Oracle® Hospitality Oracle Hospitality eCommerce Integration Cloud

PA-DSS 3.1 Implementation Guide
Release 18.1
E87988-01

March 2018

ORACLE

Contents

Preface

This document describes the steps that you must follow in order for the Oracle Hospitality eCommerce Integration Cloud Service (eCommerce Integration Cloud) 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 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 (v3.1). 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 eCommerce Integration Cloud Service installation to support your PCI DSS compliance efforts.

Revision History

Date	Description of Change
March 2018	• Initial publication

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 Oracle Hospitality eCommerce Integration Cloud'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 with 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 eCommerce Integration Cloud in a PCI DSS compliant manner.

1 Executive Summary

The Oracle Hospitality eCommerce Integration Cloud Service version 18.1 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, Suite 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 Oracle Hospitality eCommerce Integration Cloud Version 18.1 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/

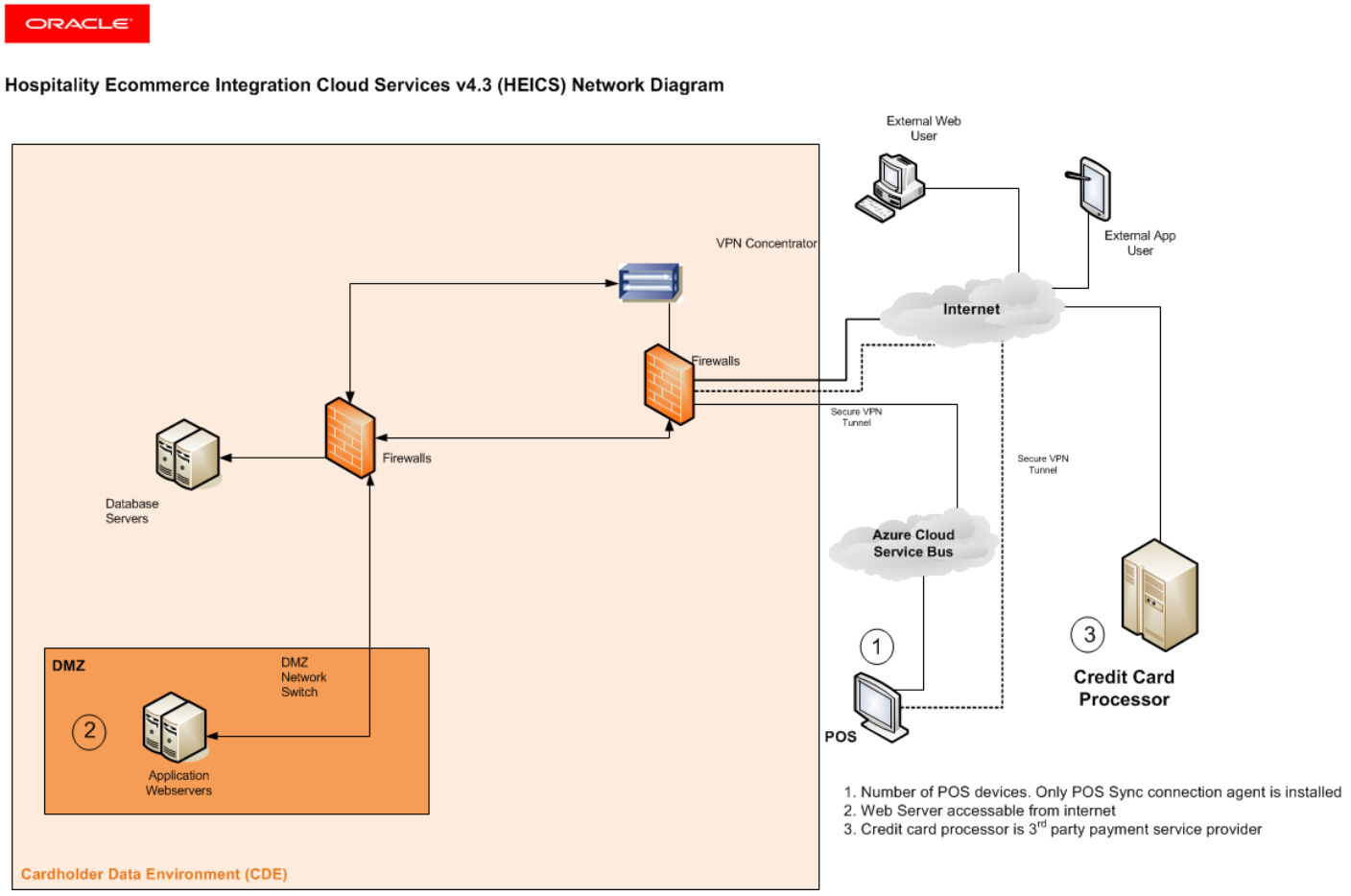
Payment Application Summary

<table>
<tr><td>Payment Application Name</td><td colspan="2">Oracle Hospitality eCommerce Integration Cloud Payment Gateway (OHEICS)</td><td>Payment Application Version</td><td colspan="2">18.1</td></tr>
<tr><td>Payment Application Description</td><td colspan="5">eCommerce Integration Cloud is an eCommerce framework that supports all sectors of the foodservice and hospitality markets.</td></tr>
<tr><td>Typical Role of the Payment Application</td><td colspan="5">Typically integrates with: a Point of Sale (POS) system(s) in a quick service restaurant, third party mobile application, or a website.</td></tr>
<tr><td rowspan="3">Target Market for Payment Application (check all that apply)</td><td>☒</td><td>Quick Service Restaurant</td><td>☒</td><td>Hotels</td><td>☒</td><td>Stadiums</td></tr>
<tr><td>☒</td><td>Casinos</td><td>☒</td><td colspan="2">Casual Dining</td></tr>
<tr><td>☒</td><td colspan="4">Others: Anyone who sells a food, beverage or retail item</td></tr>
<tr><td rowspan="4">Stored Cardholder Data</td><td colspan="5">The following is a brief description of files and tables that store cardholder data.</td></tr>
<tr><td colspan="3">File or Table Name</td><td colspan="2">Description of Stored Cardholder Data</td></tr>
<tr><td colspan="3">The following database tables and file store cardholder data:
<code>[dbo].[OrderPayment]</code>
<code>[dbo.][orderpaymentdetails]</code>
<code><last transaction logfile></code></td><td colspan="2">Cardholder details
Cardholder details
Last 4 digits of PAN</td></tr>
<tr><td colspan="5">Individual access to cardholder data is logged as follows:
Clear-text PAN is never logged by the payment application.</td></tr>
<tr><td rowspan="2">Components of the Payment Application</td><td colspan="5">The following are the application-vendor-developed components which comprise the payment application.</td></tr>
<tr><td colspan="5">eCommerce Integration Cloud Payment Gateway</td></tr>
<tr><td rowspan="2">Required Third Party Payment Application Software</td><td colspan="5">The following are additional third party payment application components required by the payment application:</td></tr>
<tr><td colspan="5">None</td></tr>
<tr><td rowspan="2">Supported Database Software</td><td colspan="5">The following are database management systems supported by the payment application:</td></tr>
<tr><td colspan="5">Oracle 12c, MS SQL Server 2008, 2012</td></tr>
<tr><td></td><td colspan="5">The following are other third party software components required by the payment application:</td></tr>
</table>

<table>
<tr><td>Other Required Third Party Software</td><td colspan="6">None</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">None</td></tr>
<tr><td>Payment Application Authentication</td><td colspan="6">Refer to the Credit/ Debit Cardholder Dataflow Diagram in the section below.</td></tr>
<tr><td>Payment Application Encryption</td><td colspan="6">Refer to the Cardholder Data Encryption & Key Management (PA-DSS 2.3, 2.4, and 2.5) section.</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">Refer to the Credit/ Debit Cardholder Dataflow Diagram in the section below.</td></tr>
<tr><td>Description of Listing Versioning Methodology</td><td colspan="6">The Oracle Hospitality eCommerce Integration Cloud versioning consists of three levels, Major, Minor, & Maintenance Release (MR): <Major>.<Minor>.<MR>.<Maintenance>
• Major changes include significant changes to the application and would have an impact on PA-DSS requirements.
• Minor changes include small changes such as minor enhancements and may or may not have an impact on PA-DSS requirements.
• Maintenance release changes include bug fixes or rollups and would have no negative impact on PA-DSS requirements and are indicated by the MR (X). Based on the above versioning methodology the application version being listed with the PCI SSC is: 18.1.</td></tr>
</table>

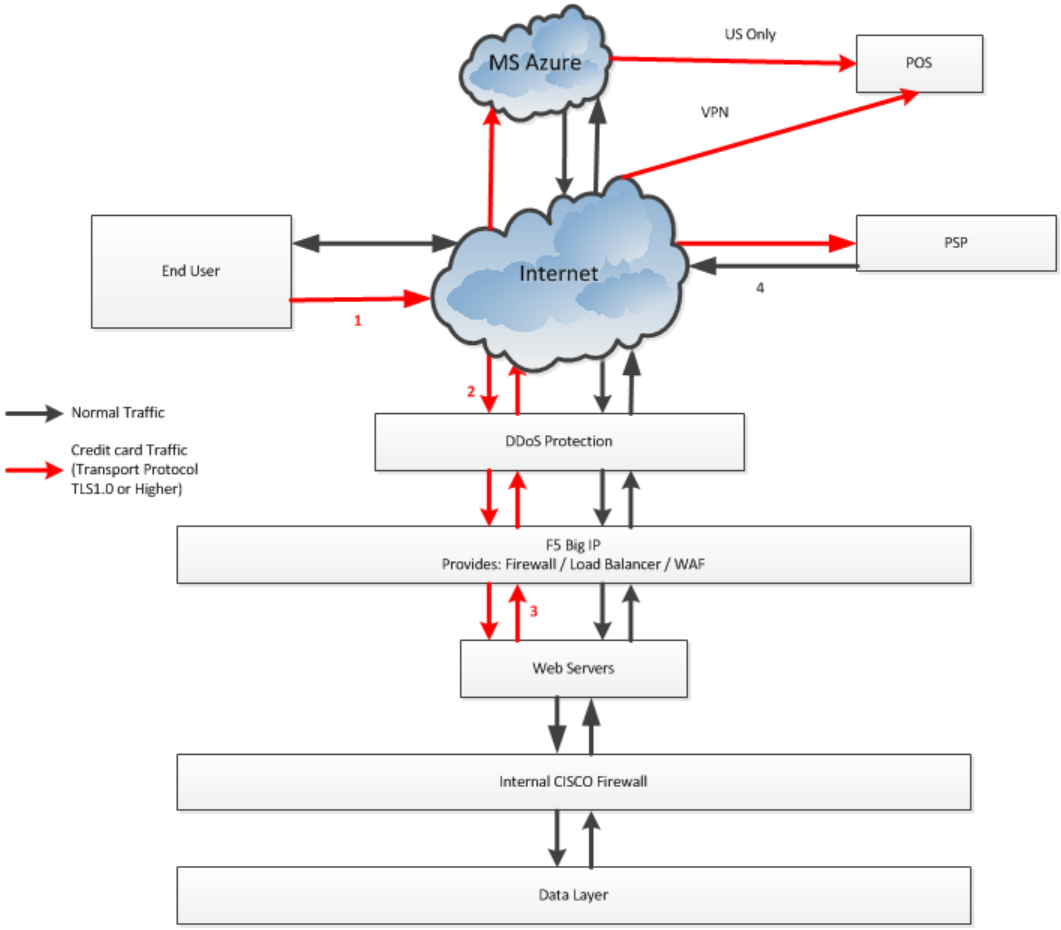
Typical Network Implementation

Below is an example network diagram of the eCommerce Integration Cloud Service.



Credit/Debit Cardholder Dataflow Diagram

Here is an example of a Data Flow diagram.



1. Web user enters card details in browser
2. Browser sends to the web server using HTTPS encrypted connection (TLS1.0 and above)
3. Application calls the PSP web service using an HTTPS encrypted connection
4. PSP sends back response (Auth/Reject)
5. All workflows are for the Sales process

NB:- on success response from PSP, last four digits of PAN are stored in DB.

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 Oracle Hospitality eCommerce Integration Cloud 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

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

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

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

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4)

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

There are no commissioned versions of the Oracle Hospitality eCommerce Integration Cloud (using the payment gateway) that 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 including the Primary Account Number (PAN), Cardholder Name, Expiration Date, or the Service Code:

- A customer defined retention period must be defined with a justification relating to business, legal and/ or regulatory reason.
- Cardholder data exceeding the customer-defined retention period or when no longer required for legal, regulatory, or business purposes must be securely deleted.
- To securely delete Cardholder Data you must configure a scheduled job within MS SQL Server® to automatically securely delete Cardholder Data by:
    - Accessing the Microsoft SQL Server® Management Studio.
    - Go to the **SQL Server Agent** section, open the **Jobs** folder and select the **Purge Payments** job and name the task accordingly.
    - Go to the **Select a Page** header, select the **Schedules** page and add the date and time for the desired cardholder data purge schedule to run.

      Note: If more than one database requires database purging, you must create a purge job for each database.
- Cardholder Data must be securely deleted from the eCommerce Integration Cloud Service application:

  This operation will purge cardholder data for *ALL* Clients.

    1. Login as System Administrator and go to the Administration **Tools** dashboard.
    2. Go to the **Purge Payment**s header, select the **Purge** button.
- 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)

The application does not allow unmasked credit card data to display on customer receipts, with the exception of the last four digits of the Primary Account Numbers (PAN), in order to comply with the PCI Data Security Standard requirement.

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

The application uses Advanced Encryption Standard (AES) Rijndael 256-bit to encrypt credit card data and complies with the PCI Data Standard.

Automatic key encryption rotates the encryption key each time the credit card data is encrypted. When the credit card encryption is requested a new encryption key automatically generates to encrypt the data. After the encryption is complete, the encryption key is not persisted anywhere and another new key generates when the next credit card data encryption request is received. In this way the encryption key is automatically rotated with every new credit card data encryption request. The key is never stored anywhere in the database or on the hard disk; and there is no need for manual key rotation.

Removal of Historical Cryptographic Material (PA-DSS 2.6)

Previous versions of this software application encrypted cardholder data; all cryptographic material (encryption keys and encrypted cardholder data) must be securely deleted. This historical data must be securely removed from the database.

Oracle Hospitality eCommerce Integration Cloud has the following versions that previously encrypted cardholder data:

- Any version prior to 3.0
- Version 3.0

The release of version 18.1 introduces a new Key Management scheme then the previous version 3.0 of the application. When upgrading from any version prior to version 3.0 to the new version 18.1, all previous cardholder data must be purged and the old encryption key must be securely removed from the database.

To remove previously saved encryption keys, use the Purge utility in the application **Dashboard** and follow these steps:

1. Log in as the System Administrator and go to the **Administration Tools**.
2. Go to the **Client** section and select the **Delete History of Clientpassword** option to remove the previous encryption keys.

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.

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job. This ensures access to sensitive information is restricted, password protected, and based on a need-to-know basis.
To maintain a secure environment you must:

1. Create restricted access to sensitive data based on the user's job function and role.
2. Restrict access to customer passwords by resellers or integration specialists.
3. Use strong application and system passwords. Customers, resellers, and integration specialist must always create PCI DSS-compliant complex passwords to access the payment application.

Creating New Users and Passwords

To create a new user and assign a password:

1. Login as the System Administrator and go to the **Administration Tools.**
2. Select **Create User**, and in the Security section enter the User's information (including the User's New Password), select **Confirm Password**, and then select **Save**.
   All Passwords must contain at least:
   - Eight characters

- One number
- One upper case and one lower case letter
- One non-alphanumeric character

Assign Unique User IDs

You must assign a unique user ID to each person with computer access. Assigning a unique identification (ID) to each person with access ensures that each individual is accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to known and authorized users.

Oracle Hospitality recognizes the importance of establishing unique IDs for each person with computer access. No two users can have the same ID, and each person's activities can be traced, provided the client site maintains proper configuration and adheres to privilege level restrictions based on a need-to-know basis. While Oracle Hospitality makes every possible effort to conform to Requirement 8 of the PCI Data Security Standard, certain parameters, including proper user authentication, remote network access, and password management for non-consumer users and administrators, for all system components, depend on site specific protocol and practices. To ensure strict access control of the application, always assign unique usernames and complex passwords to each account. Oracle mandates applying these guidelines to not only application passwords, but also to the system passwords including your Windows® password. Oracle Hospitality advises users to control access, via unique usernames and PCI-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

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 at least one of the following three methods to authenticate users: (PCI DSS 8.2 / PA-DSS 3.1.4)
    a. Something you know, such as a password or passphrase
    b. Something you have, such as a token device or smart card
    c. Something you are, such as a biometric
5. The payment application must NOT require or use any group, shared, or generic accounts and passwords (PCI DSS 8.5 / PA-DSS 3.1.5)

6. The payment application requires passwords must to be at least 7 characters and includes both numeric and alphabetic characters (PCI DSS 8.2.3 / PA-DSS 3.1.6)
7. The payment application requires passwords to be changed at least every 90 days (PCI DSS 8.2.4 / PA-DSS 3.1.7)
8. The payment application keeps password history and requires that a new password is different than any of the last four passwords used (PCI DSS 8.2.5 / PA-DSS 3.1.8)
9. The payment application limits repeated access attempts by locking out the user account after not more than six logon attempts (PCI DSS 8.1.6 / PA-DSS 3.1.9)
10. The payment application sets the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (PCI DSS 8.1.7 / PA-DSS 3.1.10)
11. The payment application requires the user to re-authenticate to re-activate the session if the application session has been idle for more than 15 minutes. (PCI DSS 8.1.8 / PA-DSS 3.1.11)

Properly Train and Monitor Admin Personnel

It is your responsibility to institute proper personnel management techniques for allowing system administration 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 often 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.

System administrators cannot see payment information in the eCommerce Integration Cloud Service tools and database only masked or encrypted data appears in the application.

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

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

An automated audit trail must be implemented for all system components to reconstruct the following events:

- All actions taken by any individual with root or administrative privileges.
- Access to all audit trails.
- Invalid logical access attempts.
- Use of identification and authentication mechanisms.
- Initialization of the audit logs.
- Creation and deletion of system-level objects.
- Record at least the following audit trail entries for all system components for each event:
- User identification.
- Type of event.
- Date and time.
- Success or failure indication.

- Origination of event.
- Identity or name of affected data, system component, or resource.

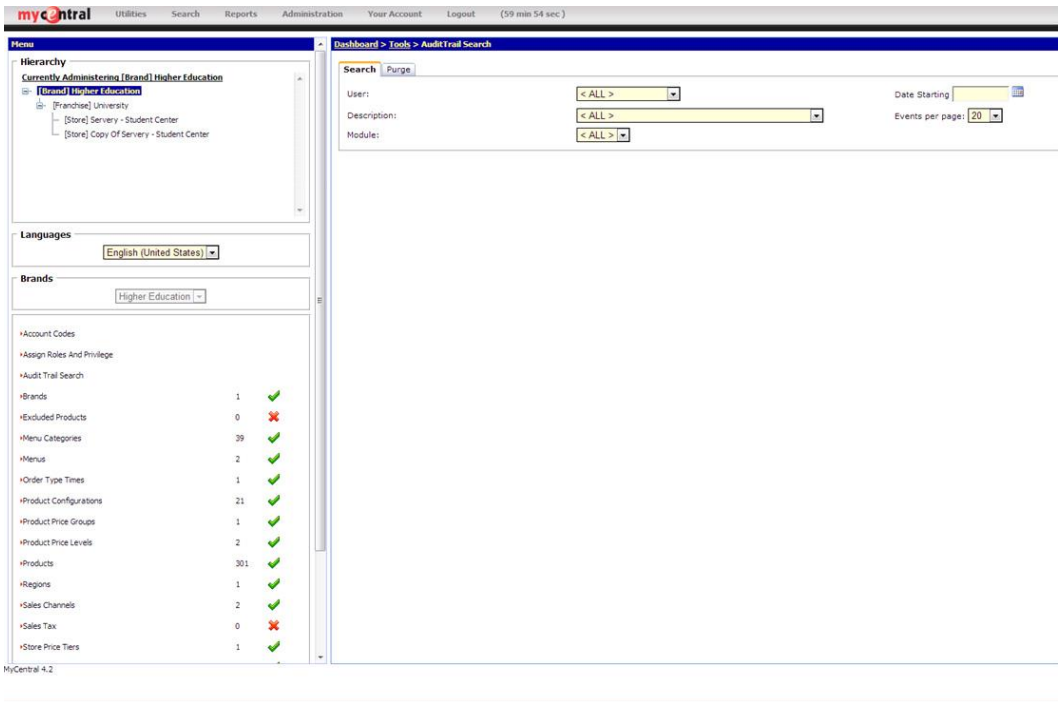
The advent of open database structure means that anyone with system level access to the database server (Oracle 12c, SQL server 2008 or 2012) has access to system components covered under this requirement, and thus would require logging of user access and activity as detailed in Requirement 10 of the PCI Data Security Standard.

Audit Trail

The application provides a comprehensive Audit Trail logging utility in the Tools dashboard. Using the Audit Trail log system administrators with the privilege can track specific user activities in the application.

Using the Audit Trail filter you can search by:

- **User**
- **Description** of the change
- **Module** in which a change was made
- A **Date Starting** and **Date Ending** range option



When an Audit Trail search is initiated with no filters applied, all of the user and system activity appears.

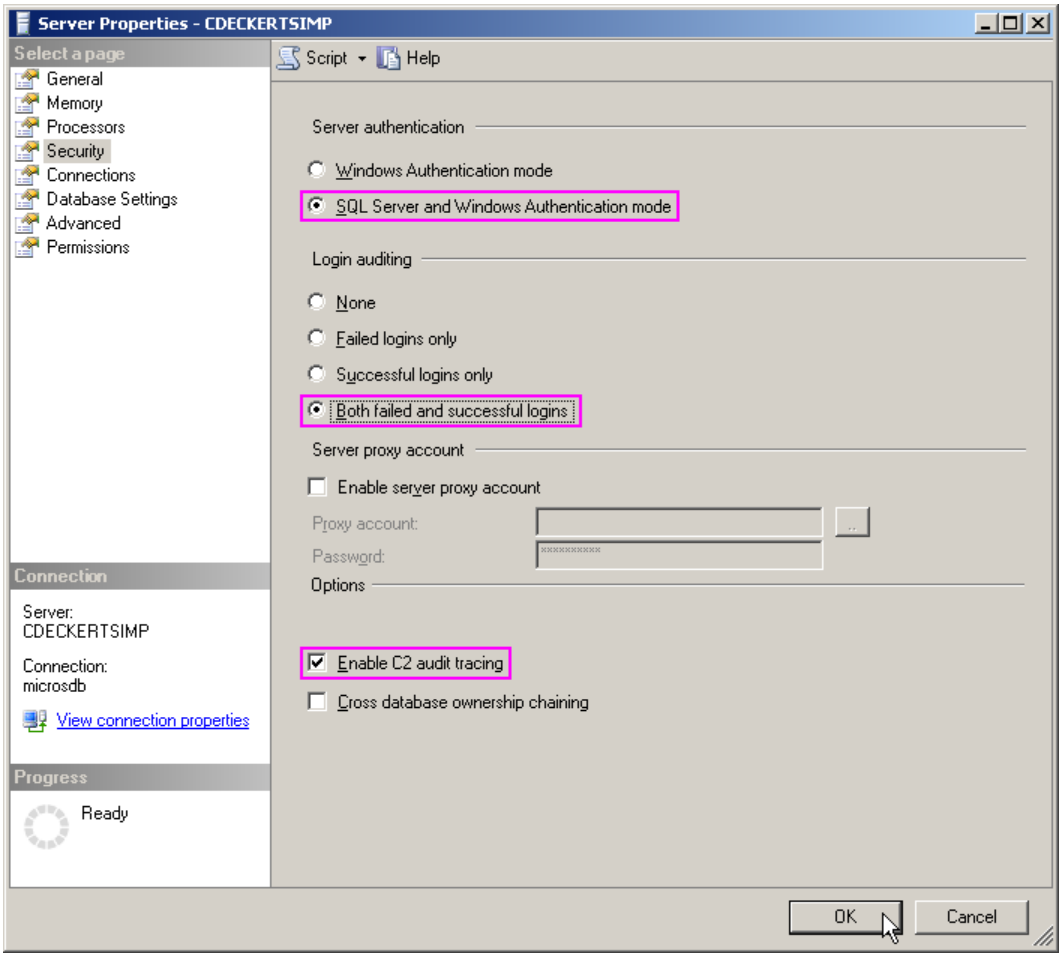
To use the Audit Trail logging feature you must have the privilege assigned to your user name. A system administrator can configure a user's roles and assign the Audit Trail privileges to specific user roles. This provides strict control of access to the Audit Trail logging tool. The Audit Trail privileges provide the ability to view and delete Audit Trail entries.

For customers interested in implementing more extensive auditing within Microsoft SQL Server®, see below:

For information on C2 audit tracing for MS SQL Server® 2008, go to the following link from the Microsoft Developer Network website: https://msdn.microsoft.com/en-us/en%20us/library/ms187634%28v=SQL.100%29.aspx. Complete the following steps to enable C2 audit tracing.

Microsoft® SQL Server

1. Go to the Microsoft SQL Server® Management Studio, select and highlight the specific server.
2. Right-click the server and select **Properties**.
3. Select and highlight **Security**.
4. Select the following options as listed below:



a. In the **Server Authentication** section, select the **SQL Server and Windows Authentication mode** option.
b. In the **Login auditing** section, select the **Both failed and successful logins** option.
c. In the **Options** section, select the **Enable C2 audit tracing** checkbox.
d. Click **OK.**

For guidance on auditing when administering an Oracle 12c Database, refer to the *Oracle 12c Database Administration Security Guide*.

In accordance with the PCI Data Security Standard, Oracle Hospitality mandates activity logging on the database server for Oracle Hospitality related actions taken by any individual with root or administrative privileges via enabling the audit trail feature. Always enable audit logs for systems that store, process, and transmit cardholder data. To ensure your site is in compliance with Requirement 10 of The PCI Data Security Standard, "Track and monitor all access to network resources and cardholder data," consult the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

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

Oracle Hospitality eCommerce Integration Cloud 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.

Refer to the *Oracle MICROS Hardware Wireless Networking Best Practices Guide* for more information. This document is located on the Oracle Help Center at http:/ / docs.oracle.com/ cd/ E81005_01/ index.html.

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

Oracle Hospitality eCommerce Integration Cloud does not require the use of any insecure services or protocols. Here are the services and protocols that Oracle Hospitality eCommerce Integration Cloud does require:

The application uses HTTPS to ensure credit card data is transmitted across public networks in a manner compliant with the PCI Data Security Standard. When transmitting cardholder data over the Internet always use TLS and when transmitting wirelessly, always use the highest level of encryption available.

Always restrict access based on a media access code (MAC) address. For more information, refer to the *Oracle MICROS Hardware Wireless Networking Best Practices Guide* at http:/ / docs.oracle.com/ cd/ E81005_01/ index.html.

Because of the PCI Data Security Standard, Oracle Hospitality mandates each site use secure encryption transmission technology, for example, IPSEC, VPN or TLS when sending cardholder information over public networks, including when using wireless connections, e-mail, and services such as Telnet, FTP, etc. When sending credit card numbers via e-mail, customers and resellers must use an email encryption solution.

Modems should not reside in application servers unless absolutely necessary. If a modem is installed, it should be kept powered off or disabled except when needed. For added security, the modem should be configured to use automatic call back and data encryption. Firewalls will not protect against attacks via the modem.

All non-console administrative access must be encrypted using technologies such as SSH, VPN or TLS (transport layer security) for web-based management and other non-console administrative access. Telnet or rlogin must never be used for administration.

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

Never store cardholder data on Internet-accessible systems (for example, 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 Oracle Corporation employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism. The means two of the following three authentication methods must be used:

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

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

Oracle Hospitality eCommerce Integration Cloud delivers patches and updates in a secure manner.

Oracle Hospitality may occasionally provide the eCommerce Intgration Cloud software updates remotely. To comply each site must develop usage policies for critical employee

facing technologies (i.e., remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/ digital assistants (PDAs), email usage, and Internet usage) to define proper use of these technologies for all employees and contractors.

To comply, ensure the usage policies require the following:

- Require explicit management approval to use the devices.
- Require that all device use is authenticated with username and password or other authentication item (such as a token).
- Require a list of all devices and personnel authorized to use the devices.
- Require labelling of devices with owner, contact information, and purpose.
- Require acceptable uses for the technology.
- Require acceptable network locations for the technology.
- Require a list of company-approved products.
- Require automatic disconnect of modem sessions after a specific period of inactivity.
- Require activation of modems used by vendors only when needed by vendors, with immediate deactivation after use.
- Prohibit the storage of cardholder data onto local hard drives, floppy disks or other external media when accessing such data remotely via modem.
- Prohibit cut-and-paste and print functions during remote access.

Oracle Hospitality recommends all customers and resellers/ integrators use a personal firewall product if computer is connected via VPN or other high-speed connection, to secure these “always-on” connections, per PCI DSS standards as documented on page 5.

To ensure your information security policy is setup in compliance with Requirement 12 of The PCI Data Security Standard, “Maintain a policy that addresses information security,” consult the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

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

You must always use and implement remote access security features. The default settings in the remote access software must be changed so that a unique username and complex password is used for each customer.

Never use the default password. Adhere to the PCI DSS password requirements established in PA-DSS 3.1 and 3.2 when creating the new, strong password. Passwords must contain at least 8 characters, including a combination of numbers and letters. Adhere to the same PCI DSS password requirements when creating customer passwords.

Connections must only be allowed from specific, known IP/ MAC addresses. Strong authentication or complex passwords for logins must be used. Encrypted data transmission and account lockout after a certain number of failed attempts must be enabled. The systems must be configured so that a remote user must establish a Virtual Private Network (VPN) connection via a firewall before access is allowed.

Logging functions must be enabled for security purposes. Access to customer passwords must always be restricted. For more information, refer to the OHEICS Customer Support Access Policy document.

For more information on Requirement 8 of the PCI Data Security Standard, “Assign a unique ID to each person with computer access,” consult the PCI Security Standards Council website, https:/ / www.pcisecuritystandards.org/ .

Data Transport Encryption (PA-DSS 11.1.b)

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

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

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

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

Refer to the Dataflow diagram for an understanding of the flow of encrypted data associated with Oracle Hospitality eCommerce Integration Cloud, in the above Credit/ Debit Cardholder Dataflow Diagram section.

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

The Oracle Hospitality eCommerce Integration Cloud application 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)

The eCommerce Integration Cloud application facilitates non-console administration to the application to support menu, product, application specific configuration and reporting.

All non-console administrative access must be encrypted using technologies such as SSH, VPN, or TLS (transport layer security) for web-based management and other non-console administrative access. Telnet or rlogin must never be used for administration.

Network Segmentation

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

Refer to the standardized Network diagram for an understanding of the flow of encrypted data associated with Oracle Hospitality eCommerce Integration Cloud.

Firewalls are devices that control computer traffic allowed between an entity's internal networks and untrusted external networks, including traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

In accordance with the PCI Data Security Standard, Oracle Corporation mandates every site, including wireless environments, install and maintain a firewall configuration to protect data. Configure your network so that databases and wireless access points *always* reside behind a firewall and have no direct access to the Internet.

Personal firewall software must be installed on any mobile and employee owned computers with direct connectivity to the Internet, such as laptops used by employees, which are used to access the organization's network. The firewall software's configuration settings must not be alterable by employees.

Because of the PCI Data Security Standard, Oracle Corporation mandates each site ensure that servers, databases, wireless access points, and any medium containing sensitive data reside behind a firewall. The firewall configuration must restrict connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks.

The firewall configuration must also place the database in an internal network zone, segregated from the demilitarized zone (DMZ) with the web server. A DMZ can be used to separate the Internet from systems storing cardholder data.

Customers and resellers/ integrators should establish and maintain payment applications so that cardholder data is not stored on Internet-accessible systems.

As a PCI compliant measure, HEICS v18.1 does not require the database server and web server to be on the same server.

To ensure your firewall configuration is set up in compliance with Requirement 1 of the PCI Data Security Standard, "Install and maintain a firewall configuration to protect cardholder data", consult the PCI Security Standards Council website, https:/ / www.pcisecuritystandards.org/ .

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.

Web Server	
Processor	Single Quad Core
Operating System	Microsoft Windows 2008 R2 Server Standard Edition (64-Bit) – with latest service packs and security patches.
Base Software	Internet Information Services (IIS) 7.x Microsoft .NET Framework 4.0, 4.5.2
Memory	8GB RAM
Hard Disk	C: system drive (as required)

Database Server	
Processor	Single Quad Core
Operating System	Microsoft Windows 2008 R2 Server Standard Edition (64-Bit) – with latest service packs and security patches.
Base Software	SQL Server 2008 R2 Standard Edition – with latest service packs and security patches Microsoft .NET Framework 4.0

Memory	16GB RAM
Hard Disk	Separate system and data drives, SAN may be required, minimum 100GB for data storage.

Appendix A Inadvertent Capture of PAN

Appendix A provides instructions for addressing the inadvertent capture of PAN on the following supported operating systems:

- Linux
- **Error! Reference source not found.**
- **Error! Reference source not found.**

Addressing Inadvertent Capture of PAN on Linux

Clear Swap Space

To clear the swap file on Linux systems execute the following commands:

1. To review and swap usage go to the command line and enter: `free`

```
root@Orthanc:~ # free
             total       used       free     shared    buffers     cached
Mem:       1034368     693128     341240          0     215448     235824
-/+ buffers/cache:     241856     792512
Swap:       524280      49576     474704
```

2. Enter the command: `swapoff -a (requires elevated privs)`
3. Enter the command: `swapon -a (requires elevated privs)`
4. Now the swap should be clean. To review and swap usage space go to the command line and enter: `free`

```
coalfire@ubuntu:~$ sudo swapoff -a
[sudo] password for coalfire:
coalfire@ubuntu:~$ sudo swapon -a
coalfire@ubuntu:~$ free
             total       used       free     shared    buffers     cached
Mem:       2050976     269184    1781792          0      10632     194308
-/+ buffers/cache:      64244    1986732
Swap:      2097148          0    2097148
```

Disable Swap Space

An alternative to clearing the swap space is to disable the swap space. Disabling the swap space can be risky to the operation of your system. With no swap space, the Linux/ Unix operating system will automatically kill processes if the amount physical RAM needed for all running processes is exceeded.

To disable the swap space comment out the swap entry in / etc/ fstab.

Encrypt Swap Space

The following steps explain encrypting swap through the use of dm-crypt. This requires you to run a 2.6 kernel. In the example below the swap partition is located in / dev/ VolGroup00/ LogVol01. This is the default swap partition for RedHat systems. It is not required that the swap partition is part of an LVM. As described previously, the dm-crypt can encrypt disk partitions (/ dev/ hda2) or whole disks (/ dev/ hda). Change the commands to fit the path to your swap partition location. Before executing the following commands make sure you understand the following concepts:

- Entering `-d` specifies cryptsetup to use `/dev/random` as the key file.

- Entering the `create` command creates a mapping with the name, swap backed by the device, `/dev/VolGroup00/LogVol01`

When encrypting your swap partition, you will need to temporarily turn off swap. This means you need to shut all unnecessary applications to free up memory. If this memory is not free, you will be unable to turn off the swap space. The best practice to implement this is to boot the system into single user mode. This shuts down most services with the exception of a single root shell.

1. To boot the system into single user mode, run the following command: `# /sbin/telinit s`
2. To turn off the swap space run the following command: `# swapoff -a`
3. To ensure a completely clean and sterile swap space, you must overwrite swap partition with random data. This prevents the recovery of any data written to swap before the encryption process. The shred command overwrites the specified file or device with random data, enter the command: `# shred -v /dev/VolGroup00/LogVol01`
4. Create a file named /etc/crypttab. The main page includes the details of the crypttab.

   Use the following example to verify the values for your system:

   a. The first field creates an encrypted block device called swap: `/dev/mapper`
   b. The second field specifies the underlying block device: `/dev/VolGroup00/LogVol01`
   c. The third field specifies the encryption password: `/dev/random`
   d. The forth field specifies the encrypted device as a swap device with an encryption cypher and uses AES encryption and unpredictable IV values: `swap /dev/VolGroup00/LogVol01 /dev/random swap,cipher=aes-cbc-essiv:sha256`

5. Edit the `/etc/fstab` to point to the encrypted block device, `/dev/mapper/swap` instead of `/dev/VolGroup00/LogVol01`. The current file should resemble the following example:

   ```
   /dev/VolGroup00/LogVol01  swap  swap  defaults  0 0
   ```

   Change the file to resemble this example:

   ```
   /dev/mapper/swap  swap  swap  defaults  0 0
   ```

6. Reboot your system to create the encrypted swap space using the following command: `# reboot -n`
7. Alternatively, if you do not reboot you can create the encrypted swap partition using the following commands:

   ```
   # cryptsetup -d /dev/random create swap
   /dev/VolGroup00/LogVol01

   # mkswap /dev/mapper/swap

   # swapon -a
   ```

Addressing Inadvertent Capture of PAN on 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 System 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`
   In the event you need 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 System Pagefile.sys on Shutdown

You can enable the option to clear the 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**.

Addressing Inadvertent Capture of PAN on 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 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.

Enable System Management of PageFile.sys

To enable clearing the Pagefile.sys on 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.**

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: _____