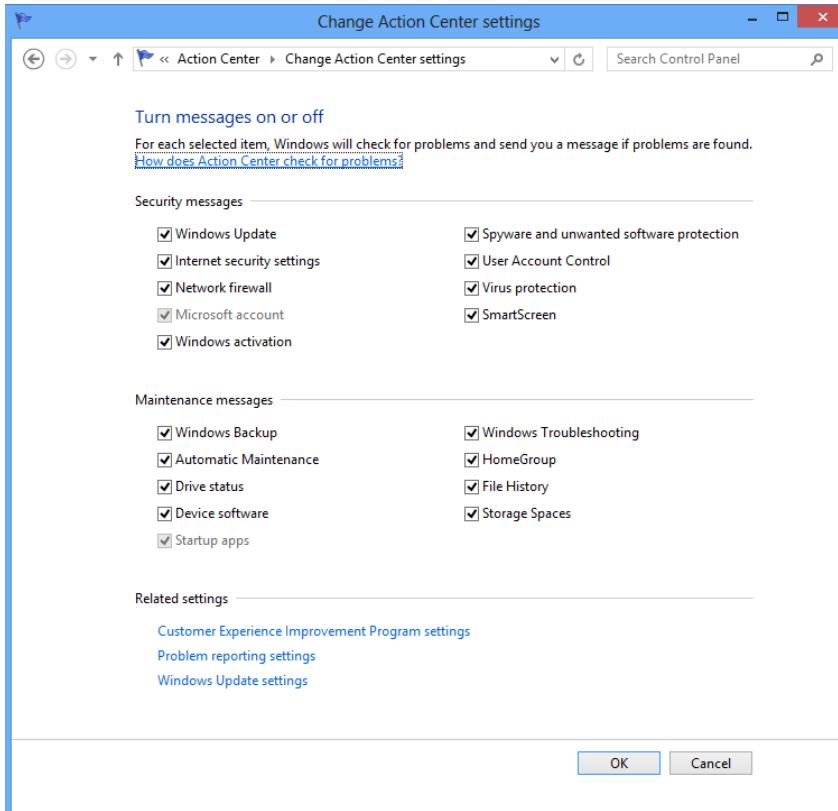
Disabling Windows Error Reporting – Microsoft Windows 8

1. From the desktop hold down the “Windows” key and type “I” to bring up the “Settings” charm, select “Control Panel”.
2. Open the **Action Center**

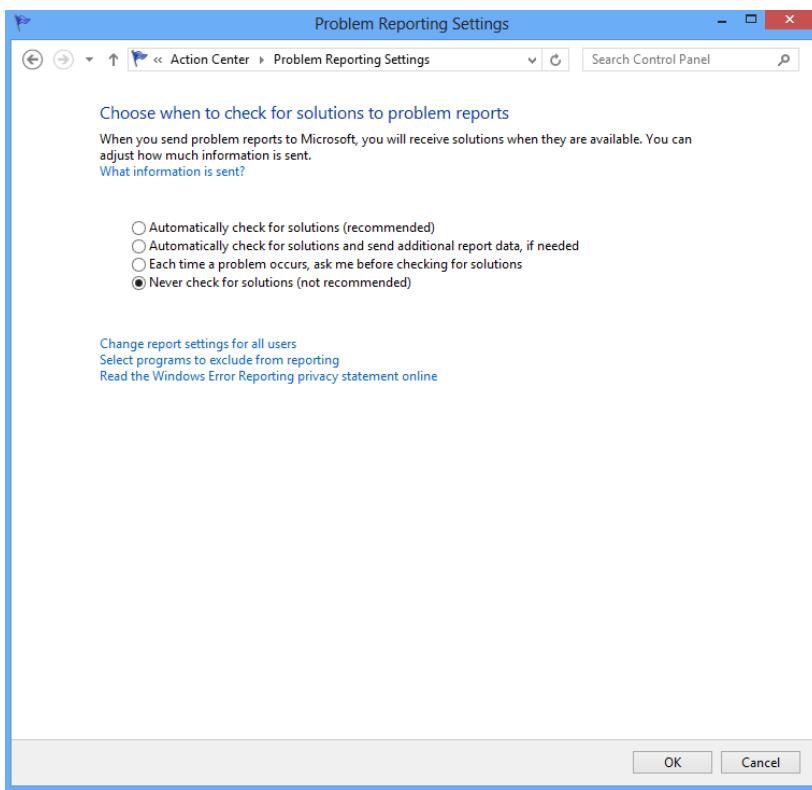
- Select “Change Action Center settings”:



3. Select "Problem reporting settings":



4. Select “Never check for solutions”:



Select “Microsoft Windows 7

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 **Turn off system protection**, click **Apply**, and then click **OK** until you return to the System dialog box.
5. Restart the computer.

Encrypt PageFile.sys

Your hard disk must be formatted using NTFS to perform this operation.

1. Click the **Start** button and enter cmd in the search field.
2. Right-click cmd.exe and select **Run as Administrator**.
3. Enter the command: `fsutil behavior set EncryptPagingFile 1`
To disable encryption, enter 0 instead of 1.
4. Enter the command: `fsutil behavior query EncryptPagingFile`
5. Verify that the command prompt returns: `EncryptPagingFile = 1`

Clear the System PageFile.sys on Shutdown

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

1. Click the **Start** button and enter `regedit` in the search field.
2. Right-click `regedit.exe` 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 **Computer** and select **Properties**.
2. On the **System** dialog box, click **Advanced system settings**.
3. On the **Advanced** tab, click **Settings** for Performance.
4. On the **Advanced** tab, click **Change**.
5. Deselect **Automatically manage page file size for all drives**, select **Custom size**, and set the following fields:
 - a. Initial Size: the amount of Random Access Memory (RAM) available.
 - b. Maximum Size: 2x the amount of RAM.
6. Click **OK** until you return to the **System** dialog box.
7. Restart the computer.

Disable Error Reporting

1. Click the **Start** button, select **Control Panel**, and then click **Action Center**.
2. Click **Change Action Center settings**, then click **Problem reporting settings**.
3. Select **Never check for solutions**, then click **OK**.