# Oracle® Hospitality Suite8 Property

PA-DSS 3.1 Implementation Guide
Release 8.10.0.X
Part Number: E72360-01

May 2016

ORACLE

# Contents

# 1 Preface

This document describes the steps that you must follow in order for your 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 3.1 dated May 2015). You can download the PCI PA-DSS 3.1 can be downloaded 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 (v3.1). 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 Suite8 Property installation to support your PCI DSS compliance efforts.

The PA-DSS Implementation Guide is disseminated to all customers, resellers, and integrators with the application. Oracle will distribute this guide to new customers through the Oracle Help Center at http://docs.oracle.com.

## Revision History

| Date | Description of Change |
|---|---|
| October 06, 2015 | • Initial publication |
| April, 2016 | • Updated |

This PA-DSS Implementation Guide is reviewed and updated on a yearly basis, when there are changes to the underlying application changes, 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 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 Suite8 Property in a PCI DSS compliant manner.

# 2 Executive Summary

Suite8 Property 8.10.0.X has been Payment Application - Data Security Standard (PA-DSS) validated, in accordance with PA-DSS Version 3.1. 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 8.10.0.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:

- 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** | Suite8 Property | | **Payment Application Version** | 8.10.0.X | | |
| **Payment Application Description** | 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. Suite8 Property needs additional payment providers to process online credit card transactions. Suite8 Property offers individual hotels an economic solution that helps efficiently manage their operations. | | | | | |
| **Typical Role of the Payment Application** | Suite8 Property function as on premise based solution for hotels to manage guest information, reservations and check out. | | | | | |
| **Target Market for Payment Application (check all that apply)** | ☐ | Retail | ☐ | Processors | ☐ | Gas/Oil |
| | ☐ | e-Commerce | ☐ | Small/medium merchants | | |
| | ☒ | Others (please specify): Hospitality Solution | | | | |

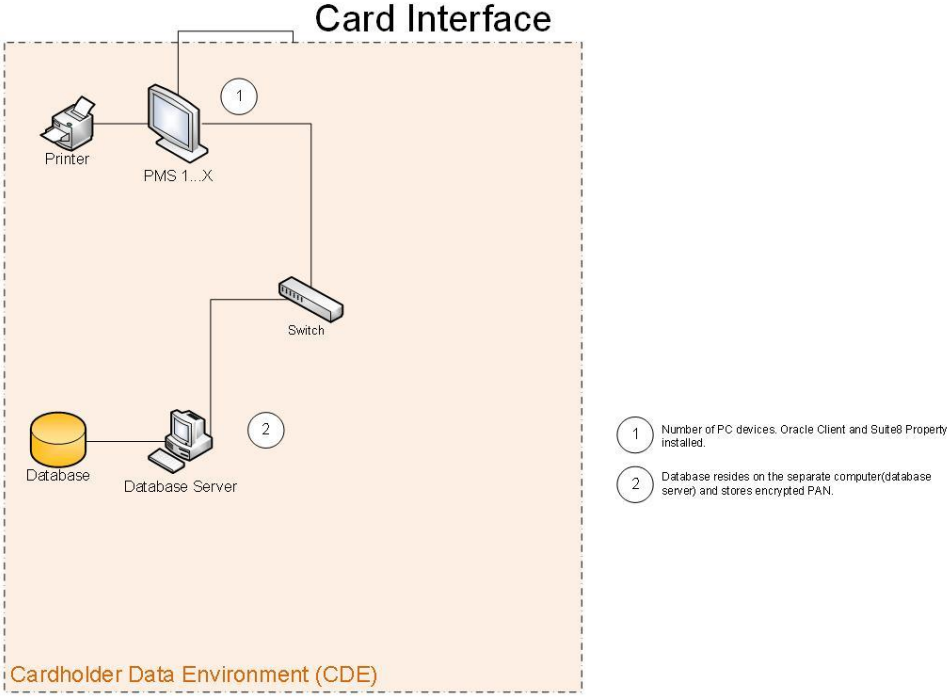
| | | |
|---|---|---|
| **Stored Cardholder Data** | The following is a brief description of files and tables that store cardholder data. | |
| | File or Table Name | Description of Stored Cardholder Data |
| | Database table XCCS | Primary Account Number (PAN)<br>Cardholder Name<br>Expiration Date |
| | **Individual access to cardholder data is logged as follows:**<br>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 'XXXXXXXXXXXXXX9999'. | |
| **Components of the Payment Application** | The following are the application-vendor-developed components which comprise the payment application: | |
| | • Fideliov8.exe: Primary and only PMS application. Manage all functionality.<br>• Several additional dll's used from fideliov8.exe | |
| **Required Third Party Payment Application Software** | The following are additional third party payment application components required by the payment application: | |
| | No 3rd party payment applications are required by the payment application. | |
| **Supported Database Software** | The following are database management systems supported by the payment application: | |
| | • Oracle Database 11.2.0.4<br>• Oracle Database 12.1.0.2 | |

<table>
<tr><td rowspan="2">Other Required Third Party Software</td><td colspan="6">The following are other third party software components required by the payment application:</td></tr>
<tr><td colspan="6">• Oracle Database Client 11.2.0.4 or<br>• Oracle Database Client 12.1.0.2 in relation to the used database version<br>• Crystal Reports Runtime 12.2.0 to run Crystal reports</td></tr>
<tr><td rowspan="2">Supported Operating System(s)</td><td colspan="6">The following are Operating Systems supported or required by the payment application:</td></tr>
<tr><td colspan="6">Latest Supported Versions of:<br>• Windows 7 SP1<br>• Windows 8</td></tr>
<tr><td>Payment Application Authentication</td><td colspan="6">• The application using Username/password authentication.<br>• The authentication can be done either using Suite 8 Password Management or external LDAP server<br>• In case Suite 8 Password Management is used, only PBKDF2 hash of the password is stored.<br>• Stored passwords are rendered unreadable using a strong, one-way cryptographic algorithm, based on approved standards.<br>• A unique input variable is concatenated with each password before the cryptographic algorithm is applied</td></tr>
<tr><td>Payment Application Encryption</td><td colspan="6">• Encrypted algorithms use AES256.<br>• Oracle Transparent Data Encryption (Oracle Wallet) is used additional for the sensitive data protection</td></tr>
<tr><td rowspan="4">Supported Payment Application Functionality</td><td>☐</td><td>Automated Fuel Dispenser</td><td>☐</td><td>POS Kiosk</td><td>☐</td><td>Payment Gateway/ Switch</td></tr>
<tr><td>☐</td><td>Card-Not-Present</td><td>☐</td><td>POS Specialized</td><td>☐</td><td>Payment Middleware</td></tr>
<tr><td>☐</td><td>POS Admin</td><td>☐</td><td>POS Suite/General</td><td>☐</td><td>Payment Module</td></tr>
<tr><td>☐</td><td>POS Face-to-Face/POI</td><td>☐</td><td>Payment Back Office</td><td>☐</td><td>Shopping Card & Store Front</td></tr>
<tr><td>Payment Processing Connections</td><td colspan="6">Suite8 Property does not authorize credit/debit card transaction without external provider.</td></tr>
<tr><td>Description of Listing Versioning Methodology</td><td colspan="6">Suite8 Property versioning has three levels, Major, Minor, and Build: <Major>.<Minor>.<Build><br>• Major changes include significant changes to the application and would have an impact on PA-DSS requirements.</td></tr>
</table>

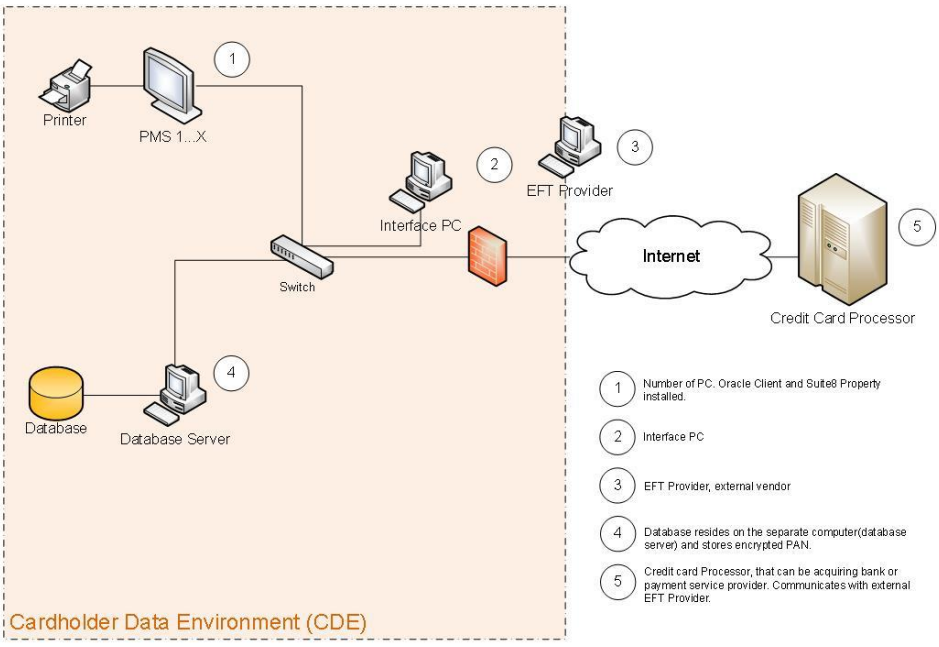
| | |
|---|---|
| | • Minor changes include small changes such as minor enhancements and may or may not have an impact on PA-DSS requirements.<br>• Build changes include bug fixes or rollups and would have no negative impact on PA-DSS requirements and are indicated by the WILDCARD (X).<br>Based on the above versioning methodology the application version being listed with the PCI SSC is: 3.1.X. |

# Typical Network Implementation

Suite8 Property Network Diagram without Credit Card Interface

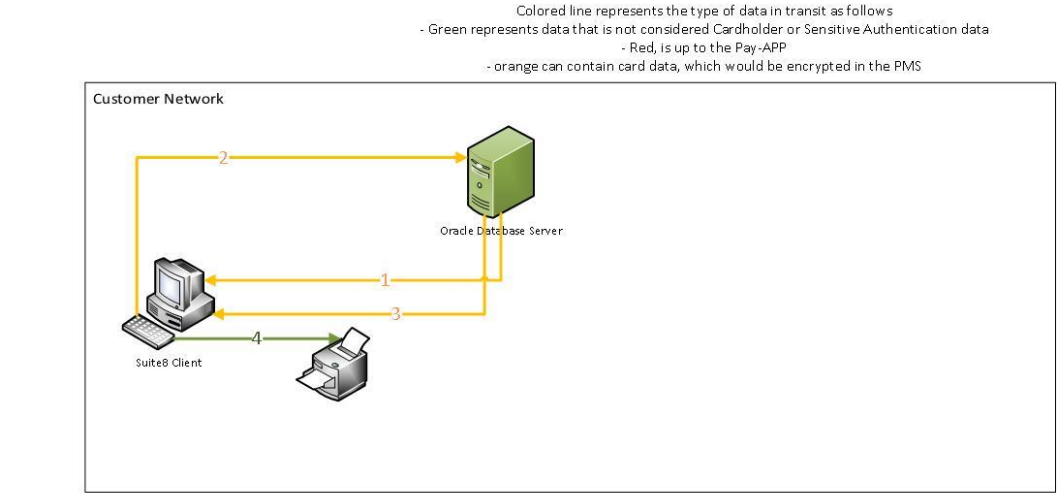



Suite8 Property Network Diagram with Credit Card Interface



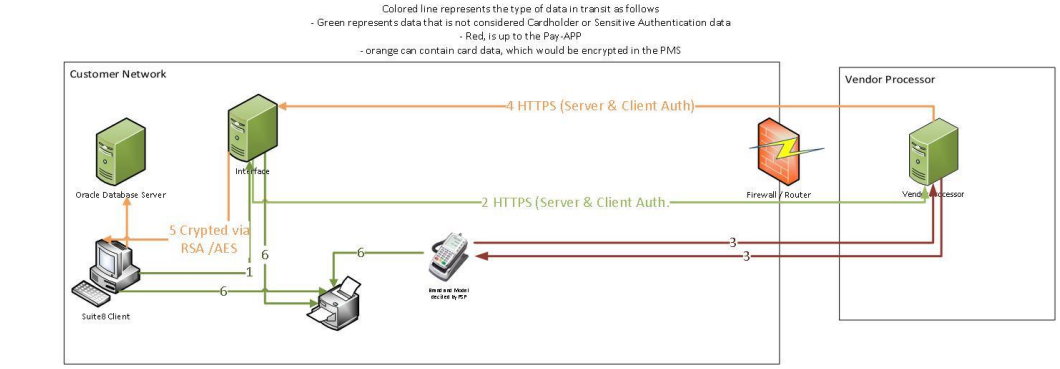
# Credit/Debit Cardholder Dataflow Diagram

## Oracle Hospitality Suite8 Property without CC Interface



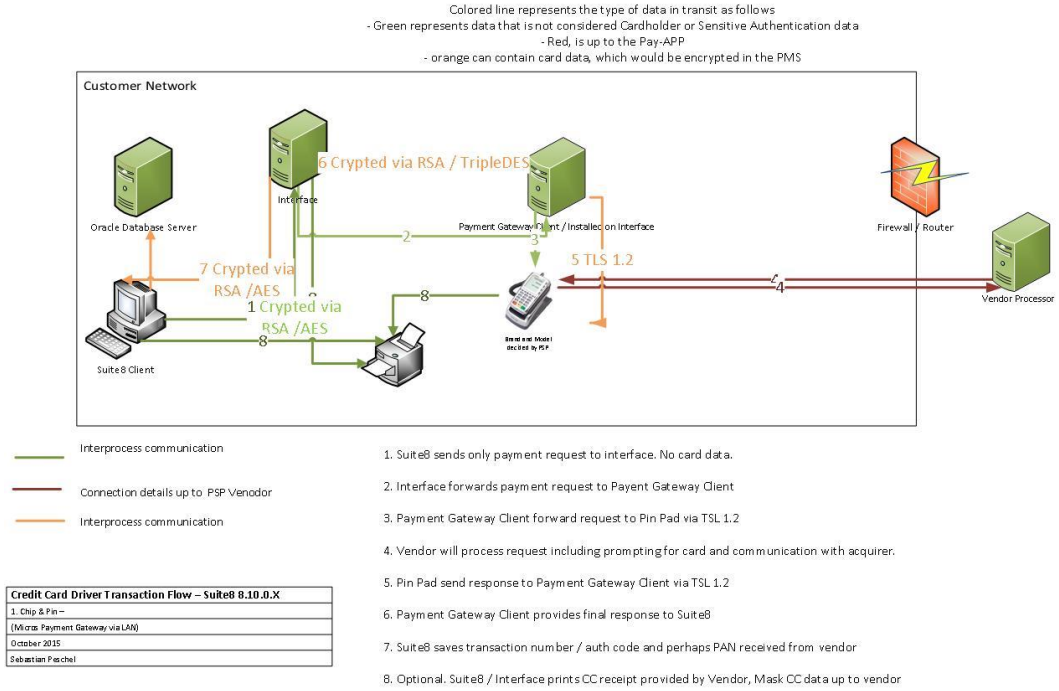

| Credit Card Data – Suite8 8.10.0.X |
|---|
| No Interface |
| |
| October 2015 |
| Sebastian Peschel |

## Oracle Hospitality Suite8 Property chip&pin SixCards HTTPS




| Credit Card Driver Transaction Flow – Suite8 8.10.0.X |
|---|
| 1: Chip & Pin – |
| (SixCards via HTTPS) |
| June 17th 2015 |
| Sebastian Peschel |

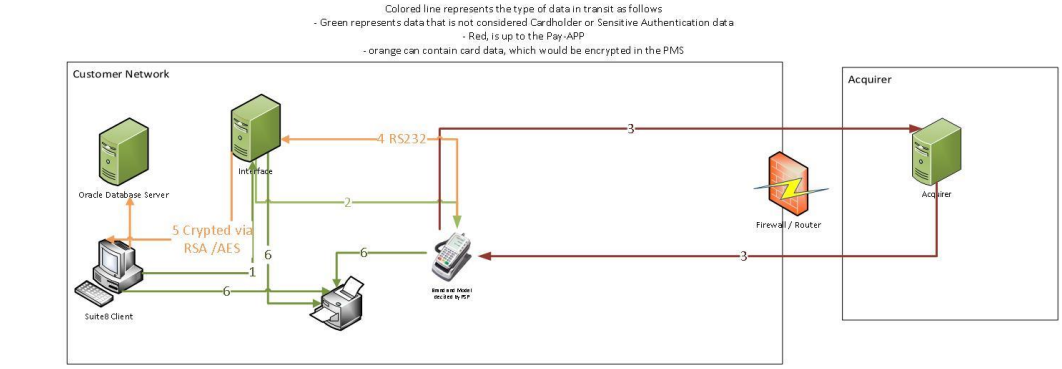
## Oracle Hospitality Suite8 Property chip&pin MPG Lan




1. Suite8 sends only payment request to interface. No card data.
2. Interface forwards payment request to Payent 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

| Credit Card Driver Transaction Flow – Suite8 8.10.0.X |
|---|
| 1. Chip & Pin – |
| (Micros Payment Gateway via LAN) |
| October 2015 |
| Sebastian Peschel |

## Oracle Hospitality Suite8 Property chip&pin NETS Manison SteriaPay




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 aquirer.
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

| Credit Card Driver Transaction Flow – Suite8 8.10.0.X |
|---|
| 1. Chip & Pin – |
| (Manison, NETS, SteriaPAY, ZVT) |
| October 2015 |
| Sebastian Peschel |

## Difference between PCI Compliance and PA-DSS Validation

As the software and payment application developer, our responsibility is to be PA-DSS validated. We have tested, assessed, and validated the payment application against PA-DSS Version 3.1 with our independent assessment firm (PAQSA) to ensure that our platform conforms to industry best practices when handling, managing, and storing payment-related information.

The PA-DSS Validation is intended to ensure that 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.

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 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

# 3 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 Suite8 Property did not store SAD. Therefore, there is no need for secure deletion of this historical data by the application as required by PA-DSS v3.1.

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

Oracle Hospitality does not store Sensitive Authentication Data (SAD) 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 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

## Secure Deletion of Cardholder Data (PA-DSS 2.1)

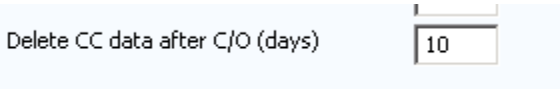
The following guidelines must be followed when dealing with Cardholder Data (Primary Account Number (PAN); Cardholder Name; Expiration Date; or Service Code):

- 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:
  - 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




- 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**.

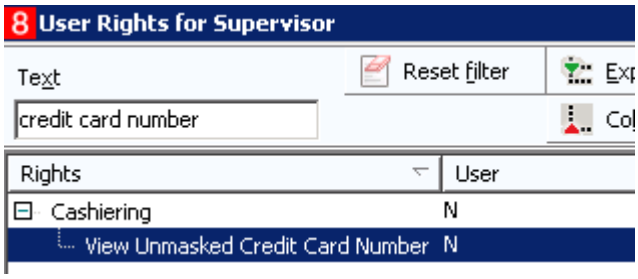
## All PAN is Masked by Default (PA-DSS 2.2)

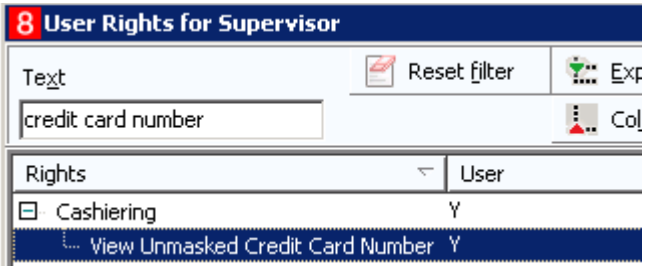
Suite8 Property masks all PAN by default in all locations that display PAN (screens, paper receipts, printouts, reports, etc. by displaying only the last four digits and the others are masked The payment application displays PAN in the following locations.

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

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 ->



## 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 v3.1.

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

- You must restrict access to encryption keys to the fewest number of custodians necessary.
- You must store encryption keys securely in the fewest possible locations and forms.
- Key custodians must sign the Key Custodian form provided in Appendix B to acknowledge that they understand and accept their key custodian responsibilities

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.
- 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.

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

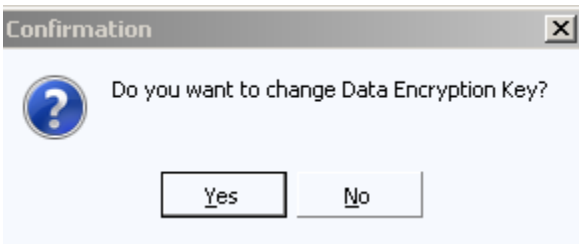
Suite8 Property has the following versions that previously encrypted cardholder data:

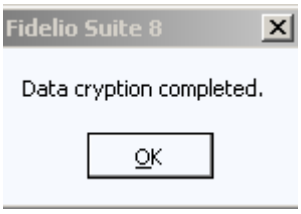
- 8.7.X
- 8.8.X
- 8.9.X

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 (PA-DSS 3.1 and 3.2)

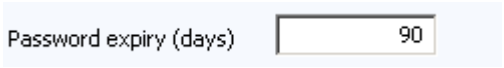
The PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by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

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 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 the following method to authenticate users: (PCI DSS 8.2 / PA-DSS 3.1.4)
    a. Something you know, such as a password or passphrase
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 that passwords are configured to be at least 7 characters and include 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)

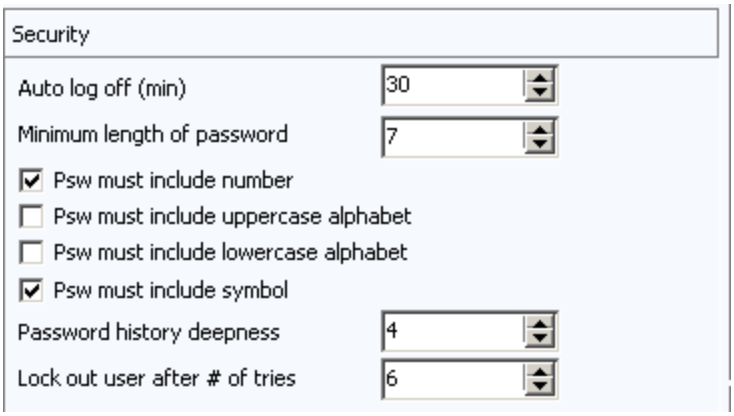
8. The payment application keeps password history and requires that a new password is different than any of the last four passwords used (PCI DSS 8.2.5 / PA-DSS 3.1.8)
9. The payment application limits repeated access attempts by locking out the user account after not more than six logon attempts (PCI 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 a Suite8 Property user. Do not change the default password expiry days to more than 90 per user:




Before validate and proof the default Suite8 Property settings:

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




- 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.

Stored passwords are rendered unreadable using a strong, one-way cryptographic algorithm, based on approved standards.

A unique input variable is concatenated with each password before the cryptographic algorithm is applied.

## 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 and 4.4.b)

**4.1.b**: Suite8 Property logging is always turned on and cannot be deactivated per PCI DSS 10.2 and 10.:

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*

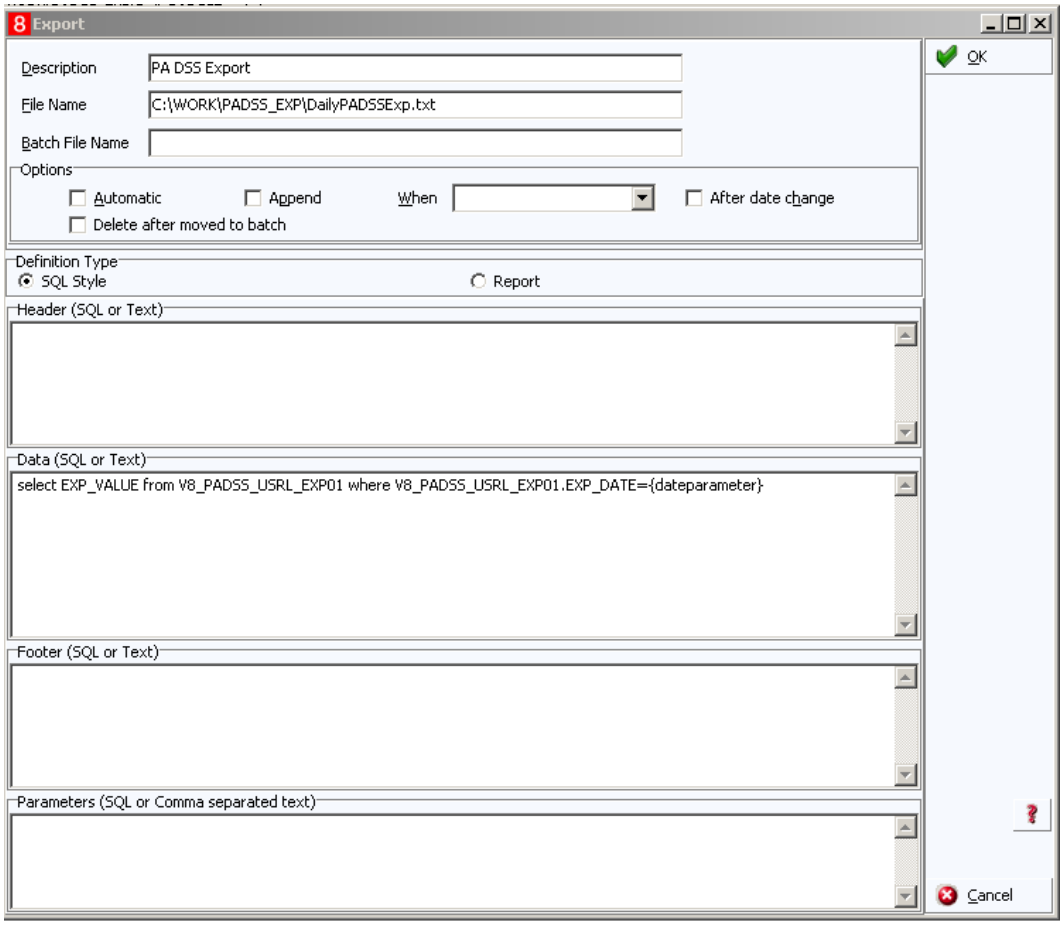
*10.3.6 Identity or name of affected data, system component, or resource.*

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

**4.4.b**: 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



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

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:

**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.

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

Suite8 Property does not require the use of any insecure services or protocols. Here are the services and protocols that 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.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. The means one of the following three authentication methods must be used:

Oracle Hospitality ONLY support by using Bomgar 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 link which was provided by the support agent via mail.

Instruction how to use Bomgar in a secure manner can be found in ***EAME Bomgar Customer Guide.pdf***

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

We deliver software and/or updates via remote access to customer networks using 'Bomgar' remote access.

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.*

Use a personal firewall product if computer is connected via VPN or other high-speed connection, to secure these "always-on" connections, per PCI Data Security Standard 1.3.10.

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

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

Suite8 Property Support only use Bomgar as a connection tool. A client needs to acknowledge each and every connection manually by selecting a link which was provided by the support agent via mail.

Instruction how to use Bomgar in a secure manner can be found in EAME Bomgar Customer Guide.pdf

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

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 Suite8 Property.

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

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 (PA-DSS 12.1)

Suite8 Property 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.

## 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 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

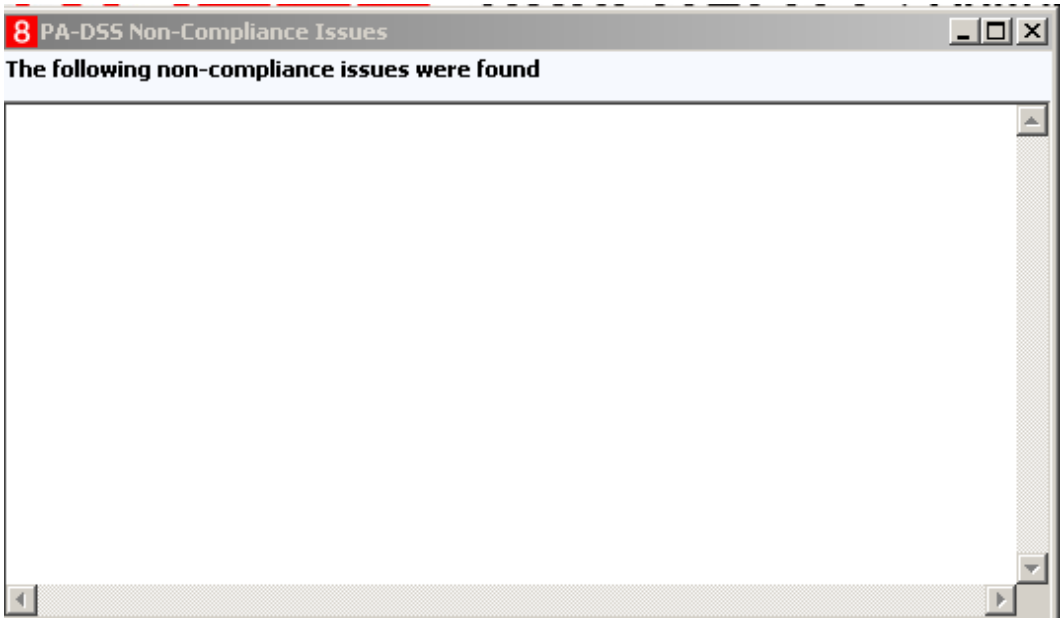
Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2
- Microsoft Windows 8
- 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 11.2.04 or Oracle Database 12.2.0.2

## Payment Application Initial Setup & Configuration

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

Help -> Check PA DSS Compliance




Any non-compliance issues must be resolved.

# 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

## Microsoft Windows 8

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

### Disable System Management of PageFile.sys

1. Right-click **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 and enter `Control Panel`.
2. Click **Control Panel**, then click **Action Center**.
3. Click **Change Action Center settings**, then click **Problem reporting settings**.
4. Select **Never check for solutions**, then click **OK**.

## 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**.

# Appendix B Encryption Key Custodian

<Company Logo Here>

<Company Address Here>

## ENCRYPTION KEY CUSTODIAN
### CONFIDENTIALITY STATEMENT

By signing this acknowledgement, I, _____, in my role as <enter role name here>, represent and warrant the following:

1. I understand that as an encryption key custodian for <Company Name>'s credit card processing software package(s), I may have access to certain information which is non-public, confidential, and/or proprietary in nature; and
2. I acknowledge and agree that any such information is highly sensitive and is required to be treated in the strictest confidence; and
3. I acknowledge and agree that any confidential information I obtain in the course of my performance as an encryption key custodian shall remain confidential and shall not be disclosed by me to anyone.

Any questions concerning my confidentiality obligation or confidential matters shall be raised with my supervisor or with <Company Name> management.

I understand and agree to the foregoing.

Sign Name: _____

Print Name: _____

Date: _____