Oracle® Hospitality Simphony

PA-DSS Implementation Guide
Release 2.8
Part Number: E66804-01

April 2016

ORACLE

Contents

Preface

This document describes the steps that you must follow in order for your Oracle Hospitality Simphony 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 April 2015). You can download the PCI PA-DSS 3.1 standards 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 Oracle Hospitality Simphony installation to support your PCI DSS compliance efforts.

Revision History

Date	Description of Change
September 2015	• Initial publication
October 2015	• Minor edit
March 2016	• Added references to the Key Manager content now found in the *Simphony Security Guide*
April 2016	• Minor edit (WS6 name)

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/en/industries/hospitality/ to view or download the current version of this guide, and refer to the Oracle Hospitality Simphony Release Notes and this guide's Revision History to learn what has been updated or changed. In order to ensure your PCI DSS compliance, you need to subscribe to receive email Oracle Security Alerts by clicking the Critical Patch Updates link on the Oracle Technology Network at http://www.oracle.com/technetwork/index.html. This provides you timely information on any possible updates to the PA-DSS Implementation Guide that you need to know about in order to continue to use Oracle Hospitality Simphony version 2.8 in a PCI DSS compliant manner.

1 Executive Summary

Oracle Hospitality Simphony 2.8 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.
361 Centennial Parkway Suite 150
Louisville, CO 80027

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 Simphony Version 2.8 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 Simphony</td><td>Payment Application Version</td><td colspan="2">2.8</td></tr>
<tr><td>Payment Application Description</td><td colspan="5">Oracle Hospitality Simphony is a SaaS Enterprise ready Point-Of-Sale solution, capable of scaling from a single site operating a few workstations to an Enterprise deployment with hundreds of properties and thousands of workstations. Simphony is capable of operating multiple types of concepts within each property including table service, fast casual, and retail. Simphony is a payment application designed for the hospitality industry.</td></tr>
<tr><td>Typical Role of the Payment Application</td><td colspan="5">Oracle Hospitality Simphony can perform both card present and card-not-present transactions with CVV2. Debit and other PIN-based transactions are not supported. The application is comprised of a POS workstation, an application server and a database server.</td></tr>
<tr><td rowspan="3">Target Market for Payment Application (check all that apply)</td><td>☒</td><td>Retail</td><td>☐</td><td>Processors</td><td>☐ Gas/Oil</td></tr>
<tr><td>☐</td><td>e-Commerce</td><td>☐</td><td colspan="2">Small/medium merchants</td></tr>
<tr><td>☒</td><td colspan="4">Others (please specify): Hospitality</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 Transaction database tables, store cardholder data:
SECURE_DETAIL
MREQUESTS,
MREQUESTS_BAK
CCBATCH_AUTH_DETAIL
CHECKS_PROCESS_DATA</td><td colspan="2">The following Cardholder data is stored:
Full PAN
Cardholder Name
Expiration date</td></tr>
<tr><td colspan="5">Individual access to cardholder data is logged as follows:
Full Pan Data is never logged in the application; the last 4 digits of the PAN are logged for troubleshooting purposes.</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">Application Server(s)
Database Server(s)
POS Operations (Ops)</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>
</table>

Supported Database Software	The following are database management systems supported by the payment application:
	• Oracle Database 11g • Oracle Database 12c • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2012 • Microsoft SQL Server Express • SQLite
Other Required Third Party Software	The following are other third party software components required by the payment application:

	• For Microsoft Windows Server 2008 R2
	  o Microsoft Internet Information Systems (IIS) version 7.5
	• For Microsoft Windows Server 2012
	  o Microsoft Internet Information Systems (IIS) version 8
	• For Microsoft Windows Server 2012 R2
	  o Microsoft Internet Information Systems (IIS) version 8.5
	  IIS is used by the payment application to communicate via the web with network clients
	• Red Hat JBoss – version AS 5.1.0
	  JBoss is used by the eBusiness Reporting and Analytics Advanced back office reports application

Supported Operating System(s)	The following are Operating Systems supported or required by the payment application:
	• Microsoft Windows Embedded POSReady 2009 • Microsoft Windows Embedded POSReady 7 • Microsoft Windows 7 SP1 • Microsoft Windows 8.1 • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Oracle Enterprise Linux versions 6.3, 6.4, and 6.5 (database servers only) Dependent Software: • Oracle Database • Microsoft SQL Server Dependent Hardware: • Oracle MICROS PC Workstation 2015 - POSReady 2009 • Oracle MICROS Workstation 610 - Microsoft Windows Embedded 8.1 Industry Pro Retail • DT365 Tablet - Windows Embedded POS Ready 7 • MC-40 – Microsoft Windows Embedded Mobile 7 • Oracle MICROS Workstation 5A - Windows Embedded POS Ready 2009

<table>
<tr><td></td><td>

Oracle MICROS mTablet E-Series 11 inches - Microsoft Windows Embedded 8.1 Industry Pro Retail
Oracle MICROS mTablet E-Series 8 inches - Microsoft Windows Embedded 8.1 Industry Pro Retail

Workstation Printers:

Epson TM-88 Model II
Epson TM-88 Model III
Epson TM-88 Model IV
Epson TM-88 Model V
Epson TM-P60
Epson TM P60 II
Epson TM-U295
Epson TM-U220B

</td></tr>
<tr><td>Payment Application Authentication</td><td>
POS Application Terminal (transactions)
The Employee can use one of several methods to authenticate on the POS Application Terminal, they include:

Biometrics (fingerprint)
Employee Magnetic Card
Employee Number/Pin

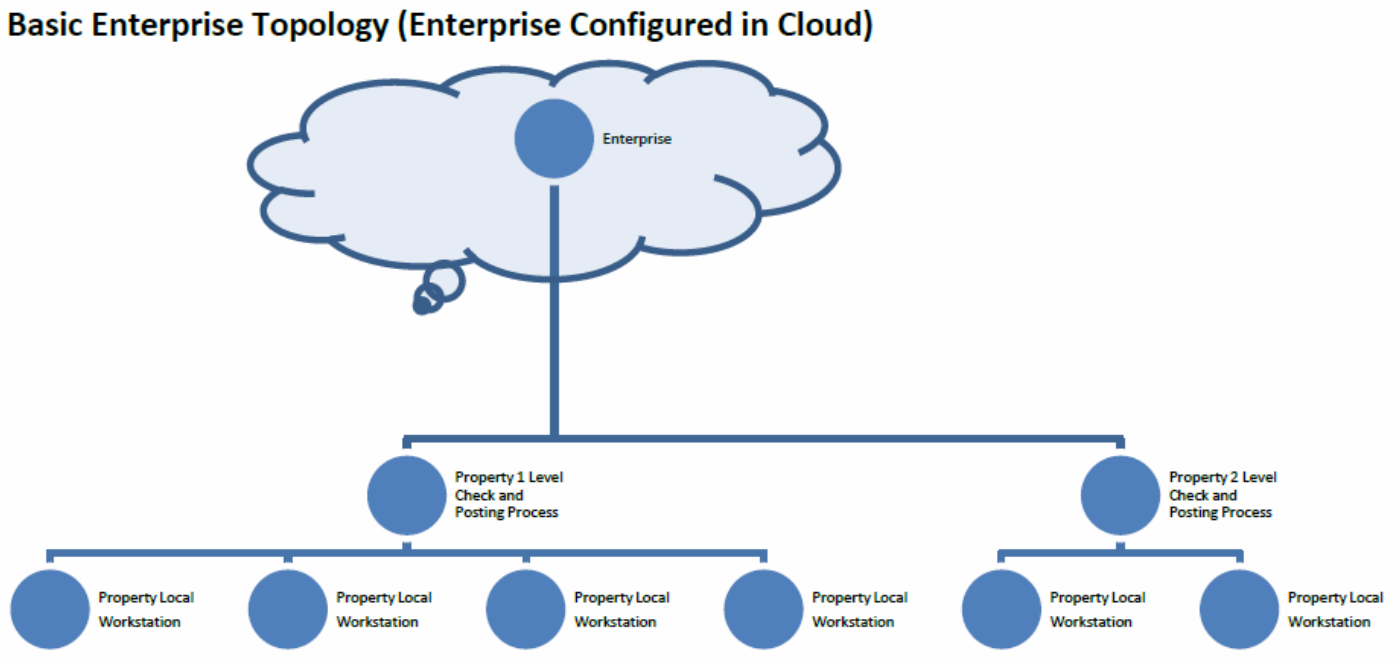
Enterprise Management Interface
The Enterprise Management Console (EMC) requires:

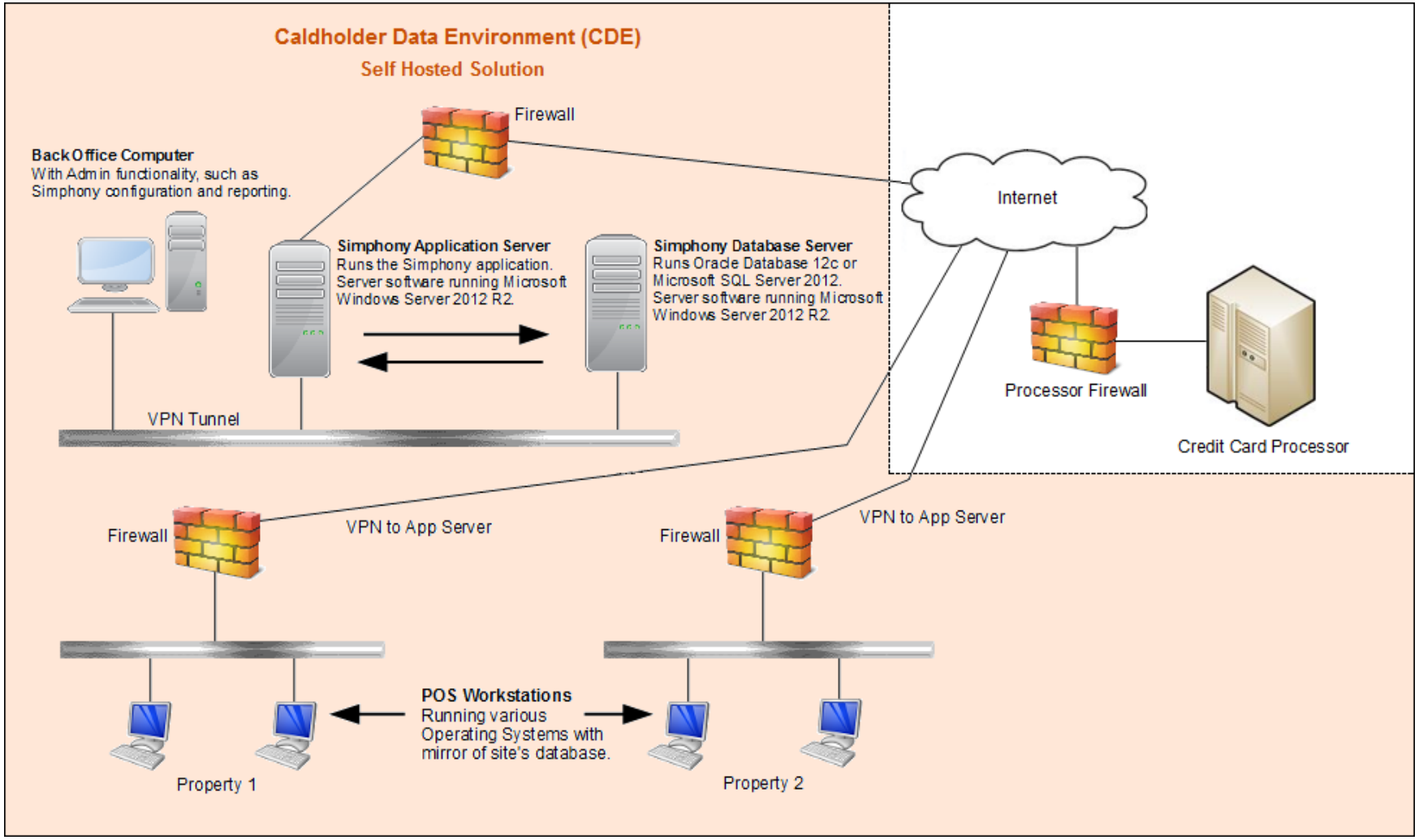
Unique Username
Password – must contain Uppercase, Number, Symbol and a minimum of 8 characters
Passwords are hashed with SHA-256 with random salt

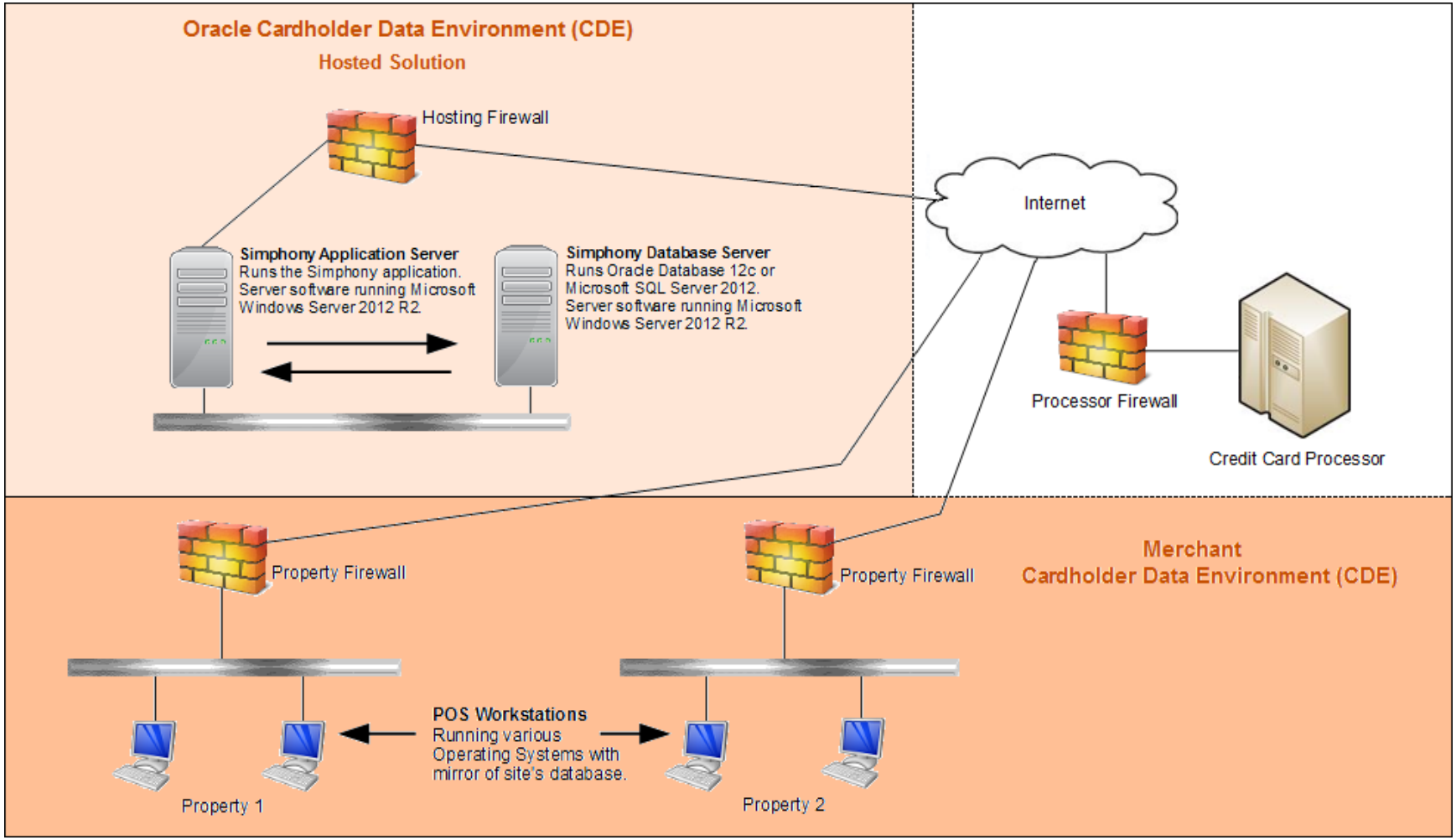
</td></tr>
<tr><td>Payment Application Encryption</td><td>See Appendix A for information about the payment application encryption used by Oracle Hospitality Simphony version 2.8.</td></tr>
<tr><td>Supported Payment Application Functionality</td><td>
<table>
<tr><td>☐</td><td>Automated Fuel Dispenser</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>
</table>
</td></tr>
</table>

Payment-processing Connections	**Table Service** The operator drops off a check at the customer table. The customer provides a payment card to the operator; the card is authorized using the POS terminal. The terminal communicates directly with the payment processor using secure transmission protocols. The authorization is approved and the card data is saved in the transaction detail and a voucher is printed. The operator returns the voucher to the customer and typically gratuity is added and the customer signs the voucher. The operator then returns to the POS terminal and performs the final payment on the transaction and fills in the gratuity field. The transaction is now finalized. **Quick Service** The cashier asks for payment directly from the customer after the ordering process. The customer provides a payment card to the operator; the card is authorized using the POS terminal. The terminal communicates directly with the payment processor using secure transmission protocols. Once authorization is complete, the POS performs the final payment on the transaction. The transaction is now finalized. A customer receipt or voucher is often presented to the customer for their signature. Approved Payment Processors: • Merchant Link • First Data • Elavon • Shift4 • FreedomPay
Description of Listing Versioning Methodology	Oracle implements wild card versioning and follows a versioning methodology for the application in the format of [NN].[N].[X].[XXXX] (where N represents a number): • Changes made at the Major level include architectural changes to the application and impact PA-DSS requirements or the security of the application • Changes made at the Minor level include minor changes to the application that may or may not impact PA-DSS requirements • Changes at the Patch level include one or more changes made at the build level, do not impact PA-DSS requirements or the security of the application and are indicated by a PA-DSS wildcard (X) • Changes at the Build level are daily changes that include partial or full changes made on a daily basis. Changes at this level do not impact PA-DSS requirements or the security of the application and are indicated by a PA-DSS wildcard (X). The versions of the payment application listed on the PCI SSC web site are listed as Major.Minor.

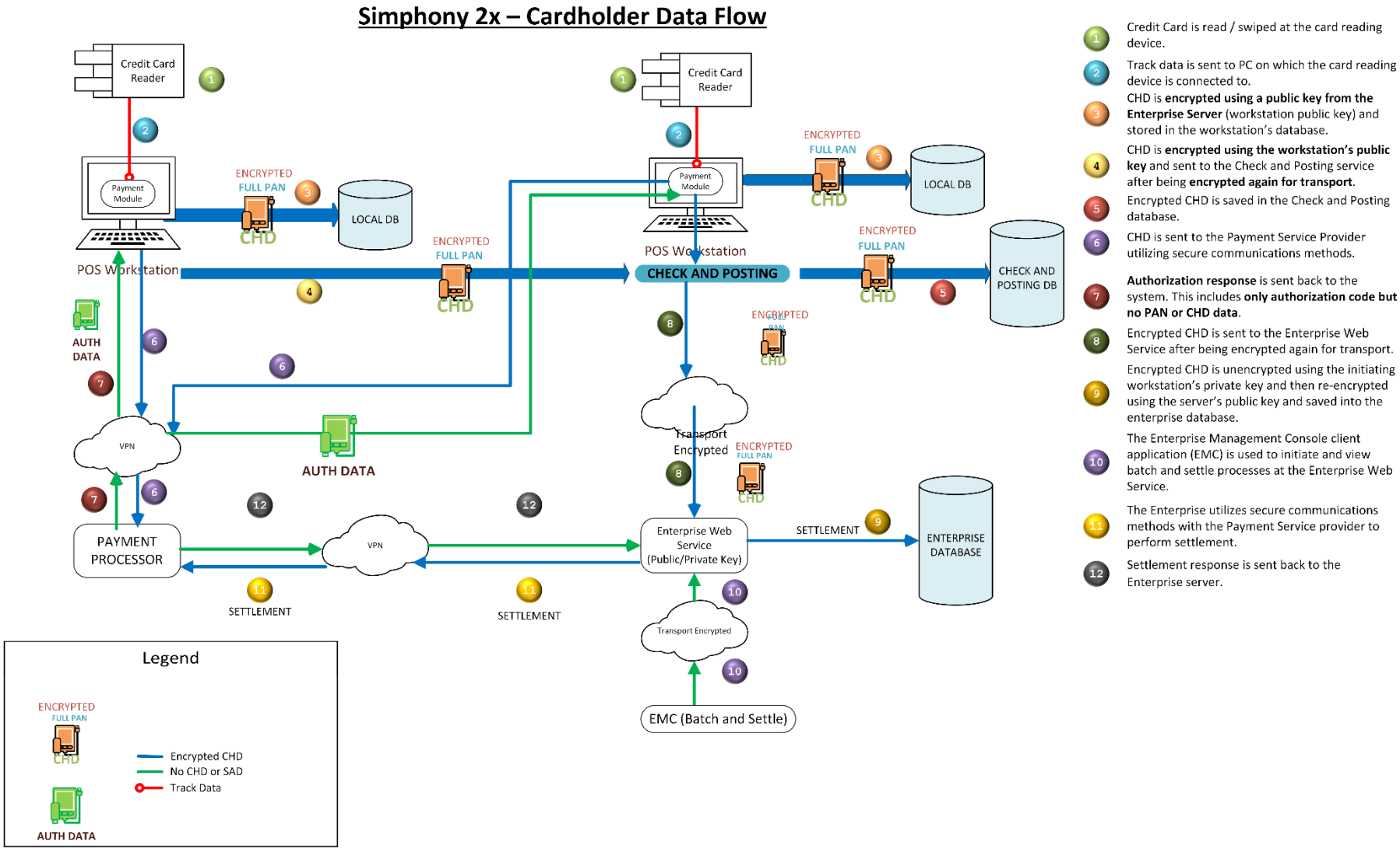
Typical Network Implementations




Caldholder Data Environment (CDE)
Self Hosted Solution
Firewall
Back Office Computer
With Admin functionality, such as
Simphony configuration and reporting.
Simphony Application Server
Runs the Simphony application.
Server software running Microsoft
Windows Server 2012 R2.
Simphony Database Server
Runs Oracle Database 12c or
Microsoft SQL Server 2012.
Server software running Microsoft
Windows Server 2012 R2.
Internet
Processor Firewall
Credit Card Processor
VPN Tunnel
Firewall
VPN to App Server
Firewall
VPN to App Server
POS Workstations
Running various
Operating Systems with
mirror of site's database.
Property 1
Property 2


Oracle Cardholder Data Environment (CDE)
Hosted Solution
Hosting Firewall
Internet
Simphony Application Server
Runs the Simphony application.
Server software running Microsoft
Windows Server 2012 R2.
Simphony Database Server
Runs Oracle Database 12c or
Microsoft SQL Server 2012.
Server software running Microsoft
Windows Server 2012 R2.
Processor Firewall
Credit Card Processor
Property Firewall
Property Firewall
Merchant
Cardholder Data Environment (CDE)
POS Workstations
Running various
Operating Systems with
mirror of site's database.
Property 1
Property 2

Credit/Debit Cardholder Dataflow Diagram



	Data Element	DataStore	DataStore	System that Stores Data	How is Data Secured	How is Access to DataStore Logged
Cardholder Data	Primary Account Number (PAN)	Yes	• SECURE_DETAIL • MREQUEST • MREQUESTS_BAK • CCBATH_AUTH_DETAIL • CHECKS_PROCESS_DATA	Database	AES256	Access to this table logged by database software
	Cardholder Name [1]	Yes	• SECURE_DETAIL • MREQUEST • MREQUESTS_BAK • CCBATH_AUTH_DETAIL • CHECKS_PROCESS_DATA	Database	AES256	Access to this table logged by database software
	Service Code	NA	NA	NA	NA	NA
	Expiration Date	Yes	• SECURE_DETAIL • MREQUEST • MREQUESTS_BAK • CCBATH_AUTH_DETAIL • CHECKS_PROCESS_DATA	Database	AES256	Access to this table logged by database software
Sensitive Authentication Data	Full Magnetic Stripe Data	No	NA	NA	NA	NA
	CAV2/CVC2/CVV2/CID	No	NA	NA	NA	NA
	PIN/PIN Block	No	NA	NA	NA	NA

[1] *These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.*

Difference between PA-DSS Validation and PCI Compliance

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

As the software and payment application developer, our responsibility so 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 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.

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

The 12 Requirements of the PCI DSS:

Build and Maintain a Secure Network and Systems

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

Protect Cardholder Data

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

Maintain a Vulnerability Management Program

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

Implement Strong Access Control Measures

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

Regularly Monitor and Test Networks

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

Maintain an Information Security Policy

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

Additional PCI DSS Requirements for Shared Hosting Providers

Requirement A.1 (Appendix A): Shared hosting providers must protect the cardholder data environment.

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

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

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

Removal 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.

Previous versions of Oracle Hospitality Simphony did not store SAD. Therefore, there is no need for secure deletion of this historical data by the application as required by PA-DSS v3.0.

Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

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

Secure Deletion of Cardholder Data (PA-DSS 2.1)

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

- A customer defined retention period must be defined with a business justification
- 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 that you must securely delete:

- SECURE_DETAIL
- MREQUESTS
- MREQUESTS_BAK
- CCBATCH_AUTH_DETAIL
- CHECKS_PROCESS_DATA

- Cardholder Data must be securely deleted within the transaction database. To securely delete Cardholder Data you must perform the steps as outlined in the Removal Historical Sensitive Authentication Data (PA-DSS 1.1.4) section.
- All underlying software (this includes operating systems and/or database systems) must be configured to prevent the inadvertent capture of PAN

Preventing the Inadvertent Capture of PAN data:

The payment application point-of-sales (POS) operations collects PAN data from a manual user entry or from a magnetic stripe card reader. Some magnetic card readers encrypt the swipe and no special measures are taken by the application code to protect the encrypted swipe while in transit to the processor.

Non-encrypting readers and manual entry PAN data are placed in a class called a SafeByteArray. The card data is stored as a linked list of byte in memory to prevent PAN data from being found in contiguous blocks of memory by a scanning tool. In addition to the linked list of bytes, each byte of the card data is masked using a primitive Caesar cipher shift mechanism to further hide the contents of the list while in transit in memory to the processor. Once the SafeByteArray arrives at the network endpoint, each byte is fetched by the processor code to place in the transmission buffer.

The SafeByteArray is the default way we store any PAN data in our payment objects. The payment objects themselves along with their SafeByteArrays are immediately encrypted with the Server Public key once successful authorization is acquired in the payment application. No further access to PAN data occurs until the payment object is used at the Hosting Center during the credit card settlement process.

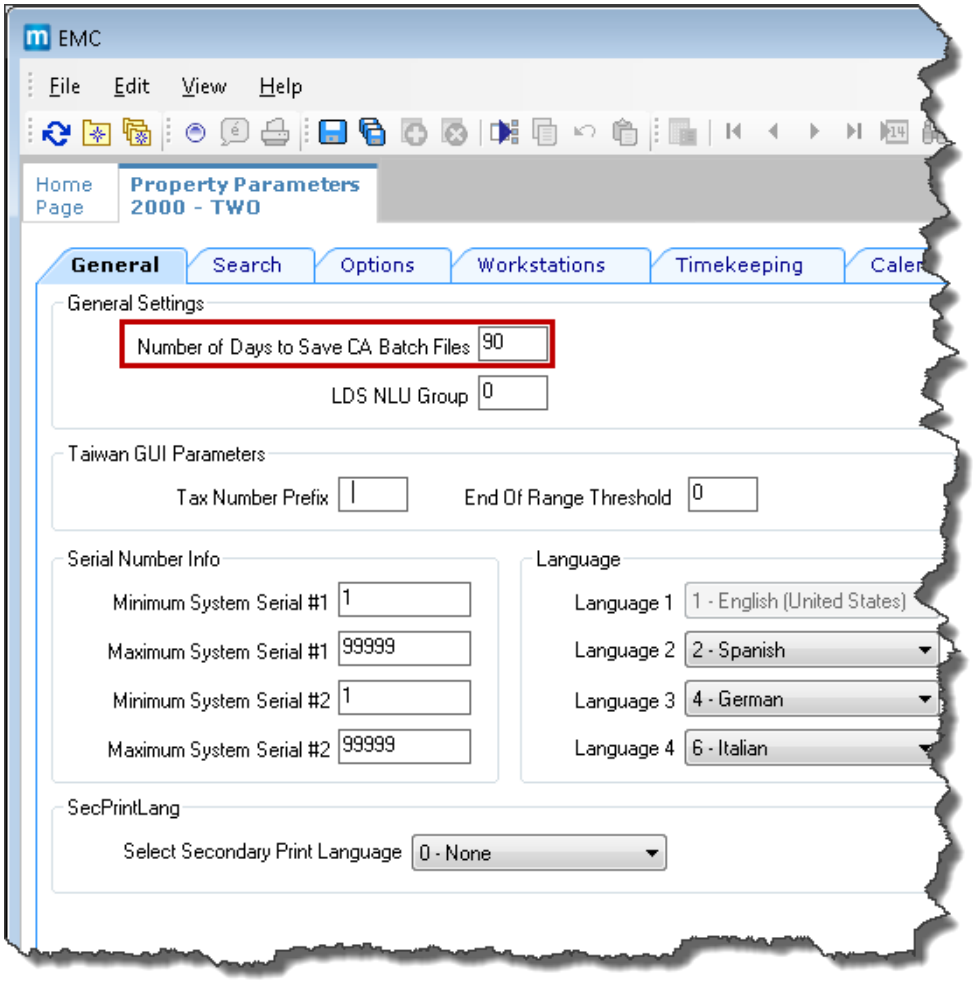
Purging Cardholder Data

To program the system to purge temporarily stored cardholder data (CHD), there are two places within the Simphony Enterprise Management Console (EMC) that need to be configured.
First, configure the system from the Enterprise level. To begin:

1. Access the EMC and select the Enterprise level.
2. Click the **Setup** tab and select the Enterprise Parameters module.
3. Select the **Misc** tab and look for the Purging section.
4. Scroll down to the **Checks** job under the **Purge Type** column.
5. Enter the desired number of days to keep check detail information under the **Days To Keep** column and **Save**.

Once the defined threshold is reached, check detail data is purged on a daily basis. Next, credit authorization (CA) batch purging is configurable. To configure credit card batch purging:

1. Access the EMC and select a property.
2. Click the **Setup** tab and select the Property Parameters tab.
3. From the General tab, General Settings section, enter the desired value in the **Number of Days to Save CA Batch Files** field and **Save**.



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

Oracle Hospitality Simphony does not have the ability to display full PAN for any reason and therefore, there is no configuration details to be provided as required for PA-DSS

v3.1. Oracle Hospitality Simphony masks all Primary Account Numbers (PAN) by default in all locations that display PAN (screens, paper receipts, printouts, reports, etc.) by displaying only the last four digits of the (PAN).

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

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
- A sample Key Custodian form has been provided in Appendix B for key custodians to acknowledge that they understand and accept their key custodian responsibilities must be signed.

Encryption keys should be rotated on a regular basis and the keys are purged as part of the standard Oracle Hospitality Simphony key rotation process.

Key management activities must be performed per PCI DSS standards. This includes:

- Performing the key rotation as outlined in the *Simphony Security Guide* (in Appendix D) on the required schedule per PCI-DSS standards
- Manage the pass phrases used to perform the key rotation operation
- Restrict access to the Key Management functions by assigning the correct permissions to the authorized users

During the key rotation process, the following is performed automatically:

- Generation of strong cryptographic keys
- Secure cryptographic key distribution
- Secure cryptographic key storage
- Removal of obsolete keys

Oracle Hospitality Simphony temporarily stores cardholder data, but does not have the ability to output PAN data for storage outside of the payment application.

All PAN must be rendered unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs). The payment application uses an encryption methodology with dynamically generated keys to automatically encrypt all locations/methods where cardholder data is stored.

Oracle Hospitality Simphony uses credit card masking and AES256 encryption to ensure credit card data is stored in a manner compliant with the PCI Data Security Standard.

Oracle Hospitality recommends that customers or resellers\integrators rotate the keys every 180 days. The *Simphony Security Guide* (in Appendix D) contains more information about key rotation. Key rotation must perform the following:

- Generation of strong cryptographic keys

- Secure cryptographic key distribution
- Secure cryptographic key storage
- Cryptographic key changes for keys that have reached the end of their crypto-period
- Retire or replace keys when the integrity of the key has been weakened and/or when known or suspected compromise. If retired or replaced cryptographic keys are retained, the application cannot use these keys for encryption operations.
- Manual clear-text cryptographic key-management procedures require split knowledge and dual control of keys
- Prevention of unauthorized substitution of cryptographic keys

Removal of Historical Cryptographic Material (PA-DSS 2.6)

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

- Simphony 2.6
- Simphony 2.7

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
- The *Simphony Security Guide* document (in Appendix D) states that Simphony automatically decrypts the historical cardholder data and re-encrypts it
- All encryption keys and previous cryptograms are securely deleted by the key rotation process as reviewed in Appendix D in the *Simphony Security Guide* document

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:

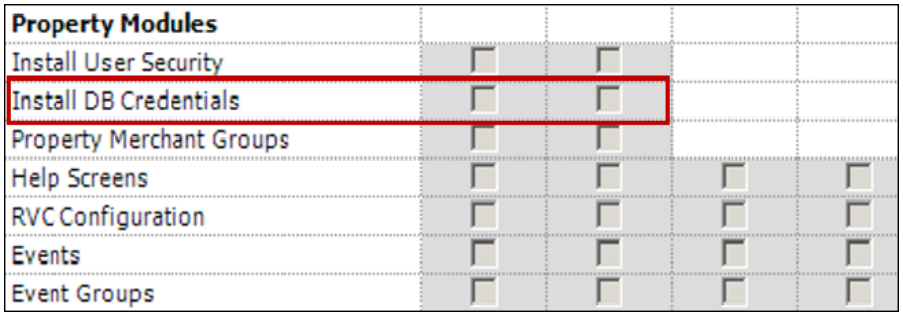
1. The payment application must not use or require the use of default administrative accounts for other necessary or required software (for example, database default administrative accounts) (PCI DSS 2.1 / PA-DSS 3.1.1)
2. The payment application must enforce the changing of all default application passwords 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 at least one of the following three methods to authenticate users: (PCI DSS 8.2 / PA-DSS 3.1.4)
    - Something you know, such as a password or passphrase
    - Something you have, such as a token device or smart card
    - 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)

How to create a PCI compliant password in the Simphony Enterprise Management Console (EMC)

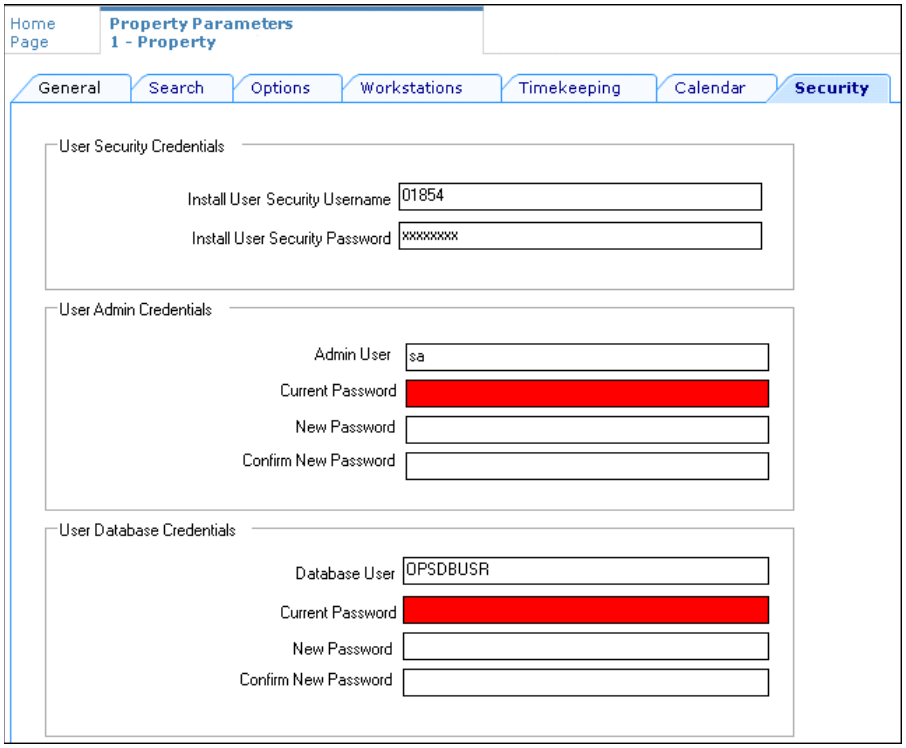
Property Password Maintenance

To comply with Requirement 2 of the PCI Data Security Standard, change your Oracle Hospitality Simphony Property's Database Username and Database Password and System Administrator (SA) Password for the Workstations.

1. Navigate to EMC, Roles, and the EMC Modules tab.
2. Ensure the employee's assigned Role has **Install DB Credentials** View and Edit access enabled for the user(s) making the change and click **Save**.



3. Navigate to EMC, Property Parameters, and select the **Security** tab.



4. Enter the **Install User Security Username** and **Install User Security Password** under the User Security Credentials section so implementation specialists can authenticate workstations on the Enterprise.
5. Enter the user defined **Admin User** name and **Current Password** (for the Admin Database user) under the User Admin Credentials section to allow for the building of a database on workstations.

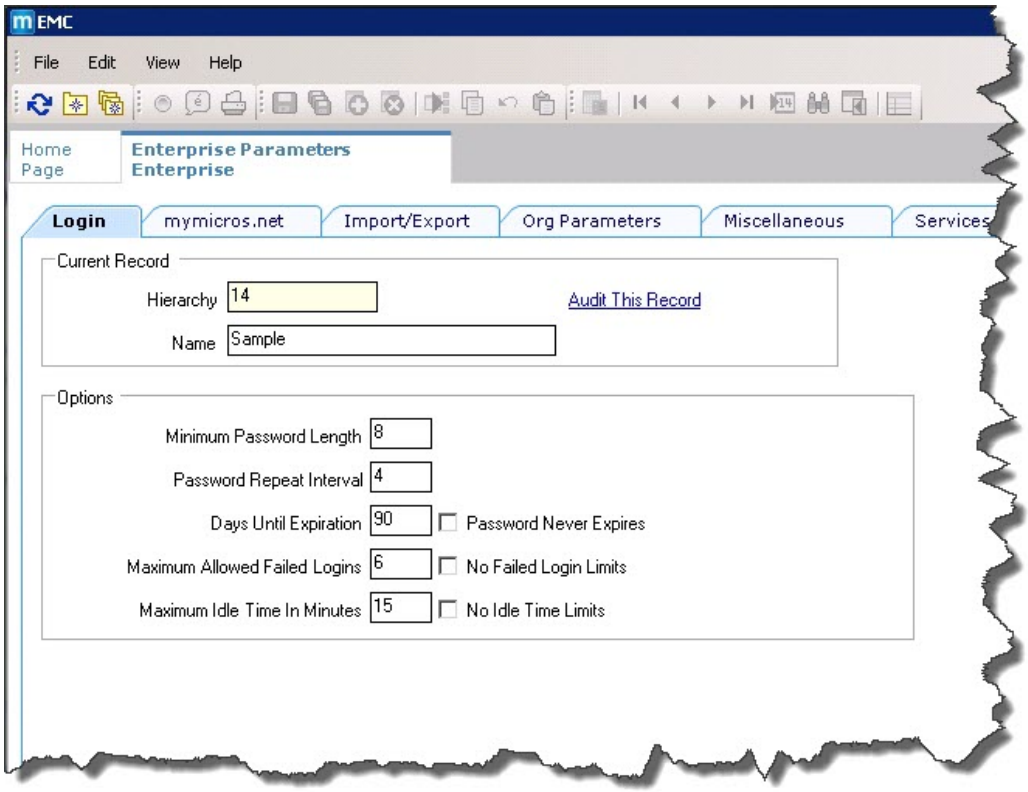
6. Enter the **Database User** name and **Current Password** under the User Database Credentials section to set the logon credentials to allow the performance of database downloads to workstations.
7. Click **Save**.
8. Reboot workstations for the changes to take effect.

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.

To ensure strict access control of the Oracle Hospitality Simphony application, always assign unique usernames and complex passwords to each account. Oracle Hospitality mandates applying these guidelines to not only Simphony passwords but to Microsoft Windows operating system passwords as well. Furthermore, 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.

Creating Secure Passwords

To comply with Requirement 8 of the PCI Data Security Standard, ensure the following options in the EMC are configured as shown below:



In the EMC, Enterprise Parameters, Login Tab, Enhanced Password Security Tab, ensure these available options are configured as follows:

1. Ensure the Minimum Password Length is at least 8.
2. Ensure the Password Repeat Interval is at least 4.
3. Ensure the Days Until Expiration is not greater than 90.
4. Ensure the Maximum Allowed Failed Logins is not greater than 6.
5. Ensure the Maximum Idle Time in Minutes is not greater than 15.

Oracle Hospitality mandates changing your master username password in the EMC, following the above guidelines, after logging in for the first time.

Oracle Hospitality Simphony, as tested in our PA-DSS validation, meets, or exceeds these requirements for the following additional required applications or databases:

- Oracle Hospitality Simphony
- eBusiness Back Office applications
- Transaction database(s)
- eBusiness Back Office database(s)

Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to systems with cardholder data, and for access controlled by the application. The requirements apply to the payment application and all associated tools used to view or access cardholder data.

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

Properly Train and Monitor Admin Personnel

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

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

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

4.1.b: Oracle Hospitality Simphony has PA-DSS compliant logging enabled by default. This logging is not configurable and may not be disabled. Disabling or subverting the logging function of Simphony in any way results in non-compliance with PCI DSS.

4.1.b: Oracle Hospitality Simphony must have logging turned on and configured per PCI DSS 10.2 and 10.3 as follows:

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

10.2.1 All individual user accesses to cardholder data from the application

10.2.2 All actions taken by any individual with administrative privileges in the application

10.2.3 Access to application audit trails managed by or within the application

10.2.4 Invalid logical access attempts

10.2.5 Use of the application's identification and authentication mechanisms (including but not limited to creation of new accounts, elevation of privileges, etc.) and all changes, additions, deletions to application accounts with root or administrative privileges

10.2.6 Initialization, stopping, or pausing of the application audit logs

10.2.7 Creation and deletion of system-level objects within or by the application

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

10.3.1 User identification

10.3.2 Type of event

10.3.3 Date and time

10.3.4 Success or failure indication

10.3.5 Origination of event

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

Disabling or subverting the logging function of Oracle Hospitality Simphony in any way results in non-compliance with PCI DSS.

4.4.b: Oracle Hospitality Simphony facilitates centralized logging.

1. To enable the Oracle server audit trail, set the AUDIT_TRAIL static parameter within the Parameter file, which has the following properties:
   AUDIT_ TRAIL = { none | os | db |db, extended |xml |xml,extended }

The following list provides a description of each setting:

- none or false: Auditing is disabled
- db or true: Auditing is enabled with all audit records stored in the database audit trail (SYS.AUD$)
- db,extended: As db, but the SQL_BIND and SQL_TEXT columns also populated
- xml: Auditing is enabled, with all audit records stored as XML format OS files
- xml,extended: As xml, but the SQL_BIND and SQL_TEXT columns are also populated
- os: Auditing is enabled with all audit records directed to the operating system's audit trail

---

Note: The AUDIT_TRAIL static parameter cannot be equal to 'none' or 'false' in order to comply with Requirement 10 of The PCI Data Security Standard.

The AUDIT_SYS_OPERATIONS static parameter enables or disables the auditing of operations issued by users connecting with SYSDBA or SYSOPER privileges, including the SYS user. All audit records are written to the OS audit trail.

Note: The AUDIT_SYS_OPERATIONS static parameter must be set to 'true' to comply with Requirement 10 of The PCI Data Security Standard.

The AUDIT_FILE_DEST parameter specifies the OS directory used for the audit trail when the os, xml, and xml extended options are used. It is also the location for all mandatory auditing specified by the AUDIT_SYS_OPERATIONS parameter.

Note: Privileged access to the database, starting and stopping of the database, and structural changes (such as adding a data file) is audited.

No audit actions are captured until audit actions are defined. The *Oracle Database Security Guide* contains more information on how to define audit actions.

2. Use the AUDIT statement to setup detailed auditing. The AUDIT statement can be used to track the occurrence of SQL statements in subsequent user sessions, specific SQL statements or all SQL statements authorized by a particular system privilege, and track operations on a specific schema object.

For detailed information on using the AUDIT statement, see the AUDIT section of the Oracle Database SQL Reference, http://download.oracle.com/docs/cd/B19306_01/server.102/b14200/statements_4007.htm#i2059073.

The *Oracle Database Security Guide* (in the Database Auditing: Security Considerations chapter) contains more information about auditing and is available for download from Oracle's website at www.oracle.com.

The EMC Audit Trail

In accordance with the PCI Data Security Standard, Oracle Hospitality mandates activity logging on the database server for all 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. The Simphony database audit trail utility is automatically enabled by default and requires no initial configuration.

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

For information on C2 audit tracing for MS SQL Server, refer to the following link from the Microsoft Developer Network website, http://msdn.microsoft.com/en-us/library/ms187634(v=SQL.100).aspx

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

Oracle Hospitality Simphony supports various wireless technologies and the wireless networking device(s) chosen can vary. All wireless vendor guidance on how to properly secure these devices should be followed per PCI Data Security Standard 1.2.3, 2.1.1, and 4.1.1.

The *MICROSHW_Wireless Networking Best Practices* document contains more information about making supported wireless devices PCI compliant per the standards listed below. Use this guide as a reference to assist you when installing Oracle MICROS wireless hardware. The PCI DSS Wireless Guideline Informational Supplement version 2.0 references several security methods. This document specifies the highest possible security method for each device.

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. The *Simphony Security Guide* contains more information about the encryption key rotation process.
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.

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

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

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

4 Services and Protocols (PA-DSS 8.2)

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

Simphony utilizes the following protocols when supporting wireless network connections for payment devices:

- SOAP used by XML Web service
- TCP\IP and proprietary protocol

Oracle Hospitality Simphony utilizes the following card readers for the payment process:

Manufacturer	Model	Card Reader
Oracle Hospitality Workstations	Integrated Unit	Yes
ViVOtech	4500/4800	Yes
MagTek	DynaPro Audio Jack Reader	Yes
MagTek	DynaPro Mini Card Reader	Yes
VeriFone	e231 Sleeve	Yes
VeriFone	e232 Sleeve	Yes

Required Third Party software:

- Microsoft .net Framework Runtime
- Microsoft Visual C++ Runtime
- Microsoft Web Service Extensions Runtime
- Microsoft SQL Server Native Client
- Oracle ODP.net database driver

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.) The enabling of the following ports is recommended to keep systems storing cardholder data separate from Internet connection access. Enable Firewall settings accordingly.

Simphony Enterprise Ports

Service	Port Number	Configurable?
Simphony/EGateway (Oracle Database)	1521	Yes
Simphony/EGateway (SQL Database)	1433	Yes
Simphony v2/EGateway (After upgrade/install of 2.6)	8080	Yes
EMC/Remote EMC	8080	Yes
Reporting and Analytics Advanced (formerly mymicros.net)	80 - Browser 81 - myLabor service	Yes

Simphony Property Ports

Service	Port Number	Configurable?
ServiceHost v2	8080	Yes
ServiceHost as a Service (no Ops)	8071	Yes
Print Controller	8080	Yes
IP Printer Listening	9100	No
Banquet Printing	9100	No
KDS Client (Display)	8080	Yes
KDS Controller Service	8080	Yes
Client Application Loader (server selection screen)	TCP 7300, UDP 7301	No
Client Application Loader (property selection screen)	8080	Yes
Credit Card Batching	8080	Yes
Cash Management Lite	5100	No

Service	Port Number	Configurable?
NetTCPRelayBinding (TMS/Azure)	TCP: 9350, 9351, 9352	No
NetTCPRelayBinding (TMS/Azure)	HTTP: 80	No

Traffic Note

In general, all traffic is initiated by the workstation and requires only outbound TCP connections to the outside of the property. Check the site configuration as there will most likely be exceptions to this rule.

Other ports: Make sure to check the wrapper.conf for environment-specific mymicros ports. Simphony Application Server file path:

<*Drive letter*>: *MICROS**mymicros**myPortal**server**default**conf*

PCI-Compliant Remote Access (PA-DSS 10.1)

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

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric

Simphony supports most types of two-factor remote solutions and does not require any specific one to be used. All two-factor vendor guidance should be followed to use that technology correctly and you should choose one that clearly uses two of the above. No configuration of Simphony is required to accomplish this.

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

Oracle Hospitality Simphony delivers patches and updates in a secure manner:

This section describes how payment application updates and patches are delivered to the merchant. The method used must provide a secure chain of trust per requirements in PA-DSS 7.2.a, including:

- **Timely development and deployment of patches and updates.**
  Starting in January 2011, Critical Patch Updates (CPU) are released on the Tuesdays closest to the 17th of the months of January, April, July, and October. The Critical Patch Updates and Security Alerts page on Oracle's web site always list the dates of release for the next four Critical Patch Updates, thus effectively providing a one-year notice to customers.

  On the Thursday before the release of each CPU, a PreRelease Advisory is published by Oracle. Both the PreRelease Advisory and the CPU Release Documentation are posted on the Critical Patch Updates and Security Alerts page on Oracle's web site located at http://www.oracle.com/technetwork/topics/security/alerts086861.html.
- **Delivery in a secure manner with a known chain-of-trust.**
  Software patches and updates are delivered from the My Oracle Support webpage.

  As outlined in the *Oracle Customer Support Security Practices* document:

  My Oracle Support is the key website service for providing interactions with Global Customer Support (GCS) for Oracle programs and hardware, including (Service Request) SR access, knowledge search / browse, support communities and technical forums.

  My Oracle Support employs the following security controls:
  - My Oracle Support is an HTTPS extranet website service using TLS 1.2 encryption for data transmitted over the Internet
  - Your registration on My Oracle Support uses a unique Customer Support Identifier (CSI) linked to your Support contract(s)
  - Each CSI has at least one customer-designated My Oracle Support Customer User Administrator. Your Customer User Administrators approve / reject requests from users for new accounts and CSI associations to existing accounts; you are responsible for provisioning and de-provisioning your users on a timely basis.
  - Your Customer User Administrator can control which features your users may access on My Oracle Support (for example, write access to SRs can be enabled or disabled for a given user)
  - Your Customer User Administrator can view users associated with its CSIs, and has the ability to remove access privileges for users
  - My Oracle Support SR Attachments (documents uploaded as part of the My Oracle Support SR create / update process) are saved into a dedicated GCS repository. Your communications with this repository are secured using Hypertext Transfer Protocol over Secure Socket Layer (https).

- **Delivery in a manner that maintains the integrity of the deliverable.**

  When a patch is downloaded from My Oracle Support's Automated Release Updates (ARU) page, the patch's digital signature should be verified. This is a relatively simple manual process.

  There are several free file integrity validation tools available on the web that can verify the Message Digest 5 (MD5) or Secure Hash Algorithm (SHA-1) checksum for the downloaded patch file. You can use a tool like the Microsoft File Checksum Integrity Verifier, or a similar MD5 and SHA-1 checksum utility.

  Choose and download the validation tool that you want to use. Once a patch has been downloaded, run your file integrity validation tool against it and compare the hash value generated by the validation tool to the hash value that corresponds to the patch on the ARU page. Both hash values should exactly match each other to confirm the file's integrity. Once you have validated the patch file's integrity, deploy the patch as soon as possible.

As a development company, we keep abreast of the relevant security concerns and vulnerabilities in our area of development and expertise. Members of the Oracle Hospitality Simphony Development team subscribe to:

- Microsoft's Technical Security Notifications. The goal of this service is to provide accurate information you can use to protect your computers and systems from malicious attacks. These bulletins are written for IT professionals, contain in-depth technical information, and e-mails are digitally signed with PGP.
- Oracle Critical Patch Update Alert E-mails. The announcements are sent to communicate when Critical Patch Update Advisories and Security Alerts are released.

Once we identify a relevant vulnerability, we work to develop & test a patch that helps protect Oracle Hospitality Simphony against the specific, new vulnerability. Vendors and dealers are contacted to encourage them to install the patch. Typically, merchants are expected to respond quickly to and install available patches within 30 days.

PCI-Compliant Remote Access (PA-DSS 10.2.3)

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

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited. As outlined in the *Oracle Customer Support Security Practices* document:

Collaboration Tools

Oracle Global Customer Support (GCS) uses two main collaboration tools to review issues reported to Oracle: Oracle Web Conferencing (OWC) for programs and Oracle Shared Shell for hardware. Both tools share the following common features:

- You control and participate actively in all sessions. You control the session, what navigation is undertaken, what data is displayed and what commands are

issued. You also have the ability to shut down the session at any time for any reason.

- TLS 1.2 encryption is provided for data transmitted over the Internet

Additional details about OWC and Shared Shell:

If users and hosts within the payment application environment may need to use third party remote access software such as Oracle Web Conferencing (OWC) and Shared Shell, etc. to access other hosts within the payment-processing environment, special care must be taken.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment-processing environment).

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

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

Data Transport Encryption (PA-DSS 11.1)

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either using TLS 1.1 or higher and Internet protocol security (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 TLS 1.1 (or higher) and 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)

In Oracle Hospitality Simphony, these settings are *not* user configurable.

Communication is secured using RSA 1024. PAN data is immediately encrypted with the Enterprise Server Public key once successful authorization is acquired in the payment application using RSA 12024. When the payment object arrives at the Enterprise, it is decrypted and re-encrypted using AES 256 for local storage in the database (Oracle Database or Microsoft SQL Server). No further decryption of PAN data occurs until the payment object is used during the settlement process.

Refer to the Credit/Debit Cardholder Dataflow Diagram for an understanding of the flow of encrypted data associated with Oracle Hospitality Simphony.

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

Oracle Hospitality Simphony 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)

Oracle Hospitality Simphony does not support non-console administration and we do not recommend using non-console administration. Should you ever choose to do this, you must use SSH, VPN, or TLS 1.1 or higher for encryption of this non-console administrative access.

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 Simphony.

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 Embedded POSReady 2009
- Microsoft Windows Embedded POSReady 7
- Microsoft Windows 7 SP1
- Microsoft Windows 8.1
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 R2
- Oracle Database 11g
- Oracle Database 12c
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server Express

- SQLite

Payment Application Initial Setup & Configuration

Additional Resources

- *Oracle Hospitality Simphony 2.8 Installation Guide*
- *Simphony Security Guide*

Appendix A

Data Security

Data security is a vital component of the Oracle Hospitality Simphony version 2.8 services infrastructure. Critical financial, transactional, and sensitive data is protected as it is routed between the Simphony service hosts and between the service hosts and the Enterprise application servers. In addition to securely transmitting these types of data, addition steps have been taken to securely store any data deemed to be sensitive, e.g. credit card data, within any database that it is written to.
In this section of the document, we will walk through the data security of the model by following the journey of a check that is rung up and transmitted across the property and up to the Enterprise. Along the way, we will examine the security that is in place for that part of the process.

The following topics are covered:

- Overview
- Client Authentication Key Generation
- Client Secure Data Storage
- Service to Service Data Transmission
- CAPS to Enterprise Data Transmission
- Enterprise Secure Data Storage

Overview

All checks that are rung up on a client are stored in the client's local database. If that check contains sensitive data (like credit card data), the sensitive information is encrypted prior to storing the information in the database. This check information is transmitted to the Check and Posting Service (CAPS) and then CAPS will relay the information up to the Simphony Enterprise. In environments like Table Service Restaurants and Quick Service Restaurants with drive thru operations, it is also quite common for a check to be passed around from client to client as it is being serviced.

Ultimately, the data that is collected by the Simphony OPS client is routed to the Enterprise where it is used for post transaction processing activities like credit card batch and settlement. The security layers and mechanisms within in Simphony to protect both the sensitive data that is stored and transmitted by Simphony are covered in the remainder of this section of the document.

It should be noted that to maintain system performance, not every message that is exchanged between the services hosts or with the Enterprise is encrypted. Messages that do not require security, such as status, heartbeat, and database updates, are not encrypted. Messages pertaining to transactional, financial and secure data are encrypted.

Client Authentication Key Generation

As mentioned in the Service Authentication section of this document, a username and password must be entered prior to being able to use a Simphony OPS client. In addition to authorizing the client to perform transactions, a RSA 1024-bit strength key pair, called the Authentication Keys, is exchanged between the OPS client service and the application server.

The key information is stored in the MCRSPOS.SEC_AUTH_KEYS table in the Enterprise database. This table contains both of the public and private halves of the key pairs as well as the version information for the pair. If the client is ever re-authenticated with the Enterprise, a new key pair will be generated. A new record will be written to the database for the client who includes the new keys in addition to a version number.

The OPS client service encrypts and stores the public half of the key pair locally in a local file (secdata.bin). This key is used in the encryption process for secure data storage.

Client Secure Data Storage

The Simphony client is capable of encrypting data which is deemed secure prior to storing it in the client database, e.g. credit card authorization data. The method used to secure this data is the same one which is used to encrypt messages that are exchanged between the Ops clients and CAPS on the property.

The secure data is encrypted using a one-time generated AES256 key. Then the AES256 key is encrypted using the public half of the Authentication Key which it was issued when the client was authorized. Finally, both the encrypted data and the encrypted key are stored in the SECURE_DETAIL table of the client database. The KEY ID of the Client's Key Pair is also stored in Secure Detail and is passed around together with the check.

Service to Service Data Transmission

At some point in time, it will be necessary for the secure data that has been gathered at the client to be transmitted to either another OPS client or the CAPS for posting purposes. When that time arrives, the OPS client will package together a message which contains the following information:

- The secure data encrypted using the one time AES256 key
- The encrypted AES256 key
- [KEY ID of the Authentication Key]
- The remaining check data, e.g., header information, menu items, discounts, service charges, etc.

The client will request the public half of the RSA 1024-bit key that is unique to the receiving service. Then, the client will encrypt the message contents with a one-time generated AES256 key and encrypt the AES256 key using the public half of the RSA key that was obtained from the receiving service.

It should be noted that any secure data which is transmitted, is actually encrypted again at this point in time. The first encryption took place prior to storing the data in the database. Then, it was encrypted again prior to sending it out.

Finally, the Ops client will transmit the message to the receiving service. The receiving service will use the private half of the key pair to decrypt the AES256 key, and then decrypt the message information with the one-time key. The message contents are then stored in the Ops client or CAPS database.

Since the secure data was encrypted using a one-time key that itself was encrypted using a key pair issued by the Simphony Enterprise, the secure data cannot be decrypted by the receiving service and is thus stored in its encrypted format.

The last point to note is that clients will periodically and dynamically change their RSA key pairs. There are no user settings to control how frequently this change can occur and the system will manage when it should be done.

CAPS to Enterprise Data Transmission

The only service that can transmit check data to the Enterprise is the Check and Posting Service (CAPS). The CAPS uses the same data transmission methodology as is used by the service-to-service process. The difference though, is that the public half of the RSA key pair is issued from the Enterprise. This key pair, referred to as the Transmission Key, can be changed by an authorized user from the Key Manager module within EMC.

Once the message from the CAPS is received at the Enterprise, the application server will use the private half of the Transmission key pair to decrypt the AES256 key and use the AES256 key to decrypt the message contents.

Enterprise Secure Data Storage

If the message received from CAPS contains secure data within it, the Enterprise application service will go through the following process to break down the message and store it. Just like on the clients, the Enterprise uses the SECURE_DETAIL table for storing the information.

Instead of storing the data collected from the properties using the keys that were generated on the property, this data is encrypted using a series of keys which are managed by the administrator and the system as described below. The keys are maintained in the MCRSCACHE database, which is a separate database from where SECURE_DATA table is located. This design allows a system administrator to physically separate the secure data from the keys to encrypt the data if desired.

Encryption Keys

A Pass Phrase is used to encrypt Encryption Keys. The Pass Phrase itself is encrypted by AES256 encryption and stored in the PASSPHRASE table.
ENCRYPTION KEYS are used to encrypt SECURE DETAIL in the Enterprise database. When Simphony is installed, the system administrator configures the passphrase that will be will used by the system to encrypt the secure data stored in the database. The system will generate, encrypt, and store a key in the MCRSCACHE.PPHASE table using AES256 encryption which is based upon the passphrase entered. This key is referred to as the master key.
The passphrase is also used as the seed data for a second AES256 key. This second key will be used to encrypt the secure data which is stored in the MCRSPOS.SECURE_DETAIL table. Prior to storing the second key in the MCRSCACHE.EKEY, it is encrypted using the master key.

Storing and Reading Encrypted Data

When a message containing secure data is received at the Enterprise, the decrypted contents of the message are encrypted using the active key in the MCRSCACHE.EKEY table prior to storing the data in the MCRSPOS.SECURE_DETAIL table.
To encrypt the data, the system must first decrypt the master key stored in the MCRSCACHE.PPHRASE table. Then, the currently active key in the EKEY table is looked up and decrypted using the master key. The decrypted key from the EKEY table is then used to encrypt the secure data. The encrypted data is written to the SECURE_DATA table along with a reference to the ID of the EKEY record which was used to encrypt the data.
Processes like credit card batch and settlement need to have access to the decrypted secure data for them to perform their tasks. In order to decrypt the data, the reverse process of encrypting the data must be used. The master key is decrypted and used to decrypt the proper EKEY. Once that is done, the EKEY is used to decrypt the secure data so that it can be processed.

Enterprise Key Rotation

Rotating the Enterprise keys can be a costly operation from a system performance perspective. After a system has been live for a long period of time, there could be hundreds of thousands of secure records in the database. The encryption mechanism developed for Simphony takes this fact into consideration and ensures that the process of rotating the keys will not impact the system performance.
The Enterprise keys can be rotated at any time using the Key Manager module within EMC. There is no limitation on the frequency at which at keys can be rotated. The user needs to enter the current passphrase and then a new passphrase to start the process. After entering in the correct information, the system will generate a new master key and store it in the PPHRASE table. The keys which are currently stored within the EKEY table are decrypted one at a time using the old master key and written back into the EKEY as a new record which has been encrypted using the new master key. Over time, all of the secure data which was encrypted using an EKEY is purged out of the system. Before writing the new records into the EKEY table, the rotation process checks to see if the key

is still referenced by any records in the SECURE_DETAIL table. If there are no more records referencing that key, it will not be written back into the table. A new record is also added to the table which contains a new encryption key derived from the new passphrase. Any new records that need to be written to the MCRSPOS.SECURE_DETAIL table will be encrypted using the key. Once the new records have been written to the database, the key rotation process will delete the rows in the EKEY table that were encrypted using the old master key. As a result of the fact that EKEY records that are no longer in use, were not written out as new records encrypted by the new master, results in the unused EKEY being purged from the system. Then the old master key record in the PPHRASE table will then be deleted. Once the process is completed, the PPHRASE table will have a single record in it. The EKEY table will contain only the records which are still referenced by data stored in the SECURE_DETAIL table plus the new key which will be used for new secure records that are going to be written to the database.

Appendix B

Encryption Key Custodian Sign Off Form

<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: _____